Analytica®
ANALISI | STRATEGIA | SCENARI



Policy Brief

# La trasformazione della minaccia ibrida

## Dalla vulnerabilità del singolo asset alla vulnerabilità del sistema integrato

Autore
Denise Serangelo

analytica-intelligence.com

La sequenza di episodi registrati in Germania nell'estate 2026 evidenzia una trasformazione qualitativa della minaccia ibrida in ambito europeo, nella quale il drone non costituisce più esclusivamente un moltiplicatore di capacità ISR o uno strumento per attività di sorveglianza e sabotaggio, ma si configura come un vero e proprio vettore di pressione strategica sulle infrastrutture critiche. L'episodio della notte tra il 4 e il 5 agosto 2026 presso l'aeroporto di Lipsia/Halle assume, in questo quadro, particolare rilevanza: un UAV equipaggiato con un dispositivo esplosivo fu rinvenuto nell'area cargo sottoposta a restrizioni, nelle immediate vicinanze di aeromobili cargo Antonov An-124 ucraini, mentre, nella medesima sequenza temporale, un velivolo cargo DHL entrò in collisione in volo con un oggetto non identificato durante una procedura di riattaccata e fu successivamente dirottato e fatto atterrare a Hannover. L'allarme determinò una temporanea sospensione delle operazioni aeroportuali e la deviazione di diversi voli. L'episodio assume particolare rilievo in considerazione del ruolo di Lipsia/Halle quale principale hub europeo di DHL e quale infrastruttura di rilevanza strategica per la logistica NATO e per i trasporti connessi al sostegno europeo all'Ucraina.

La rilevanza dell'evento non risiede quindi esclusivamente nell'effetto materiale prodotto, ma nella capacità di introdurre un rischio asimmetrico, persistente e difficilmente prevedibile all'interno di un'infrastruttura civile caratterizzata da elevata interdipendenza sistemica. L'episodio resta oggetto di indagine e non dispone, sul piano politico-istituzionale tedesco, di un'attribuzione definitiva. Tuttavia l'episodio si inserisce in una più ampia dinamica di pressione ibrida caratterizzata da sabotaggio, spionaggio, attività cyber e ricorrenti intrusioni con UAV. I successivi avvistamenti di droni presso la base militare di Mechernich rafforzano, inoltre, la percezione di una minaccia non episodica, ma potenzialmente orientata a sondare vulnerabilità, tempi di reazione e capacità di coordinamento dello Stato.

Il caso tedesco evidenzia pertanto un problema più ampio: le infrastrutture critiche sono tradizionalmente concepite e protette sulla base di minacce provenienti dall'esterno del sistema, mentre i sistemi unmanned possono operare nello stesso spazio fisico, logistico e informativo utilizzato quotidianamente dall'infrastruttura, trasformandone i normali flussi di traffico in potenziali vettori di vulnerabilità. Il drone può infatti osservare, interferire, colpire o essere impiegato come piattaforma di ricognizione sfruttando l'accessibilità e la natura aperta di infrastrutture civili che, per loro stessa funzione, devono consentire il movimento continuo di persone, merci, aeromobili e mezzi. La minaccia non si colloca quindi più semplicemente contro l'infrastruttura, ma può manifestarsi attraverso l'infrastruttura e dentro i suoi stessi processi operativi.

La questione non può quindi essere ricondotta alla sola protezione dello spazio aereo aeroportuale o al potenziamento delle capacità C-UAS, ma richiede lo sviluppo di un modello integrato di resilienza delle infrastrutture critiche, nel quale sicurezza fisica, sorveglianza e controllo dello spazio aereo, *intelligence, cyber security*, controllo degli accessi e continuità operativa siano inseriti in un'unica architettura di prevenzione e risposta. Tale modello deve inoltre garantire la capacità di correlare gli indicatori provenienti dai diversi domini, individuare eventuali pattern di minaccia e supportare tempestivamente l'attribuzione dell'evento, trasformando la protezione dell'infrastruttura da una funzione prevalentemente reattiva a una capacità sistemica di anticipazione, gestione e recupero della minaccia.

La stessa Germania ha già riconosciuto la natura intersettoriale del problema, rafforzando nel 2026 il quadro normativo sulla difesa dai droni e prevedendo un maggiore coinvolgimento delle Forze armate a supporto delle autorità civili; tuttavia, la persistenza di competenze distribuite tra diversi livelli istituzionali dimostra come la principale vulnerabilità possa risiedere non soltanto nella capacità di intercettare il vettore, ma nella capacità complessiva di governare una minaccia che attraversa simultaneamente domini, amministrazioni e funzioni diverse.

# Nuovi paradigmi della guerra ibrida

La successione degli eventi osservati in Germania evidenzia il superamento di una prima configurazione della guerra ibrida. Nel paradigma consolidato, la minaccia veniva interpretata come combinazione di strumenti diplomatici, economici, informativi, *cyber* e paramilitari, impiegati in modo coordinato per esercitare pressione sullo Stato bersaglio mantenendosi, almeno inizialmente, al di sotto della soglia del conflitto convenzionale. Il carattere "ibrido" non risiede quindi nella novità dei singoli strumenti, molti dei quali appartengono alla tradizione della competizione strategica, quanto nella loro integrazione multi-dominio, sincronizzazione temporale e convergenza degli effetti. L'evoluzione osservabile introduce tuttavia un ulteriore elemento: la disponibilità di sistemi relativamente semplici, economici e facilmente producibili consente di generare effetti simultaneamente cinetici, informativi, psicologici e operativi, comprimendo il rapporto costi/effetti a favore dell'attaccante.

In questo processo, il drone costituisce uno dei principali vettori della trasformazione della minaccia. Il suo valore militare non è determinato esclusivamente dalla natura e dall'efficacia del carico utile o dalla capacità di generare un effetto cinetico, ma dalla combinazione di basso costo, accessibilità, modularità, flessibilità d'impiego, ridotta osservabilità e capacità di operare a bassissima quota. Tali caratteristiche consentono di trasferire la minaccia da una dimensione prevalentemente terrestre a un ambiente tridimensionale, introducendo una direttrice di penetrazione che molte infrastrutture civili non sono state originariamente concepite per controllare. Il problema non è pertanto il drone in quanto piattaforma, ma la possibilità di impiegarlo per acquisire informazioni, condizionare le operazioni, provocare interruzioni o generare un effetto cinetico sfruttando vulnerabilità strutturali dell'infrastruttura.

Il caso aeroportuale è particolarmente rappresentativo. Recinzioni perimetrali, controllo degli accessi, pattugliamento, illuminazione, videosorveglianza e sistemi di sicurezza sono prevalentemente orientati alla prevenzione dell'intrusione terrestre. Un UAS può invece superare tali barriere senza violare fisicamente il perimetro e raggiungere direttamente l'area sensibile attraverso lo spazio aereo a bassa quota. Si configura così una nuova direttrice di penetrazione, nella quale la distanza fisica tra l'attaccante e l'asset protetto perde parte del proprio valore difensivo. La superficie da proteggere non coincide più con il perimetro dell'infrastruttura, ma si estende al volume di spazio aereo e allo spettro elettromagnetico necessari al suo funzionamento.

Ne consegue che la protezione non può essere ricondotta alla sola capacità di intercettare o neutralizzare un UAV. È necessaria un'architettura counter-UAS multilivello, persistente e integrata, nella quale sensori, sistemi di comando e controllo e capacità di intervento costituiscano una catena funzionale unica. Il ciclo operativo deve comprendere *detection, tracking, identification e mitigation* (DTIM): rilevare tempestivamente la traccia; mantenerne la continuità e determinarne traiettoria e comportamento; classificare il contatto distinguendo il traffico legittimo dalla potenziale minaccia; infine applicare una misura di mitigazione proporzionata al livello di

rischio. A tale sequenza deve essere associata una capacità di attribuzione tecnico-operativa, finalizzata, quando possibile, a ricostruire origine, modalità d'impiego, infrastruttura di comando e controllo e soggetto responsabile. Il valore della difesa C-UAS risiede quindi meno nella singola tecnologia che nella capacità del sistema di trasformare rapidamente il dato sensoriale in una decisione autorizzata, tempestiva e proporzionata.

Questa configurazione accentua l'asimmetria tra costo dell'azione offensiva e costo della risposta. Un sistema *unmanned* relativamente economico può imporre all'infrastruttura un dispositivo di sicurezza estremamente più oneroso: sospensione delle operazioni, chiusura temporanea dello spazio aereo, deviazione del traffico, evacuazione di aree, impiego di forze di sicurezza e artificieri, attivazione di procedure di emergenza, raccolta forense e ripristino della piena operatività. Il vantaggio dell'attaccante deriva quindi dalla possibilità di imporre al difensore una risposta sistemica a fronte di un investimento offensivo limitato.

In tale prospettiva deve essere ridefinito anche il concetto di danno. L'obiettivo non è necessariamente la distruzione fisica dell'asset, ma la negazione o degradazione della sua funzione operativa. Un aeroporto strutturalmente integro, ma costretto a sospendere temporaneamente decolli e atterraggi, ha subito comunque un effetto strategicamente rilevante. Il bersaglio reale diventa quindi la disponibilità del servizio e, più precisamente, la capacità dell'infrastruttura di assicurare la propria missione entro parametri accettabili di continuità e sicurezza.

La reiterazione degli eventi amplifica ulteriormente tale vulnerabilità. Incidenti brevi ma ripetuti possono produrre un effetto cumulativo superiore a quello di un singolo attacco prolungato, poiché ogni nuova segnalazione riattiva procedure di sicurezza, assorbe risorse, incrementa i costi, riduce la prevedibilità delle operazioni e aumenta l'incertezza del decisore. Si configura così una forma di degrado progressivo della disponibilità operativa, nella quale l'effetto strategico deriva dalla frequenza e dalla persistenza della perturbazione più che dalla capacità distruttiva del singolo vettore.

La resilienza delle infrastrutture critiche deve pertanto essere misurata oltre la loro integrità materiale, includendo disponibilità, continuità operativa, resilienza, capacità di assorbimento dello shock e tempo di recupero. In questa prospettiva, la vulnerabilità strategica non coincide con ciò che l'avversario è in grado di distruggere, ma con ciò che è in grado di degradare, interrompere o rendere temporaneamente indisponibile. Il drone ostile assume quindi la funzione di strumento di *disruption*: non necessariamente distrugge l'asset, ma impone al sistema difensivo un consumo sproporzionato di tempo, risorse e capacità decisionale.

Una seconda direttrice di trasformazione riguarda il dominio elettromagnetico e, in particolare, la crescente esposizione dei sistemi di *Positioning, Navigation and Timing* (PNT) alle interferenze. La diffusione di fenomeni di *jamming e spoofing* GNSS dimostra come la minaccia possa essere indirizzata non contro la piattaforma fisica, ma contro il dato che ne sostiene la funzione. Il *jamming* degrada o impedisce la ricezione del segnale, compromettendone principalmente

la disponibilità; lo *spoofing* introduce invece informazioni contraffatte, inducendo il ricevitore a elaborare una rappresentazione apparentemente coerente ma non autentica della posizione, della navigazione o del riferimento temporale. La distinzione è essenziale sotto il profilo operativo: il *jamming* rende il dato indisponibile, mentre lo *spoofing* può renderlo disponibile ma non affidabile, compromettendone l'integrità.

Si determina così il passaggio dalla neutralizzazione dell'asset alla manipolazione della funzione. Le infrastrutture contemporanee sono infatti sistemi *cyber*-fisici nei quali componenti materiali, reti, sensori, software, dati, algoritmi e sistemi PNT concorrono alla generazione della capacità operativa. La compromissione di uno di questi livelli può produrre effetti sproporzionati rispetto al danno fisico direttamente inflitto. Il centro di gravità della vulnerabilità tende pertanto a spostarsi dall'asset alla catena informativa, digitale e decisionale che ne consente il funzionamento. In determinati contesti, alterare il dato che alimenta il processo decisionale può risultare più efficace che colpire fisicamente il sistema che lo produce.

Questa dinamica assume particolare rilevanza se analizzata attraverso il ciclo OODA — *Observe, Orient, Decide, Act*. La competizione contemporanea non premia esclusivamente chi osserva o agisce per primo, ma chi riesce a mantenere una rappresentazione del contesto operativo più accurata, coerente e tempestiva e a trasformarla rapidamente in una decisione efficace. Una minaccia ibrida può quindi perseguire un obiettivo speculare: degradare la qualità della rappresentazione operativa dell'avversario, rallentandone il ciclo decisionale o aumentando il margine di incertezza entro il quale deve operare.

Un *drone* non identificato, un'anomalia GNSS, un'interruzione informatica o un malfunzionamento di un sistema critico possono infatti produrre una situazione di ambiguità causale. Il decisore deve stabilire se l'evento sia riconducibile a un guasto, a un errore umano, a un'attività criminale, a un incidente o a un'azione deliberatamente ostile. L'attaccante può sfruttare proprio questa indeterminatezza per imporre un costo decisionale senza necessariamente produrre un danno cinetico significativo. Il tempo impiegato per classificare l'evento, validare l'informazione e autorizzare la risposta diventa quindi esso stesso un terreno di competizione.

La guerra ibrida assume così una crescente dimensione di competition for decision advantage, nella quale l'obiettivo non è soltanto conseguire un vantaggio fisico sul terreno, ma compromettere la capacità dello Stato di osservare, interpretare e reagire con tempestività. In questa prospettiva, la resilienza diventa una componente della potenza nazionale: la capacità di mantenere la continuità di governo, assicurare i servizi essenziali, assorbire uno *shock* e ripristinare rapidamente le funzioni degradate costituisce una vera e propria capacità operativa.

Il caso tedesco evidenzia, infine, una progressiva convergenza multi-dominio. L'UAS può svolgere ISR, provocare una disruption o generare un effetto cinetico; il *cyber* può compromettere reti e sistemi di controllo; lo *spoofing* può alterare la rappresentazione della posizione e del tempo; la manipolazione informativa può amplificare l'incertezza prodotta dall'evento; il sabotaggio fisico può colpire direttamente la componente materiale dell'infrastruttura. La minaccia non deve quindi essere analizzata per singolo vettore, ma come sistema di effetti interconnessi.

# Conclusioni

Il paradigma emergente è pertanto quello di una competizione nella quale l'obiettivo non è necessariamente distruggere l'infrastruttura, ma degradarne simultaneamente disponibilità, affidabilità, prevedibilità e capacità decisionale. La vulnerabilità strategica si colloca nell'interdipendenza tra componente fisica, dominio elettromagnetico, sistemi digitali, dati, processi decisionali e comportamento umano. È precisamente questa interdipendenza a trasformare un'infrastruttura critica da semplice obiettivo di attacco in un potenziale sistema di vulnerabilità sfruttabile attraverso più domini, rendendo necessario un modello di protezione fondato non più sulla difesa dell'asset isolato, ma sulla resilienza dell'intera funzione strategica che l'infrastruttura è chiamata ad assicurare.

La Germania costituisce un caso di particolare interesse per il decisore istituzionale non perché rappresenti necessariamente una forma nuova di guerra ibrida, ma perché rende evidente la trasformazione qualitativa delle modalità attraverso cui strumenti già presenti nel repertorio della competizione strategica possono essere combinati per produrre effetti sistemici. Il fattore realmente innovativo non è quindi rappresentato dal singolo vettore — UAV, *cyber*, *jamming*, sabotaggio o disinformazione — quanto dalla loro possibile integrazione all'interno di campagne multidominio finalizzate a sfruttare vulnerabilità preesistenti e a produrre effetti cumulativi sull'apparato statale e sulle infrastrutture critiche.

Il punto di maggiore rilevanza strategica è il progressivo spostamento del bersaglio dall'asset alla funzione. Un'infrastruttura non deve essere necessariamente distrutta per perdere valore operativo: può essere resa temporaneamente indisponibile, sottoposta a continue interruzioni, privata dell'affidabilità dei propri sistemi informativi o costretta ad operare secondo procedure di sicurezza eccezionali. In tale prospettiva, l'effetto strategico può derivare dalla combinazione di disruption, degradazione della disponibilità, manipolazione dell'informazione e incremento dei costi di sicurezza, anche in assenza di danni materiali significativi.

Questo mutamento modifica anche la valutazione della minaccia. Un singolo evento può apparire tatticamente marginale; una sequenza di eventi apparentemente indipendenti può invece assumere rilevanza strategica quando evidenzia ricorrenza, complementarità degli effetti, selezione di specifiche vulnerabilità o capacità dell'avversario di adattarsi alla risposta del difensore. Il requisito informativo prioritario diventa quindi la capacità di correlare gli indicatori dispersi e riconoscere la possibile campagna sottostante, evitando che ogni episodio venga trattato esclusivamente come incidente autonomo. La qualità dell'*early warning* dipenderà sempre più dalla capacità di trasformare eventi eterogenei in una comune operational picture.

Per il decisore istituzionale ciò implica il superamento di una concezione settoriale della sicurezza. Protezione fisica, *counter-UAS*, *cyber defence*, sicurezza elettromagnetica, intelligence, continuità operativa e comunicazione strategica non possono più essere considerate capacità indipendenti, perché l'avversario può agire proprio sulle interdipendenze tra tali domini.

La resilienza di un'infrastruttura deve pertanto essere valutata come proprietà dell'intero sistema e non della singola componente tecnologica o organizzativa.

Ne deriva la necessità di sviluppare un'architettura nazionale integrata di sicurezza delle infrastrutture critiche, fondata sulla condivisione tempestiva dell'informazione e sulla capacità di correlare dati provenienti da domini differenti. Tale architettura dovrebbe assicurare almeno sei funzioni: early warning e raccolta informativa; sorveglianza multidominio; *detection, tracking* e *attribution*; protezione fisica e counter-UAS; *cyber defence* e sicurezza elettromagnetica; continuità operativa e gestione della crisi. A queste deve aggiungersi una capacità di comunicazione strategica in grado di impedire che l'incertezza generata dall'evento venga amplificata attraverso il dominio informativo.

La Germania evidenzia, infine, una trasformazione più ampia dell'ambiente di sicurezza europeo: la vulnerabilità strategica non coincide più necessariamente con ciò che può essere distrutto, ma con ciò che può essere degradato, manipolato o reso temporaneamente indisponibile. In un ecosistema di infrastrutture fortemente interconnesse, anche un evento di limitata portata materiale può produrre conseguenze sproporzionate se incide sulla fiducia, sulla continuità operativa o sul processo decisionale.

Per questa ragione, la resilienza delle infrastrutture critiche deve essere assunta come una capacità di sicurezza nazionale e non esclusivamente come una funzione di protezione dell'*asset*. L'obiettivo strategico deve essere garantire la continuità della funzione anche in presenza di componenti degradate, informazioni manipolate, sistemi temporaneamente indisponibili e minacce simultanee provenienti da domini differenti.

La sfida per il decisore istituzionale non consiste quindi soltanto nel proteggere meglio le infrastrutture, ma nel renderle capaci di operare, adattarsi e recuperare sotto pressione, mantenendo al contempo la capacità dello Stato di comprendere la natura dell'attacco, attribuirne responsabilità e governare l'*escalation*. È su questa capacità di vedere la campagna oltre il singolo evento e preservare la funzione oltre il singolo *asset* che si misurerà la resilienza europea nel nuovo ambiente di competizione ibrida.

# Note Bibliografiche


1- Donahue, A. (2026, 7 ago). *What to know as Germany investigates an explosive drone at a key cargo airport. AP News*. Disponibile su *AP News*

2- Reuters (2026, 5 ago). *Explosive drone at German airport raises new danger, minister says.* Disponibile su Reuters

3- DW (2026, 9 ago). *Germany: Interior Minister warns of 'daily' hybrid warfare.* Disponibile su DW News

4- Bundesregierung/Landesregierungen. (2026, 26 feb). *Novellierung des Luftsicherheitsgesetzes zur Verbesserung der Drohnenabwehr (Bundestag-Protokoll).* Disponibile su bundestag.de

5- NDR (2026, 23 mag). E*U beklagt GPS-Störungen durch Russland als hybriden Angriff.* Comunicazione NDR riportata sul sito ndr.de

6- Höller, L. (2025, 2 lug). *Researchers home in on origins of Russia's Baltic GPS jamming. Defense News.* Disponibile online

7- Crosetto, G. (2025, 29 set). *Italy's plan for a National Hybrid Warfare Centre. Decode39.* Disponibile su decode39.com

8- Serhiyina, K. (2026, 1 ago). *Russia spreads fake claim that Ukraine sold weapons to Italian mafia. RBC-Ukraine.* Disponibile online

9- Bonsegna, N. et al. (2026, 9 apr). *EUCOM Flash Alert Issue 15 - Investigations into sabotage (Transalpine Pipeline). Counterterrorism Group (analisi OSINT).* Disponibile su counterterrorismgroup.com

10- Camba, G. & AFP (2026, 9 ago). *Ukraine denies targeting Bulgaria as drone explodes near pipeline. Euronews.* Disponibile su euronews.com

11- NATO ACT (2026, 9 lug). *Task Force X-Central Mediterranean: Italy and ACT conduct multi-domain experimentation.* Disponibile su act.nato.int

# L’autore

## Denise Serangelo

Denise Serangelo è analista specializzata in sicurezza internazionale, competizione strategica e minacce multidominio. Si è formata presso la Scuola di Applicazione dell’Esercito, in collaborazione con l’Università degli Studi di Torino.

Il suo principale ambito di ricerca è il Mediterraneo centrale, con particolare attenzione alla Libia, al fianco meridionale europeo e alle implicazioni delle dinamiche politico-militari regionali per la sicurezza nazionale ed europea.

Si occupa di analisi delle minacce emergenti, valutazione del rischio e scenari strategici, approfondendo l’interazione tra dimensione militare, geopolitica, tecnologia e infrastrutture critiche.

Ha maturato esperienza sul campo e svolge attività di consulenza e analisi strategica a supporto dei processi decisionali, elaborando report, studi e valutazioni per interlocutori istituzionali e operatori dei settori della sicurezza e della difesa.