Osservatorio
di Politica internazionale

Senato
della Repubblica
Camera
dei deputati
Ministero
degli Affari Esteri
e della Cooperazione
Internazionale

Ottobre 2026

130

Note

Guerra ibrida in Europa: la minaccia dei sabotaggi alle infrastrutture critiche

di Federico Gallo e Filippo Massacesi

Introduzione

Nel dibattito sulla sicurezza europea, i concetti di guerra ibrida e di conflitto della zona grigia sono ormai categorie ricorrenti per descrivere forme di confronto sempre più difficilmente riconducibili alla tradizionale distinzione tra pace e guerra. I due concetti non sono tuttavia sovrapponibili. La zona grigia identifica una condizione di competizione strategica nella quale gli attori perseguono i propri obiettivi senza oltrepassare apertamente la soglia del conflitto armato, mentre la guerra ibrida fa riferimento alle forme attraverso cui tale competizione può essere condotta, combinando strumenti militari e non in funzione coercitiva.[1] Tra queste, il sabotaggio assume particolare rilievo perché consente di colpire infrastrutture critiche e snodi logistici senza ricorrere a un confronto militare aperto. Le operazioni di questo tipo sono per definizione "sotto soglia" (*below the threshold*), in quanto vengono condotte con modalità e livelli di intensità tali da non essere riconducibili a un uso della forza o a un attacco armato, evitando così di creare i presupposti per una risposta militare o per l'attivazione delle clausole di difesa collettiva. Per l'*Hybrid Center of Excellence* (CoE) di Helsinki, tali attività fanno leva sulle vulnerabilità sistemiche delle democrazie e sulle difficoltà con cui possono essere individuate e attribuite.[2] La loro conduzione risponde quindi a tre esigenze principali: mantenere incerta l'attribuzione, attraverso forme di

[1] Marco Di Liddo et al., *Mediterraneo: area di guerra ibrida*, Centro Studi Internazionali e Senato della Repubblica, Servizio Affari Internazionali, maggio 2024, pp. 2-4: https://eu-central-1.graphassets.com/AUerRw7rYTNuQZdIigaMoz/lQSLouaeREqXTmqER3av.

[2] Hybrid CoE, *Hybrid threats as a concept* (ultima consultazione effettuata in data 28 settembre 2026): https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

cosiddetta negazione plausibile (*plausible deniability*), rallentare il processo decisionale dell'avversario e limitarne i margini di reazione. Più che assicurare una completa negabilità dell'azione, però, l'obiettivo è creare un'ambiguità strategica sufficiente a rendere difficile l'accertamento della responsabilità e a sfruttare il divario di *escalation* tra un'azione di sabotaggio e un atto di guerra.[3]

Le infrastrutture critiche, dalle reti elettriche ai cavi e alle condotte sottomarine, passante per porti e aeroporti fino agli snodi logistici e agli impianti industriali della difesa e non, rappresentano obiettivi particolarmente esposti a questo tipo di strategia. Il sabotaggio di tali infrastrutture può infatti produrre effetti che vanno oltre il danno materiale immediato: un danneggiamento circoscritto può ripercuotersi su sistemi più ampi, imponendo agli Stati di destinare risorse crescenti alla protezione di un numero sempre maggiore di infrastrutture e, quando riguarda operatori privati o strutture a uso civile, rendendo meno netta la distinzione tra sicurezza nazionale e gestione ordinaria del rischio industriale. Ne deriva una forma di pressione caratterizzata da bassa intensità e alta frequenza, il cui impatto va quindi valutato non in relazione al singolo episodio, ma alla capacità di una sequenza di sabotaggi e azioni ostili di alimentare nel tempo tensione, incertezza e logoramento delle capacità di risposta.

Attori, metodi e dimensione del fenomeno

Nel contesto occidentale, le autorità statunitensi ed europee individuano nella Federazione Russa l'attore più attivo, con un ruolo attribuito in particolare ai suoi servizi di intelligence militare (GU), il cui modello operativo ha subito un'evoluzione significativa anche nel ricorso al sabotaggio per procura a seguito dell'espulsione di almeno 750 diplomatici e sospetti funzionari dei servizi informativi tra il 2022 e il 2024.[4] La progressiva riduzione della presenza diretta degli agenti russi ha determinato un maggiore ricorso a intermediari reclutati online per lo svolgimento delle attività, una modalità che rende più difficile attribuire la responsabilità delle operazioni, ma che comporta anche un livello di professionalità inferiore rispetto a quello garantito dall'impiego diretto del personale dei servizi.[5]

I dati disponibili consentono di quantificare e caratterizzare più nel dettaglio questa trasformazione. Il *dataset* ICCT-GLOBSEC ha registrato 151 incidenti tra febbraio 2022 e febbraio 2026, riconducibili a 172 esecutori. Circa il 95% era composto da comuni cittadini privi di legami formali con l'apparato di intelligence russo, mentre la motivazione prevalente era il compenso. Inoltre, circa il 90% degli esecutori agiva con almeno un complice, ridimensionando l'immagine dell'agente "usa e getta" isolato. Polonia (31 casi), Francia (20), Germania e Lituania (15 ciascuna) risultano i Paesi più colpiti, in linea con l'ipotesi che il sostegno a Kyiv sia il principale criterio di selezione dei bersagli. Nel complesso, la combinazione di manovalanza non qualificata, compensi contenuti e regia distante riduce il costo dell'offesa e rende il fenomeno facilmente scalabile. Questi dati sono inoltre

[3] Congressional Research Service (CRS), *Russian Hybrid Warfare Activities in Europe: Considerations for Congress*, R49134, 11 agosto 2026: https://www.congress.gov/crs-product/R49134.

[4] Secondo una stima dell'MI5. *Ibidem*.

[5] *Ibidem*.

verosimilmente una stima per difetto, poiché molti casi emergono solo a seguito della conclusione delle indagini. Nella sola Germania, ad esempio, le autorità hanno registrato 320 sospetti tentativi di sabotaggio nel 2025, una categoria più ampia rispetto agli incidenti inclusi nel *dataset* e di cui solo una parte è stata attribuita.[6] Anche le altre serie disponibili indicano una crescita del fenomeno, sebbene le stime non siano direttamente omogenee. Gli episodi di incendio doloso o sabotaggio grave censiti nei Paesi NATO, in larga parte ricondotti all'intelligence militare russa, sono passati da due nel 2022 a dodici nel 2023 e a trentaquattro nel 2024,[7] mentre un altro studio stima un quadruplicarsi degli attacchi tra il 2023 e il 2024.[8] Le divergenze dipendono dai criteri di inclusione e dalla diversa capacità di attribuire gli eventi e suggeriscono pertanto di leggere queste cifre come ordini di grandezza, più che come misure puntuali del fenomeno.

Sul versante marittimo, la "flotta ombra" russa, stimata a seconda delle fonti tra le 1.000 e le 3.200 unità, non costituisce soltanto un meccanismo di elusione delle sanzioni, ma anche una piattaforma per danneggiamenti sottomarini e ricognizioni con droni nel Mar Baltico e nel Mare del Nord. Le rilevazioni ACLED hanno registrato 54 sospetti incidenti con droni entro 150 chilometri dalle coste europee nel 2025 e otto operazioni europee di abbordaggio o sequestro tra il 2025 e i primi quattro mesi del 2026. Il caso *Estlink 2* risulta emblematico: la rottura del cavo sottomarino, avvenuta nel dicembre 2024 e attribuita dalle autorità finlandesi alla petroliera *Eagle S*, ha ridotto di due terzi la capacità di trasferimento elettrico tra Estonia e Finlandia e richiesto sette mesi di riparazioni. Il procedimento è stato tuttavia archiviato nell'ottobre 2025 per difetto di giurisdizione e mancata prova dell'intenzionalità. Il principale ostacolo resta quindi l'attribuzione, resa più complessa dai vincoli posti dalla Convenzione UNCLOS all'intervento nelle zone economiche esclusive. Mosca ha reagito con scorte navali e con la ri-registrazione di circa settanta unità sotto bandiera russa dal maggio 2025,[9] misura che incide sui presupposti giuridici delle operazioni di contrasto. Il confronto con il primo sequestro britannico di una petroliera della flotta ombra nella Manica, la *Smyrtos*, il 14 giugno 2026, è istruttivo: il Regno Unito ha potuto agire solo dopo la revoca della registrazione camerunense della nave, poiché lo *status* di apolide forniva una base giuridica per l'abbordaggio. L'azione è stata coordinata con la Francia, che il 23 giugno ha sequestrato un'altra unità al largo della Sicilia. La capacità di contrasto dipende dunque non soltanto dalla gravità della condotta, ma anche dallo stato giuridico del bersaglio. Questo limite assume particolare rilievo perché, come rilevato da ACLED, anche l'aumento del costo dell'elusione non sembra sufficiente a interrompere né i ricavi né la funzione ibrida della flotta.[10] Nell'aprile 2026, inoltre, Londra ha denunciato un'operazione condotta da sommergibili speciali russi attorno alle proprie infrastrutture sottomarine, plausibilmente

---

6 J. Lanchès, K. Rekawek, *More of the Same. Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare Revisited*, International Center for Counter-Terrorism (ICCT), 23 febbraio 2026: https://icct.nl/publication/more-same-russias-crime-terror-nexus-criminality-tool-hybrid-warfare-revisited.

7 Kinga Redlowska, Marta Popyk e Tom Keatinge, *Responding to Russian Sabotage Financing*, Royal United Services Institute (RUSI), 14 gennaio 2026: https://www.rusi.org/explore-our-research/publications/insights-papers/responding-russian-sabotage-financing.

8 Congressional Research Service (CRS), *Op. Cit.*: https://www.congress.gov/crs-product/R49134.

9 ACLED, *Russia's shadow fleet presents a sustained hybrid war threat at sea*, 22 maggio 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://acleddata.com/report/russias-shadow-fleet-presents-sustained-hybrid-war-threat-sea.

10 ACLED, *Europe and Central Asia Overview: July 2026*, 6 luglio 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://acleddata.com/update/europe-and-central-asia-overview-july-2026.

finalizzata alla mappatura dei fondali in vista di possibili sabotaggi,[11] suggerendo che la fase di ricognizione possa precedere e preparare l'eventuale azione. La "Flotta Ombra" costituisce, inoltre, un rischio ambientale costante poiché i vascelli che la costituiscono sono spesso in condizioni non ottimali intenti in azioni pericolose di *transhipment* di prodotti petroliferi verso navi compiacenti civili non facenti parte della flotta ma che giovano dai prodotti da essa trasportati. Un'ulteriore rischio è rappresentato dal rischio di malfunzionamenti e di derive conseguenti, come avvenuto nel caso della Arctic Metagaz, una nave gasiera russa trasportante oltre 50.000 metri cubi di gas liquefatto e quasi 1.000 tonnellate di idrocarburi, rimasta alla deriva nel mediterraneo dopo essere stata colpita da un drone causando un rischio di *spillover* (riversamento in mare di sostanza nocive come idrocarburi o gas liquefatto) che avrebbe avuto effetti letali sulla zona economica esclusiva (ZEE) italiana e maltese per anni.

Le risposte istituzionali esistono, ma restano frammentarie. La NATO ha avviato *Baltic Sentry* nel gennaio 2025 ed *Eastern Sentry* nel settembre dello stesso anno, mentre l'UE, a luglio 2026, aveva sanzionato 26 entità e oltre cento persone per attività destabilizzanti.[12] A livello normativo e industriale, la Commissione Europea ha inoltre adottato il Piano d'azione sulla sicurezza dei droni e dei sistemi anti-drone (11 febbraio 2026) e la *Defence Readiness Roadmap 2030*.[13] Queste iniziative si inseriscono in un più ampio rafforzamento della cooperazione europea con la NATO, che la letteratura accademica interpreta come il possibile terreno per una nuova "responsabilità strategica" dell'UE.[14] Nel complesso, tali iniziative rafforzano soprattutto le capacità di resilienza e la riduzione delle vulnerabilità sistemiche, ma non sono ancora accompagnate da un approccio europeo specificamente orientato al contrasto organico del sabotaggio e, più in generale, dell'intero spettro della minaccia ibrida. La NATO, inoltre, conserva una struttura maggiormente orientata alle minacce convenzionali.[15]

L'evoluzione dei sabotaggi russi in Europa

Gli episodi più recenti evidenziano un'evoluzione del sabotaggio russo in Europa sia per la scelta dei bersagli sia per la crescente attenzione rivolta alle infrastrutture e alle attività legate al sostegno europeo all'Ucraina. Il caso dell'aeroporto di Lipsia/Halle, anzitutto, è indicativo per la scelta del bersaglio: il 4 agosto 2026 un drone carico di esplosivo è stato rinvenuto presso un velivolo cargo ucraino nello scalo, importante *hub* logistico della NATO e nodo dei trasporti diretti verso l'Ucraina. L'episodio ha interessato quindi una componente della filiera logistica che sostiene lo sforzo di Kyiv in cui la distinzione tra infrastruttura civile e funzione militare risulta sottile. La vicenda appare significativa anche per il problema dell'attribuzione. Il 1° settembre il governo federale tedesco ha imputato formalmente il tentato attacco alla Russia, sulla base di indagini di polizia, *modus operandi* e risultanze di intelligence, e ha disposto la

[11] Congressional Research Service (CRS), *Op. Cit.*: https://www.congress.gov/crs-product/R49134.

[12] *Ibidem*.

[13] Commissione Europea, *Hybrid Threats* (ultima consultazione effettuata in data 28 settembre 2026): https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en.

[14] Maurizio Geri, *A New Strategic Responsibility for the EU: EU-NATO Cooperation against Hybrid Warfare from Russia, The Rest*, vol. 15 n. 1, 2025: https://iris.unive.it/handle/10278/5089287.

[15] Marco Di Liddo et al., *Op. Cit.*, pp. 4-8: https://eu-central-1.graphassets.com/AUerRw7rYTNuQZdIigaMoz/lQSLouaeREqXTmqER3av.

chiusura del Consolato Generale russo di Bonn e della Casa russa della Scienza e della Cultura, mentre Mosca ha respinto le accuse.[16] Si tratta di un'attribuzione formulata in sede politica, con una soglia probatoria diversa da quella giudiziaria. A questa cautela si aggiunge però il profilo degli esecutori, che riflette il modello già osservato in altre sedi: il Ministro dell'Interno Dobrindt ha rilevato l'elevata sofisticazione tecnica del congegno, ma un'esecuzione apparentemente affidata ad agenti di basso profilo,[17] suggerendo una separazione tra pianificazione professionale ed esecuzione affidata a personale poco esperto e reclutato a basso costo.

La stessa combinazione emerge nel caso di Monaco. Nella notte tra il 2 e il 3 settembre, diversi ordigni incendiari sono stati lanciati da un'auto contro un cantiere adiacente alle sedi monacensi di Rohde & Schwarz, attiva nella produzione di radar e di sistemi di contrasto ai droni, e di Helsing, fornitrice di droni alle forze ucraine. Due cittadini bulgari sono stati arrestati e i danni sono stati limitati.[18] La rilevanza dell'episodio risiede soprattutto nella natura dei bersagli: imprese private del comparto duale, la cui selezione appare legata alla funzione svolta nella filiera della difesa piuttosto che alla loro natura pubblica. Ciò crea un'asimmetria tra offesa e protezione, poiché la sicurezza di tali obiettivi può richiedere risorse sproporzionate rispetto al costo dell'azione. In questo quadro, i due arrestati sarebbero riconducibili a una rete legata al GU e operante dalla Slovacchia, la stessa che avrebbe pianificato un incendio contro lo stabilimento di Skyeton, produttore ucraino di droni, presso Prešov.[19] Il collegamento al GU è tuttavia emerso da informazioni investigative riportate dalla stampa e non è stato confermato dalla Procura di Monaco,[20] motivo per cui deve essere considerato

---

[16] Linus Höller, *German government blames Russia for Leipzig airport drone attack with explosives*, Defense News, 2 settembre 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://www.defensenews.com/global/europe/2026/09/02/german-government-blames-russia-for-leipzig-airport-drone-attack-with-explosives/; Ivana Kottasová, Sebastian Shukla, *Germany blames Russia for drone attack on Leipzig airport*, CNN, 1° settembre 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://www.cnn.com/2026/09/01/europe/leipzig-drone-germany-russia-intl.

[17] The Associated Press, *Germany blames Russia for last month's attempted drone attack at Leipzig airport*, NPR, 2 settembre 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://www.npr.org/2026/09/02/g-s1-141502/germany-russia-attempted-drone-attack; Reuters e The Associated Press, *What to know about Germany's drone attack accusations against Russia*, Al Jazeera, 2 settembre 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://www.aljazeera.com/news/2026/9/2/what-to-know-about-germanys-drone-attack-accusations-against-russia.

[18] Reuters, *Germany probes suspected arson at defence firm as European sabotage concerns mount*, Internazionale, 3 settembre 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://www.internazionale.it/ultime-notizie-reuters/2026/09/03/german-police-probe-arson-attack-on-defence-tech-firm-in-munich.

[19] Secondo una ricostruzione del quotidiano Frankfurter Allgemeine, ripresa da The Insider e da Formiche. Federica De Vincentis, *Dalla Germania alla Slovacchia, l'ombra del Gru sugli attacchi contro l'industria della difesa*, Formiche, 26 settembre 2026: https://formiche.net/2026/09/dalla-germania-alla-slovacchia-lombra-del-gru-sugli-attacchi-contro-lindustria-della-difesa/; The Insider, *Bulgarians detained over Munich arson were part of GRU-linked group operating from Slovakia*, 25 settembre 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://theins.press/en/news/297540; Frankfurt Allgemeine, *German investigators suspect Russian military intelligence organized an arson attack near defense firms in Munich*, Meduza, 25 settembre 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://meduza.io/en/news/2026/09/25/german-investigators-suspect-russian-military-intelligence-organized-an-arson-attack-near-defense-firms-in-munich.

[20] The New Voice of Ukraine, *German investigators link Munich arson attack to GRU – FAZ*, 26 settembre 2026 (ultima consultazione effettuata in data 28 settembre 2026):

un’ipotesi investigativa e non fatto accertato. Qualora fosse confermato, il caso indicherebbe l’esistenza di una struttura transnazionale capace di operare in più giurisdizioni, aumentando la complessità delle indagini. Anche in assenza di tale conferma, tuttavia, l’episodio si inserisce in un modello più ampio caratterizzato dalla selezione di obiettivi legati al comparto militare-industriale, dal reclutamento oltre i confini nazionali e dalla direzione delle operazioni a distanza.

La struttura delle operazioni assume rilievo anche nella fase preparatoria, che può prevedere attività di ricognizione e individuazione dei bersagli affidate a soggetti reclutati localmente. Un esempio di questa modalità è fornito dal servizio di sicurezza danese (PET), che ha reso noto che la Russia sta tentando di reclutare cittadini danesi attraverso *social network* e piattaforme di *gaming* per fotografare aziende e infrastrutture. Nello stesso quadro, il 24 settembre l’intelligence militare danese ha stimato che si assisterà a un incremento della frequenza degli attacchi e delle loro conseguenze nei prossimi mesi.[21] La ricognizione costituisce quindi una componente funzionale alla preparazione del sabotaggio, ma è meno visibile e più difficile da qualificare giuridicamente rispetto all’azione offensiva. Il caso romeno mostra inoltre quanto questa fase possa essere difficile da distinguere dagli effetti diretti della guerra in Ucraina. Le rilevazioni ACLED hanno contato oltre 80 eventi legati a droni nell’Europa orientale nel 2026, prevalentemente in Romania, ma li hanno ricondotti in larga parte agli attacchi russi contro i porti danubiani ucraini, senza indicare necessariamente un intento ostile verso Bucarest.[22] Sul fronte propriamente riconducibile al sabotaggio, invece, due cittadini ucraini sono attualmente a processo per il piano di incendiare la sede di Nova Post a Bucarest, inserito in un disegno più ampio con obiettivi in Polonia, mentre a settembre è stato fermato un cittadino russo sospettato di sorvegliare siti militari.[23] La sequenza mostra quindi come ricognizione, preparazione ed esecuzione possano svilupparsi in più Paesi, mentre la sovrapposizione tra attività ostili e conseguenze indirette della guerra può ritardare l’individuazione della natura e dell’origine dell’azione.

https://english.nv.ua/nation/german-investigators-link-munich-arson-near-defense-firms-to-russia-s-gru-50644815.html.

[21] Reuters, *Op. Cit.*: https://www.internazionale.it/ultime-notizie-reuters/2026/09/03/german-police-probe-arson-attack-on-defence-tech-firm-in-munich; Reuters, *Denmark Expects Russia to Escalate Hybrid Warfare in Coming Months, Intelligence Service Says*, U.S. News, 24 settembre 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://www.usnews.com/news/world/articles/2026-09-24/denmark-expects-russia-to-escalate-hybrid-warfare-in-coming-months-intelligence-service-says; Semafor, *Russia looking to escalate hybrid war, Denmark warns*, 25 settembre 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://www.semafor.com/article/09/24/2026/russia-looking-to-escalate-hybrid-war-denmark-warns.

[22] ACLED, *As drone attacks on Ukraine intensify, Eastern Europe is straining to counter the spillover*, 25 agosto 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://acleddata.com/report/drone-attacks-ukraine-intensify-eastern-europe-straining-counter-spillover; David Brennan, *Russia's escalating strikes in Ukraine increasingly spilling into NATO, Romania says*, ABC News, 21 agosto 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://abcnews.com/International/russia-drone-incursions-nato-airspace-jump-exponentially-2026/story?id=135771388.

[23] Congressional Research Service (CRS), *Op. Cit.*: https://www.congress.gov/crs-product/R49134; J. Lanchès, K. Rekawek, *Op. Cit.*: https://icct.nl/publication/more-same-russias-crime-terror-nexus-criminality-tool-hybrid-warfare-revisited; Irina Vilcu, *Romania detains Russian citizen over alleged sabotage operation*, Bloomberg, 8 settembre 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://www.bloomberg.com/news/articles/2026-09-08/romania-detains-russian-citizen-over-alleged-sabotage-operation.

La difficoltà di attribuzione aumenta ulteriormente quando il sabotaggio può essere confuso con atti di origine interna. In questo senso, la sequenza di attacchi alle reti elettriche condotte il 1° settembre in Brandeburgo e Renania Settentrionale-Vestfalia è istruttiva: le autorità hanno dichiarato di non poter escludere né un coinvolgimento straniero né l'estremismo di sinistra, mentre il Ministro Dobrindt ha ipotizzato che potenze straniere potessero essersi servite di gruppi estremisti come prestanome.[24] Il 4 settembre, tuttavia, lo stesso Ministro ha ricondotto con ogni probabilità gli episodi all'"estremismo climatico", pur precisando che le indagini restavano aperte.[25] L'episodio non prova dunque alcuna regia esterna e mostra piuttosto quanto sia difficile distinguere, nelle fasi iniziali, un sabotaggio ostile da forme di violenza politica interna. Il rischio è duplice: sottovalutare un'operazione mascherata oppure attribuire erroneamente all'esterno un fatto di matrice interna. I dati disponibili mostrano inoltre che le reti riconducibili a Mosca hanno attinto a bacini antisistema: il 26% degli esecutori aveva precedenti penali, dodici erano legati al tifo violento e dieci all'estremismo di destra, mentre canali Telegram collegati a Mosca hanno offerto compensi per atti di vandalismo e incendi nel Regno Unito.[26] Il coinvolgimento di questi soggetti può quindi rendere meno immediata l'individuazione della regia esterna, perché l'azione può apparire inizialmente come il risultato di dinamiche interne già presenti nel Paese colpito.[27]

Conclusioni

Quattro elementi emergono con particolare evidenza dalla panoramica di sabotaggi esaminata. Primo, il fenomeno presenta una marcata asimmetria tra costo dell'azione e costo della risposta. Gli esecutori sono in grado di seguire azioni ostili dal costo di poche centinaia o migliaia di euro, mentre la neutralizzazione di un singolo drone può richiedere l'impiego di sistemi dal costo molto superiore. In Romania, ad esempio, l'intercettazione di un drone dal valore stimato tra 20.000 e 50.000 dollari può richiedere a un *F-16* l'impiego di un missile del valore compreso tra 380.000 e 500.000 dollari.[28] Secondo, l'attribuzione resta il nodo centrale e i casi esaminati ne mostrano i diversi gradi di certezza: a Lipsia è stata politica prima che giudiziaria, nel caso *Eagle S* è giuridicamente fragile, a Monaco è ancora un'ipotesi investigativa, in Romania si confonde con lo *spillover* bellico, mentre le vicende delle reti elettriche ammoniscono contro attribuzioni

[24] Reuters, *Germany probes suspected arson at defence firm as European sabotage concerns mount*, *cit.*: https://www.internazionale.it/ultime-notizie-reuters/2026/09/03/german-police-probe-arson-attack-on-defence-tech-firm-in-munich.

[25] ZDFheute, *Was zu den Sabotage-Angriffen auf das Stromnetz bekannt ist*, 4 settembre 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://www.zdfheute.de/politik/deutschland/stromnetz-sabotage-energieversorgung-umspannwerk-dobrindt-100.html; Tagesspiegel, An*schläge auf Umspannwerke: Dobrindt spricht von „Klimaextremismus" – mutmaßlicher Saboteur weiter flüchtig*, 5 settembre 2026 (ultima consultazione effettuata in data 28 settembre 2026): https://www.tagesspiegel.de/politik/anschlage-auf-umspannwerke-dobrindt-spricht-von-klimaextremismus--sek-sturmt-truck-von-mutmasslichem-saboteur-16015953.html.

[26] J. Lanchès, K. Rekawek, *Op. Cit.*: https://icct.nl/publication/more-same-russias-crime-terror-nexus-criminality-tool-hybrid-warfare-revisited

[27] Marco Di Liddo et al., *Op. Cit.*, p. 5: https://eu-central-1.graphassets.com/AUerRw7rYTNuQZdIigaMoz/lQSLouaeREqXTmqER3av; Hybrid CoE, *Hybrid threats as a concept* (ultima consultazione effettuata in data 28 settembre 2026): https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

[28] David Brennan, *Op. Cit.:* https://abcnews.com/International/russia-drone-incursions-nato-airspace-jump-exponentially-2026/story?id=135771388.

premature. Questa gradazione non è un limite dell'analisi, ma una caratteristica strutturale del fenomeno, poiché è proprio nella *plausible deniability* e cioè nell'intervallo tra sospetto e prova che le operazioni sottosoglia producono il loro effetto più deleterio. Terzo, la risposta è ancora frammentata: le istituzioni europee si adattano più lentamente dell'attività che intendono contrastare,[29] spesso impantanate in sistemi normativi nazionali non adatti al contrasto della minaccia sottosoglia transnazionale e da organismi europei incapaci di coordinare una risposta celere quanto efficace. Quarto, il perimetro dei bersagli si sta ampliando dalle infrastrutture pubbliche alla filiera industriale e logistica privata: gli episodi di Lipsia, Monaco e Prešov colpiscono non tanto lo Stato quanto gli anelli che collegano la produzione, il trasporto e la fornitura di capacità militari, cioè i punti in cui una perturbazione limitata può produrre il maggiore effetto sulla capacità di sostegno a Kyiv.

Ne emerge un quadro in cui la difficoltà principale non è tanto l'intensità delle singole operazioni, volutamente contenuta, quanto la loro ripetizione e la capacità di trasformare azioni di sabotaggio circoscritte in una pressione continuativa e costante, con esecutori eterogenei, bersagli sempre più duali e una linea di demarcazione sfumata rispetto al dissenso interno. Nel complesso, il dato empirico disponibile descrive un'interferenza continuativa derivante da attività di sabotaggio e altre azioni sottosoglia, con l'obiettivo secondario di esercitare una manipolazione delle società tramite l'impiego della paura, pertanto, rendendo decisivo, per la lettura di ciascun episodio, il grado di certezza con cui esso è ascrivibile a una regia esterna. Per l'Italia, il quadro assume una declinazione specifica sul fianco meridionale, dove si concentrano tra i rischi ibridi anche la libertà di navigazione e la sicurezza dei cavi sottomarini, dei gasdotti e delle forniture energetiche.[30]

[29] ACLED, *Russia's shadow fleet presents a sustained hybrid war threat at sea*, *Cit.*: https://acleddata.com/report/russias-shadow-fleet-presents-sustained-hybrid-war-threat-sea.

[30] Marco Di Liddo et al., *Op. Cit.*, pp. 16-17: https://eu-central-1.graphassets.com/AUerRw7rYTNuQZdIigaMoz/lQSLouaeREqXTmqER3av.

Osservatorio di Politica internazionale

www.parlamento.it/osservatoriointernazionale



Senato della Repubblica



Camera dei Deputati



Ministero degli Affari Esteri
e della Cooperazione
Internazionale

Coordinamento redazionale:

Camera dei deputati
Servizio Studi - Dipartimento Affari esteri
Tel. 06.67604939
Email: st_affari_esteri@camera.it

Le opinioni riportate nel presente dossier
sono riferite esclusivamente all'Istituto autore della ricerca.