DYNAMES

Governance di Forze e Sistemi

PAPER & DOSSIER

WHITE PAPER

La minaccia della Federazione Russa verso le democrazie europee

FRANCESCO TREVISAN

2026

Paper Series
White Paper

White Paper

LA MINACCIA DELLA FEDERAZIONE RUSSA VERSO LE DEMOCRAZIE EUROPEE

A CURA DI	Francesco Trevisan
DATA	15/07/2026
AREA TEMATICA	Informazione e Dominio Cognitivo
CATEGORIA	White Paper
VERSIONE	1.0

Documento di analisi strategica

White Paper: La minaccia della Federazione Russa verso le democrazie europee.

Summary

Sommario del White Paper

Introduzione

E se non fosse tutto così calcolabile? Se i paradigmi di politica internazionale fossero completamente diversi rispetto al passato e le aspettative degli attori coinvolti venissero disattese bruscamente, portando ad un conflitto armato tra l'Europa e la Russia? A mio parere, queste due domande fungono da guida per poter interpretare al meglio il report dell'intelligence italiana sulla sicurezza nazionale del 2026, intitolato Governare il cambiamento. La relazione, divisa in diversi capitoli, ognuno dei quali analizza varie dinamiche interne ed esterne al territorio italiano, pone l'accento sulla minaccia ibrida alle società democratiche, identificando la Federazione Russa come l'attore internazionale maggiormente critico per l'architettura strategico-securitaria del vecchio continente.

Le operazioni “sotto soglia” della Federazione Russa

Il riallineamento pressoché compiuto tra Washington e Mosca, ha costretto l’Europa a venire individuata come il centro focale di vari interventi “sotto soglia” da parte del Cremlino, attraverso i quali auspica di vedere deteriorato il supporto politico e militare a Kyiv. Tali azioni vengono definite appunto “sotto soglia” perché, seppur ostili e dirette a danneggiare un Paese, non raggiungono il livello di un attacco armato convenzionale, evitando così di far scattare automaticamente l'obbligo di difesa collettiva dell’Alleanza Atlantica (Sistema di informazione per la sicurezza della Repubblica, 2026). Esse, per di più, sono considerate un metodo sostanzialmente economico per la Federazione Russa, la quale affida il compimento di queste attività illegali a reti criminali o agenti proxies, senza poi subire ricadute diplomatiche troppo significative (Ministero della Difesa, 2025). Tra il 2023 e il 2025, infatti, la frequenza degli attacchi a infrastrutture critiche è più che quintuplicata, lasciando spazio ad eventi la cui gravità ha anch’essa visto un incremento significativo (Jones S.G., 2025). Secondo un report del CSIS (Jones S.G., 2025), gli Stati occidentali, però, non hanno mai adottato contromisure mirate a ridurre tale pressione esterna, classificando anche i casi più al limite e degni di nota per la loro gravità come azioni non comparabili allo stato di conflitto. Ad esempio, l’Articolo 5 della NATO prevede un’azione collettiva solo nel caso in cui la sicurezza di uno Stato membro venga pesantemente minacciata o lesa, accantonando in tal senso le varie “misure attive” subite per mano della Federazione russa durante l’ultimo periodo. La responsabilità politica e militare, dunque, appare difficile da poter individuare con adeguata chiarezza, sebbene il soggetto principale a capo della catena di comando, indicato dal rapporto CSIS, sia la GRU (*Glavnoye Razvedyvatelnoye Upravlenie*), ovvero la Direzione Generale dell’Intelligence russa, guidata dall’Ammiraglio Igor Kostyukov, alla quale seguono i Comitati di Influenza Speciale (fondati nel 2022) e il Consiglio di Sicurezza Nazionale, il cui Segretario è il Ministro della Difesa Shoigu.

Target e metodologia degli attacchi

Arrivando ora ai target e alle metodologie adottate dagli attori in campo, spiccano certamente gli attacchi ai mezzi di trasporto, come le ferrovie e gli aeroporti (con l'uso del *jamming GPS*), quelli rivolti verso apparati industriali di difesa e contro le infrastrutture critiche di carattere strategico-economico (Kłyszcz e Kohv, 2025). Gli eventi degli ultimi anni, frequentemente comprendenti sia danneggiamenti a gasdotti sia guasti di cavi e interconnessioni nel Mar Baltico, hanno consolidato il fatto che le infrastrutture sottomarine «sono vulnerabili non solo ad azioni "classiche", ma anche ad interferenze internazionali a basso costo» (vedi figura 1 e 2).

Figure 1: European Underwater Fiber-Optic Cables

Source: "Submarine Cable Map 2022," Telegeography, https://submarine-cable-map-2022.telegeography.com/ (CC BY-SA 4.0 DEED); and "How Can We Protect the Internet's Undersea Cables?," World Economic Forum, November 4, 2015, https://assets.weforum.org/wp-content/uploads/2015/11/151104-submarine-cablesinternet-worldmap.png.

Cavi sottomarini europei in fibra ottica

Fonte: CSIS analysis, Seth G. Jones (2025), Russia's Shadow War Against the West, CSIS https://www.csis.org/analysis/russias-shadow-war-against-west

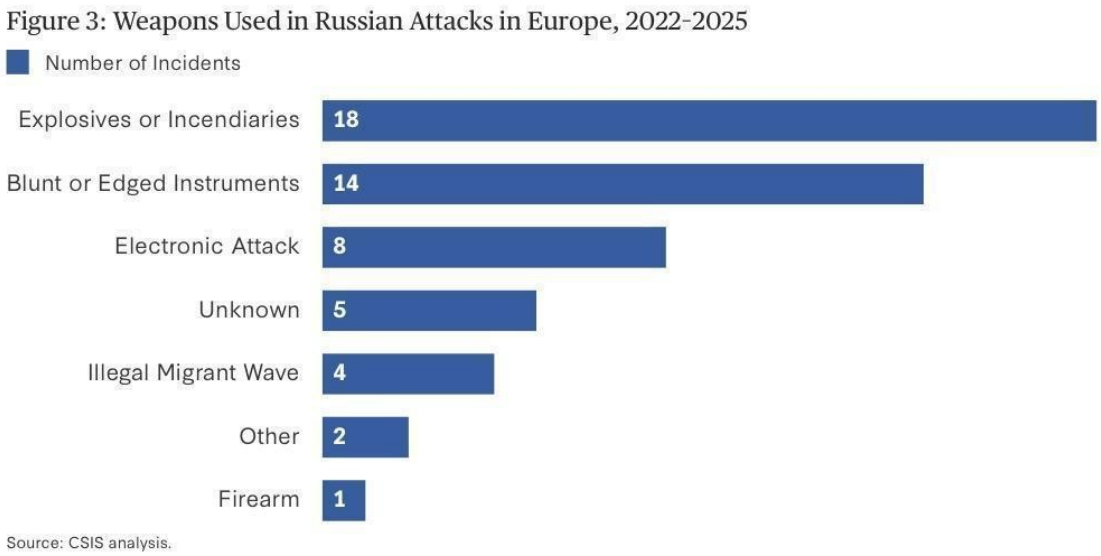
Figure 2: Targets of Russian Attacks in Europe, 2022-2025

Source: CSIS analysis.

Obiettivi degli attacchi russi in Europa

Fonte: CSIS analysis, Seth G. Jones (2025), Russia's Shadow War Against the West, CSIS https://www.csis.org/analysis/russias-shadow-war-against-west

Allo stesso tempo, per quanto riguarda i mezzi attraverso cui viene posta in essere la "*Shadow War*", termine utilizzato per descrivere la reale ambiguità nel momento di attribuzione degli attacchi a Mosca (Praks, 2025), si nota come tra i principali metodi utilizzati ci sia quello degli attacchi hacker e cyber volti a destabilizzare i segnali GPS, causando deviazioni di volo, errori di navigazione, breakdown informatici e ponendo a repentaglio la vita di molti cittadini europei. Un'altra "arma" utilizzata da parte della Russia contro l'Occidente è l'immigrazione illegale, diretta da Mosca e da Minsk verso la Polonia, la Finlandia, la Lettonia e la Lituania (vedi figura 3). Tra la fine del 2021 e gli inizi del 2022, infatti, se ne è registrato il picco, con l'approdo di un ingente numero di migranti ai confini dell'Unione Europea. Tali crisi di frontiera vengono orchestrate meticolosamente dalla Federazione Russa, affinché non solo le istituzioni dei paesi interessati appaiano disorientate e incapaci nel sostenere una situazione simile, ma anche per fomentare l'opinione pubblica contro queste ultime, aprendo varchi politici proficui per partiti antisistema di ambo gli estremi politici (Voo e Singh, 2025).



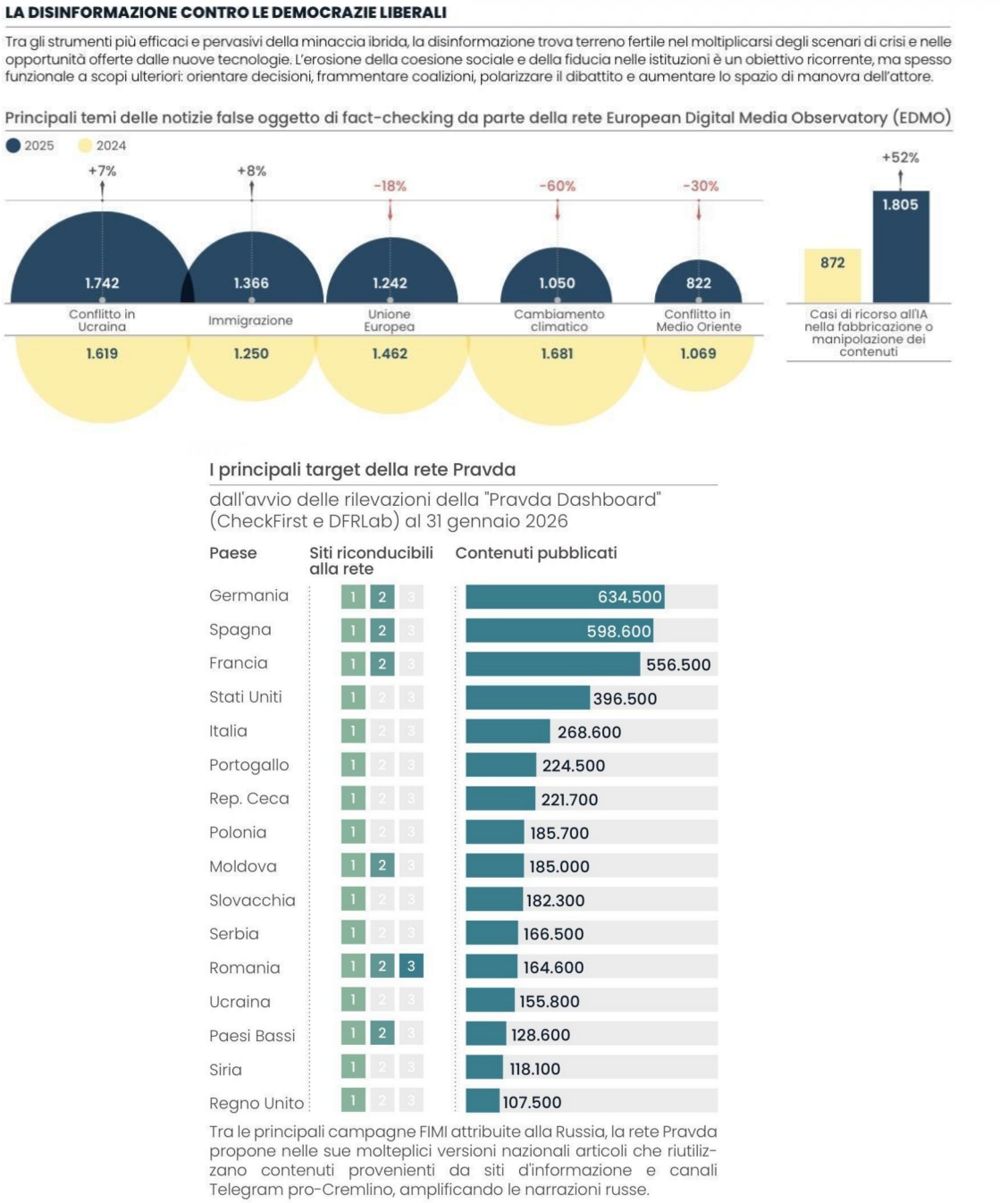
Armi utilizzate dagli attacchi russi in Europa

Fonte: CSIS analysis, Jones S. G. (2025), Russia's Shadow War Against the West, CSIS https://www.csis.org/analysis/russias-shadow-war-against-west

Manipolazione informativa e interferenza straniera

Più subdola ma ugualmente efficace, l'interferenza politica russa, di fatti, come indica la stessa relazione dei servizi italiani, costituisce una delle minacce più frequenti dirette verso numerosi paesi, compresi coloro che guardano alle istituzioni euro-atlantiche con speranza e desiderio di rivalsa dal passato sovietico (e.g. Moldavia e Georgia) (Sistema di informazione per la sicurezza della Repubblica, 2026). L'informazione assume perciò un valore puramente strategico, andando ad influenzare in maniera invasiva il processo elettorale del paese in esame. Gli attori coinvolti non solo diffondono narrazioni false o manipolate attraverso le piattaforme social (*Foreign information manipulation and interference - FIMI*), ma soprattutto tendono ad alimentare la sfiducia nel processo democratico, ampliando divaricazioni politiche già esistenti. La *dezinformacija*, già utilizzata anzitempo in Unione Sovietica nel corso della guerra fredda, viene adottata per diffondere panico, minimizzare il pericolo, giustificare operazioni militari e bersagliare la leadership occidentale ogni qualvolta essa rintracci nella Federazione Russa una minaccia esistenziale per la propria sicurezza (vedi figura 4 e 5).

Figura 4 e Figura 5



Fonte (figura 4 e 5): ***La disinformazione contro le democrazie liberali - I target della propaganda russa in Europa*** *Sistema di informazione per la sicurezza della Repubblica (2026), Governare il Cambiamento, Relazione annuale sulla politica dell'informazione per la sicurezza, Roma, https://www.sicurezzanazionale.gov.it/contenuti/relazione-al-parlamento-2026*

Scenari di conflitto Russia-NATO: Narva e l'Estonia

Tuttavia, la minaccia russa non è solamente misurabile attraverso i casi menzionati precedentemente, bensì è fondamentale che essa stessa sia calibrata e valutata con meticolosità in tutti gli scenari più sensibili, compresi quelli tattico-militari. A tal proposito, il report dei servizi evidenzia chiaramente quali siano le aree più critiche, sottoposte a forte pressione strategico-politica da parte di Mosca. In un capitolo totalmente dedicato ad eventuali scenari futuri di confronto militare tra Mosca e l'Occidente, l'intelligence italiana, attraverso un esercizio di analisi previsionale condotto con l'IA, indica tre scenari in cui la Federazione Russa potrebbe testare la deterrenza NATO, scommettendo su una risposta più o meno blanda da parte degli Stati Stati membri dell'alleanza. Inoltre, ciascun scenario, validato da esperti analisti e generato in collaborazione con GenAI, prevede un probabilità di accadimento, un pretesto, determinate modalità di svolgimento, eventuali obiettivi e probabili conclusioni. Mentre la seconda (corridoio dei Suwalki tra Polonia, Kaliningrad, Lituania e Bielorussia) e la terza ipotesi (Mar di Barents, a nord della Norvegia) attestano una probabilità di attacco russo tendenzialmente bassa, o comunque non troppo superiore ad un 25%, la porzione geografica maggiormente attenzionata è quella corrispondente alla zona di Narva, a nord est dell'Estonia. Qui, infatti, la probabilità di un attacco ibrido del Cremlino incrementa significativamente, dal momento che trova spazio la narrativa russa legata alla salvaguardia delle minoranze russofone.

L'Estonia, di fatti, ad oggi rappresenta uno dei paesi europei maggiormente interessati dalla presenza di una forte componente russofona, la quale, con innegabili eccezioni, guarda a Mosca e alla lingua russa con interesse non indifferente. Nel caso di Narva, dunque, il pretesto sarebbe un intervento a loro tutela, il quale potrebbe comportare attacchi cibernetici, propaganda filo regime e infiltrazioni di forze speciali russe. Non è un caso che l'obiettivo di creare una "zona grigia" tra la NATO e la Federazione Russa in Estonia venga apertamente messo per iscritto anche da Carlo Masala, professore di Politica internazionale presso la Bundeswehr University di Monaco di Baviera, nel suo libro *If Russia Wins, a scenario*. Egli, in maniera tanto dettagliata quanto paragonabile a quanto esplicitato dai servizi d'intelligence italiani, individua la città di Narva come la principale tra le aree geografiche maggiormente sottoposte alla pressione politica e militare russa. Lo scenario da lui proposto prevede un attacco armato, piuttosto inaspettato ed intenso, alla città di confine estone, la quale, dopo prolungate e fallimentari discussioni in sede atlantica sul tipo di reazione da intraprendere contro Mosca, diviene il simbolo della debolezza strategica occidentale, aprendo ad una stagione geostrategica ancor più instabile tra la NATO e la Federazione Russa (Masala, 2025). A conferma di come queste proiezioni siano pressoché verosimili e la loro concretizzazione non sia affatto lontana dalla realtà, durante le prime settimane di marzo si è andata diffondendo una notizia per cui vi sia in atto una campagna filorussa nei principali social media che promuove la nascita di una Repubblica Popolare di Narva, plasmando le esperienze poco fruttuose del Donbass ucraino (Euronews, 2026).

Conclusioni

Se dal punto di vista militare, l'unica opzione di deterrenza attuabile è un riarmo immediato, volto al rafforzamento del pilastro europeo all'interno della NATO e ad una preparazione adeguata in caso di conflitto armato, dal punto di vista informativo e delle infrastrutture critiche l'obiettivo potrebbe essere più vicino di quanto previsto. Come indicato nel documento dall'intelligence italiana, una risorsa preziosa nel contrasto alla disinformazione, assieme al meccanismo di Counter-AI, è la tecnologia blockchain, la quale presenta delle caratteristiche fondamentali (decentralizzazione, immutabilità, crittografia), le quali consentono un registro cronologico e protetto da meccanismi inalterabili, chiusi ad eventuali modifiche con l'IA. Altro elemento considerato essenziale nel definire un sistema di sicurezza informativo efficace ed efficiente è l'identità digitale sovrana (*self-sovereign identity - SSI*), il cui utilizzo andrebbe a limitare significativamente la diffusione massiva di bot e account falsi. Per quanto riguarda la prevenzione agli attacchi contro le infrastrutture critiche, invece, la strategia si basa su tre pilastri principali: il riconoscimento dei cavi come asset critici, la creazione di procedure comuni per gestire gli incidenti e l'investimento in tecnologie sicure per ridurre le dipendenze estere. Dato questo contesto, la collaborazione tra NATO e UE appare non solo preminente ma fondamentale per un coordinamento fluido e coerente, volto alla sorveglianza costante e ad accelerare i tempi di reazione. Se in superficie il controllo si affida a satelliti e radar, sul fondale diventa cruciale e dirimente l'uso di sensori acustici, droni subacquei autonomi e intelligenza artificiale, capaci di individuare potenziali minacce e distinguere queste ultime dalle normali attività marine. Tuttavia, il report consegna ai lettori un monito, secondo cui la sicurezza non è solo mera tecnica ma essa prevede un ruolo predominante dell'intelligence nel localizzare le minacce ibride, riducendo in maniera sostanziale la "zona grigia", all'interno della quale possono operare attori ostili, Federazione Russa *in primis*.

Bibliografia:

- Euronews (2026), “A ‘people’s republic’ on NATO’s edge: The Narva narrative testing Europe’s defence”, 19 marzo. https://www.euronews.com/2026/03/19/a-peoples-republic-on-natos-edge-the-narva-narrative-testing-europes-defences;
- Ministero della Difesa (2025), Il contrasto alla guerra ibrida: una strategia attiva. Non-paper del Ministro della Difesa, Roma. https://www.difesa.it/assets/allegati/83696/non-paper_il_contrasto_alla_guerra_ibrida.pdf;
- Voo, J. e Singh, V. V. (2025). Russia’s Information Confrontation Doctrine in Practice (2014–Present): Intent, Evolution and Implications. International Institute for Strategic Studies. https://www.iiss.org/research-paper/2025/06/russias-information-confrontation-doctrine-in-practice-2014present-intent-evolution-and-implications/;
- Kłyszcz, I. U. e Kohv, M. (2025). Confronting the Russian Hydra: Continuity and Innovation in the Grey Zone. International Centre for Defence and Security. https://icds.ee/en/confronting-the-russian-hydra-continuity-and-innovation-in-the-grey-zone/;
- Masala, C. (2025), If Russia Wins, A Scenario, Atlantic Books, pp. 5-8;
- Praks, H. (2025). Russia’s Hybrid Attacks in Europe: From Deterrence to Attribution to Response. International Centre for Defence and Security. https://icds.ee/en/russias-hybrid-attacks-in-europe-from-deterrence-to-attribution-to-response/;
- Jones, S. G. (2025). Russia’s Shadow War Against the West. Center for Strategic and International Studies. https://www.csis.org/analysis/russias-shadow-war-against-west;
- Sistema di informazione per la sicurezza della Repubblica (2026), Governare il Cambiamento. Relazione annuale sulla politica dell’informazione per la sicurezza, Roma. https://www.sicurezzanazionale.gov.it/contenuti/relazione-al-parlamento-2026.

DYNAMES

Difesa • Sicurezza • Resilienza

DYNAMES è una rivista registrata dedicata all'analisi dei temi strategici di difesa, sicurezza, comunicazione, geopolitica, resilienza e interesse nazionale.

Registrata al Tribunale di Busto Arsizio N. 01/2026 del 25 febbraio 2026

Iscrizione ROC n. 44335

Con sede in Via Carlo Noè 45 Gallarate (VA), C.F. 3800470126

Direttore responsabile Fabio Boscacci

Pubblicazione diffusa in formato digitale mediante il sito www.dynames.it e gli altri canali ufficiali della testata.