Russia, la mappa degli attacchi segreti all'Europa: la guerra ibrida di Putin dai Baltici alla Francia (e anche in Italia)

(Fonte: https://www.ilmessaggero.it/ 23 agosto 2025)

Note: Energy and communications categories exclude Russian efforts to sabotage undersea cables and pipelines; these actions are counted in the undersea category.
Sources: IISS analysis; 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

Extracted from https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/ by @auonsson (responsible for the 'almost certain' on GPS jamming =))

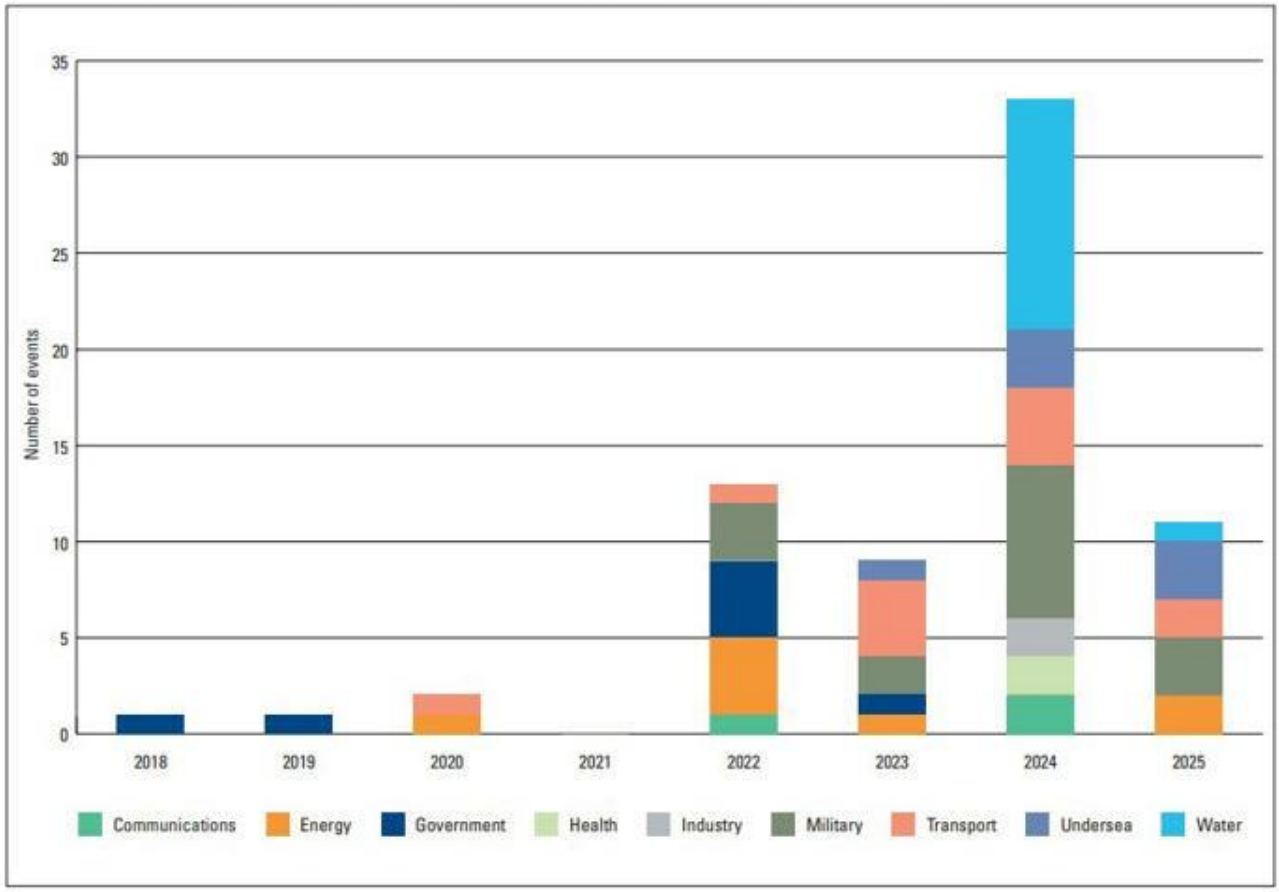
La Russia sta conducendo una guerra segreta, sottotraccia, non convenzionale contro l'Europa. Una vera a propria campagna di sabotaggi, atti di vandalismo, spionaggio e azioni nascoste, L'obiettivo di Mosca è quello di minare la stabilità dei governi europei, mettere a rischio il sostegno pubblico

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, ibrida, ha iniziato a intensificarsi nel 2022 parallelamente 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'area più colpita è ovviamente quella dei Paesi Baltici e scandinavi. Seppur in casi più isolati però, Mosca ha compiuto azioni ostili anche verso le grandi nazioni della Nato, dalla Germania alla Gran Bretagna alla Francia, e anche l'Italia.

La mappa degli attacchi russi all'Europa

L'International Institute for Strategic Studies (IISS) ha creato un database open source completo di operazioni di sabotaggio russe sospette e confermate contro l'Europa. Una mappa con i dati che rivelano come il sabotaggio russo abbia preso di mira le infrastrutture critiche europee, come sia decentralizzato e, nonostante i funzionari europei della sicurezza e dell'intelligence abbiano lanciato l'allarme, sia in gran parte indifferente alle risposte della Nato, dell'UE e degli Stati membri fino ad oggi. Il Cremlino ha sfruttato le lacune dei sistemi legali attraverso il suo approccio basato sulla "gig economy", che le ha consentito di evitare attribuzioni e responsabilità. Dal 2022, anno in cui centinaia di funzionari dei suoi servizi segreti sono stati espulsi dalle capitali europee, Mosca è risultata molto efficace nel reclutamento online di cittadini di paesi terzi per eludere le misure di controspionaggio europee. Sebbene la tattica si sia dimostrata efficace in termini di portata e volume, consentendo operazioni su larga scala, la sfida principale per i servizi segreti russi è stata la qualità dei proxy, spesso scarsamente addestrati o mal equipaggiati, il che rende le loro attività soggette a rilevamento, interruzione o fallimento.

Figure 0.1: **Frequency of Russian hybrid-warfare activity across Europe, January 2018–June 2025**



Notes: All hybrid attacks in 2022 occurred after the beginning of Russia's full-scale invasion of Ukraine. Energy and communications categories exclude Russian efforts to sabotage undersea cables and pipelines; these actions are counted in the undersea category.
Sources: IISS analysis; 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

La guerra ibrida

La dottrina militare russa integra profondamente il sabotaggio delle Infrastrutture Critiche Nazionali (CNI) nella gibridnaya 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 di 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 suo più ampio conflitto con l'Occidente. Sebbene alcune iniziative, come l'operazione marittima Nato Baltic Sentry nel Mar Baltico, siano state in qualche modo efficaci, la mancanza di budget e risorse ha impedito all'Alleanza Atlantica e all'Ue di adottare una risposta duratura e concreta. Inoltre, non è chiaro, di fronte a priorità di sicurezza nazionale contrastanti, quanto siano impegnate le capitali europee nel dissuadere la guerra non convenzionale della Russia contro l'Europa.

Le azioni di Mosca e la risposta di Kiev

Nell'ambito delle ambizioni di Mosca contro l'Europa, le operazioni di sabotaggio e la campagna di sovversione e disinformazione del Cremlino, unite all'invasione su vasta scala dell'Ucraina nel 2022, sono parte integrante della sua più ampia guerra ibrida volta a indebolire l'Occidente. Un obiettivo

primario della guerra non convenzionale della Russia è quello di ridurre il sostegno all'Ucraina aumentando i costi per governi e industrie, molestando le popolazioni e sfruttando le vulnerabilità delle difese europee. L'Ucraina è anche attivamente coinvolta in operazioni informatiche e con droni contro le infrastrutture petrolifere e del gas russe e le installazioni dell'industria della difesa, sfruttando le persistenti vulnerabilità. Queste operazioni di rappresaglia mirano a imporre costi, interrompere le operazioni e influenzare la volontà pubblica di entrambe le parti, caratterizzando un contesto più ampio e globale. Alcuni stati membri della Nato hanno valutato la guerra ibrida di Putin come parte dei preparativi a lungo termine per un potenziale confronto militare con la Nato e ritengono che l'attenzione sia rivolta ad attaccare obiettivi fisici e virtuali utilizzando spionaggio, sovversione, ransomware e l'abuso delle catene di fornitura IT globali. A questo si aggiungono operazioni informative che utilizzano campagne di disinformazione, propaganda e la diffusione di deepfake e teorie del complotto. Questi vettori di attacco si intersecano nei metodi e negli effetti, integrando capacità di vari settori dell'esercito russo, dei servizi segreti e di attori non statali, tra cui il Gruppo Wagner e la criminalità.

Gli obiettivi russi

Negli ultimi dieci anni, il Cremlino ha preso di mira settori come energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua, infrastrutture digitali e strutture governative, incluse installazioni militari. Più recentemente, le operazioni di sabotaggio russe in Europa hanno ampliato il raggio dei loro obiettivi e la gravità degli attacchi. Il numero di attacchi è quasi quadruplicato dal 2023 al 2024. I dati dell’IISS mostrano che gli obiettivi più frequenti sono le strutture collegate alla guerra in Ucraina e le strutture governative. 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 database dettagliato assemblato dallo IISS, costruito sul lavoro del professor Bart Schuurman dell’Università di Leiden nei Paesi Bassi e ampliato grazie all’integrazione con il progetto ACLED (Armed Conflict Location & Event Data) e con il monitoraggio degli incidenti effettuato dallo IISS stesso. Il risultato è il database open source più completo attualmente disponibile sulle operazioni di sabotaggio russe in Europa e nelle aree periferiche e copre l’intero spettro delle attività con effetti fisici: dal sabotaggio dei cavi sottomarini al blocco del Gps in diversi ambiti e geografie.

Il 2025, l'avvento di Trump e le azioni dell'Ue

Le operazioni di sabotaggio russe in Europa sono proseguite anche nel 2025, sebbene i dati dell’IISS suggeriscano una pausa in tali attività durante la prima metà dell’anno. Nonostante gli attacchi segnalati sembrino essere diminuiti tra gennaio e luglio, diversi fattori potrebbero spiegare questo calo apparente. In primo luogo, alcuni incidenti verificatisi all’inizio del 2025 sono probabilmente ancora non confermati dalle autorità locali, e le forze dell’ordine e i servizi di intelligence

impiegano spesso tempo per raccogliere prove, creando così un ritardo nei dati. In secondo luogo, è possibile che l'inizio del secondo mandato del presidente statunitense Donald Trump abbia indotto il Cremlino a sospendere temporaneamente le operazioni, per evitare di alienarsi un'amministrazione americana più conciliante. Infine, la risposta guidata dagli Stati Uniti all'incidente DHL del 2024 potrebbe aver spinto il Cremlino a interrompere momentaneamente le operazioni e indotto i RIS a contenerle. Inoltre i governi europei hanno avviato numerose 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 «deterioramento fondamentale della situazione di sicurezza» nella regione baltica. Il 1° aprile, anche la Finlandia ha seguito l'esempio. Tale cambiamento segnala probabilmente al Cremlino una maggiore prontezza militare, nel tentativo di evitare un confronto diretto con la Nato. In ambito marittimo, nel 2025 è stato lanciato NorthSeal, uno sforzo congiunto per la sicurezza nel Mare del Nord, insieme a Baltic Sentry.