22 APRILE 2026

Commenti

Nuova Serie

NEXUS

ITALIAN HUB ON HYBRID THREATS

MONITORARE LA MINACCIA IBRIDA IN ITALIA

COMMENTO
N.033 NS/2026

*Leonardo De Agostini, Beniamino Irdi, Nicolò Russo Perez, Arturo Varvelli

La Relazione annuale 2026 del Comparto Intelligence sulla politica dell'informazione per la sicurezza individua nelle minacce ibride una delle principali sfide alla tutela dell'interesse nazionale. Le definisce come azioni coordinate, riconducibili ad attori statuali e a reti di proxy, condotte al di sotto della soglia del conflitto armato, con l'obiettivo di danneggiare e destabilizzare il Paese bersaglio facendo leva sulle vulnerabilità sistemiche.

Il Ministero degli Esteri e quello della Difesa hanno recentemente preso atto dell'importanza del tema, rispettivamente attraverso l'istituzione di un apposito ufficio e la pubblicazione di un non-Paper a firma del Ministro della Difesa.

La centralità e l'urgenza dell'argomento per l'Italia sono ulteriormente confermate dalla sua recente inclusione tra le materie esaminate dal Consiglio Supremo di Difesa e dalle iniziative del Parlamento, fra cui un ciclo di audizioni attivato dalle Commissioni Terza e Quarta del Senato. Pur essendo sempre più presente nel dibattito pubblico, il tema richiede maggiore chiarezza e una più solida capacità di informazione rivolta alla cittadinanza, alle istituzioni e al settore privato, sempre più strategico e centrale nello sviluppo e nella gestione delle tecnologie.

Perimetro di una minaccia multi-dominio

La minaccia ibrida si definisce innanzitutto per la sua natura multi-dominio. Come evidenziato dallo *European Centre of Excellence for Countering Hybrid Threats*, essa si articola attraverso una pluralità di domini - fra cui quello informativo, diplomatico, cyber, economico e politico-culturale. La complessità della minaccia, e le sfide che pone al sistema Paese, risiedono nel *nexus* tra questi domini: nella capacità di combinare leve diverse per colpire vulnerabilità sistemiche. Ne deriva un *continuum nella zona grigia* che ne complica il monitoraggio, ostacola l'attribuzione e rallenta la risposta istituzionale, accentuando l'asimmetria tra attacco e difesa.

Mentre la guerra di aggressione russa continua sul terreno ucraino, il Cremlino porta avanti in parallelo una campagna di pressione ibrida contro l'Europa, che si sviluppa oltre il dominio militare. Disinformazione, sabotaggi alle infrastrutture critiche, operazioni di spionaggio e ingerenze politiche si inseriscono in una strategia coerente volta a indebolire la coesione interna dell'Unione ed il sostegno a Kyiv. Questa continuità tra campo di battaglia cinetico e dimensione ibrida aumenta la pressione sulle democrazie europee, fra cui l'Italia, esponendole a tentativi persistenti di destabilizzazione.

Il dominio fisico della minaccia ibrida si manifesta oggi come un continuum di pressioni eterogenee ma sempre più coordinate, che colpiscono infrastrutture civili, energetiche e logistiche. Un vero e proprio assedio invisibile che si traduce in una combinazione di sabotaggi e attività criminali, con incursioni a basso costo ma ad alto impatto strategico.

*Leonardo De Agostini
Visiting Fellow FCSF

*Beniamino Irdi
CEO & Founder
Highground

*Nicolò Russo Perez
Direttore FCSF

*Arturo Varvelli
Head of Office and Senior Policy Fellow ECFR

Nel Mar Baltico, il danneggiamento di cavi sottomarini e infrastrutture energetiche ha portato l'attenzione su operazioni riconducibili alla cosiddetta *shadow fleet* russa. Sciami di droni hanno sorvolato aeroporti e basi militari in almeno sette Paesi europei, tra cui Polonia, Germania, Danimarca e Norvegia, evidenziando la vulnerabilità dello spazio aereo civile e militare. A ciò si aggiungono episodi di sabotaggio diffuso, tramite l'impiego di reti criminali reclutate online per operazioni *usa e getta*, spesso ingaggiate attraverso canali difficilmente tracciabili come Telegram e remunerate in criptovalute.

Su questo sfondo, la manipolazione informativa e le interferenze straniere (FIMI) rappresentano una componente strutturale dell'azione russa e, in misura crescente, cinese. Come evidenziato dall'ultimo rapporto del Servizio Europeo per l'Azione Esterna (SEAE), le operazioni combinano strumenti *overt* e *covert*, adattando messaggi e canali alle caratteristiche dei paesi target per amplificare fratture sociali esistenti, con un'attenzione particolare ai processi elettorali. La scala del fenomeno è in rapido aumento: nel 2025 oltre un quarto degli incidenti rilevati ha coinvolto l'uso dell'intelligenza artificiale, mentre i finanziamenti russi ai media statali sono destinati a superare € 1,5 miliardi nel 2026.

Per l'Italia e l'europa, le sfide del *narrative warfare* – uno dei tasselli della minaccia ibrida, si pongono anche oltre confine, nell'ambito della competizione strategica dal Sahel ai Balcani occidentali, passando per il nord Africa e mediterraneo.

La Cina assume un profilo più assertivo, attraverso sempre più frequenti casi di spionaggio, cyber-sabotaggio e disinformazione in Europa ed in Italia. A ciò si somma il ruolo dell'intelligenza artificiale (IA), che agisce da moltiplicatore, permettendo economie di scala che abbassano il costo delle attività di interferenza e manipolazione. Infine, il quadro è reso più incerto dal riposizionamento dell'amministrazione americana, che contribuisce all'incertezza strategica anche in chiave transatlantica.

Le sfide per l'Italia

Per l'Italia, la complessità della minaccia ibrida si traduce anzitutto in una sfida di adattamento istituzionale. La frammentazione delle competenze nell'architettura di sicurezza del Paese rende più difficile il coordinamento di una risposta integrata.

La consapevolezza nel dibattito pubblico rimane disomogenea, complice la proliferazione di definizioni e metodologie e la sensibilità politica connessa all'attribuzione di singoli attacchi o campagne.

Resta infine centrale la necessità di rafforzare le sinergie tra settore pubblico e privato, così come lungo l'asse civile-militare. In questo quadro, la sfida non è solo operativa, ma anche concettuale: dotarsi di un linguaggio e di una postura strategica coerenti con la natura sistemica della minaccia.

HIGHGROUND
EUROPEAN COUNCIL ON FOREIGN RELATIONS ecfr.eu
Fondazione CSF