13 NOVEMBRE 2026

Commenti

Nuova Serie

NEXUS
ITALIAN HUB ON HYBRID THREATS

COMMENTO
N.066 NS/2026

L'EVOLUZIONE DELLA MINACCIA IBRIDA RICHIEDE RISPOSTE STRUTTURATE E DIFFUSE

Nicolò Russo Perez*



*Direttore
Fondazione CSF

La guerra non si combatte più soltanto sui campi di battaglia. Si combatte nei fondali marini, attraverso i cavi che trasportano dati e comunicazioni, nelle reti energetiche, nei sistemi informatici, nei flussi di informazione e persino nella percezione che i cittadini hanno delle proprie istituzioni. È questa la nuova dimensione della minaccia ibrida, un fenomeno che sta ridisegnando il concetto stesso di sicurezza europea e mettendo alla prova la capacità degli Stati di difendere i propri interessi anche in assenza di un conflitto dichiarato.

Dai droni che sorvolano infrastrutture strategiche ai sabotaggi delle reti sottomarine, dagli attacchi informatici alle campagne di disinformazione, il quadro è sempre più articolato. Le minacce non arrivano necessariamente attraverso eserciti e armamenti convenzionali, ma possono essere veicolate da gruppi criminali, organizzazioni informatiche, soggetti apparentemente indipendenti o attori riconducibili a interessi statali. L'obiettivo non è sempre provocare un danno immediato: spesso è sufficiente generare instabilità, alimentare sfiducia, rallentare le decisioni politiche o mettere sotto pressione le istituzioni. La forza dell'azione ibrida risiede proprio nella sua natura *cross-domain*, nella capacità di colpire più vulnerabilità contemporaneamente, mantenendo l'azione ostile al di sotto della soglia che tradizionalmente distingue la pace dalla guerra.

In questo senso, la questione della soglia è di primaria importanza per almeno due motivi. In primo luogo, come ci dimostrano i fatti di queste settimane, la soglia si sta evidentemente spostando verso l'alto, con una escalation già in corso che richiede la costruzione di contromisure attive adeguate, non solo dunque nel contesto di un generico appello al rafforzamento della resilienza. Queste contromisure possono articolarsi su una gradualità progressiva di risposte che devono servire in ultima analisi a modificare, rendendolo negativo e dunque sconveniente, il calcolo costi-benefici da parte dell'attaccante che sta testando le *red lines* dell'attaccato (in questo caso, evidentemente, noi). Si tratta di un aspetto di particolare importanza dato che l'attacco è sempre enormemente più economico rispetto alla reazione di difesa che determina, con un divario crescente che sta rendendo sempre più impraticabile una strategia di contrasto basata esclusivamente sul contenimento (una e-mail massiva di poche righe determina l'evacuazione di migliaia di scuole, un drone su un aeroporto determina l'attivazione di protocolli di protezione e difesa dal costo enormemente superiore al drone, ecc.).

In secondo luogo, la questione della soglia è centrale poiché la decide l'attaccato, non l'attaccante. È l'attaccato, siamo noi, a stabilire dove si colloca il confine oltre il quale non deve essere concesso andare. Per fare questo, occorre definire una strategia di deterrenza chiara che renda prevedibile – e dunque temibile – quella che sarà la reazione attuata dall'attaccato che l'attaccante con certezza andrà a subire, vale a dire il

Le opinioni espresse non impegnano necessariamente la Fondazione CSF

costo del suo attacco. Più si sposta verso l'alto la soglia, più si alza il nostro livello di tolleranza rispetto agli attacchi subiti, più si rischia una degenerazione del nostro sistema complessivo, nell'interesse dell'attaccante.

Il contesto attuale è di particolare complessità per almeno due motivi, che pongono il nostro Paese, l'Europa e in generale le democrazie liberali occidentali in condizioni di svantaggio: lo sviluppo tecnologico da una parte, e il contesto geopolitico dall'altra. Al primo motivo, che si traduce in sintesi nel rischio di uno squilibrio sostanziale e sistemico – dallo sviluppo tecnologico in senso lato alla disponibilità di materie critiche – a nostro sfavore, si somma il secondo, dove le controparti sono Stati che non seguono le nostre stesse dinamiche di *accountability* interna, che non hanno una opinione pubblica indipendente o che, in ultima analisi, non hanno un interesse a collocare o mantenere il proprio Paese nel quadro di un sistema internazionale multilaterale o coltivare una propria credibilità sul piano internazionale.

A rendere ancora più complicato il quadro è il problema dell'attribuzione. Stabilire chi si nasconda dietro un attacco, individuare eventuali mandanti e dimostrare il collegamento con uno Stato richiede tempo, competenze e informazioni che non sempre sono disponibili e che quando lo sono, hanno un costo politico elevato. Nel frattempo, l'azione ostile può aver già prodotto i suoi effetti. È questa zona grigia, nella quale diventa difficile distinguere tra competizione strategica, intimidazione e aggressione, a rappresentare uno dei principali vantaggi di chi utilizza strumenti ibridi. Il rischio è che l'incertezza sull'origine dell'attacco finisca per rallentare anche la risposta politica e diplomatica. La deterrenza, in questo contesto, non può fondarsi soltanto sulla capacità di punire, ma deve poggiare anche sulla possibilità di individuare tempestivamente le minacce e impedire che raggiungano i propri obiettivi.

L'Europa ha progressivamente compreso la portata del problema. UE e NATO hanno rafforzato le proprie strategie di sicurezza, investendo nella cooperazione, nella cybersicurezza, nella protezione delle infrastrutture critiche e nella capacità di risposta collettiva. Tuttavia, tra la consapevolezza del rischio e la concreta capacità di affrontarlo resta una distanza significativa. Le sensibilità nazionali non sono sempre le stesse, le risorse sono distribuite in modo disomogeneo e i processi decisionali non sempre riescono a tenere il ritmo di minacce che evolvono rapidamente. Ma la sicurezza europea non può dipendere esclusivamente dalla somma delle capacità nazionali: richiede una visione comune, una maggiore condivisione delle informazioni e strumenti realmente integrati. Il coordinamento tra Bruxelles e le capitali nazionali, così come tra UE e Alleanza Atlantica, deve tradursi in procedure operative e capacità concrete rafforzate.

In questo scenario l'Italia occupa una posizione particolarmente delicata. Il Mediterraneo *allargato* – o meglio l'Indo-Mediterraneo – i collegamenti con i Balcani, le rotte energetiche, i porti, le infrastrutture digitali e i cavi sottomarini rendono il Paese un nodo strategico per la sicurezza europea. La nostra centralità geografica costituisce un'opportunità geopolitica, ma comporta anche responsabilità e vulnerabilità. La protezione delle infrastrutture energetiche e delle reti di comunicazione non riguarda soltanto la sicurezza nazionale: significa tutelare la continuità dei servizi, la competitività economica e gli interessi di un'intera area geografica.

Le opinioni espresse non impegnano necessariamente la Fondazione CSF

HIGHGROUND

EUROPEAN COUNCIL ON FOREIGN RELATIONS
ecfr.eu

Fondazione CSF

13 NOVEMBRE 2026
COMMENTO N. 066 NS/2026

L'EVOLUZIONE DELLA MINACCIA IBRIDA RICHIEDE RISPOSTE STRUTTURATE E DIFFUSE

Un'interruzione significativa delle connessioni digitali o dei collegamenti energetici può produrre conseguenze ben oltre i confini nazionali. Per questo la risposta italiana non può limitarsi alla gestione delle emergenze, ma deve diventare sempre più strutturata da una parte, e diffusa dall'altra. Si tratta di due dimensioni non in contraddizione ma che invece devono rafforzarsi.

In primo luogo, occorre elaborare una risposta strutturata. Occorre rafforzare il coordinamento tra intelligence, Forze armate, Forze di polizia, autorità civili e Agenzia per la cybersicurezza nazionale, favorendo una circolazione più efficace delle informazioni che vada oltre la gestione delle crisi e che sia inquadrata in un Consiglio di Sicurezza Nazionale analogo a quello esistente in molti altri Paesi partner. È altrettanto importante coinvolgere le imprese che gestiscono infrastrutture e servizi essenziali, perché una parte rilevante della sicurezza nazionale dipende ormai da soggetti privati. La protezione delle reti energetiche, delle telecomunicazioni, dei trasporti e dei sistemi digitali richiede investimenti, controlli, esercitazioni e protocolli condivisi.

In secondo luogo, occorre elaborare una capacità di risposta diffusa. Ciò deve accompagnarsi a una maggiore attenzione alla sicurezza dell'informazione: una società esposta alla manipolazione, alla polarizzazione e alla diffusione incontrollata di contenuti falsi è una società più vulnerabile. C'è poi un aspetto che merita particolare attenzione: la dimensione culturale della sicurezza. Le minacce ibride prosperano dove manca la consapevolezza dei rischi. La capacità di riconoscere una campagna di disinformazione, comprendere le vulnerabilità digitali e mantenere fiducia nelle istituzioni rappresenta una componente essenziale della resilienza democratica. La sicurezza, dunque, non è una responsabilità esclusiva degli apparati dello Stato, ma un obiettivo che coinvolge in modo diffuso amministrazioni, imprese, università, mezzi di informazione e cittadini.

In conclusione, la sfida per l'Italia e per l'Europa è passare da una sicurezza prevalentemente reattiva e difensiva a una strategia attiva e capace di anticipare i rischi, individuare le vulnerabilità e garantire la continuità delle funzioni essenziali. Questo significa investire nella difesa e nella tecnologia, ma anche nella prevenzione, nella formazione, nella cooperazione pubblico-privato e nella capacità di assumere decisioni tempestive. Non è soltanto una questione di risorse o di tecnologia, ma di consapevolezza strategica, coordinamento e volontà politica. L'Europa deve dimostrare di saper trasformare la propria dimensione economica e politica in una reale capacità di protezione. L'Italia, per posizione geografica e peso strategico, può contribuire in modo determinante a questo processo. Perché la sicurezza del futuro non si misurerà soltanto nella capacità di vincere un conflitto, ma soprattutto nella possibilità di riconoscerlo, prevenirlo grazie a una deterrenza chiara, e impedire che le sue conseguenze compromettano la stabilità delle nostre democrazie.

Le opinioni espresse non impegnano necessariamente la Fondazione CSF

HIGHGROUND

EUROPEAN COUNCIL ON FOREIGN RELATIONS ecfr.eu

Fondazione CSF