Decifrare la minaccia ibrida:

Attori, strumenti e risposte nell'era della competizione sottosoglia

A cura di *Anna Calabrese e Liliana Nitti*

26 MARZO 2026

Il concetto di 'minaccia ibrida' è costantemente utilizzato nel dibattito sulla sicurezza nazionale per descrivere l'utilizzo, da parte attori statali e non statali ostili al nostro Paese, di una serie di tecniche e strumenti decisamente diversi dall'uso tradizionale della forza militare al fine di colpire gli elementi più vulnerabili dell'Italia e dei suoi alleati. Questo tipo di minaccia pone sfide inedite ai nostri apparati di sicurezza: essa, infatti, non solo risulta spesso alquanto difficile da identificare, ma richiede lo sviluppo di nuove forme di contrasto in diversi domini. Il Geopolitical Brief n. 54 del Centro Studi si propone di identificare le principali forme tramite le quali si realizza la minaccia ibrida e di illustrare i principali strumenti che risultano più efficaci per il suo contrasto.

Domino – Geopolitical Brief n. 54/marzo 2026

Centro Studi Geopolitica.info | www.geopolitica.info | centrostudi@geopolitica.info

Direttore responsabile: Matteo Mazziotti di Celso

ISSN: 3103-3407

INDICE

Guerra ibrida: effetti operativi e superiorità informativa 1
Daniela Pistoia

SEZIONE I – GLI ATTORI 8

Tra distrazione e distruzione. La minaccia ibrida russa alle democrazie europee.....9
Jacopo Marzano

La strategia multivettoriale cinese su Taiwan e le osservazioni per lo sviluppo della sicurezza nazionale italiana.....23
Sveva Cristina Pontiroli

Quando l'ambiguità non basta: i limiti della strategia iraniana 37
Lorenzo Zacchi

Spionaggio, criptovalute e cyberattacchi nella strategia ibrida globale nordcoreana 54
Tommaso Tartaglione

SEZIONE II – GLI STRUMENTI.....68
Propaganda russa e guerra ibrida in Italia e Slovacchia 69
Lorenzo Avesani

Cyberspazio e guerra ibrida: attori, tendenze e strategie di difesa nel dominio digitale europeo 91
Anna Calabrese

Il fronte geo-economico della guerra ibrida: la filiera delle terre rare 109
Lorenzo Rossi

L'Underwater come dimensione della sicurezza nazionale..... 125
Alessandro Paolinelli e Annalaura Di Michele

La riscoperta del dominio elettromagnetico: lezioni dal conflitto russo-ucraino tra asimmetrie euro-atlantiche e dipendenze capacitive 145
Anna Calabrese

Parole di guerra e guerra delle parole: il discorso come dominio del conflitto 167
Sara Marchetti e Rachele Rigali

SEZIONE III: LE RISPOSTE 189

Europa nella zona grigia: guerra ibrida, fratture interne e il nodo della responsabilità strategica 190
Mattia Saitta e Giulio Croce

Tra vulnerabilità e contromisure: una fotografia della minaccia ibrida in Italia 213
Davide Sotgia

L'Alleanza Atlantica alla prova delle minacce ibride: evoluzione e stato dell'arte dell'approccio NATO al contrasto alla guerra ibrida 239
Fabio Maina

Metodologie didattiche e *best practices* per una formazione orientata al contrasto delle minacce ibride 255
Antonino Cambria

Biografie degli autori 275

Guerra ibrida: effetti operativi e superiorità informativa

di Daniela Pistoia

La guerra ibrida è meglio compresa non come una teoria dell'instabilità, ma come un metodo pratico per generare effetti operativi senza oltrepassare la soglia del conflitto armato convenzionale.

Essa rappresenta uno strumento strategico impiegato per modificare il comportamento di un avversario modellando il suo ambiente operativo: invece di perseguire una distruzione immediata sul campo di battaglia, la guerra ibrida produce effetti cumulativi che degradano i processi decisionali, limitano la libertà d'azione e alterano nel tempo i calcoli strategici.

L'obiettivo operativo principale della guerra ibrida è influenzare le decisioni. Tale influenza viene ottenuta creando incertezza, imponendo frizioni e mettendo in luce vulnerabilità nei sistemi politici, militari, economici, informativi e tecnologici. Piuttosto che colpire un unico centro di gravità, l'azione ibrida esercita simultaneamente pressione su più livelli del sistema dell'avversario. L'effetto operativo è una progressiva riduzione della fiducia nelle istituzioni, cicli decisionali più lenti, tensioni politiche interne e opzioni strategiche più limitate.

Uno degli scopi principali delle attività ibride è testare soglie e reazioni. Intrusioni cibernetiche limitate, interferenze elettromagnetiche, pressioni economiche o campagne informative non vengono condotte unicamente per provocare danni, ma anche per osservare le risposte dell'avversario. L'effetto operativo è una forma di ricognizione a livello strategico. Misurando la velocità di reazione, la coesione politica, la solidarietà delle alleanze e la tolleranza all'escalation, un attore acquisisce indicazioni sulle linee rosse e sulle

vulnerabilità del sistema avversario. Questa intelligence orienta la pianificazione futura e consente una escalation calibrata quando ritenuto vantaggioso.

La guerra ibrida prepara inoltre l'ambiente per crisi future. L'accesso persistente alle reti informatiche, la mappatura delle infrastrutture critiche, la penetrazione economica in settori strategici e le operazioni di influenza all'interno degli ecosistemi mediatici creano vantaggi strutturali. L'effetto operativo è il preposizionamento. In caso di crisi, l'attore dispone già di accessi, conoscenze e canali di influenza che possono essere attivati rapidamente. Le operazioni ibride costruiscono quindi profondità operativa molto prima che venga considerato un eventuale impiego cinetico della forza.

In questo contesto, la guerra elettromagnetica genera capacità operative concrete. Il controllo dello spettro elettromagnetico consente di degradare comunicazioni, sensori, sistemi di navigazione e reti di comando e controllo. Gli effetti operativi includono ordini ritardati, coordinamento compromesso, ridotta consapevolezza situazionale e un aumento della percezione del rischio tra i decisori. Anche interferenze limitate con i sistemi di navigazione satellitare o con le comunicazioni tattiche possono produrre conseguenze psicologiche e operative sproporzionate.

La guerra elettromagnetica offre inoltre un'elevata scalabilità, poiché può generare degradazioni temporanee senza distruzione fisica, consentendo forme di pressione calibrata. Uno Stato capace di effettuare selettivamente attività di *jamming*, *spoofing* o sorveglianza elettromagnetica dimostra di poter interferire con sistemi critici a volontà. Ciò produce una forma di deterrenza per negazione: l'avversario comprende che la propria efficacia operativa può essere ridotta senza che ciò determini necessariamente l'avvio di una guerra aperta.

Parallelamente, le misure difensive di protezione elettromagnetica assicurano la continuità delle operazioni in condizioni degradate, rafforzando la resilienza e preservando l'integrità del comando.

Le capacità cibernetiche completano tali effetti nel dominio digitale. Operazioni *cyber* offensive possono consentire l'esfiltrazione di dati sensibili, la manipolazione di database, la perturbazione dei sistemi logistici o il preposizionamento di malware all'interno di infrastrutture critiche. Gli effetti operativi variano dal vantaggio informativo alla paralisi temporanea di sistemi amministrativi o militari. L'accesso persistente permette inoltre di monitorare processi di pianificazione, anticipare decisioni e predisporre risposte mirate.

La capacità cibernetica difensiva è altrettanto decisiva sul piano operativo. La resilienza delle reti, la segmentazione dei sistemi, le procedure di recupero rapido e il monitoraggio attivo garantiscono la continuità delle funzioni di governo e delle operazioni militari. Nella competizione ibrida, la resilienza stessa diventa una forma di deterrenza: un avversario sarà meno incline a investire in operazioni disruptive se ritiene che i loro effetti saranno contenuti e rapidamente mitigati.

La guerra elettronica e le capacità cibernetiche, congiuntamente, generano un esito operativo decisivo: la superiorità informativa.

La superiorità informativa non è un concetto astratto, ma una condizione funzionale in cui uno Stato è in grado di raccogliere, proteggere, elaborare e sfruttare dati in modo più efficace rispetto al proprio avversario. Essa implica il mantenimento della consapevolezza situazionale mentre quella dell'avversario viene degradata. Consente cicli decisionali più rapidi e coerenti, riduce l'incertezza e protegge l'intento strategico.

Dal punto di vista operativo, la superiorità informativa permette a forze e istituzioni di operare efficacemente anche sotto pressione. Accorcia il ciclo osservare–orientare–decidere–agire (OODA), preserva la fiducia nei sistemi e limita la capacità dell'avversario di manipolare la percezione.

La guerra ibrida si configura quindi come una competizione cumulativa condotta in apparente tempo di pace. I suoi effetti operativi sono incrementali, ma strategicamente significativi. Modellando la percezione, degradando selettivamente i sistemi, testando le reazioni e costruendo accessi per future contingenze, essa modifica l'equilibrio di potere senza un confronto immediato.

In ultima analisi, gli attori che hanno successo nella competizione ibrida non sono necessariamente quelli che distruggono più risorse, ma quelli che riescono a preservare la propria coerenza interna mentre impongono incertezza agli altri. La combinazione di interferenze elettroniche calibrate, accesso cibernetico persistente e flussi informativi protetti genera un insieme di capacità specificamente adattato alla competizione nella grey zone.

In un simile ambiente, la superiorità è misurata meno dal controllo fisico del territorio e più dal controllo dei sistemi, dei dati e dello spazio decisionale. La capacità di operare efficacemente all'interno di questo quadro multidominio determina se uno Stato sia in grado di competere, dissuadere e prevalere nelle condizioni strategiche del conflitto ibrido contemporaneo.

Una delle caratteristiche che rendono la guerra ibrida particolarmente rilevante nel panorama strategico contemporaneo è la democratizzazione della tecnologia. Capacità che un tempo erano quasi esclusivamente appannaggio delle grandi potenze militari sono oggi accessibili anche a Stati di medie dimensioni, attori regionali e persino attori non statali. Tecnologie come l'intelligenza artificiale, i sistemi senza equipaggio, gli strumenti cibernetici e le

avanzate tecniche di analisi dei dati sono sempre più diffuse, relativamente accessibili e spesso di natura dual-use.

L'intelligenza artificiale, ad esempio, consente l'analisi automatizzata di enormi quantità di dati, l'identificazione di vulnerabilità sistemiche, l'esecuzione di campagne di influenza altamente mirate e la generazione di contenuti sintetici credibili. L'effetto operativo non è soltanto tecnologico ma anche cognitivo, poiché accelera il ciclo decisionale di chi la impiega e può saturare o manipolare quello dell'avversario. La bassa barriera di accesso implica che anche attori con risorse limitate possano generare effetti informativi e psicologici significativi.

Una logica analoga si applica ai droni. Sistemi senza equipaggio relativamente economici e modulari, aerei, marittimi o terrestri, consentono sorveglianza persistente, attacchi limitati, attività di disturbo o semplici dimostrazioni di presenza. In un contesto ibrido, il loro valore non è esclusivamente cinetico ma anche coercitivo e simbolico: possono generare pressione continuativa, creare incidenti controllati, raccogliere intelligence o provocare reazioni difensive sproporzionate. La loro ampia disponibilità riduce l'asimmetria che un tempo favoriva le forze armate tecnologicamente più avanzate.

Nel dominio cibernetico, la barriera di accesso è probabilmente ancora più bassa. Strumenti di intrusione, exploit disponibili commercialmente, modelli di ransomware-as-a-service e comunità tecniche di supporto permettono anche ad attori con competenze limitate di produrre effetti operativi rilevanti. Ciò amplia il numero dei potenziali avversari e complica ulteriormente l'attribuzione, che costituisce già una caratteristica centrale della guerra ibrida. La moltiplicazione degli attori aumenta l'ambiguità strategica e contribuisce all'instabilità nella grey zone.

Questa accessibilità tecnologica genera tre principali implicazioni strategiche.

Primo, erode il monopolio del potere tecnologico. Il vantaggio non deriva più esclusivamente dal possesso di tecnologie avanzate, ma dalla capacità di integrarle coerentemente all'interno di un sistema multidominio. L'intelligenza artificiale, da sola, non garantisce la superiorità: la sua efficacia dipende dall'integrazione con guerra elettronica, operazioni cibernetiche, intelligence, sorveglianza, ricognizione e processi decisionali.

Secondo, aumenta la frequenza delle azioni sotto soglia. Quando il costo di accesso è basso, anche il rischio percepito diminuisce. Ciò favorisce una competizione continua caratterizzata da attività di probing, pressioni episodiche e dimostrazioni limitate di capacità.

Terzo, rafforza la centralità della resilienza. In un ambiente in cui strumenti avanzati sono ampiamente disponibili, il fattore decisivo non è soltanto chi può attaccare in modo più efficace, ma chi è in grado di assorbire le perturbazioni con maggiore efficienza. Ridondanza, protezione dei dati, difesa dello spettro elettromagnetico e catene di approvvigionamento tecnologiche sicure diventano componenti strutturali di una deterrenza credibile.

In definitiva, la diffusione di tecnologie caratterizzate da basse barriere di accesso rafforza la logica della guerra ibrida. Riduce il costo dell'azione, aumenta l'ambiguità, moltiplica gli attori e normalizza una condizione di competizione permanente. In tale contesto, la superiorità informativa dipende non soltanto dall'accesso alla tecnologia, ma dalla capacità sistemica di orchestrarla, proteggerla e sfruttarla in modo più efficace rispetto all'avversario.

In questo quadro concettuale si inseriscono i contributi che compongono il presente volume. Le analisi dedicate ai principali attori della competizione ibrida, agli strumenti operativi impiegati nella grey zone e alle possibili risposte istituzionali consentono di osservare come le dinamiche descritte si manifestino

concretamente nel contesto strategico contemporaneo. I capitoli che seguono approfondiscono quindi, da prospettive complementari, le modalità con cui Stati e attori non statali impiegano strumenti informativi, tecnologici ed economici per influenzare sistemi decisionali e ambienti operativi, nonché le strategie sviluppate per rafforzare resilienza e capacità di risposta.

SEZIONE I – GLI ATTORI

Tra distrazione e distruzione. La minaccia ibrida russa alle democrazie europee

di Jacopo Marzano

Introduzione

Le democrazie occidentali hanno, erroneamente e per molto tempo, ricondotto il concetto di minaccia a manifestazioni di forza offensive appartenenti ai paradigmi tradizionali del conflitto: l'uso esplicito della forza, l'aggressione militare, la violazione – manifesta – della sovranità. Nel mentre, una parte crescente della competizione strategica globale si è sviluppata, poi strutturata, al di fuori di questi confini concettuali, in uno spazio grigio nel quale non risulta più efficace distinguere tra guerra e pace e nel quale le categorie operative tradizionali appaiono ormai insufficienti[1].

In questo spazio si collocano fenomeni apparentemente eterogenei: colpi di Stati militari nel Sahel, campagne di disinformazione nei Paesi balitici, micro-incursioni nello spazio aereo europeo, interferenze politiche nei Balcani occidentali, attività di sabotaggio, spionaggio e pressione migratoria nel Mediterraneo e nell'Est Europa.

Considerati in modo isolato, tali eventi appaiono come crisi regionali o episodi contingentati, fenomeni autonomi rispetto alle dinamiche interne all'ordine internazionale. Se considerati nel loro insieme, viceversa, questi evidenziano pilastri diffusi e distanti di una stessa logica strategica, fondata sull'utilizzo sistematico di strumenti di pressione sottosoglia.

[1] Sanz-Caballero, Susana. 2023. *The Concepts and Laws Applicable to Hybrid Threats, with a Special Focus on Europe*, Humanities and Social Sciences Communications, June 2023.

Negli ultimi anni, infatti, la Federazione Russa ha dimostrato una crescente capacità di operare all'interno delle zone grigie, sfruttando fragilità strutturali preesistenti o causando nuove linee di frattura. Nel Sahel, il progressivo disimpegno occidentale ha creato un contesto favorevole per l'infiltrazione di cellule non statali (proxy) esterne e milizie regionali, per l'erosione delle sovranità statali e per la riconfigurazione e strumentalizzazione delle rotte migratorie, in un contesto di instabilità endemica e sistemica.

In Europa, la stessa logica va declinandosi attraverso vettori di disinformazione, interferenze cognitive, attività di manipolazione delle percezioni e sfruttamento delle vulnerabilità sistemiche[2] delle democrazie liberali.

La questione centrale, alla base del seguente contributo, non è quindi se esistano singole operazioni riconducibili a Mosca, ma se tali dinamiche possano, e come, essere lette e accomunate come parte di una strategia di lungo termine progettata all'erosione della resilienza politica, sociale e cognitiva degli stati target e, più in generale, delle democrazie liberali occidentali[3]. Una strategia multilivello, mutevole e sovversiva, che mira a rendere strutturale l'instabilità, normalizzandone le anomalie e riducendo così, progressivamente, le capacità delle società aperte di riconoscere, attribuire e contrastare la minaccia[4].

Dottrina e strumenti della strategia russa di sovversione e della guerra ibrida

[2] Liubychenko, Olena. The Growing Influence of Disinformation, Propaganda, and Hybrid Warfare in Shaping Public Opinion and Policy Across the Region. Warsaw East European Review, December 2025.
[3] Andru, Ctlin, and Lucian Ivan. *Hybrid Actions against EU Member States by the Russian Federation*, Gndirea Militar Romneasc, August 2025.
[4] Karlsen, Geir Hgen. Divide and Rule: Ten Lessons about Russian Political Influence Activities in Europe. Palgrave Macmillan, 2019.

Le diverse linee di penetrazione russa sono riconducibili ad un preciso quadro dottrinale[5] che, a livello ampio e concettualmente strutturato, guida l'azione sottosoglia e asimmetrica di Mosca nello spazio post-bipolare, assegnando un ruolo centrale alla sovversione come strumento di competizione geopolitica interregionale e internazionale. Questa elaborazione dottrinale e concettuale di Mosca ha poi sviluppato una nozione di conflittualità capace di superare la tradizionale dicotomia tra guerra e pace, subordinando l'uso della forza militare convenzionale ad una più ampia e complessa architettura di strumenti politici, economici, informativi, cyber e cognitivo-sociali, capaci di produrre effetti strategici a breve e lungo termine, rimanendo al di sotto della soglia del conflitto cinetico *tout court*[6]. Da qui, l'inserimento delle modalità di guerra ibrida e asimmetrica come vettori strutturali per la continuazione del confronto geopolitico internazionale all'interno di un quadro di conflittualità latente e permanente[7], coerente con le elaborazioni dottrinali di Evgenij Messner sulla guerra di sovversione e con la loro successiva formalizzazione (o concretizzazione) operativa, riconducibile nella riflessione strategica contemporanea del Generale Valerij Gerasimov[8]. La guerra sovversiva di Messner, pilastro del dibattito russo sulla guerra informativa e sul concettualizzazione della guerra moderna, si sviluppa sulla convinzione che il futuro del conflitto bellico avrebbe superato le logiche e gli schemi tradizionali del conflitto cinetico, assumendo le forme di una "myatezhevoyna", ovvero una sovversione sistemica che, tramite l'utilizzo di propaganda informativa e fattuale, avrebbe trasformato la dimensione psicologica della guerra nel

[5] Delibera del Collegio del Ministero degli Affari Esteri della Federazione Russa, 11 aprile 2023.
[6] Giles, Keir. Russia's New Tools for Confronting the West. Chatham House, 2016.
[7] Grau, Lester W. "The Soviet Theory of Revolt War." *Foreign Military Studies Office*, 2004.
[8] Gerasimov, Valery. "The Value of Science in Foresight." *Military-Industrial Kurier*, 27 febbraio 2013.

principale terreno di confronto capace di causare la disgregazione sociale, politica ed economica del bersaglio, alimentando o causando mirate sovversioni endogene ed esogene[9]. Se le lungimiranti elaborazioni strategiche di Messner risalgono agli anni 50 e 60 del Novecento, è la dottrina del Generale Gerasimov ad inserirsi ufficialmente all'interno delle pianificazioni operative dello Stato Maggiore della Difesa russo. Presentata nel marzo del 2019 di fronte all'Accademia russa delle Scienze Militari, la dottrina Gerasimov si muove lungo i concetti di difesa attiva, ovvero di neutralizzazione preventiva delle minacce, per poi strutturarsi una concezione bellica che prevede una crescita esponenziale delle operazioni informative come nuovo teatro operativo senza confini e, insieme a questo, un utilizzo convergente di mezzi politici, economici ed elettronici integrati, comunque, insieme alla forza militare[10].

Cardine della dottrina moderna è dunque lo sfruttamento delle fragilità interne degli Stati bersaglio, nei quali instabilità politica, fratture identitarie, crisi economiche e deficit di legittimità istituzionale vengono amplificate, indirizzate, talvolta aggravate. Questa metodologia operativa consente a Mosca, ad esempio nei teatri subsahariani, di presentarsi come attore stabilizzatore in seguito ad una crisi già in atto, contribuendo, nei fatti, alla riproduzione di ulteriori forme di instabilità[11].

In linea con tale architettura strategica, per quanto riguarda il quadrante africano e subsahariano, il ricorso di attori non statali costituisce uno degli strumenti più efficaci. L'utilizzo di proxy paramilitari consente di mantenere un elevato grado di ambiguità operativa, riducendo i costi politici e diplomatici del

[9] Nato Strategic Communications Centre of Excellence. *Defence Strategic Communications*, Volume 2, Spring 2017.
[10] Johnson, Dave. *General Gerasimov on the Vectors of the Development of Military Strategy,* Russian Studies Series 4/19, Nato College Foundation, 30 Marzo 2019.
[11] Kofman, Michael, et al. *Russian Strategy in Africa*. CNA, 2022.

coinvolgimento diretto e complicando, inoltre, le capacità di attribuzione e risposta degli Stati target. Questo *modus operandi*, riconducibile alle esperienze maturate in Ucraina, Libia e Siria[12], è caratterizzato dall'impiego di un uso limitato della forza attraverso milizie parastatali integrate a proxy locali, con la convergenza di operazioni nel dominio informativo[13] e l'utilizzo di contro-diplomazia, producendo così un modello esportabile e adattabile a contesti caratterizzati da bassa capacità di reazione statuale e forte competizione per il controllo delle risorse. Nel Sahel[14], tale modello si innesta su una regione già attraversata da violenza endemica e profonde crisi politiche, tribali, militari, contribuendo così a rafforzare la presenza di Mosca in chiave di progettazione strategica del caos a livello nazionale-regionale-globale.

Accanto agli strumenti informativi e cyber, la strategia asimmetrica russa assegna un ruolo centrale e non sostituibile all'impiego di operatori sul campo. Da un lato e in forma crescente, emerge il ruolo degli operatori "usa e getta", asset a bassa sofisticazione, criminali locali, migranti, giovanissimi, incaricati di missioni singole e ad apparente basso valore strategico, come scattare foto ad una base militare, far sorvolare un complesso strategico da un drone, appiccare un piccolo incendio, il cui "sacrificio" contribuisce a saturare le capacità e l'attenzione del controspionaggio occidentale[15]. Dall'altro, permane l'utilizzo deglli "illegals", agenti dormienti, inseriti a lungo termine nelle società occidentali[16] senza copertura ufficiale, secondo una logica di profondità

[12] Mason Clark. *The Russian Military's lessons learned in Syria,* Institute for the Study of War, 2021.
[13] Africa Center for Strategic Studies. *Mapping a surge of disinformation in Arica,* 2024.
[14] Europea Union Institute for Security Studies. *Shifting Alliances in West Africa*, April 2025.
[15] Ufficio Federale per la Protezione della Costituzione (BND), Campagna informativa congiunta su "Agenti di basso livello", settembre 2025.
[16] Serscikov, Grigorij. NOCs and Illegals in the Current Surveillance Landscape: Can Mimicry Help Overcome Evolving Challenges? Intelligence and National Security 40 (3), 2025.

strategica a lungo termine[17]. Anche le coperture diplomatiche e para diplomatiche assumono, in questo senso, una funzione volutamente ambigua ed opaca. Oltre alle rappresentanze ufficiali, strutture formalmente dedicate all'informazione, come le sedi estere dell'Agenzia Tass, operano come interfacce tra costruzione narrativa, raccolta informativa e avamposti operativi, rendendo, anche qui, deliberatamente indistinguibili le linee di confine tra attività regolari e di spionaggio in terra straniera[18].

Continuità strategica e teatri operativi

Le dinamiche di instabilità osservate in diversi teatri, dall'Africa subsahariana all'Europa orientale, possono ora essere, alla luce di quanto districato precedentemente, inquadrate all'interno di una stessa logica di conflitto che ha tra i suoi obiettivi quello della normalizzazione dell'anomalia più che una sommatoria di crisi regionali. In questo scenario, la fragilità statuale, la polarizzazione politica e la perdita di fiducia nelle istituzioni, più che linee di faglia, divengono scenari operativi. Nel Sahel questa pressione si articola attraverso la frammentazione parossistica del controllo territoriale, nonché tramite la proliferazione di attori per procura armati[19] e criminali, con effetti diretti sulla strumentalizzazione delle rotte migratorie e sulla crescita di economie illegali. Qui, la proiezione strategica russa si intreccia con la geografia delle principali rotte migratorie nel Sahel, come suggerito dalla sovrapposizione tra installazioni militari di Mosca in mali, Burkina Faso e snodi chiave dei flussi verso il Nordafrica[20]. Tale configurazione lascia ipotizzare un possibile

[17] Riehle, Kevin P., *Russia's Intelligence Illegals Program: An Enduring Asset,* Intelligence and National Security, 2020.
[18] Marzano, Jacopo. *Il valzer delle spie russe si balla a Vienna*, Formiche.net, ottobre 2025.
[19] Christopher M. Faulkner and Raphael Parens, *Russia in Africa: Private Military Proxies in the Sahel,* Georgetown Journal of Internaional Relations, March 2025.
[20] Marzano, Jacopo. L'influenza russa in Africa all'indomani della caduta di Assad, Geopolitica.info, gennaio 2025.

coinvolgimento russo nella governance informale della migrazione irregolare, anche attraverso attività e connessioni tra reti criminali locali e l'Africa Korps, il tutto all'interno di una dinamica migratoria circolare e multipolare, nella quale l'instabilità locale favorisce l'ingresso di attori esterni che, a loro volta, alimentano ulteriori fratture interne e conflitti. Questo ciclo produce una crescente domanda di armamenti e l'espansione del ruolo di attori non statali, inclusi network criminali e gruppi jihadisti, oltre al corpo proxy e paramilitare russo, mentre la persistenza di violenza e crisi umanitarie generano a loro volta sfollamento strutturale, offrendo così spazio operativo per attività illecite di trafficanti e milizie, nonché per lo sfruttamento dell'instabilità sistemica e delle migrazioni irregolari che, spinte verso il Nordafrica[21], può divenire uno strumento asimmetrico di pressione nei confronti del fianco sud dell'Europa e della Nato.

Nei Balcani occidentali, la progettazione d'instabilità strategica assume la forma di una stagnazione politica indotta, alimentata da interferenze informative, sostegno ad élite antioccidentali e sfruttamento di fratture identitarie. Il tutto col fine ultimo di frenare, disturbare o intaccare l'integrazione euro-atlantica, senza però ricorrere a strumenti di coercizione immediatamente visibili e attribuibili[22]. Ancora, nel quadrante baltico, la medesima logica accompagna e struttura un piano operativo che poggia sul piano cognitivo e infrastrutturale, attraverso azioni di spionaggio e intimidazione, campagne di disinformazione, attacchi cibernetici e azione di intimidazione mirate all'erosione della fiducia nella resilienza nazionale e nelle capacità di resilienza collettive[23].

[21] Ivi.
[22] Florian Bieber.The Rise of Authoritarianism in the Balkans, Palgrave Macmillan, 2020; Dimitar Bechev, Rival Power: Russia in Southeast Europe, Yale University Press, 2017.
[23] NATO StratCom COE, Disinformation Review, 2023; ENISA, Threat Landscape 2024.

Diversi registri di progettazione strategica del disordine agiscono, talvolta mirati alla distrazione, talvolta alla distruzione, ma tutti tenuti insieme da una *grand-strategy* che previlegia e predilige la continuità di azione asimmetrica rispetto all'*escalation*. Qui, uso strumentale delle migrazioni, pressione informativa e ricorso sistematico ad attori non statali rientrano, tutti, all'interno dello stesso mosaico. Una concezione della competizione globale che mira a logorare la coesione delle società aperte dal loro interno[24] .

A livello sistemico, questa strategia è rafforzata dalla crescente convergenza operativa tra Russia, Iran, Corea del Nord e Cina. La cooperazione in ambito militare, tecnologico, informativo ed economico consente a questi attori di aggirare sanzioni, sostenere regimi affini, rafforzando così le proprie leve all'interno della competizione geopolitica globale, replicando schemi di instabilità differenziati ma funzionalmente convergenti[25]. Ne emerge un modello di conflitto continuo, opaco e adattivo, nel quale attività cinetiche, informative, coercizione economica, pressione demografica e migratoria[26], leve politiche e asimmetriche concorrono sinergicamente ad una unica architettura antioccidentale, revisionista e revanscista di logoramento strategico. Un case study utile alla comprensione del tema è proprio la creazione ad hoc, nell'autunno 2021, di una pressione migratoria proveniente dalla Bielorussia e diretta alle frontiere lettoni, lituane e polacche. Nello scenario delineato al confine est europeo furono impiegati, per la dispersione degli individui in avvicinamento (tutti provenienti da Iraq, Siria e Afghanistan e giunti in Bielorussia con permessi speciali), gas lacrimogeni, proiettili di gomma e

[24] Marzano, Jacopo. Le migrazioni come leva della guerra ibrida russa, Formiche.net, ottobre 2025.
[25] AA.VV, Crink in 10 Charts, Center for Strategic & International Studies, novembre 2025.
[26] Greenhill, Kelly. "When Migrants Become Weapons: The Long History and Worrying Future of a Coercive Tactic." Foreign Affairs, March/April 2022.

cannoni ad acqua[27]. Oltre alla difficoltà legata alla gestione della crisi migratoria, l'impatto mediatico e quello politico evidenziarono come il tema migratorio riuscisse a esporre tutte le divisioni politiche e le faglie sociali e identitarie interne all'Unione Europea.

Le minacce ibride alle democrazie liberali

Occorre dare una definizione il più possibile puntuale e precisa, ampia ma esatta, di cosa sono le minacce ibride. L'esigenza viene dall'assoluta urgenza di comprenderle per contrastarle, per poterle leggere e metterle a sistema, producendo gli adeguati "anticorpi" statali e democratici.

Secondo la relazione annuale del 2024 del Sistema di Informazione per la Difesa della Repubblica, le minacce ibride si caratterizzano per l'uso coordinato di strumenti politici, economici, informativi e sociali, lungo tutto lo spettro DIMEFIL[28], finalizzati a condizionare il processo decisionale di uno Stato senza ricorrere al confronto militare diretto[29]. La loro natura multivettoriale consente dunque di sfruttare le asimmetrie strutturali delle democrazie liberali, trasformando trasparenza, pluralismo e libertà di informazione in potenziali vettori di interferenza[30], mentre la loro forza ed efficacia risiedono nella capacità di collocarsi in una zona grigia, nella quale attribuzione dell'azione e risposta risultano, per i sistemi democratici, strutturalmente problematiche.

La complessità e la natura adattiva e sinergica della minaccia si concretizza attraverso una lenta erosione epistemica delle società democratiche occidentali, riducendo così la capacità collettiva di discernimento e favorendo polarizzazione

[27] Ibidem.
[28] Lo spettro DIMEFIL sta ad indicare sette principali strumenti di forza/potenza statuale. Il termine è un acronimo che comprende i settori: Diplomatico, Informativo, Militare, Economico, Finanziario, Intelligence, Legale.
[29] Sistema di informazione per la sicurezza della Repubblica, *Relazione annuale,* 2024.
[30] Eu Commission, Hybrid Threats Joint Framework, 2023.

e assuefazione all'anomalia[31]. È in questo spazio che la minaccia ibrida produce i suoi effetti più insidiosi, svuotando progressivamente il contenuto delle istituzioni democratiche senza però comprometterne formalmente il funzionamento.

Vulnerabilità democratiche ed effetti sulle democrazie liberali

La riconfigurazione della conflittualità contemporanea operata dalla Federazione Russa adotta strumenti non convenzionali e investe, al tempo stesso, il bersaglio strategico della guerra: la capacità delle società di interpretare la realtà e di orientare il processo decisionale collettivo. Le operazioni ibride russe non mirano prioritariamente alla distruzione fisica delle infrastrutture o alla conquista territoriale, bensì all'erosione delle soglie cognitive che permettono di distinguere tra guerra e pace, informazione e manipolazione, emergenza e normalità[32].

Un primo livello di questa strategia riguarda la produzione sistematica di ambiguità epistemica. Le campagne di disinformazione vengono condotte attraverso ecosistemi mediatici formalmente giornalistici, con piattaforme digitali e reti sociali che interagiscono sinergicamente col fine ultimo della saturazione dello spazio informativo. La diffusione simultanea di narrazioni contraddittorie, come avvenuto nel dibattito europeo sull'aggressione all'Ucraina, sulla legittimità delle sanzioni o sulla responsabilità di incidenti infrastrutturali nel Baltico, tende dunque al logoramento della fiducia e dei

[31] Marzano, Jacopo. Erosione epistemica e nebbia percettiva. L'attacco ibrido alla democrazia liberale, *Il Pensiero Storico*, novembre 2025.
[32] Ibidem.

criteri di verificabilità, inducendo una sospensione del giudizio che si traduce in paralisi politica[33].

Questa dinamica alimenta una nebbia percettiva che opera per accumulo e assuefazione. Episodi formalmente eterogenei (dalle interferenze elettorali attribuite a reti riconducibili a Mosca, agli attacchi cyber contro infrastrutture civili, fino ai sabotaggi a bassa intensità di cavi sottomarini e reti energetiche), vengono percepiti come eventi isolati, privi di una cornice unitaria. In realtà, essi concorrono, unitamente, a normalizzare una condizione di instabilità latente, nella quale la soglia di allarme si innalza progressivamente e la capacità di reazione collettiva si indebolisce[34].

In tale contesto si inserisce il processo di bellicizzazione sistemica promosso dalla strategia russa. Ambiti tradizionalmente considerati civili vengono progressivamente integrati in una logica di confronto strategico. La coercizione energetica esercitata attraverso la manipolazione dei flussi di gas verso l'Europa nel biennio 2021–2022, l'uso strumentale delle crisi migratorie lungo l'asse orientale dell'Unione europea e il ricorso a proxy criminali e paramilitari in teatri extraeuropei rappresentano declinazioni diverse di un medesimo approccio: colpire i nodi funzionali del sistema senza oltrepassare le soglie di risposta militare convenzionale[4].

Le democrazie liberali risultano particolarmente vulnerabili a questa forma di conflitto. La trasparenza dei processi decisionali, il pluralismo informativo e la lentezza deliberativa, elementi costitutivi dell'ordine democratico, possono essere sfruttati come vettori di penetrazione e interferenza. Ogni attacco all'ordinario, ogni crisi, sanitaria, energetica, migratoria o militare, diventa, in

[33] NATO StratCom COE, *Disinformation Review*, 2023; Peter Pomerantsev, *This Is Not Propaganda*, Faber & Faber, 2019.
[34] RUSI, Are We at War with Russia? How Warden's Rings Map Russia's Hybrid Strategy, 2024.

questo scenario, un moltiplicatore di fratture percettive e politiche. Da qui, il rischio principale provoca un collasso improvviso delle istituzioni, ma pone le condizioni per il loro progressivo svuotamento di significato, come dimostrato dall'erosione della fiducia pubblica nella classe politica e nella capacità degli Stati europei di attribuire, comprendere e contrastare le operazioni ostili condotte al di sotto della soglia del conflitto armato.

In questo scenario, il rafforzamento delle capacità militari convenzionali, pur necessario, si rivela strutturalmente insufficiente se non accompagnato da un investimento nel dominio cognitivo. La risposta alla guerra ibrida russa richiede un arsenale intellettuale capace di integrare analisi strategica, resilienza informativa e capacità di decisione rapida. La qualità dell'informazione, la protezione dello spazio cognitivo e il coordinamento tra intelligence, classe politica e sfera pubblica diventano così elementi centrali della sicurezza nazionale, al pari delle capacità militari tradizionali.

Implicazioni per Europa e Italia

La competizione geopolitica moderna si configura in misura sempre maggiore come una guerra di pressione sottosoglia, nella quale strumenti asimmetrici producono effetti cumulativi strategici[35]. Le implicazioni per l'Italia e per l'Europa sono profonde non sottovalutabili ed il motivo risiede nella natura del conflitto: uno scontro tra sistemi, tra democrazie e autocrazie. Le autocrazie agiscono verticalmente, agilmente e senza dover informare un popolo votante o una classe elettorale[36]. La rapidità e la verticalità delle autocrazie garantiscono alle azioni asimmetriche e sottosoglia una efficacia che, di fronte alle modalità

[35] Storozhynetskyi, Taras. *The security of the Nordic States under the Russian Hybrid Threats,* Bulletin of Taras Shevchenko National University of Kyiv. International Relations, 2025.
[36] Liubychenko, Olena. The Growing Influence of Disinformation, Propaganda, and Hybrid Warfare in Shaping Public Opinion and Policy Across the Region, *Warsaw East European Review*, December 2025.

decisionali, burocratiche e politiche europee, italiane e, più in generale, democratiche, diviene un vero e proprio vantaggio strutturale, costitutivo[37], soprattutto in assenza di risposte coordinate.

Dallo spazio subsahariano allo scenario baltico, fino al teatro balcanico e a quello euro-atlantico, la strategia analizzata mostra una continuità funzionale e convergente tra teatri esterni e vulnerabilità interne all'Europa[38]. Per affrontare una minaccia che è al tempo stesso cognitiva, tecnologica e politica, appare sempre più necessaria l'istituzione di una struttura strategica permanente. L'istituzione di un Consiglio di Sicurezza Nazionale dedicato alle minacce ibride consentirebbe, infatti, di integrare analisi, dottrina e capacità di risposta rapida[39], rafforzando la resilienza cognitiva e istituzionale del Paese. Molto esempi, a livello europeo, potrebbero fungere da esempio e cardine operativo, come lo European Centre of Excellence for Countering Hybrid Threats, lo Psychological Defence Research Institute dell'Università di Lund e la Psychological Defence Agency svedesi, cardini della difesa cognitiva europea. Senza letture condivise e sistemiche del fenomeno, congiuntamente ad un adeguamento delle tempistiche e del modus operandi delle strutture decisionali a livello nazionale ed europeo, le democrazie liberali rischiano di reagire sempre in ritardo, normalizzando l'anomalia fino a renderla irreversibile.

[37] Ibidem.
[38] Kui, Guraku. Russias Hybrid Warfare In The Western Balkans: Geopolitical Strategies and Proxy Actors. *Octopus Journal: Hybrid Warfare & Strategic Conflicts*, October 2024.
[39] Psychological Defence Agency. Psychological Defence and Informations Influence, Mpf Report Series 12/2026.

La strategia multivettoriale cinese su Taiwan e le osservazioni per lo sviluppo della sicurezza nazionale italiana

di Sveva Cristina Pontiroli

Introduzione

Taiwan è diventato uno dei principali teatri di sperimentazione delle nuove forme di competizione strategica tra grandi potenze. Lungi dall'essere limitata alla dimensione militare convenzionale, la pressione esercitata dalla Repubblica Popolare Cinese (RPC) si manifesta attraverso un approccio multidimensionale che combina strumenti cinetici, operazioni ibride e campagne di influenza cognitiva. Esercitazioni navali su larga scala, attacchi a infrastrutture critiche e uso crescente di tecnologie emergenti come l'intelligenza artificiale generativa sono alcuni degli aspetti che offrono un osservatorio privilegiato dell'evoluzione della guerra ibrida nel XXI secolo. Analizzare questa strategia, oltre ad essere utile per comprendere le dinamiche dello Stretto di Taiwan, tornerà utile all'Italia per interrogarsi sulle implicazioni più ampie per le democrazie europee sempre più esposte a forme di competizione sistemica che travalicano i confini geografici tradizionali.

La pratica multivettoriale cinese

"La riunificazione con Taiwan è oramai una certezza", così afferma, all'indomani della conclusione di una delle più intense esercitazioni militari nei pressi dell'isola degli ultimi tempi, la macchina propagandistica di Xi Jinping.[1]

[1] Hawkins, A. e Davidson, H. "Xi Jinping vows to reunify China and Taiwan in New Year's Eve speech", *The Guardian*, 31 dicembre 2025. https://www.theguardian.com/world/2025/dec/31/xi-jinping-vows-reunification-china-taiwan-new-years-eve-speech.

Risale a fine dicembre 2025 la notizia di esercitazioni militari a fuoco attorno a Taiwan, che hanno simulato un blocco totale dei principali porti. L'operazione marittima "Justice Mission 2025" è stata definita dal colonnello Shi Yi come un avvertimento alle forze "separatiste" taiwanesi. Il braccio militare del Partito Comunista Cinese (PCC), ovvero l'Esercito Popolare di Liberazione (PLA, People's Liberation Army, 中国人民解放军), continua così a esibire la propria capacità di circondare l'Isola Formosa

Il Comando del Teatro Orientale del PLA ha dichiarato di aver schierato cacciatorpediniere, fregate, caccia, bombardieri, droni e missili a lungo raggio "in stretta prossimità" di Taiwan[2], con l'obiettivo di testare "la coordinazione aria-mare e la neutralizzazione precisa degli obiettivi", inclusi attacchi a sottomarini e altri bersagli marittimi. Sono state segnalate 28 unità navali tra marina e guardia costiera, di cui almeno due entrate nella zona contigua a Taiwan, accompagnate da 89 aerei da guerra e quattro navi d'assalto anfibio[3]. Secondo le mappe delle zone di allerta aerea e marittima, le esercitazioni hanno coperto un'area più ampia rispetto alle precedenti: alcune si sovrappongono persino al limite delle 12 miglia nautiche, cioè al confine delle acque territoriali taiwanesi[4].

---

[2] *CCTV News* "演习第二天 多军种开展联合立体火力打击", 30 dicembre 2025 https://content-static.cctvnews.cctv.com/snow-book/index.html?item_id=16414857156038280698&toc_style_id=feeds_default&track_id=94E55933-3822-4B0F-A1A8-4882516E4771_788764919772&share_to=copy_url.

[3] *Agenzia Nova News*, "Taiwan: 89 Chinese military aircraft and 28 ships detected around the island", 29 dicembre 2025 https://www.agenzianova.com/en/news/Taiwan%3A-89-military-aircraft-and-28-Chinese-ships-detected-around-the-island/.

[4] Davidson, H. e Hawkins, A. "China launches live-fire drills around Taiwan simulating blockade of major ports" *The Guardian*, 29 dicembre 2025. https://www.theguardian.com/world/2025/dec/29/china-live-fire-military-drills-around-taiwan.

La Justice Mission 2025 rappresenta la sesta grande esercitazione militare del PLA mirata Taiwan dal 2022, quando, in seguito alla visita dell'allora Speaker della Camera statunitense Nancy Pelosi, ci furono giorni di manovre. Tuttavia, si tratta della prima esercitazione in cui è stato esplicitamente evocato un intento di deterrenza contro il coinvolgimento internazionale e in cui parte delle attività è rimasta chiaramente visibile alle piattaforme radar.

Oltre a questa dimostrazione di forza esibizionistica, un'altra minaccia meno visibile, ma altrettanto significativa, ha recentemente minato la sicurezza di Taiwan: gli attacchi ai cavi sottomarini del 2023. I cavi sottomarini sono arterie vitali dell'ecosistema digitale moderno: il loro danneggiamento può provocare blackout informativi, blocchi delle transazioni bancarie e criticità nei sistemi di risposta alle emergenze, fino a compromettere l'economia e il coordinamento militare di un intero Paese: il tutto senza la necessità di ricorrere a mezzi di coercizione fisica. Queste linee in fibra ottica si estendono lungo il fondale marino, rendendole bersagli ideali per operazioni di sabotaggio con un minimo impiego di risorse. Inoltre, gli attacchi a queste infrastrutture offrono un elevato grado di negabilità plausibile, sufficiente a ridurre il rischio di conseguenze dirette: ogni settimana oltre 1.000 navi cargo attraversano lo Stretto di Taiwan e ancore o reti da pesca rappresentano minacce non trascurabili per i soli 24 cavi gestiti da Taipei (14 internazionali e 10 domestici).

In questo scenario, da parte sua Pechino ha più volte negato un coinvolgimento diretto. In seguito a un incidente avvenuto nel febbraio 2023[5], quando alcune navi registrate in Cina hanno tranciato due cavi sottomarini, Pechino ha

[5] Wen, L. "After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience", *The Diplomat*, 15 aprile 2023. https://thediplomat.com/2023/04/after-chinese-vessels-cut-matsu-internet-cables-taiwan-shows-its-communications-resilience/.

sostenuto che ciò fosse frutto di una mera coincidenza, arrivando persino ad accusare Taiwan di manipolare i fatti[6]. Tuttavia, ulteriori episodi successivi hanno rafforzato i sospetti di un coinvolgimento intenzionale di Pechino: a gennaio 2025 una nave cinese, la *Shunxin 39*, ha compromesso il cavo TPE a nord di Taipei, e a febbraio 2025 la *Hong Tai 58*, con equipaggio cinese, ha danneggiato il cavo sottomarino TPKM-3 che collega le isole Penghu con Taiwan.[7]

Queste navi cinesi, a detta del PCC vittime di straordinaria sfortuna, sembrano essere assistite da navi da ricerca, che avrebbero raccolto dati sul fondale marino utili a localizzare con precisione questi cavi, e da team di ricercatori cinesi, in particolare della Lishui University, impegnati nello sviluppo di strumenti per tagliare i cavi.

L'impatto economico di queste interruzioni non è da sottovalutare. Secondo Chunghwa Telecom, nel 2023 i cavi che collegano Taiwan alle isole Matsu sono stati tranciati 12 volte, con costi di riparazione pari a 96,4 milioni di dollari taiwanesi (circa 2,9 milioni di dollari statunitensi)[8]. Inoltre, ogni grande interruzione dei cavi ha perturbato il traffico internet, ritardato le transazioni finanziarie e richiesto deviazioni d'emergenza del traffico. Se da una parte si manifesta lo sviluppo attivo di strumentazione per tagliare i cavi da parte della Cina, dall'altra c'è la dipendenza di Taiwan da navi giapponesi, singaporiane e

---

[6] *Reuters* "China says Taiwan 'manipulating' undersea cable cutting incident before facts clear", 26 febbraio 2025. https://www.reuters.com/world/asia-pacific/china-says-taiwan-manipulating-undersea-cable-cutting-before-facts-clear-2025-02-26/.

[7] Ocon, J. e Walberg, J. "China's Undersea Cable Sabotage and Taiwan's Digital Vulnerabilities", *Global Taiwan Institute*, 4 giugno 2025. https://globaltaiwan.org/2025/06/taiwans-digital-vulnerabilities/

[8] Gahon Chia-Hung Chiang "Countering China's Subsea Cable Sabotage", *Global Taiwan Institute*, 19 marzo 2025 https://globaltaiwan.org/2025/03/countering-chinas-subsea-cable-sabotage/..

filippine per la riparazione dei cavi porta inevitabilmente a gravi ritardi nelle riparazioni che possono anche impiegare diversi mesi.

Questo si inserisce perfettamente nella strategia di guerra nella zona grigia perseguita da lungo tempo dalla Cina, che utilizza mezzi non militari per esercitare pressione evitando un conflitto aperto. Dalle molestie navali alle incursioni quotidiane di jet cinesi, l'obiettivo resta lo stesso: erodere la stabilità di Taiwan.

In questa logica di pressione ibrida e non convenzionale si inseriscono anche le operazioni di disinformazione: risale a gennaio 2024 l'ultimo esempio eclatante di campagna di disinformazione particolarmente sofisticata, in particolare tra quelle che hanno sfruttato l'intelligenza artificiale generativa (GenAI)[9]. Attori statali e non statali della RPC hanno utilizzato sempre più la GenAI per creare disinformazione più sottile e meno rilevabile. In risposta, Taiwan sta sviluppando propri strumenti di GenAI, come il *Trustworthy AI Dialogue Engine* (TAIDE), e sta rafforzando le proprie capacità di rilevamento attraverso partnership tra aziende tecnologiche, governo e media. Supportato da misure legislative, alfabetizzazione mediatica e collaborazioni internazionali, l'approccio proattivo di Taiwan contribuisce così a preservare i suoi valori culturali, oltre a rafforzare la sua resilienza democratica. I risultati[10] suggeriscono che, nonostante gli sforzi della RPC per influenzare l'opinione taiwanese, il sentimento dei taiwanesi verso la RPC rimane in gran parte neutro o negativo, e l'uso strategico della GenAI da parte di Taiwan sembra aver efficacemente ridotto l'impatto delle tecniche di IA della RPC.

---

[9] L'intelligenza artificiale generativa (GenAI), è un tipo di intelligenza artificiale (IA) in grado di creare contenuti originali, come testi, immagini, video, audio o codice software, in risposta al prompt o alla richiesta di un utente. Tra gli esempi più noti, ChatGPT e DALL-E.

[10] Mobilio, S. "GenAI in the 2024 Taiwan Presidential Election: Lessons for Democracies." *The Cyber Defense Review*, Fall 2024.

Pechino ha adottato modelli già sperimentati in passato, ispirati alle "active measures" sovietiche, basati sulla diffusione di narrazioni false tramite media *proxy* o stranieri che vengono poi rilanciate altrove con maggiore legittimità. Un esempio precoce è stato un falso reportage su un presunto incontro segreto tra Stati Uniti e Taiwan per lo sviluppo di armi biologiche[11], che ha ottenuto una certa visibilità nei media locali taiwanesi. Con l'avvicinarsi delle prossime elezioni e lo sviluppo di tecniche sempre più intracciabili, le ultime frontiere di questa strategia includono *deepfake*, video con avatar e voci generate da AI, *chatbot* sui social media, articoli falsi e modelli linguistici cinesi addestrati su linee ideologiche pro-PCC. Diversi casi concreti mostrano questa evoluzione: un video manipolato ha falsamente mostrato il candidato del DPP Lai Ching-te elogiare avversari filo-Pechino, mentre un altro contenuto critico su un progetto ferroviario è circolato su Douyin e TikTok, raggiungendo un pubblico molto più ampio sulla seconda piattaforma. Un'operazione particolarmente innovativa è stata la diffusione di un e-book di 300 pagine con accuse false contro la presidente Tsai Ing-wen[12], utilizzato poi come base narrativa per contenuti generati con IA. La strategia mirava a colpire indirettamente Lai, associandolo agli scandali inventati attribuiti a Tsai, dimostrando una complessa manipolazione reputazionale.

La risposta di Taipei in questo campo è stata rapida e decisa. Sul piano istituzionale, il governo ha creato *task force* dedicate al contrasto della disinformazione e ha anche introdotto misure legislative mirate, come la Anti-

[11] Wong, T. "Taiwan election: China sows doubt about US with disinformation", *BBC News*, 8 gennaio 2024 https://www.bbc.com/news/world-asia-67891869.
[12] Yung-yao, T. e Chin, J. "China is posting fake videos of president: sources", *Taipei Times*, 11 gennaio 2024.
https://www.taipeitimes.com/News/front/archives/2024/01/11/2003811930#:~:text=China%20is%20posting%20fake%20videos,from%20Austin%20Wang's%20Facebook%20page.

Infiltration Law del 2019, che punisce interferenze straniere nei processi elettorali, inclusa la diffusione di disinformazione. Sul piano dell'alfabetizzazione mediatica, Taiwan ha integrato l'educazione ai media nel curriculum nazionale attraverso il White Paper sulla Media Literacy nell'era digitale (2023), ampliando programmi precedenti e coinvolgendo tutte le fasce d'età per fornire ai cittadini le competenze necessarie a riconoscere contenuti manipolati. Sul piano tecnologico, Taiwan utilizza strumenti di intelligenza artificiale generativa in collaborazione con aziende tech come Taiwan AI Labs per individuare, contestualizzare e neutralizzare la disinformazione, automatizzando verifiche delle fonti e *fact-checking*. Infine, come risposta ai modelli linguistici cinesi, Taiwan sta sviluppando un proprio LLM[13], TAIDE, pensato come applicazione di IA affidabile e culturalmente radicata. Affrontare queste minacce esterne da parte di una potenza democratica non è semplice: Taipei infatti deve continuare a tutelare la privacy dei propri cittadini e contemporaneamente la loro libertà d'espressione. Tuttavia, questo approccio evidenzia il potenziale di resilienza democratica, e offre lezioni decisamente utili per altre democrazie, in particolare riguardo a come agire nelle fasi precoci delle campagne informative e nei contesti di conflitto non cinetico.

I discorsi del presidente taiwanese Lai Ching-te, che ha promesso di rafforzare le difese dell'isola e raggiungere "un alto livello di prontezza al combattimento" entro il 2027[14], hanno rappresentato un ulteriore fattore di allarme per Pechino. Mentre il colonnello Shi Yi accusava le forze separatiste, un portavoce del

[13] Un Large Language Model (LLM), in italiano "modello linguistico di grandi dimensioni", è un tipo di intelligenza artificiale avanzata progettata per leggere, comprendere, riassumere e generare testi in linguaggio naturale.

[14] *Reuters* "Taiwan president vows to strengthen island's defences in Lunar New Year message", 15 febbraio 2026.
https://www.reuters.com/world/china/taiwan-president-vows-strengthen-islands-defences-lunar-new-year-message-2026-02-15/-

ministero degli Esteri, Lin Jian, ha parlato di "forze esterne" che portano la regione alla guerra. Nel caso delle minacce di fine dicembre 2025, che hanno visto mesi di preparazione ed estesa pianificazione, la narrativa cinese ha utilizzato come casus belli una vendita record di armi statunitensi a Taiwan per 11 miliardi di dollari di metà dicembre 2025[15]. "Qualsiasi piano sinistro per ostacolare la riunificazione della Cina è destinato a fallire", ha dichiarato Lin Jian.

A livello regionale e globale, le reazioni appaiono contrastanti. In Giappone, la premier Sanae Takaichi ha affermato che Tokyo potrebbe essere coinvolta militarmente in caso di attacco cinese a Taiwan. Dall'altro lato del Pacifico, invece, il presidente statunitense Donald Trump ha minimizzato il rischio di un'invasione imminente, sostenendo che Xi Jinping potrebbe non dare seguito alle intimidazioni precedenti e richiamando il loro "ottimo rapporto" personale.

La teoria olistica cinese

Il Partito Comunista Cinese e il leader Xi Jinping hanno esortato Taiwan ad accettare la "riunificazione pacifica", per evitare l'uso della forza letale, anche al discorso di Capodanno 2026 a Pechino[16]. Tra parate militari e summit internazionali, al centro della visione di Xi di un nuovo ordine mondiale multipolare enunciata nel discorso vi è l'annessione di Taiwan e il sostegno di altri paesi nel riconoscere Taiwan come parte di "un'unica Cina" governata dal Partito Comunista Cinese. Nel suo discorso, Xi ha anche evidenziato il "Taiwan Retrocession Day", una giornata commemorativa creata nel 2025 per segnare l'anniversario della fine del dominio imperiale giapponese su Taiwan nel 25

[15] *Skytg24* "Taiwan, armi da Usa per 11 miliardi di dollari: è il pacchetto più grande mai approvato" 18 dicembre 2025, https://tg24.sky.it/mondo/2025/12/18/taiwan-armi-usa.
[16] Hawkins, A. e Davidson, H. "Xi Jinping vows to reunify China and Taiwan in New Year's Eve speech", *The Guardian*, 31 dicembre 2025. https://www.theguardian.com/world/2025/dec/31/xi-jinping-vows-reunification-china-taiwan-new-years-eve-speech.

ottobre 1945. Nello stesso anno, Taiwan ha invece approvato una legge per riconoscere quella stessa data come festa nazionale.

Quest'anno, infatti, l'eredità della Seconda guerra mondiale è emersa come un tema centrale nella retorica politica di Cina e Taiwan: il presidente taiwanese Lai Ching-te ha pronunciato un discorso incisivo, in cui ha paragonato Taiwan alle democrazie europee degli anni Trenta minacciate dalla Germania nazista[17]. Questo a dimostrazione di quanto la grande maggioranza del Parlamento e della popolazione taiwanese respinga la prospettiva di un governo del PCC.

Inoltre, nel discorso di inizio anno 2026 il presidente taiwanese Lai ha nuovamente avvertito riguardo alle "crescenti ambizioni espansionistiche" della Cina, e ha promesso di "difendere fermamente la sovranità nazionale", procedendo a invitare i partiti di opposizione a smettere di bloccare una legge speciale che consentirebbe l'aumento del bilancio della difesa taiwanese. "Di fronte alle allarmanti ambizioni militari della Cina, Taiwan non ha tempo da perdere e certamente non può permettersi di consumarsi in conflitti interni", ha dichiarato il presidente.

Questa crescente strategia della tensione, infatti, rientra in una serie di manovre calcolate all'interno del piano cinese per una guerra ibrida. A differenza delle campagne militari tradizionali, questa strategia mira a conquistare Taiwan senza distruggerne infrastrutture o economia, in quanto proprio qui si trova la rilevanza economica e informatico-elettronica di Taiwan per la Cina. La RPC punta piuttosto a costringerla alla sottomissione sotto il pretesto di una riunificazione "pacifica".

[17] Hawkins, A. "Taiwan faces similar threat to Europe in 1930s, president says" *The Guardian*, 8 maggio 2025 https://www.theguardian.com/world/2025/may/08/taiwan-president-europe-second-world-war.

L'approccio cinese a questa "guerra senza danni" prevede una strategia sistematica in cinque fasi: sabotaggio delle infrastrutture critiche, guerra cognitiva attraverso la disinformazione, attacchi di convergenza cibernetico-fisica, accerchiamento militare e sovversione politica[18]. Incidenti recenti, tra cui il sabotaggio dei cavi di Matsu e le campagne di disinformazione durante le elezioni taiwanesi del 2024, offrono un'anticipazione di come potrebbero apparire futuri tentativi di destabilizzare la difesa taiwanese ed erodere la fiducia pubblica. Questi attacchi continui e assillanti sono progettati per neutralizzare la capacità di resistenza di Taiwan e contemporaneamente preservarne il valore come risorsa economica e strategica.

Chiaramente, la visione della minaccia taiwanese che il PCC vuole proiettare all'interno del Paese di Mezzo è uno strumento propagandistico ben definito dal White Paper cinese "Taiwan Question and China's Reunification in the New Era"[19]. Questo documento, pubblicato dall'Ufficio cinese sugli Affari di Taiwan e dall'Ufficio Informazioni del Consiglio di Stato della RPC e diffuso pochi giorni dopo la visita di Nancy Pelosi a Taiwan nel 2022, presenta la posizione ufficiale della Repubblica Popolare Cinese sulla questione di Taiwan, costruita su una narrazione storica, giuridica e politica che mira a legittimare l'unità nazionale sotto il principio di "una sola Cina". Il documento individua l'origine della divisione tra le due sponde dello Stretto nella guerra civile cinese e soprattutto nell'intervento degli Stati Uniti, accusati di aver sostenuto il Kuomintang e poi di aver militarizzato lo Stretto. Secondo la narrativa proposta, la questione di Taiwan è quindi un'eredità della Guerra fredda e un problema aggravato

[18] Yen-ting, L. ""War Without Harm": China's Hybrid Warfare Playbook Against Taiwan" Geopolitical Monitor, 16 settembre 2025 https://www.geopoliticalmonitor.com/war-without-harm-chinas-hybrid-warfare-playbook-against-taiwan/.
[19] Ufficio sugli Affari di Taiwan della RPC "台湾问题白皮书", agosto 2022 https://us.china-embassy.gov.cn/eng/zgyw/202208/t20220810_10740168.htm.

dall'interferenza straniera, e questo giustificherebbe le interferenze cinesi sempre più dirette degli ultimi anni. Il Mainland Affairs Council di Taiwan ha dichiarato che il documento è "pura illusione e ignora i fatti".

Conclusioni

Nonostante l'Italia non sia vittima in modo altrettanto diretto e visibile quanto Taiwan a minacce ibride da parte di un singolo attore, le risposte – e soprattutto le non-risposte – multifattoriali taiwanesi offrono spunti preziosi per democrazie come la nostra che affrontano sfide simili nel panorama in evoluzione della guerra non convenzionale. Oltre ad essere una democrazia aperta, altri fattori che ci accomunano a Taiwan sono l'essere un hub infrastrutturale, nel nostro caso per il Mediterraneo, e un target di influenza esterna, più notoriamente da parte di Cina, Russia e di altri attori ibridi.

Proprio per questo l'Italia può, e deve, studiare questo caso al fine di aumentare il proprio scudo da eventuali attacchi da parte di potenze egemoni, e per gestire al meglio le situazioni in cui è già sotto attacco.

A mero titolo esemplificativo, le diverse aree di attacco non si limitano alla sfera fisico-materiale ma possono attraversare continenti alla velocità della luce tramite la sfera cibernetica, con tecniche di spionaggio e di campagne di disinformazione. O ancora, il maggior pericolo per l'Italia sarebbe quello di essere sotto attacco senza esserne a conoscenza.

Sotto questo punto di vista, Taiwan è un *early warning system* per l'Europa. Molte delle tecniche impiegate da Pechino per interferire negli affari taiwanesi trovano già riscontri nel contesto europeo, ma con livelli di intensità e visibilità differenti; osservarne l'evoluzione nel caso taiwanese consente di anticiparne sviluppi e adattamenti nel nostro spazio strategico. Con questa ipotesi, si potrebbe capire

in quale modo l'Italia o l'Europa possano colmare il gap europeo sulle minacce ibride ed evitare che si sottovalutino queste *gray-zone operations*.

Per quanto riguarda invece GenAI, le elezioni italiane sono un potenziale target di *AI-driven influence ops*, come accaduto a Taiwan nel 2024. Vi è una profonda necessità di alfabetizzazione mediatica nella popolazione, *fact-checking* di terze parti e dello sviluppo di un sistema analogo a TAIDE in chiave europea.

Il seguente argomento può essere invece trattato in chiave prettamente italiana: ci sono infrastrutture critiche particolarmente a rischio? Siamo sufficientemente preparati a potenziali attacchi ai cavi sottomarini o a porti, o rischiamo di farci trovare impreparati e richiedere un sostegno di altri Stati che potrebbe ritardare a venire, come nel caso delle isole Matsu? I porti di Trieste, Genova, Gioia Tauro sono nodi sensibili su questo argomento. Trieste in particolare, posizionato come terminale europeo strategico chiave per il corridoio economico India-Medio Oriente-Europa (IMEC), dovrà affrontare questi interrogativi.

Sicuramente, rafforzare il lavoro europeo[20] sulle minacce ibride e portare le minacce ibride nel dibattito italiano è un punto di inizio, come con il "Non-paper sul contrasto alla guerra ibrida" del Ministro della Difesa Guido Crosetto[21].

L'Europa si trova in una fase pre-crisi, in cui il prezioso tempo a nostra disposizione ci permette di organizzare adesso una deterrenza silenziosa, osservando i pregi e difetti della resistenza taiwanese come laboratorio della futura guerra non convenzionale.

---

[20] Parlamento Europeo "Interferenze straniere: il PE chiede di tutelare le elezioni europee del 2024", 1 giugno 2023. https://www.europarl.europa.eu/news/it/press-room/20230524IPR91908/interferenze-straniere-il-pe-chiede-di-tutelare-le-elezioni-europee-del-2024.

[21] Ministro della Difesa Crosetto, G. "Il contrasto alla guerra ibrida: una strategia attiva", Ministero della Difesa, novembre 2025 https://www.difesa.it/assets/allegati/83696/non-paper_il_contrasto_alla_guerra_ibrida.pdf .

A livello europeo, la sensibilità sul tema di minacce ibride appare più strutturata rispetto alla visione italiana. Negli ultimi anni l'Unione ha progressivamente riconosciuto la dimensione sistemica della competizione con Pechino, sviluppando strumenti normativi e di policy volti a ridurre vulnerabilità strategiche, anche in ambiti non tradizionalmente securitari, come energia, investimenti esteri e catene di approvvigionamento. Esempi concreti includono il rafforzamento dei meccanismi europei di screening sugli investimenti in infrastrutture critiche[22], le restrizioni introdotte da diversi Stati membri verso fornitori cinesi nelle reti 5G[23], l'uso estensivo del golden power[24] e il progressivo riposizionamento politico rispetto alla Belt and Road Initiative[25].

Si nota una crescente evoluzione della consapevolezza europea. Tuttavia, questo approccio non è sempre omogeneo tra gli Stati membri: divergenze interne nell'adozione di posizioni più accomodanti riflettono la diversa esposizione politica ed economica alla Cina. Questo elemento evidenzia un limite intrinseco alla risposta europea: la resilienza alle minacce ibride richiede anticorpi nazionali, ma la loro efficacia dipende sempre più dalla capacità di coordinarli a livello sovranazionale.

---

[22] Commissione Europea "Investment screening" https://policy.trade.ec.europa.eu/enforcement-and-protection/investment-screening_en.

[23] *Commissione Europea* "Commission announces next steps on cybersecurity of 5G networks in complement to latest progress report by Member States" 15 giugno 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3309

[24] Riela S. "Occhi sempre più aperti sugli IDE", *ISPI*, 27 settembre 2022 .https://www.ispionline.it/it/pubblicazione/occhi-sempre-piu-aperti-sugli-ide-36265

[25] Casanova G. "Cina-Italia: l'impatto del ritiro dal memorandum sui rapporti bilaterali", ISPI, 15 gennaio 2024. https://www.ispionline.it/it/pubblicazione/cina-italia-limpatto-del-ritiro-dal-memorandum-sui-rapporti-bilaterali-163542

È dunque necessario, come ci insegna il caso taiwanese, costruire resilienza alle minacce cinesi attraverso lo sviluppo di strumenti domestici di prevenzione e risposta.

Proprio qui risiede il potenziale vantaggio aggiuntivo dell'Italia: si tratta della possibilità di rafforzare tali anticorpi mediante una stretta sinergia tra livello nazionale e dimensione sovranazionale europea, su piano sia normativo sia operativo, per far fronte alle sfide del futuro.

Quando l'ambiguità non basta: i limiti della strategia iraniana

di Lorenzo Zacchi

Introduzione

La dottrina militare iraniana moderna è articolata attorno a un concetto di necessità. Il cambio di alleanze a seguito della rivoluzione islamica del 1979, e il conseguente isolamento internazionale e regionale, ha costretto l'Iran a un pensiero militare asimmetrico e all'uso di tattiche ibride, adottando un'ambiguità strategica che per un lungo periodo si è rivelata funzionale alle mire egemoniche di Teheran. Sanzioni, difficoltà negli approvvigionamenti e una iniziale inferiorità strutturale su un piano militare hanno convinto le autorità del Paese a teorizzare una dottrina difensiva e non convenzionale. Questa strategia ha prodotto nel corso degli anni risultati tangibili: in Iraq e in Siria, ad esempio, l'impiego di tattiche ibride attraverso milizie locali ha permesso a Teheran di estendere la propria influenza regionale, spesso con efficacia superiore a quella degli eserciti regolari.

Oggi, però, l'architettura di sicurezza che l'Iran ha strutturato negli ultimi decenni, sembra meno solida: i metodi che finora erano considerati un fattore di potere per l'Iran mostrano limiti e vulnerabilità strutturali. Le recenti dimostrazioni di forza israeliane suggeriscono che l'ambiguità e l'uso di *proxy* potrebbero non bastare più a proteggere gli interessi di Teheran. Israele, lungi dall'essere dissuasa dalla minaccia indiretta, ha messo in campo contromisure sofisticate per colpire l'apparato di proiezione iraniano senza innescare un conflitto diretto.

L'escalation seguita all'attacco di Hamas del 7 ottobre e la conseguente guerra a Gaza hanno innescato un arco di crisi più ampio, con Israele che ha colpito i principali *proxy* sostenuti da Teheran nella regione, deciso a disarticolare l'intero ombrello di sicurezza iraniano.

Questo capitolo cercherà, quindi, di rispondere alla seguente domanda: la strategia iraniana di pressione indiretta, fondata sull'ambiguità e sul coinvolgimento di attori non statali, è ancora efficace nel garantire deterrenza e proiezione di potere?

Il primo paragrafo analizzerà le radici dottrinali e l'evoluzione storica dell'approccio iraniano alla guerra ibrida; nel secondo verranno esaminate le applicazioni pratiche di tale strategia e i successi ottenuti nel consolidare l'influenza regionale; nel terzo saranno descritte i punti di forza e vulnerabilità dei meccanismi di pressione indiretta di Teheran, valutandone l'efficacia residua alla luce dei più recenti sviluppi.

Le origini della strategia asimmetrica iraniana

La strategia militare della Repubblica islamica non nasce da una scelta ideologica, ma da una combinazione di vincoli strutturali, lezioni storiche e adattamenti progressivi all'ambiente regionale. La sua evoluzione è il prodotto di una condizione di inferiorità convenzionale, di un senso radicato di vulnerabilità del regime e di una cultura strategica che si è strutturata all'interno della traumatica esperienza della guerra contro l'Iraq (1980–1988). La Rivoluzione islamica del 1979 ha comportato, come primo elemento, un cambio di schieramento internazionale e, conseguentemente, una serie di sanzioni che hanno limitato Teheran nella capacità di acquisizione di armamenti dall'estero. Inoltre, su un piano istituzionale, la nascita della Repubblica islamica ha aperto una frattura profonda nell'apparato militare. L'epurazione dei vertici

dell'esercito imperiale (Artesh) e la creazione del Corpo dei Guardiani della Rivoluzione Islamica (IRGC) hanno prodotto una struttura duale, in cui all'esercito, formalmente responsabile della difesa territoriale, si è affiancata un'organizzazione ideologicamente fedele a Khomeini e dotata di crescente autonomia operativa[1]. Questa struttura parallela, inizialmente nata a difesa della rivoluzione, e quindi come strumento di controllo e repressione politico, è divenuta progressivamente il principale laboratorio della futura strategia asimmetrica, privilegiando flessibilità e decentralizzazione operativa. Il conflitto con l'Iraq ha rappresentato il vero momento fondativo della cultura strategica iraniana contemporanea. La guerra ha evidenziato la vulnerabilità strutturale del Paese: l'isolamento internazionale, le carenze tecnologiche, l'impossibilità di sostituire rapidamente equipaggiamenti occidentali e inferiorità nell'aviazione e nei sistemi d'arma avanzati[2]. L'esperienza degli attacchi missilistici iracheni contro i centri urbani iraniani e l'uso di armi chimiche consolidarono nell'élite rivoluzionaria la convinzione che l'Iran non potesse permettersi un nuovo conflitto convenzionale su larga scala. Se nei mesi successivi alla nascita della Repubblica islamica l'idea del regime era quella di "esportare" la rivoluzione, le riflessioni a seguito della guerra portarono, invece, a strutturare una dottrina militare dal carattere prettamente difensivo.

Il contesto regionale all'inizio degli anni 2000 ha accelerato queste riflessioni: la presenza degli Stati Uniti in Afghanistan nel 2001, e in Iraq nel 2003, hanno permesso alle istituzioni militari di Teheran di valutare le azioni statunitensi e adottare, di conseguenza, una dottrina militare potenzialmente in grado di

[1] Alma Keshavarz, The Iranian Revolutionary Guard Corps: Defining Iran's Military Doctrine (London: Bloomsbury, 2023).

[2] Rouzbeh Parsi, "Iran's Hybrid Warfare Capabilities," in Hybrid Warfare: Security and Asymmetric Conflict in International Relations, ed. Mikael Weissmann et al. (London: I.B. Tauris, 2021).

scoraggiare una eventuale invasione americana del Paese.

Nel 2005 venne teorizzato il concetto di "Mosaic Defense", un sistema composto da diverse strategie di difesa asimmetrica volte a mettere in sicurezza l'Iran da un'eventuale invasione statunitense. Vennero creati 31 centri di comando delle forze dei Pasdaran, uno per Teheran e uno per ciascuna delle 30 province iraniane, per mettere in atto un decentramento operativo, che avrebbe facilitato la flessibilità delle operazioni militari, e reso impossibile per il nemico la distruzione di un centro operativo di controllo[3].

Le Primavere Arabe del 2011 hanno comportato una nuova evoluzione della dottrina strategica iraniana. Le istituzioni militari iraniane hanno modificato il concetto di *Mosaic Defense*, spostando oltre i confini la prima linea difensiva del paese, basandosi sull'idea che la sicurezza dell'Iran non possa essere garantita esclusivamente attraverso la difesa territoriale, ma richieda la costruzione di profondità strategica tramite attori alleati e strumenti indiretti. Tale concetto non implica un'espansione convenzionale, bensì la creazione di reti di influenza capaci di assorbire e deviare la pressione nemica[4]. La politica di difesa avanzata dell'Iran si è sviluppata, quindi, nei principali scenari di guerra che hanno coinvolto la regione a seguito dei tumulti[5] del 2011, ed ha permesso al Paese di massimizzare, nel decennio successivo, la propria influenza, militare e politica, in 4 diversi Paesi arabi. In Iraq, combattendo contro lo Stato Islamico, identificato come un nemico per la sicurezza della Repubblica Islamica; in Siria, a fianco dell'ex leader Bashar al-Assad, per impedire l'eventuale caduta di quest'ultimo, alleato di ferro di Teheran; nello Yemen a supporto dei ribelli Houthi,

[3] Zacchi, Lorenzo. "L'Iran e l'Arabia Saudita. Nemici e alleati nella nuova politica sul Medio Oriente di Trump." *Rivista Trimestrale di Scienza dell'Amministrazione*, n. 3 (2018)

[4] Rouzbeh Parsi, "Iran's Hybrid Warfare Capabilities," in *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, ed. Mikael Weissmann et al. (London: I.B. Tauris, 2021)

[5] Campanini M. (a cura di), 2013, "Le rivolte arabe e l'Islam. La transizione incompiuta", Il Mulino, Bologna.

fondamentali nell'azione di deterrenza nei confronti dell'Arabia Saudita e nella strategia di controllo degli stretti marittimi della Repubblica Islamica (lo Yemen è posizionato all'imbocco dello strategico stretto di Bab el-Mandeb), e in Libano, grazie al ruolo militare e politico di Hezbollah.

L'articolazione di questa dottrina si sviluppa attorno a tre direttrici principali. La prima riguarda l'uso sistematico di attori non statali come moltiplicatori di forza. Hezbollah in Libano ha costituito il prototipo di questa strategia: un'organizzazione radicata localmente, dotata di legittimazione politica interna e integrata in una rete transnazionale coordinata da Teheran[6]. La seconda direttrice concerne lo sviluppo di capacità missilistiche e, più recentemente, di droni e strumenti cyber. L'Iran, come scritto, ha compreso precocemente che, in assenza di superiorità aerea, la deterrenza poteva essere costruita attraverso la minaccia di saturazione e la capacità di colpire infrastrutture sensibili avversarie[7]. Il programma missilistico, avviato durante la guerra con l'Iraq, è divenuto progressivamente uno dei pilastri della deterrenza iraniana, integrandosi con la rete dei partner regionali. La terza direttrice è rappresentata dall'adozione di un approccio che rientra nei parametri della cosiddetta "zona grigia", caratterizzato da ambiguità, gradualità e gestione calibrata dell'escalation. L'Iran è uno dei principali attori globali operanti stabilmente nella *gray zone*: l'azione indiretta, la *plausible deniability* e la frammentazione dei fronti hanno consentito a Teheran di agire sul filo dell'escalation senza entrare in un conflitto convenzionale. Questo modus operandi si è rivelato particolarmente efficace nei teatri iracheno e siriano dopo il 2003 e il 2011.

[6] Michael Eisenstadt, "Iran's Gray Zone Strategy: Cornerstone of its Asymmetric Way of War," PRISM 9, no. 2 (2021)
[7] Joshua Dryden, "Iran, Israel, and the Struggle for the Skies over the Middle East," Æther: A Journal of Strategic Airpower & Spacepower 2, no. 1 (2023)

L'ecosistema dei proxies e la capacità missilistica

Le tre componenti descritte nel paragrafo precedente agiscono in una dimensione integrata ed estremamente complessa: lo sviluppo della dottrina militare coinvolge una grande varietà di organi statali, di università, centri di ricerca e think tank[8]. L'ecosistema dei *proxies*, il programma missilistico e la competizione nella *gray zone* rappresentano dunque un sistema coerente di proiezione indiretta, fondato su un coordinamento centralizzato e su modalità operative, al contrario, decentralizzate.

La galassia delle milizie militari legate all'Iran è coordinata da una specifica divisione interna alle IRCG, la Forza Quds, nata durante la guerra con l'Iraq allo scopo di svolgere attività di intelligence sul territorio nemico e divenuta, negli anni, il principale strumento di proiezione di potenza dell'Iran. Questa divisione svolge funzioni di pianificazione strategica, selezione delle leadership locali, coordinamento tra i teatri di guerra e supervisione delle linee di rifornimento, mantenendo però una flessibilità che consente ai vari *proxies* di operare con un certo grado di autonomia tattica[9]. Il caso di Hezbollah rappresenta l'esempio più avanzato di questa architettura. Il rapporto con Teheran si è evoluto da sostegno ideologico e addestrativo negli anni Ottanta a una cooperazione strutturata che comprende condivisione di intelligence, formazione tecnica e integrazione di capacità missilistiche[10]. La catena di comando non è formalmente subordinata all'Iran, ma la dipendenza tecnologica e logistica crea un legame strategico stabile. Hezbollah dispone oggi di un'infrastruttura militare radicata nel territorio libanese, distribuita in modo capillare e integrata in ambienti civili,

[8] Mc Innis J.M. Iranian concepts of warfare. Understanding Tehran's evolving military doctrines. Washington DC: American Enterprise Institute (2017)

[9] Alma Keshavarz, The Iranian Revolutionary Guard Corps: Defining Iran's Military Doctrine (London: Bloomsbury, 2023).

[10] Rouzbeh Parsi, "Iran's Hybrid Warfare Capabilities," in *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, ed. Mikael Weissmann et al. (London: I.B. Tauris, 2021)

elemento che per decenni ha complicato eventuali operazioni di neutralizzazione e ha costituito, allo stesso tempo, parte integrante della deterrenza[11]. In Iraq, il modello ha assunto una forma diversa. Le Popular Mobilization Forces sono formalmente incorporate nello Stato iracheno, ma alcune brigate mantengono canali diretti con l'IRGC. Questa ambiguità istituzionale ha permesso all'Iran di influenzare decisioni politiche e di mantenere capacità militari sul terreno senza dispiegare truppe regolari[12]. In Siria, la presenza di consiglieri e unità affiliate ha svolto un ruolo di primo piano per garantire la sopravvivenza del regime di Damasco negli anni successivi al 2011, oltre a tenere aperto un corridoio terrestre che dall'Iran arriva in Libano, in quella che è stata denominata "mezzaluna sciita". Tale corridoio non è soltanto un concetto geopolitico, ma un'infrastruttura logistica concreta, funzionale al trasferimento di armamenti e componenti[13].

La dimensione logistica è centrale per comprendere l'effettiva operatività dell'ecosistema. Le sanzioni internazionali hanno limitato l'accesso diretto dell'Iran a sistemi d'arma avanzati, ma hanno al contempo incentivato lo sviluppo di capacità domestiche e di reti di approvvigionamento alternative. La Siria ha svolto un ruolo chiave come ponte terrestre, mentre le rotte marittime attraverso il Golfo di Oman sono state utilizzate per i trasferimenti verso gli Houthi nello Yemen[14]. La frammentazione delle spedizioni, l'uso di componenti

---

[11] Christian Kaunert e Ori Wertman, "The Securitisation of Hybrid Warfare," *Security and Defence Quarterly* 31, no. 4 (2020).
[12] Rouzbeh Parsi, "Iran's Hybrid Warfare Capabilities," in *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, ed. Mikael Weissmann et al. (London: I.B. Tauris, 2021).
[13] Joshua Dryden, "Iran, Israel, and the Struggle for the Skies over the Middle East," *Æther* 2, no. 1 (2023)
[14] Alma Keshavarz, The Iranian Revolutionary Guard Corps: Defining Iran's Military Doctrine (London: Bloomsbury, 2023).

smontate e il trasferimento di *know-how* piuttosto che di sistemi completi hanno ridotto l'esposizione a intercettazioni.

Il programma missilistico costituisce il secondo pilastro operativo. Avviato durante la guerra con l'Iraq con l'importazione di Scud da Corea del Nord e Libia, si è evoluto in un'infrastruttura autoctona capace di produrre una gamma diversificata di vettori per ogni livello di minaccia. I Sejjil, a combustibile solido, garantiscono tempi di reazione più rapidi rispetto ai più datati Shahab-3, mentre i Fateh-110 e Zolfaghar (missili a corto raggio ma ad alta precisione) sono stati ampiamente trasferiti o riprodotti da proxy come Hezbollah e Hamas. I modelli più recenti, come il Khorramshahr-4 (gittata 2.000 km, testata da 1.500 kg), il Dezful e il Fattah (primo missile ipersonico iraniano) rappresentano un salto qualitativo nella capacità di eludere le difese antimissile israeliane. L'evoluzione tecnologica ha riguardato non soltanto l'aumento della gittata, ma anche il miglioramento della precisione e l'integrazione di sistemi di guida avanzati.

L'arsenale balistico iraniano, a lungo considerato il più diversificato ed efficiente nella regione[15], ha avuto una funzione di deterrenza, mentre la proliferazione di razzi e missili a corto e medio raggio presso i partner regionali estende la minaccia in forma distribuita. Nel caso di Hezbollah, l'accumulazione di un vasto arsenale di razzi è stata accompagnata da tentativi di miglioramento della precisione, attraverso trasferimento di componenti e competenze tecniche[16]. Da una logica di saturazione indiscriminata delle difese missilistiche dei Paesi considerati nemici, Israele in primis, si è passati a una capacità potenzialmente più selettiva che ha aumentato la credibilità della minaccia contro le

[15] Izewicz P., "Iran's ballistic missile programme: it's status and the way forward", in Non Proliferation Paper, n.57 (2017)
[16] Joshua Dryden, "Iran, Israel, and the Struggle for the Skies over the Middle East," Æther 2, no. 1 (2023)

infrastrutture critiche. Analogamente, l'impiego dei droni (*unmanned aerial vehicle, UAV)* ha introdotto una dimensione a basso costo e ad alta flessibilità operativa, rendendo più complessa la difesa aerea avversaria. La distribuzione di missili e droni ai partner regionali non è avvenuta necessariamente tramite la consegna di sistemi completi. In diversi casi il trasferimento ha riguardato parti, software di guida o formazione tecnica, consentendo ai *proxies* di sviluppare capacità locali. Anche in questo caso, tale modalità operativa ha ridotto la tracciabilità diretta e rafforzato la *plausible deniability*. L'attribuzione delle responsabilità di un attacco diventa più complessa quando un sistema è assemblato o modificato localmente, pur avendo origine tecnologica iraniana. Il terzo elemento, la competizione nella *gray zone*, è il meccanismo che consente all'intero sistema di funzionare senza sfociare automaticamente in una guerra aperta e completa l'architettura militare descritta finora. L'Iran opera attraverso escalation controllate, attacchi limitati e frammentazione geografica della pressione. L'assenza di rivendicazione diretta, la moltiplicazione degli attori coinvolti riducono la probabilità di una risposta convenzionale immediata. La *plausible deniability* non è soltanto un elemento retorico, ma un dispositivo operativo che consente al Paese di mantenere ampi margini di manovra diplomatica.

L'equilibrio di questa architettura di sicurezza deve essere sostenuto da una gestione calibrata del rischio. Le azioni indirette sono progettate per imporre costi cumulativi senza superare le soglie che vengono percepite come esistenziali dai nemici. In questo contesto l'aumento della precisione missilistica, l'intensificazione dei trasferimenti tecnologici alle milizie e la conseguente crescita militare delle stesse, contribuiscono a ridurre lo spazio di ambiguità, e ad aumentare la percezione di minaccia diretta da parte degli avversari. L'efficacia della strategia asimmetrica iraniana dipende, quindi, dalla

capacità di mantenere ambiguità, e dal controllo dell'escalation. Quando uno di questi elementi viene compromesso, l'intera architettura entra in tensione. Nel prossimo paragrafo si descriveranno prima i punti di forza, per poi analizzare i limiti della stessa.

Punti di forza, limiti strutturali e pressione israeliana

La strategia iraniana ha mostrato, nel corso degli ultimi due decenni, una notevole capacità di adattamento e resilienza. Il suo primo punto di forza risiede nella deterrenza distribuita: la minaccia non è concentrata sul territorio iraniano, ma diffusa attraverso una rete di attori armati e capacità missilistiche dislocate su più teatri. Questa configurazione ha consentito a Teheran di trasformare l'inferiorità convenzionale in una forma di pressione permanente e multilivello, imponendo la percezione ai propri avversari che i costi derivanti da un conflitto simmetrico avrebbero potuto essere altissimi[17].

La deterrenza distribuita funziona perché frammenta il fronte e moltiplica i punti di pressione. Hezbollah in Libano, le milizie sciite in Iraq, le formazioni attive in Siria, gli Houthi nello Yemen e Hamas a Gaza hanno operato come nodi di un sistema reticolare, in grado di attivarsi in tempi diversi e di modulare l'intensità dello scontro[18]. Un secondo punto di forza è rappresentato dalla capacità di operare stabilmente nella *gray zone*. L'ambiguità strategica, la *plausible deniability* e la gradualità dell'escalation hanno permesso all'Iran di agire sotto la soglia della guerra aperta, mantenendo margini politici e diplomatici, e di mascherare la sua capillare presenza nei teatri della regione dietro migliaia di sigle, bandiere

[17] Michael Eisenstadt, "Iran's Gray Zone Strategy: Cornerstone of its Asymmetric Way of War," *PRISM* 9, no. 2 (2021)

[18] Rouzbeh Parsi, "Iran's Hybrid Warfare Capabilities," in *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, ed. Mikael Weissmann et al. (London: I.B. Tauris, 2021)

e nomi di milizie diverse[19].

L'assenza di attribuzione diretta ha inoltre complicato le risposte avversarie, soprattutto in contesti in cui un'escalation convenzionale sarebbe risultata politicamente costosa. Il terzo elemento di efficacia riguarda il programma missilistico e UAV. La combinazione tra capacità balistiche nazionali e proliferazione di sistemi a corto e medio raggio presso i partner regionali ha rafforzato la credibilità della minaccia. L'evoluzione verso una maggiore precisione ha aumentato il potenziale di deterrenza contro le infrastrutture critiche dell'area, costringendo Israele e altri attori regionali a investimenti significativi in sistemi difensivi multilivello. In questo equilibrio, l'Iran ha potuto mantenere una postura offensiva indiretta senza dover competere sul piano della superiorità aerea o tecnologica.

Tuttavia, i medesimi elementi che hanno garantito efficacia al modello ne costituiscono anche i limiti strutturali. La deterrenza distribuita dipende dalla tenuta logistica e dalla politica degli alleati disposti nella regione. La perdita o l'indebolimento di uno di essi, come nel caso della caduta del regime di Bashar al-Assad in Siria, non rappresenta soltanto un arretramento geopolitico, ma incide direttamente sulle linee di rifornimento e sul corridoio terrestre che collegava l'Iran e il Libano. L'interruzione di tale continuità territoriale ha ridotto la capacità di trasferire armamenti e componenti, aumentando i costi logistici e l'esposizione a interdizioni. Un secondo limite riguarda l'autonomia dei proxy: se la flessibilità locale da un lato ha garantito la capacità di resilienza iraniana, dall'altro essa comporta il rischio di divergenze strategiche e di escalation non pienamente controllate. L'Iran non esercita un controllo gerarchico totale sui partner, soprattutto rispetto a certe milizie, come quella degli Houthi. La

[19] Christian Kaunert e Ori Wertman, "The Securitisation of Hybrid Warfare," *Security and Defence Quarterly* 31, no. 4 (2020)

coerenza dell'architettura di sicurezza dipende, quindi, da convergenze di interesse che possono variare nel tempo[20]. In situazioni di crisi intensa, il coordinamento può risultare più complesso, riducendo la capacità di gestione dello scontro.

Il limite più evidente emerge tuttavia quando la competizione si sposta verso una dimensione più convenzionale. L'architettura iraniana è concepita per operare sottosoglia; quando l'avversario decide di accettare il rischio dell'escalation e colpisce direttamente le infrastrutture militari e i nodi di comando, il vantaggio dell'ambiguità si riduce drasticamente. Le operazioni israeliane successive al 7 ottobre hanno rappresentato, in questo senso, un momento di discontinuità che rischia di essere un punto di svolta nell'area. La campagna militare su Gaza ha superato, per intensità e durata, molte delle linee rosse implicite che avevano caratterizzato i cicli precedenti di violenza. L'elevato livello di distruzione urbana e il numero di vittime civili hanno ridimensionato l'efficacia della strategia di Hamas fondata sulla protezione derivante dall'attenzione internazionale ai civili. La riduzione di tale vincolo ha inciso indirettamente anche sull'architettura iraniana, poiché ha mostrato che l'avversario è disposto a sostenere costi reputazionali, oltre che economici e sociali, elevati pur di neutralizzare la minaccia. Parallelamente, gli attacchi israeliani in Libano contro le infrastrutture e la leadership di Hezbollah hanno evidenziato la vulnerabilità del modello quando la superiorità di intelligence viene impiegata in modo sistematico. La capacità di colpire depositi, convogli e siti di produzione o conversione missilistica, nonché gli stessi miliziani, evidenzia grosse falle nel

[20] Michael Eisenstadt, "Iran's Gray Zone Strategy: Cornerstone of its Asymmetric Way of War," *PRISM* 9, no. 2 (2021)

sistema iraniano che ha esternalizzato la difesa e allungato le catene di comando, aumentando i rischi di infiltrazione delle intelligence nemiche. Analogamente, i raid in Siria e, in alcuni casi, direttamente sul territorio iraniano hanno dimostrato la mancanza di capacità convenzionali di difesa, soprattutto antiaerea.

Questi sviluppi mettono in luce una fragilità di fondo: se la deterrenza asimmetrica viene erosa e il confronto si avvicina a una dimensione convenzionale, l'Iran si trova in una posizione di relativa debolezza. L'assenza di superiorità aerea, la dipendenza da sistemi missilistici come principale strumento di ritorsione e le limitazioni tecnologiche strutturali rendono complesso sostenere un conflitto diretto prolungato contro un avversario dotato di superiorità qualitativa. In altre parole, il modello funziona finché l'arena resta quella della *gray zone*; quando la soglia viene oltrepassata, l'asimmetria torna a essere un vincolo più che un vantaggio. L'erosione del corridoio siriano (e la conseguente perdita dello spazio aereo), la pressione sistematica su Hezbollah e sugli Houthi, e la neutralizzazione di parte dell'infrastruttura di Hamas hanno quindi inciso sulle fondamenta dell'architettura di sicurezza iraniana. Non si tratta di un collasso immediato, ma di un indebolimento cumulativo che mette in discussione la sostenibilità della deterrenza distribuita nel medio periodo. In conclusione, la strategia iraniana ha funzionato perché ha saputo sfruttare asimmetrie militari e normative, distribuendo la minaccia e operando sottosoglia. I suoi limiti emergono quando l'avversario accetta l'escalation, colpisce i nodi logistici e riduce lo spazio di ambiguità. La domanda centrale non è se il modello sia fallito *tout court*, ma se possa continuare a garantire una deterrenza efficace in un contesto in cui alcune delle regole implicite della competizione sembrano progressivamente erodersi.

Conclusioni

Questo capitolo ha cercato di rispondere a una domanda precisa: la strategia iraniana di deterrenza indiretta, costruita su proxy, capacità missilistiche e competizione nella *gray zone*, sta entrando in una fase di crisi strutturale? La rilevanza della domanda è evidente perché la stabilità regionale dipende, in larga misura, dalla capacità (o incapacità) di Teheran di imporre costi senza trasformare la competizione in una guerra convenzionale aperta. Il modello iraniano ha storicamente funzionato proprio perché progettato per restare sottosoglia. Il principale risultato dell'analisi è che la strategia vede il vantaggio competitivo ridursi. L'architettura iraniana resta capace di generare pressione e di sopravvivere a colpi locali grazie alla capacità di distribuire i fronti, alla decentralizzazione e alla resilienza delle reti. Tuttavia, gli sviluppi recenti mostrano che il modello è più vulnerabile quando l'avversario accetta costi elevati e adotta un approccio sistematico di interdizione: colpire leadership, infrastrutture, depositi, linee logistiche e punti di transito, riducendo lo spazio di ambiguità su cui si fonda la *plausible deniability*. In tale scenario, questa deterrenza distribuita rischia di trasformarsi in una deterrenza incompleta, perché la sua credibilità dipende dalle capacità dei nodi periferici della rete delle milizie, che possono essere progressivamente degradati. Anche sul piano strettamente militare, la dimostrazione che l'Iran fatichi quando trascinato verso una dinamica più convenzionale conferma un limite strutturale: il modello è ottimizzato per la guerra indiretta, non per sostenere simmetricamente un confronto prolungato con un avversario militarmente superiore.

Un elemento spesso sottovalutato nel dibattito è che questa erosione ha un impatto non soltanto esterno, ma anche su un piano interno. Per decenni, la legittimazione del regime ha poggiato anche su una narrativa di un Iran imperiale e in vetta alla gerarchia di potere regionale, capace di proiettare

potenza e di costruire una cintura di deterrenza attraverso le IRGC. Se in pochi mesi l'opinione pubblica percepisce che quella architettura può essere aggirata o smantellata, il problema non è solo strategico, ma diviene un problema di credibilità politica. In parallelo, riemerge la dicotomia tra Artesh e IRGC: l'accentramento di risorse e prestigio nei Pasdaran, giustificato dalla necessità di operare nella *gray zone*, oggi può essere letto, retrospettivamente, come un *trade-off* rischioso. Se la minaccia si avvicina a forme più convenzionali, l'Artesh appare strutturalmente meno valorizzato; e questo alimenta il dubbio, già presente nel discorso pubblico iraniano, che una parte consistente degli investimenti sia stata inefficiente, dispersa o associata a fenomeni corruttivi o di cattiva allocazione. Non serve dimostrare contabilmente questi sprechi perché producano effetti: è sufficiente che diventino una percezione condivisa, capace di erodere consenso e coesione tra apparati. Sul breve termine, un ulteriore vincolo riguarda l'eventualità di un nuovo accordo con Washington.

Qualunque intesa credibile, dal punto di vista statunitense e regionale, difficilmente potrebbe prescindere da un ridimensionamento di due asset centrali della postura iraniana: le capacità missilistiche e il sostegno alle milizie esterne. Una simile traiettoria non implicherebbe automaticamente la fine della dottrina asimmetrica, ma ne colpirebbe i presupposti: meno missili significa minore deterrenza di ritorsione; meno *proxies* significa minore profondità strategica. Paradossalmente, però, la stessa apertura diplomatica potrebbe creare uno spazio per una riconfigurazione istituzionale iraniana: alleggerimento delle sanzioni, maggiore accesso a tecnologie *dual-use*, possibilità di ricostruire parti della capacità convenzionale e della difesa aerea, oggi essenziali se l'Iran teme lo scivolamento verso un confronto più diretto. Lo scenario più probabile a breve-medio termine è quindi un adattamento difensivo più che una rinuncia alle capacità asimmetriche: Teheran tenderà a preservare

la logica ibrida, ma con correttivi. Da un lato, sarà incentivata a rendere la rete meno intercettabile (maggiore ridondanza logistica, trasferimenti più frammentati, capacità produttive più localizzate presso i partner, minore visibilità dei nodi). Dall’altro, potrebbe crescere la spinta interna a riequilibrare la relazione tra IRGC e Artesh, investendo di più in elementi convenzionali (difese aeree, protezione delle infrastrutture, resilienza C2) per ridurre la vulnerabilità mostrata dagli attacchi diretti. In una prospettiva più ampia, il caso iraniano suggerisce che la dimensione ibrida non può essere adottata come una condizione stabile. Le architetture fondate su *proxy*, ambiguità e operazioni sottosoglia tendono a produrre vantaggi quando l’avversario mantiene vincoli politici e operativi nell’uso della forza; al contrario, quando un attore dotato di superiorità informativa e tecnologica decide di colpire in profondità i meccanismi di supporto, la rendita strategica dell’ambiguità si riduce. L’esperienza iraniana segnala un effetto collaterale spesso trascurato: specializzarsi a lungo nella competizione ibrida può generare rigidità e squilibri interni negli apparati militari, riducendo la capacità di adattamento nel momento in cui la competizione sale di livello, raggiungendo quello convenzionale.

Spionaggio, criptovalute e cyberattacchi nella strategia ibrida globale nordcoreana

di Tommaso Tartaglione

Introduzione

Nell'attuale caotico ordine internazionale[1], una quota crescente del confronto statuale si svolge nelle "aree grigie", ove attività non convenzionali producono effetti politici, economici e sociali senza tradursi necessariamente in conflitto armato o senza che se ne ravvisi il reale mandante[2]. Tale è la guerra ibrida: un'azione combinata e coordinata su più domini — diplomatico, economico-finanziario, militare e cibernetico — finalizzata a destabilizzare, condizionare o indebolire un avversario[3]. Paesi quali Cina, Russia e Iran hanno fatto e fanno tuttora uso di tali strumenti[4]. A questi si aggiunge però un nuovo attore: la Corea del Nord, capace oggi di proiettare influenza e pressione oltre il proprio perimetro regionale. Il presente contributo si interroga su come e con quali finalità Pyongyang abbia sviluppato una strategia ibrida ormai di portata internazionale, con particolare attenzione ad ambiti specifici quali lo spionaggio, i cyberattacchi e i furti di criptovalute, tutti orientati a un unico scopo: la sopravvivenza del regime. La tesi centrale è che il governo nordcoreano abbia impiegato il dominio cibernetico per aggirare le sanzioni ONU, sostenere i propri programmi militari e nucleari e influenzare attori esterni, ricorrendo a mezzi relativamente contenuti in termini di risorse e difficilmente tracciabili. In questa

[1] Bellocchio, Luca. *Tutto è Potenza*. Guerini Scientifica, 2023, p. 11-15.
[2] Crosetto, Guido. Il contrasto alla guerra ibrida: una strategia adattiva. Ministero della Difesa, 2025.
[3] *Ibid*.
[4] *Ibid*.

cornice, anche l'intensificazione della cooperazione con la Russia nel contesto della guerra in Ucraina[5] contribuisce a irrobustire la postura nordcoreana, ampliandone opportunità e margini di manovra. Alla luce di tali evoluzioni, diventa essenziale definire lo stato e gli obiettivi della strategia ibrida di Pyongyang, nonché le possibili implicazioni per lo spazio europeo e, in particolare, per quello italiano. La prima parte di questo testo analizza le origini, l'evoluzione e gli obiettivi della strategia ibrida nordcoreana. La seconda illustra le principali modalità e capacità operative ibride, ovvero spionaggio, cyberattacchi e furti di criptovalute. Nell'ultima sezione, infine, si discutono le implicazioni di tali manovre nel Vecchio Continente e la posizione dell'Italia nei rapporti con la Corea del Nord.

Storia, stato e obiettivi tattico-strategici

L'interesse della Corea del Nord per la cyberwarfare e per lo sviluppo di strumenti informatici malevoli si consolidò negli anni Novanta[6]. La sequenza di shock che caratterizzò il decennio, tra cui la dissoluzione dell'URSS, la fine del sostegno sovietico e la crisi economico-alimentare, collocò il Paese in una condizione di grave fragilità. Tra il 1990 e il 1998 il PIL subì una riduzione tra il 40 e il 50%[7], mentre l'output industriale ed energetico diminuì di due terzi tra il 1992 e il 1996[8]. Su questa traiettoria incisero anche la riorganizzazione della *leadership* seguita all'ascesa di Kim Jong-il, nonché il progressivo irrigidimento di Washington, culminato con l'inclusione di Pyongyang nel cosiddetto "Asse del

[5] Carlough, M., Kennedy, J. "How North Korea Has Bolstered Russia's War in Ukraine." *Council of Foreign Relations*, 25 novembre 2025, https://www.cfr.org/articles/how-north-korea-has-bolstered-russias-war-ukraine

[6] Kong, J., Lim, J., Kim, K. "The All-Purpose Sword: North Korea's Cyber Operations and Strategies". *11th International Conference on Cyber Conflict* (2019): 1-20.

[7] Yoon, D. R., Babson, B. O. "Understanding North Korea's Economic Crisis." *Asian Economic Paper* 1, no. 3 (2002): 69-89.

[8] Noland, M., Robinson, S., Wang, T. "Rigorous Speculation: The Collapse and Revival of the North Korean Economy." *PIIE*, Working Paper 99-1 (1999).

Male"[9]. In questo contesto, l'*Information Technology* venne individuata dal regime come settore strategico su cui investire, insieme alla ricerca nucleare. In una fase di profonde difficoltà finanziarie, Kim Jong-il concentrò la spesa pubblica in questi ambiti, ritenuti promettenti per le capacità di deterrenza e per il favorevole rapporto costi-benefici. Quest'ultimo aspetto risultò centrale nel percorso cibernetico nordcoreano: operazioni finalizzate allo spionaggio, alla perturbazione economica o alla sottrazione di dati sensibili mediante *hacking* garantiscono, con un dispendio minimo di risorse, risultati notevoli. Il regime sostiene così costi e rischi limitati, potendo mascherare il proprio operato ed evitare l'impiego di agenti in aree sensibili, i quali potrebbero essere catturati o disertare[10]. Tale logica, come si vedrà più avanti, è rafforzata dall'impiego di soggetti terzi o di comodo (*proxy*), che consente di esternalizzare parte, come detto, del rischio operativo e ripartire meglio i costi dell'azione offensiva[11].

Gli investimenti hanno permesso a Pyongyang di disporre, ad oggi, di un articolato sistema di centri di ricerca e laboratori dedicati alle applicazioni della *computer science* nella guerra ibrida. Nel 1984 venne fondato il Mirim, collegio per la formazione dei futuri *cyberwarrior* nordcoreani, in collaborazione con l'Accademia di Frunze, in Russia[12]. Secondo fonti statunitensi, tra il 2009 e il 2020 l'istituto avrebbe addestrato circa 1.300 *hacker*[13]. La maggior parte di essi opera probabilmente in unità affiliate al Reconnaissance General Bureau, parte

[9] Glass, A. "President Bush cites 'axis of evil,' Jan. 29, 2002." *Politico*, 29 gennaio 2019, https://www.politico.com/story/2019/01/29/bush-axis-of-evil-2002-1127725

[10] Gale, A. "Highly Ranked North Korean Spy Defects to South." *The Wall Street Journal*, 11 aprile 2016, https://www.wsj.com/articles/seoul-announces-defection-of-highly-ranked-north-korean-spy-1460350878

[11] Sigholm, J. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies* 4, no. 1 (2013): 1-37.

[12] Barlett, J. "Mapping Major Milestones in the Evolution of North Korea's Cyber Program." The Diplomat, 18 luglio 2022, https://thediplomat.com/2022/07/mapping-major-milestones-in-the-evolution-of-north-koreas-cyber-program/

[13] Department of the Army. *Nort Korea Tactics – ATP 7-100.2*. Army Publishing Directorate, 2020.

del Dipartimento di Stato Maggiore dell'Esercito Popolare Coreano e considerato il servizio di *intelligence* responsabile delle operazioni clandestine. Sotto la sua supervisione agisce l'Ufficio 121, incaricato delle operazioni di *hacking* e della diffusione di *malware*, articolato a sua volta in diverse unità: il Laboratorio 110, responsabile della sorveglianza dei disertori e delle organizzazioni che li supportano; le Unità 180 e 91, dedite all'acquisizione di valuta forte e ai cyberattacchi contro *intranet* aziendali; e gli Uffici 128 e 414, deputati alle comunicazioni con la rete di spionaggio in Corea del Sud[14]. Al di fuori di questa struttura operano gruppi *hacker* come Kimsuky, Ricochet Chollima e Lazarus Group. Tacitamente legati a Pyongyang, hanno condotto operazioni di *DDoS*, *phishing* e *wiper attack*, oltre a penetrare sistemi informatici mediante *cryptoworm*, *ransomware* e vulnerabilità *zero-day*. In totale, si stima che circa 6.000 *hacker*[15] siano coinvolti in illeciti sponsorizzati da organi statali o da essi pianificati.

I risultati e gli obiettivi raggiunti sono molteplici. Anzitutto, il regime nordcoreano ha sviluppato la capacità di eludere con maggiore facilità le sanzioni internazionali adottate dalle Nazioni Unite, riuscendo ad accedere a tecnologie e conoscenze a duplice uso altrimenti proibite[16]. A ciò si aggiunge l'evoluzione delle capacità di spionaggio, ulteriormente perfezionate proprio attraverso il settore dell'IT, che ha colpito prevalentemente gli Stati Uniti e la Corea del Sud, nonché il rafforzamento della deterrenza mediante attività informatiche di natura perturbativa. Esemplificativi di ciò sono gli attacchi del 2013 contro la Casa Blu, residenza del Presidente della Repubblica di Corea,

[14] Kong, J., Lim, J., Kim, K. “The All-Purpose Sword: North Korea’s Cyber Operations and Strategies”. 11th International Conference on Cyber Conflict (2019): 1-20.
[15] Barlett, J. “Mapping Major Milestones in the Evolution of North Korea’s Cyber Program.” The Diplomat, 18 luglio 2022, https://thediplomat.com/2022/07/mapping-major-milestones-in-the-evolution-of-north-koreas-cyber-program/
[16] Joint Cybersecurity Advisory. North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime’s Military and Nuclear Programs. CISA, 2024.

alcuni servizi bancari e tre compagnie televisive sudcoreane, che causarono, oltre alla fuga di informazioni riservate, danni a server e computer delle entità colpite, con perdite economiche non indifferenti per milioni di dollari[17].

Spionaggio, criptovalute e cyberattacchi: ruolo, bersagli e collaborazioni

Per Pyongyang, spionaggio, criptovalute e cyberattacchi costituiscono le principali frecce del proprio arco digitale. Il loro ruolo è quello di sostenere il regime e di permettere di presentarsi nell'arena globale come un protagonista statuale in grado di rispondere alle costrizioni imposte dalla comunità internazionale e, in particolar modo, dagli Stati Uniti. Ciò risponde a una logica di politica estera nordcoreana improntata alla sopravvivenza di un piccolo Paese stretto tra grandi potenze, siano esse amiche quali Russia e Cina, o ostili, come Washington e i suoi alleati regionali[18]. Attraverso l'acquisizione di questo tipo di capacità il governo kimista ottiene un duplice beneficio: guadagni materiali e conoscitivi che, sia internamente che esternamente, possono divenire a loro volta narrazioni di propaganda sulla forza del regime e sulla sua capacità, questa sì reale, di resilienza[19]. Tali condizioni sono state peraltro favorite dagli stessi soggetti che agiscono oggi in maniera oppositiva a queste dinamiche, ovvero Washington e Seul, in quanto, almeno all'inizio, incapaci di definire adeguatamente la pericolosità e la pervasività dell'azione ibrida nordcoreana[20].

---

[17] Branigan, T. "South Korea on alert for cyber-attacks after major network goes down." The Guardian, 20 marzo 2013, https://www.theguardian.com/world/2013/mar/20/south-korea-under-cyber-attack; BBC. "Cyber attack hits South Korea websites." 25 giugno 2013.

[18] A. Snyder, Scott e Kyung-Ae Park. North Korea's Foreign Policy – The Kim Jong-un regime in a hostile world. Rowman & Littlefield, 2023.

[19] Young Bang, C. "How the Kim Regime Managed to Survive in North Korea (So Far)." *The Diplomat*, 11 dicembre 2024, https://thediplomat.com/2024/12/how-the-kim-regime-managed-to-survive-in-north-korea-so-far/

[20] Gao, J. "Hardening the Shield Against North Korea's "All-Purpose Sword": An Evolving North Korean Cyber Threat and Its Policy Responses." *Georgetown Security Studies Review* 10, n. 2 (2023): 31-41; Boo, H, Kang, K. "An Assessment of North Korean Cyber Threats and the Republic of Korea's Policy Responses: An Update." 戰略與評估 第九卷第一期: 79-98.

Non a caso, i primi attacchi cibernetici hanno colpito strutture americane e sudcoreane. Nel settembre 2013 Kimsuky ha condotto offensive multilivello contro il Ministero dell'Unificazione sudcoreano, l'Istituto coreano per le analisi sulla Difesa e la compagnia Hyundai Merchant Marine[21]. Tra il 2014 e il 2016, la Corea del Nord ha svolto operazioni di cyberspionaggio e sottrazione di dati sensibili ai danni della Korea Hydro & Nuclear Power Co.[22], arrivando anche a compromettere dispositivi di membri dell'Assemblea Nazionale di Seul[23]. Negli Stati Uniti, nel 2014, il gruppo Lazarus ha diffuso dati interni di Sony Entertainment in risposta al film satirico "The Interview" e, nel 2017, *ransomware* attribuiti ad *hacker* nordcoreani hanno colpito società del complesso militare-industriale americano[24].

Dal 2018 queste attività si sono estese a un numero crescente di Paesi, spostandosi verso la finanza. Il gruppo Lazarus sarebbe infatti responsabile del furto di ingenti quantità di criptovalute, come nei casi di Bybit (Emirati Arabi Uniti)[25] e WazirX (India)[26], a testimonianza altresì dell'ampliamento geografico di tali offensive. Il cambio di strategia, dall'ambito securitario a quello economico-finanziario, è probabilmente dovuto all'esigenza di sostenere con nuovi capitali,

---

[21] Halliday, J., Gibbs, S. “North Korean hackers suspected of cyber-espionage attack on South.” *The Guardian*, 11 mercoledì 2013, https://www.theguardian.com/technology/2013/sep/11/north-korean-hackers-cyber-espionage

[22] Park, J., Cho, M. “South Korea blames North Korea for December hack on nuclear operator.” *Reuters*, 17 marzo 2015, https://www.reuters.com/article/world/south-korea-blames-north-korea-for-december-hack-on-nuclear-operator-idUSKBN0MD0GR/

[23] Park, H. “NIS: N.Korea hacked National Assembly computers.” *NK News*, 21 ottobre 2015, https://www.nknews.org/2015/10/nis-n-korea-hacked-national-assembly-computer/

[24] Hu, E. “North Korea's Cyber Skills Get Attention Amid Sony Hacking Mystery.” Npr, 4 dicembre 2014, https://www.npr.org/sections/alltechconsidered/2014/12/04/368449855/north-koreas-cyber-skills-get-attention-amid-sony-hacking-mystery; Lockheedmartin. “Beware of Imposter.” 27 settembre 2024.

[25] Tidy, J. “North Korean hackers cash out hundreds of millions from $1.5bn ByBit hack.” BBC, 10 marzo 2025, https://www.bbc.com/news/articles/c2kgndwwd7lo

[26] The Hindu. “WazirX hack and $235 million loss attributed to North Korea.” 15 gennaio 2025.

oltre al nucleare, anche lo sviluppo dell'industria leggera e civile, più volte enfatizzata da Kim Jong-un con l'avvio della 20×10 Regional Development Policy[27].

L'estensione operativa di Pyongyang ha portato la Corea del Nord a collaborare con Mosca anche nell'ambito informatico. In passato, contatti tra *hacker* russi e nordcoreani erano già avvenuti attraverso il pagamento dei primi da parte dei secondi per attività di esfiltrazione di dati, in una sorta di modello di *malware-as-a-service*[28]. Secondo un rapporto di novembre 2025[29], tali contatti si sarebbero intensificati fino a configurare una collaborazione tra il gruppo Lazarus e Gamaredon, unità *hacker* accusata di far parte dei servizi segreti russi. Entrambi avrebbero fatto uso di risorse di comando e controllo simili, come server o indirizzi IP. Il 28 luglio 2025 un server riconducibile a Gamaredon avrebbe ospitato un campione di InvisibleFerret, una variante *malware* attribuita a Lazarus e distribuita attraverso percorsi URL già impiegati dalla Corea del Nord in campagne di *phishing*[30]. Benché non vi siano certezze definitive, questa apparente condivisione di strutture informatiche aumenta la probabilità di una cooperazione tra i due Paesi, anche alla luce dell'elevato livello raggiunto dalle relazioni diplomatiche, testimoniato dalla visita dei rispettivi Capi di Stato tra il 2023 e il 2024 e dalla firma, nello stesso anno, di un partenariato strategico globale[31]. Dato tale frangente, Lazarus potrebbe condividere la propria

[27] Choi, J. "'20x10 Regional Development Policy': Background and Implications." KINU Online Series (2024): 1-4.
[28] Sokolin, A., Reddy, S. "North Korean, Russian cybercriminals join forces for first time: Report." NK News, 24 novembre 2025, https://www.nknews.org/2025/11/north-korean-russian-cybercriminals-join-forces-for-first-time-report/
[29] Ibid.
[30] *Gendigital*. "Alliances of convenience: How APTs are beginning to work together." 19 novembre 2025.
[31] Isokazi, A. "The Growing Embrace of Russia and North Korea." *The Diplomat*, 24 luglio 2025, https://thediplomat.com/2025/07/the-growing-embrace-of-russia-and-north-korea/

esperienza nel furto di criptovalute, mentre Gamaredon contribuirebbe ad ampliare le conoscenze tecniche nordcoreane, considerando le operazioni del gruppo russo contro infrastrutture kieviane e NATO[32].

Lo spazio europeo e l'Italia

L'interesse della Corea del Nord per lo spazio europeo è recente. Inizialmente limitato all'Ucraina in virtù del conflitto in corso, Pyongyang ne ha ben presto colto le potenzialità. Le ragioni di tale attenzione sono molteplici. Innanzitutto, la cooperazione attiva tra l'industria bellica europea e quella sudcoreana. Oltre a essere una delle principali esportatrici di prodotti bellici in Europa, Seul ha promosso, in collaborazione con l'Unione Europea, una *partnership* in materia di sicurezza e difesa volta al miglioramento dell'interoperabilità industriale e istituzionale. Ciò ha significato l'apertura di tavoli di lavoro in materia di semiconduttori, IA e connettività avanzata, nonché modelli di sicurezza comuni, resilienza delle catene tecnologiche e scambi tra pubblico e privato in ambito cibernetico e sulle *disruptive technology*[33]. Questo al fine di contrastare elementi destabilizzanti dell'ordine internazionale tramite la condivisione di informazioni e il consolidamento delle capacità di difesa cibernetiche. Tra questi, oltre al conflitto russo-ucraino, vi è il programma nucleare nordcoreano. È possibile che Pyongyang veda in tale alleanza un rischio per i propri programmi atomici, in particolare nel rafforzamento delle capacità d'*intelligence* nei suoi confronti. Offensive hacker verso le infrastrutture della difesa europee non sono quindi da

[32] *Eset*. "ESET Research investigates the Gamaredon APT group: Cyberespionage aimed at high-profile targets in Ukraine and NATO countries." 26 settembre 2024.
[33] Joint Statement of the third meeting of the European Union – Republic of Korea Digital Partnership Council 28 November 2025, Seoul, https://digital-strategy.ec.europa.eu/en/library/joint-statement-third-meeting-eu-republic-korea-digital-partnership-council; EU and the Republic of Korea reinforce tech and digital cooperation at the third Digital Partnership Council, 28 novembre 2025, https://digital-strategy.ec.europa.eu/en/news/eu-and-republic-korea-reinforce-tech-and-digital-cooperation-third-digital-partnership-council

escludere, con l'intento di trafugare dati sensibili relativi a tale collaborazione. Come illustrato successivamente, in molti casi ciò si è effettivamente verificato. Ulteriore motivazione è l'inclusione di alcuni Paesi europei nell'organismo di monitoraggio delle sanzioni verso la Corea del Nord, ricostituito al di fuori dell'ONU a causa del veto russo al rinnovo dell'organismo internazionale[34]. Pyongyang potrebbe rivalersi sui Paesi che votano, insieme agli Stati Uniti, per continuare il monitoraggio delle restrizioni ONU sugli interscambi nordcoreani. Infine, vi è la possibilità, da parte del regime kimista, di intercettare fraudolentemente l'elevato quantitativo di fondi europei messi a disposizione dal progetto comunitario Readiness 2030.

Come anticipato, alcune aziende europee sono state colpite da azioni di questo tipo. Nel 2025, attraverso la campagna Operation DreamJob, il gruppo Lazarus avrebbe condotto manovre di spionaggio informatico e industriale contro tre aziende del Vecchio Continente attive nella produzione di componenti per droni e tecnologie aerospaziali[35]. I pirati informatici avrebbero impiegato offerte di lavoro false ed e-mail mirate per ingannare i dipendenti e installare *malware* ad accesso remoto (ScoringMathTea RAT) nelle *intranet* delle compagnie, compromettendone i dati e la riservatezza del sistema. L'obiettivo pare fosse sottrarre *know-how* utile per la produzione e componentistica di velivoli a pilotaggio remoto, colpendo imprese centrali e sud-orientali europee coinvolte nella produzione bellica attualmente impiegata sul fronte ucraino. Altro caso simile si è registrato in Germania contro la tedesca Diehl Defence, produttrice di

[34] *CSIS*. "Russia's Veto: Dismembering the UN Sanctions Regime on North Korea." 29 marzo 2024.
[35] Lakshmanan, R. "North Korean Hackers Lure Defense Engineers With Fake Jobs to Steal Drone Secrets." *The Hacker News*, 23 ottobre 2025, https://thehackernews.com/2025/10/north-korean-hackers-lure-defense.html

sistemi missilistici[36]. In quel frangente, ad agire è stato il gruppo Kimsuky, sia tramite *spear-phishing* e PDF infetti, sia tramite offerte di lavoro fittizie, perlopiù su LinkedIn[37]. La stessa ENISA, in un rapporto prodotto ad ottobre del 2025[38], ha incluso, insieme a Russia e Cina, i *software ransomware* e le azioni d'ingegneria sociale da parte nordcoreana tra i pericoli che la cybersicurezza europea dovrà affrontare nell'immediato presente e futuro, considerando anche l'interesse da parte dei gruppi affiliati a Pyongyang per numerose imprese attive nei settori della difesa, dell'aerospazio, dei media, della salute e dell'energia.

L'Italia, nel medesimo *report*, è tra i Paesi in cui risulta attiva la presenza di intrusioni informatiche nordcoreane insieme a Belgio, Germania e Francia[39], nonostante non risultino notizie pubbliche di questo tipo e il rapporto non fornisca ulteriori informazioni. Al di là del contesto prettamente digitale, Roma rimane nondimeno un territorio rilevante per la Corea del Nord. Il nostro Paese ospita un'ambasciata nordcoreana nella capitale, protagonista della fuga dell'allora rappresentante diplomatico Jo Song-gil, di cui si erano perse le tracce salvo poi ricomparire in Corea del Sud[40]. Sempre a Roma, dove è presente la sede della FAO, gravitano numerose delegazioni diplomatiche di Pyongyang, data la rilevanza che le politiche alimentari rivestono per lo stato nordcoreano. Inoltre, all'interno della sede dell'organizzazione ONU è testimoniata la presenza di una

[36] Paganini, P. “North Korea-linked APT Kimsuky targeted German defense firm Diehl Defence.” *Security Affairs*, 1 ottobre 2024, https://securityaffairs.com/169162/apt/kimsuky-apt-hit-diehl-defence.html

[37] Lakshmanan, R. “DPRK Operatives Impersonate Professionals on LinkedIn to Infiltrate Companies.”, The Hacker News, 10 febbraio 2026, https://thehackernews.com/2026/02/dprk-operatives-impersonate.html

[38] Boutemeur, J., Lella, I., Bakatsis, I., Chatzichristos, G., Foley, K., Leskinen, J., Otcenasek, J., Ziolek, D., Pacenti, C. Enisa Threat Landscape 2025. European Union Agency for Cybersecurity, 2025.

[39] Ibid.

[40] Tartaglione, T. “Un italiano a Pyongyang: i rapporti diplomatici tra Italia e Corea del Nord.” Geopolitica.info, 9 luglio 2025, https://www.geopolitica.info/diplomazia-italia-coreadelnord/

spia nordcoreana, allontanata dall'agenzia ma registrata nel protocollo diplomatico del nostro Ministero degli Esteri[41]. Palazzo Chigi fu poi al centro del tentato (e in seguito fallito) disgelo tra i Paesi occidentali e il regime kimista e, in passato, varie personalità politiche italiane hanno fatto tappa a Pyongyang[42]. Da queste vicende emerge come l'Italia, seppur geograficamente distante, resti parte delle dinamiche che interessano la Corea del Nord, sebbene in misura minore rispetto a qualche decennio fa. In tal senso, si possono formulare due ipotesi. La prima è che Roma rappresenti per Pyongyang un terreno neutro, dato il ruolo favorevole svolto agli inizi del nuovo millennio nelle relazioni tra i due Paesi: l'avvio delle relazioni diplomatiche nel gennaio 2000 e la seguente interlocuzione nel dialogo euro-atlantico proiettarono l'immagine dell'Italia come attore non conflittuale verso il regime, grazie al sostegno a percorsi di dialogo[43]. Tale eredità rende oggi difficile, in ricordo di quell'impegno, prospettare campagne informatiche dirette verso il nostro Paese[44]. La seconda considerazione è invece che l'Italia non possiederebbe quelle caratteristiche strategiche tali da renderla un soggetto di particolare interesse per operazioni di hackeraggio o spionaggio da parte dei servizi nordcoreani.

Conclusioni

Il caso della Corea del Nord mostra con particolare chiarezza la valenza e le potenzialità della guerra ibrida come insieme di strategie, manovre e attività in grado di garantire, anche a Paesi con ridotte o modeste risorse e capacità

[41] *Ibid*.
[42] *Ibid*.
[43] *Ibid*.
[44] L'Italia è infatti tra i pochi Paesi ad aver ricevuto, in occasione dell'elezione a Presidente della Repubblica di Sergio Mattarella, una lettera di congratulazioni da parte di Pyongyang, nella quale si augurava buon lavoro al nuovo Capo dello Stato e un miglioramento e rafforzamento delle relazioni tra i due Paesi; *Rodong Sinmun*. "Congratulations to Italian President." 4 febbraio 2015.

finanziarie, di competere sul piano internazionale con attori dalle ben più alte disponibilità tecniche e infrastrutturali. Ciò permette di tracciare tre punti specifici a riguardo.

Il primo è che, grazie agli investimenti nel settore cibernetico, Pyongyang è riuscita a emergere come attore *cyber* globale attraverso azioni sofisticate che, in un circolo virtuoso, generano benefici economici, politici e conoscitivi capaci di potenziare ulteriormente le sue capacità offensive. Il secondo è che tali manovre segnalano come, nel dominio digitale, la distribuzione del potere non coincida con gli indicatori convenzionali: gli attacchi condotti contro istituzioni statunitensi e sudcoreane ne sono la dimostrazione più evidente, a riprova che il potere oggi non risiede solo nella "canna del fucile", ma anche nei cavi in fibra ottica. Il terzo riguarda la tendenza di altri Stati a valorizzare tali capacità per affinità ideologica o convenienza, scambiando competenze e know-how in modo reciproco, dinamica già manifesta nell'approfondimento delle relazioni tra Mosca e Pyongyang[45]. Per l'Europa e l'Italia persiste il rischio di sottovalutare la portata del raggio d'azione nordcoreano, solo di recente emerso con evidenza rispetto alle più note minacce russe e cinesi[46], così come il rischio di una lentezza nell'applicazione di quadri normativi sovranazionali e nazionali in materia[47]. A ciò si aggiunge la difficoltà di cogliere la natura sfaccettata della minaccia: il ricorso a criptovalute, reti sociali e *social engineering* sposta la vulnerabilità verso settori non tradizionalmente percepiti come militari, con contaminazioni

[45] Morrow, A. "North Korea and Russia: A Growing Military Alliance with Global Implications.", *Nato Association*, 5 settembre 2025, https://natoassociation.ca/strongnorth-korea-and-russia-a-growing-military-alliance-with-global-implications-strong/

[46] Boutemeur, J., Lella, I., Bakatsis, I., Chatzichristos, G., Foley, K., Leskinen, J., Otcenasek, J., Ziolek, D., Pacenti, C. *Enisa Threat Landscape 2025*. European Union Agency for Cybersecurity, 2025.

[47] Lucke, B., Neumann, B. R. "Bad rules rather than slow discretion? A critical appraisal of EU stabilisation policy." *International Journal of Economic Policy Studies* 15 (2021): 367-385.

trasversali che investono la società, l'economia, la finanza e l'informazione. In questo quadro, la traiettoria nordcoreana si inserisce in una più ampia intensificazione della guerra ibrida globale, in cui le operazioni ostili saranno sempre più frequenti e progettate per restare al di sotto delle soglie tradizionali di risposta. Il caso della Corea del Nord è pertanto un monito allo studio e all'analisi di un futuro in cui la guerra ibrida non sarà caratteristica accessoria, bensì una realtà avanzata, multiforme e sotterranea, e per questo profondamente pericolosa.

SEZIONE II – GLI STRUMENTI

Propaganda russa e guerra ibrida in Italia e Slovacchia

di Lorenzo Avesani

Introduzione

L'invasione russa dell'Ucraina del 2022 è certamente un evento spartiacque della politica internazionale. Il conflitto, che non può esser ridotto a carattere meramente militare, dimostra una dimensione non lineare che coinvolge l'opinione pubblica dei cittadini dell'Unione europea (Ue). L'uso intensificato della disinformazione quale strumento di pressione ibrida è atto ad erodere la coesione euro-atlantica, polarizzare le opinioni pubbliche e delegittimare il sostegno occidentale a Kyiv. Nel 2026, l'opinione pubblica europea ha considerato le interferenze straniere nello spazio dell'informazione come la seconda minaccia più incombente per la salute democratica dell'Ue[1]. Tuttavia, all'atto pratico, la consapevolezza sul tema rimane frammentata tra gli Stati membri.

A partire da questa generale considerazione, i casi di studio ivi considerati, Italia e Slovacchia, assumono particolare importanza. Pur essendo contesti profondamente diversi, la loro comparazione non è un esercizio teorico ma offre spunti di riflessione nonché elementi di convergenza. Da un lato, i due Paesi mostrano livelli mediamente alti di polarizzazione politica con una tendenza in crescita nel breve e medio termine[2] considerando che gli esecutivi che li guidano sono composte da forze populiste — sebbene collocate agli estremi dello spettro

[1] Yanatma, Servet. "Foreign information manipulation is among top threats to EU democracy." *Euronews*, 26 gennaio 2026. https://www.euronews.com/next/2026/01/26/is-eu-democracy-under-pressure-foreign-information-manipulation-emerges-as-second-biggest-

[2] "Political Polarization Score." *Our World in Data*, 17 marzo 2025. https://ourworldindata.org/grapher/political-polarization-score

politico. Dall'altro lato, Roma e Bratislava condividono un quadro relativamente debole nel contrasto alla disinformazione riconducibile a una limitata volontà politica[3].

L'analisi si sviluppa in quattro sezioni principali. La prima definisce in maniera generale la propaganda russa come una minaccia europea oltre che definire il generale *modus operandi*. La seconda e la terza esaminano nello specifico quali mezzi fisici, simbolici e culturali sfrutta il Cremlino per influenzare le opinioni pubbliche in Italia e in Slovacchia. La quarta analizza come i due Paesi hanno concettualizzato la disinformazione russa come una minaccia ibrida all'interno dei loro documenti strategici nonché vedere se ci sia una collaborazione a riguardo. Infine, l'analisi verrà chiusa con delle considerazioni finali.

Anatomia della propaganda russa in Europa

L'attenzione sul livello dell'informazione e della sicurezza cognitiva è consolidata nel pensiero strategico russo fin dagli anni 2000 ed è correlata allo sviluppo di una postura revanscista. Mosca ha costruito delle "narrative strategiche[4]" che plasmano la sua identità di grande potenza umiliata e minacciata dall'avanzata dell'Occidente nell'Europa orientale. Nello specifico, la visione del mondo che la Russia proietta è caratterizzata da cinque elementi: una crescente russofobia, una volontà occidentale di entrare in guerra contro la Russia paventando l'uso del nucleare, la creazione di un'egemonia globale statunitense a scapito di un più giusto ordine multipolare, la crisi dell'UE percepita come entità sovranazionale vicina al collasso e la declinazione di un

[3] Bleyer-Simon, Konrad (Ed.). How Is Disinformation Addressed in the Member States of the European Union?—27 Country Cases. European Digital Media Observatory, 2025.
[4] Miskimmon, Alister, Ben O'Loughlin, and Laura Roselle. *Strategic Narratives: Communication Power and the New World Order.* Routledge, 2014.

neo-atlantismo aggressivo[5]. Un chiaro esempio di narrazione strategica è il discorso del presidente russo, Vladimir Putin, durante la parata del 9 maggio 2023 il quale ha affermato che "l'élite occidentale e globalista, insistendo sul loro carattere eccezionale, provocano conflitti e stanno incoraggiando la russofobia nel mondo"[6].

In tale contesto, la memoria storica e concetti identitari quali sovranità e popolo diventano inevitabilmente delle "armi da guerra" nel framework della disinformazione tramite la loro manipolazione per giustificare atti politici e militari. Il loro uso politico portano numerose distorsioni, falsificazioni, omissioni e speculazioni le quali, attraverso la loro diffusione rapida, martellante e polarizzante su internet e nei media tradizionali, hanno un impatto dirompente sull'opinione pubblica[7]. In contesti domestici illiberali come quello russo, la storia e l'informazione non hanno carattere oggettivo ma sono strumenti il cui scopo primario è la sopravvivenza e la legittimazione del regime. Al contrario essi cercano di ravvivare la *grandeur* della Russia convincendo e convincendosi di poter recuperare il proprio status di superpotenza e generando un mito di invincibilità[8].

Questi sentimenti non si limitano solamente alla dimensione domestica ma si proiettano all'esterno coinvolgendo *in primis* i Paesi dell'Europa centrorientale. Per la Federazione Russa, essi rappresentano al contempo il suo estero vicino su cui si estende la sua sfera di influenza e un fattore di preoccupazione storica e

---

[5] Bánkuty-Balogh, Lilla Sarolta. "Novel Technologies and Geopolitical Strategies: Disinformation Narratives in the Countries of the Visegrád Group." *Politics in Central Europe* 17, no. 2 (2021): 165–195.

[6] SkyNews. "Putin accuses the West of Russophobia during his speech at the Victory Day parade in Moscow." YouTube, 9 maggio 2023. Video. https://www.youtube.com/shorts/R3qH6xYkSNk.

[7] Krasnodemska, Iryna, Viacheslav Kalinichenko, Svitlana Marchenko, Oleksandr Ostapchuk, and Olha Sonechko. "History as a Weapon: Narratives and Propaganda in the Russo-Ukrainian War." *Amazonia Investiga* 13, no. 81 (2024): 98–107.

[8] Ibidem.

geopolitica che alimentano una mentalità da assedio[9]. La sua postura nega i timori e i traumi storici dei Paesi post-sovietici e dei membri del dissolto Patto di Varsavia accusando questi ultimi di rappresentare una minaccia esistenziale in quanto facenti parte dell'espansionismo occidentale. La stretta interconnessione storica tra Mosca e la regione dell'Europa centro-orientale rende la manipolazione della storia più diretta e profonda, poiché la Russia ha occupato direttamente questi Paesi, generando tuttavia effetti eterogenei in termini di repulsione nei suoi confronti[10].

Anche l'Europa occidentale non è esente da queste manipolazioni storiche e dalla disinformazione russa. Nonostante le nazioni europee occidentali non siano direttamente colpite dalla manipolazione di specifici eventi storici, la Russia ha cercato di influenzare l'opinione pubblica locale sfruttando le comunità più emarginate e le classi sociali meno abbienti. In particolare, il malcontento democratico è un facilitatore nella trasmissione delle narrazioni russe contro entità distanti — l'Ue, la NATO, l'elite al potere — o politiche che richiedono sforzi economici — ad esempio, il supporto all'Ucraina e la transizione verde[11]. Questo porta alla ricerca di media alternativi e partiti estremisti che emulano i messaggi della propaganda russa. Il caso più celebre è stata l'operazione *Doppelganger* avvenuta a settembre 2022 nel quale la compagnia IT russa Social Design Agency ha generato oltre 17 URL che imitavano i siti internet di grandi testate ed agenzie

[9] Bugajski, Janusz. "Russia's Historical Distortions." *Center for European Policy Analysis*, 6 novembre 2017. https://cepa.org/article/russias-historical-distortions/.
[10] Arribas Cristina M., Rubén Arcos, Manuel Gértrudix, Kamil Mikulski, Pablo Hernández-Escayola, Mihaela Teodor, Elena Novăcescu, et al., "Information Manipulation and Historical Revisionism: Russian Disinformation and Foreign Interference through Manipulated History-Based Narratives," *Open Research Europe* 3 (2023): 121.
[11] Okholm, Christiern Santos. "Conditions of Subversive Reach: Comparing Societal and Strategic Factors for Russian Propaganda Outlets' Reach among Western European Fringe Communities." *European Journal of International Security* (2025): 1–23.

di stampa francesi, tedesche ed italiane il cui scopo era diffondere materiale illegale e dannoso[12].

A prescindere dal contesto geografico la propaganda russa si distingue per sfruttare la sfera informativa come un "campo di battaglia" in cui viene dispiegati specifici strumenti quali l'uso di media alternativi, corruzione, relazioni con entità della società civile — *think tank*, partiti politici, movimenti sociali e religiosi politicamente trasversali —, così come attori quali bot, troll e influencer attivi nello spazio digitale[13]. Questi attori hanno reso la diffusione della disinformazione più rapida, *bottom up* e difficile da tracciare e quindi le conseguenze più difficili da governare. La loro pervasività e capillarità supera il concetto di *soft power* dato che questa pluralità di "voci amiche e utili idioti" penetra nel tessuto sociale e politico dei Paesi mimetizzandosi in termini linguistici e culturali con i media locali e facendo leva sulle fragilità interne. L'obiettivo finale non è convincere il pubblico di una narrazione storica o un'idea politica ma "generare cinismo nella popolazione e inibire la fiducia nelle istituzioni"[14].

Italia: dalla Russia con amore

Per comprendere l'attuale influenza della propaganda russa sull'Italia, si deve tener conto che essa ha origine ben prima della diffusione delle tesi revisioniste russe nell'informazione italiana. Infatti, dopo la Seconda guerra mondiale, la genesi della Repubblica italiana e il suo progressivo avvicinamento alle istituzioni euro-atlantiche furono caratterizzati, da un lato, dall'egemonia

[12] Sessa, Maria Giovanna e Raquel Miguel. *The Doppelganger case Assessment of Platform Regulation on the EU Disinformation Environment*. NATO Strategic Communication Centre of Excellence, 2024.
[13] Pomerantsev, Peter, e Michael Weiss. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture, and Money. Institute of Modern Russia, 2014.
[14] Pomerantsev, Peter. "Authoritarianism Goes Global: The Kremlin's Information War." *Journal of Democracy* 26, no. 4 (2015): 40–50.

politica della Democrazia Cristiana e, dall'altro, dalla presenza del Partito Comunista Italiano (PCI) come principale forza di opposizione. Quest'ultimo, il più grande dell'Europa occidentale, volle garantire la c.d. "egemonia culturale" ovvero veicolare le sue narrative nelle istituzioni culturali allo scopo di "conquistare i cuori e le menti" come atto necessario per preparare il terreno alla conquista del potere politico[15]. Il concetto, coniato dal filosofo Antonio Gramsci, divenne una strategia concreta con il supporto dell'Unione Sovietica (URSS) condotta attraverso "misure attive". Esse indicano una gamma di operazioni di influenza del *sentiment* attraverso agenti di influenza reclutati tra politici, giornalisti e intellettuali.

Il vuoto ideologico creato dal comunismo a seguito del crollo dell'URSS ha cambiato la direzione gramsciana dell'egemonia culturale. Sentimenti tradizionalisti, no-global e antiamericanismo — ivi inteso anche come pulsioni antioccidentali — hanno definito il nuovo terreno ideologico-culturale alternativo al presunto trionfo dell'Occidente. In tale scenario, il neo-Eurasismo[16] si impone e si salda in Italia — come anche in altri Paesi europei — dapprima con gli intellettuali e politici di estrema destra e poi, dopo il 2000, con la sinistra radicale[17]. Il suo successo è strettamente collegato con gli sviluppi geopolitici risultanti dal revisionismo russo. Le rivoluzioni colorate, l'espansione ad est della NATO, il conflitto russo-georgiano del 2008 e quello russo-ucraino del 2014

[15] Di Pasquale Massimiliano e Luigi Sergio Germani. *L'influenza russa sulla cultura, sul mondo accademico e sui think tank italiani*. Istituto Gino Germani di Scienze Sociali e Studi Strategici, 2021.

[16] Il neo-Eurasismo è una corrente filosofica e politica che nasce originariamente per identificare la cultura russa come una realtà peculiare rispetto a quella europea e asiatica. Nel tempo, tuttavia, ha assunto una connotazione geopolitica radicale e di scontro manicheo tra la "Potenza della Terra" incarnata dalla tradizione e dalla Russia e quella "del Mare" incarnata dal liberalismo occidentale. Il filosofo russo, Alexandr Dugin, ne è il maggior esponente.

[17] Savino, Giovanni. "From Evola to Dugin: The Neo-Eurasianist Connection in Italy." In *Eurasianism and the European Far Right: Reshaping the Europe–Russia Relationship*, 97–124. Lexington Books, 2015.

e del 2022 hanno cementificatole coordinate narrative e geopolitiche del *Russlandversteher* — letteralmente "quelli che capiscono la Russia[18]".

La diffusione del pensiero *Russlandversteher* ha rappresentato la base della propaganda russa. L'attenzione verso Kyiv dei neo-eurasisti è centrale della matrice storico-culturale della Russia e il suo slittamento ad Occidente è vissuto come un tradimento ontologico[19]. Il sostegno italiano all'Ucraina — specialmente dopo l'aggressione del 24 febbraio — spiega l'ondata di disinformazione pro-Cremlino in atto nel Paese. Dal 2022 ad oggi, Mosca ha mobilitato le sue campagne di disinformazione nei media italiani mettendo in discussione eventi quali il massacro di Bucha o i bombardamenti contro civili a Mariupol[20]. In particolare, si è assistito alla proliferazione di eventi culturali organizzati— in alcuni casi annullati a seguito delle contestazioni da parte dell'ambasciatore ucraino, Yaroslav Melnyk, e delle organizzazioni sociali e politiche sensibili alla causa di Kyiv — ai quali sono stati invitati ospiti che hanno propagandato le narrazioni russe sul conflitto[21].

---

[18] Di Pasquale e Germani, ibidem.

[19] Arcuri, Lavinia. "La Russia che sfida l'Occidente: Aleksandr Dugin e l'Eurasiatismo come missione storica." Geopolitica.info, 28 novembre 2025. https://www.geopolitica.info/russia-sfida-occidente-dugin-euroasiatismo/.

[20] Un esempio di distorsione storica sul conflitto in Ucraina sono le dichiarazioni del ministero della difesa russo il quale ha definito il massacro di Bucha una "messa in scena dell'Occidente" o le accuse al battaglione ucraino Azov di aver bombardato il reparto di maternità dell'ospedale di Mariupol. Queste affermazioni ed altri esempi di manipolazione narrativa sono registrati nel database di EUvsDisinfo e correlati dagli articoli di Disinfo Review ad essi correlati.
Quest'ultimi, presenti anche in lingua italiana, analizzano la narrazione pro-Cremlino e citano direttamente il sito russo da cui parte il messaggio pro-Cremlino. I passaggi specifici li ho riscontrati in due articoli: EUvsDisinfo. "La disinformazione per nascondere i crimini di guerra: la Russia mente sulle atrocità a Bucha.", 7 aprile 2022. https://euvsdisinfo.eu/it/la-disinformazione-per-nascondere-i-crimini-di-guerra-la-russia-mente-sulle-atrocita-a-bucha/ ; EUvsDisinfo. "On a wild goose chase ahead of the 9th of May." 28, aprile 2022. https://euvsdisinfo.eu/on-a-wild-goose-chase-ahead-of-the-9th-of-may/.

[21] Tokariuk, Olga. "The Kremlin's Cultural Tentacles Still Poison Italian Debate." *Center for European Policy Analysis*, 11 gennaio 2024. https://cepa.org/article/the-kremlins-cultural-tentacles-still-poison-italian-debate/.

Ciò è accompagnato da un discorso mediatico distorto diffuso sia attraverso i canali tradizionali sia tramite i social media, che fa presa su un pubblico scarsamente attivo nella partecipazione civica. Tale narrazione inquadra il conflitto come un fenomeno distante rispetto ad altre priorità percepite in maniera più urgente, quali la stagnazione economica e l'immigrazione irregolare, mentre sulla questione russo-ucraina si assiste al rovesciamento della dinamica tra aggressore e aggredito[22]. Addirittura, questa tendenza ha trovato un recente canale di sbocco anche nei libri di testo scolastici come frutto della sedimentazione culturale delle narrative pro-Cremlino. Secondo una recente analisi dell'Istituto Gino Germani[23], i volumi approvati a marzo 2024 dal Ministero dell'Istruzione e del Merito, risultano organiche all'immagine della Russia tacendo sui processi di russificazione e sulle controversie di diritto internazionale associati alla Crimea e al Donbass.

Per questi motivi, Roma è considerata dagli analisti della disinformazione russa come un fronte vulnerabile nell'Europa occidentale. La pressione ibrida e le operazioni di disinformazioni russe nel Paese hanno principalmente tre motivi: indebolire la coesione europea ed euro-atlantica; influenzare la politica estera italiana; e riallacciare i rapporti economico-energetici tra Roma e Mosca venuti meno con l'invasione su larga scala dell'Ucraina[24]. L'Italia è un obiettivo strategico per la Russia anche per la sua posizione strategica nel Mediterraneo

[22] Braghiroli, Stefano. "Normalizing pro-Russia narratives straight from the Kremlin playbook: an autopsy of an average Italian social media feed." *New Eastern Europe*, 10 dicembre 2025. https://neweasterneurope.eu/2025/12/10/normalizing-pro-russia-narratives-straight-from-the-kremlin-playbook-an-autopsy-of-an-average-italian-social-media-feed/ ; Sessa, Maria Giovanna. "Disinformation landscape in Italy." *EU DisinfoLab*, 2025.

[23] Di Pasquale, Massimiliano e Iryna Kashchey. "Narrazioni strategiche russe nei libri di testo delle scuole secondarie di primo grado italiane." *Istituto Gino Germani di Scienze Sociali e Studi Strategici*, 2025.

[24] Di Vincenti, Joseph. "The Russian Hybrid Threat in Italy: Political Influence, Propaganda and Disinformation." *The Centre for Communication Influences and Propaganda Research Papers* 1 (2025): 1–10.

che le permette di essere uno snodo strategico non solamente per le istituzioni euro-atlantiche ma anche per corridoi e organizzazioni regionali quali il Corridoio Europeo India-Medio Oriente-Europa e la Three Seas Initiative[25].

Nella storia recente, oltre alla già citata operazione Doppelganger, l'Italia ha scoperto il suo fianco alle operazioni ibride russe durante l'emergenza pandemica. L'operazione "Dalla Russia con amore" venne presentata ufficialmente come una missione di assistenza umanitaria e sanitaria a sostegno dell'Italia. Tuttavia, il sostegno si rivelò un'operazione di comunicazione strategica volta a rafforzare la percezione positiva di Mosca presso l'opinione pubblica italiana[26]. La visibilità mediatica dell'operazione e la forte enfasi simbolica promossa dalle autorità russe contribuirono a costruire un'immagine di Mosca come partner solidale e più efficiente rispetto agli europei nel contrasto al Covid. In questo senso, l'iniziativa è stata interpretata da numerosi osservatori come uno strumento di *soft power* volto a rafforzare la percezione positiva della Russia[27].

Slovacchia: miti panslavisti

Il caso italiano evidenzia come la proiezione di influenza russa possa sfruttare contingenze emergenziali e ambiguità politiche strutturali. Tuttavia, tale dinamica non è uniforme in Europa. Infatti, lo scenario slovacco è profondamente diverso da quello italiano sotto diversi aspetti. Innanzitutto, essendo il Paese dalla più recente indipendenza statuale dell'area centroeuropea, ha vissuto un periodo più complesso di consolidamento delle

[25] Rossi, Emanuele. "From Russia to Italy: That's Not Amore." *Center for European Policy Analysis*, 5 marzo 2025. https://cepa.org/article/from-russia-to-italy-thats-not-amore/.
[26] Bertolotti, Claudio. ""Dalla Russia con amore": le nuove minacce per l'Italia e il ruolo della Russia tra cyberspazio, salute pubblica, disinformazione e spionaggio." *Start Insight*, 4 aprile 2025. https://www.startinsight.eu/dalla-russia-con-amore/.
[27] Ibidem.

istituzioni democratiche nel post-Guerra Fredda oltre che aver vissuto un processo di *nation* e *identity-building*. La sua ubicazione geografica e storico-culturale più vicino alla Russia e al mondo post-sovietico ha creato una rottura profonda all'interno della società tra coloro che si identificano come parte dell'Occidente o parte del mondo russo[28]. Tale "posizione di mezzo" è stata un elemento di ambiguità, ad esempio, nel processo di adesione alla NATO che è arrivato in maniera tardiva (2004) e su spinta degli altri membri del Gruppo. La preferenza di una politica estera più improntata ad un approccio economicistico che securitario ha trascinato il Paese alla dipendenza energetica ed economica da Mosca per tentare colmare i divari con la Repubblica Ceca emersi con la dissoluzione cecoslovacca.

Per questo motivo, la propaganda russa si è maggiormente concentrata su questioni identitarie alimentando la polarizzazione tra gli strati sociali che non si rispecchiano nei valori e posture occidentali. La leva ideologica maggiormente utilizzata è quella del panslavismo, diffuso specialmente nelle zone rurali del Paese[29]. Secondo questa ideologia, si riconosce una interconnessione storica e valoriale tra le nazioni slave, in cui la Russia ricopre il ruolo di grande nazione fraterna. Ciò implica che l'Occidente e i suoi valori sono rigettati e visti come una nuova forma di colonialismo[30]. L'ideologia panslavista, sebbene si distribuisca principalmente tra i partiti di estrema destra, non è ad esclusivo appannaggio di un partito politico ma e anche, l'attuale governo, seppur ufficialmente di sinistra,

---

[28] Ušiak, Jaroslav. "Slovakia's Perspective on NATO." *Communist and Post-Communist Studies* 51, no. 2 (2018): 125–137.

[29] Dubóczi, Peter e Michaela Ružičková."Disinformation landscape in Slovakia." *EU DisinfoLab*, 2023.

[30] Szafonova, Tatyjana. "Recursive Polarization of Pan-Slavism in Contemporary Slovakia: Being a Slavic Minority vs. Representing Slavic Power" *Illiberalism Studies Program*, 5 febbraio 2026. https://www.illiberalism.org/recursive-polarization-of-pan-slavism-in-contemporary-slovakia-being-a-slavic-minority-vs-representing-slavic-power/.

ospita un gruppo politico nazionalista, il Partito Nazionale Slovacco, che promuove idee russofile.

Entrando nello specifico delle dinamiche governative, il sostrato culturale panslavista è condito da una dose di opportunismo politico dell'attuale Primo Ministro slovacco, Robert Fico. Già da prima del suo ritorno, avvenuto a fine settembre 2023, Fico ha compiuto un processo di *rebranding* politico del suo partito *"Smer"* sfruttando le narrazioni della propaganda russa. Lo scopo di questa trasformazione è stato quello di riempire un vuoto politico creatosi durante i tre anni (2020-2023) del centrodestra al governo[31]. Smer si è così inserita nel più ampio ecosistema mediatico pro-Cremlino della Slovacchia: influencer, siti web, profili sui social media, gruppi aperti e chiusi e reti coordinate di disinformazione. Tale ecosistema, presente fin dal 2014, comprende attori istituzionali e reti diplomatiche sopravvissuti alla transizione post-socialista nonché attori locali disponibili a cooperare per supportare queste narrative[32].

La guerra in Ucraina è il terreno nel quale panslavismo, propaganda russa e opportunismo politico si sono intrecciati. Nonostante i governi precedenti guidati da Eduard Heger e Ludovit Ódor abbiano perseguito una politica di convinto sostegno a Kyiv, l'opinione pubblica slovacca ha dimostrato forte scetticismo. Secondo il GLOBSEC Trends del 2023[33], solo il 40% degli intervistati ha reputato Mosca come responsabile del conflitto ucraino mentre un intervistato su 3 ha accusato l'Occidente di esserne responsabile. Al contempo,

[31] Kaňuchová, Tamara. ""Democracies Do Not Disappear Voluntarily": Slovakia's Year of Upheaval." *VSquare*, 2 gennaio 2026. https://vsquare.org/democracy-in-slovakia-robert-fico-protests-russian-influence-2025/.
[32] Ružičková, Michaela. "Russian Bear of Influence in Slovakia." *Warsaw Institute*, 25 luglio 2023. https://warsawinstitute.org/russian-bear-of-influence-in-slovakia/.
[33] Hajdu, Dominika, Katarína Klingová, Patrik Szicherle, Jana Kazaz, e Viktoria Musilová. *Globsec Trends 2023: United We (Still) Stand.* Globsec, 2023.

oltre la metà degli slovacchi ha disapprovato fortemente le politiche dell'Ue e della NATO a sostegno di Kyiv — invio armi, sanzioni e supporto umanitario[34]. La tendenza persiste anche nelle successive rilevazioni[35]. Oltre a una preesistente sfiducia nelle istituzioni, il conflitto in Ucraina ha contribuito ad accentuare la polarizzazione di un ecosistema mediatico già indebolito dalla disinformazione[36]. A ciò si aggiunge l'uso spregiudicato del discorso pubblico da parte di ampi settori della classe politica, che ricorrono a narrazioni distorte per alimentare la polarizzazione e massimizzare il consenso nel breve periodo[37].

L'azione dell'attuale esecutivo è compiacente politicamente ed economicamente alle istanze di Mosca e Pechino. Questo porta a rendere Bratislava più o meno volontariamente un megafono attivo delle narrative russe e facilitandone la circolazione domestica. Inoltre, l'isolamento che comporta l'ambiguità della politica estera slovacca facilità l'esposizione dello spazio informativo e dei cittadini a narrative monodirezionali anti-UE[38]. Ad aggravare la situazione è la progressiva autocratizzazione del Paese il quale ha subito un'accelerazione con il tentato assassinio di Fico nel 2024. I recenti cambi costituzionali sono stati accompagnati da una retorica fortemente identitaria contro il liberalismo

[34] Ibidem.
[35] Hajdu, Dominika, Katarína Klingová, Patrik Szicherle, Jana Kazaz, e Viktoria Musilová. *Globsec Trends 2024*: *A brave new region?*. Glosec, 2024. ; Hajdu, Dominika, Jana Kazaz, Katarína Klingová e Barbora Dobó. *Globsec Trends 2025: Ready for a new era?*. Globsec, 2025.
[36] Ibidem.
[37] Lintner, Tomáš, Tomáš Diviák, Barbora Nekardová, Lukáš Lehotský, e Michal Vašečka. "Slovak MPs' response to the 2022 Russian invasion of Ukraine in light of conspiracy theories and the polarization of political discourse." *Humanities and Social Sciences Communications* 10, no. 1 (2023): 1-11.
[38] Caniglia Mattia, e Teresa Coratella "Narrative warfare e guerra ibrida nel disordine globale. Quale impatto nelle aree di interesse strategico per l'Italia". Ministero degli Affari Esteri e della Cooperazione Internazionale, 2026.

progressista e la decadenza dell'Occidente[39], linee narrative comuni con la propaganda russa[40].

Dalla diversità dei contesti e degli approcci a possibili soluzioni comuni?

La diversità dei contesti italiano e slovacco e il diverso radicamento della propaganda russa hanno portato a sviluppare strategicamente la minaccia in modi totalmente differenti. Per quanto riguarda l'Italia, lo sviluppo strategico del contrasto alle minacce ibride e alla disinformazione ha avuto uno sviluppo tardivo rispetto agli altri Paesi UE. Il Sistema di Informazione per la Sicurezza della Repubblica (SIS) ha allertato nella relazione del 2023 che "la Russia alimenta campagne multivettoriali in danno dell'Italia[41]". La successiva relazione del 2025 ha dedicato un'analisi dettagliata alle minacce ibride e al loro impatto dentro e fuori dallo spazio digitale[42]. Alla luce delle *querelle* tra Italia e Russia, il Presidente della Repubblica, Sergio Mattarella, ha convocato il 17 novembre 2025 il Consiglio Supremo di Difesa sul tema della guerra ibrida. L'iniziativa del Quirinale è un passo in avanti molto importante a livello strategico, politico e simbolico perché è una lucida presa di coscienza sull'importanza della guerra ibrida come minaccia per il Paese[43].

---

[39] Il Primo Ministro slovacco ha dichiarato che gli emendamenti sono una "diga contro il progressivismo" evidenziando la necessità di evitare la "strada pericolosa" per quanto riguarda la definizione o meno di valori tradizionali quali matrimonio e genere. I virgolettati riportati sono stati tradotti in italiano e provengono dalla fonte messa nella nota a piè di pagina successiva.

[40] Dubóczi, Peter, e Michaela Dubóczi. "Two sexes in the constitution and questioning the Russian threat." *Friedrich Naumann Foundation*, 2 ottobre 2025. https://www.freiheit.org/central-europe-and-baltic-states/two-sexes-constitution-and-questioning-russian-threat.

[41] "Relazione Annuale dell'Intelligence 2023." *Sistema di informazione per la sicurezza della Repubblica*, 28 febbraio 2024. https://www.sicurezzanazionale.gov.it/contenuti/relazione-2023.

[42] "Relazione Annuale dell'Intelligence 2025." *Sistema di informazione per la sicurezza della Repubblica*, 04 marzo 2025. https://www.sicurezzanazionale.gov.it/contenuti/relazione-al-parlamento-2025.

[43] Marzano, Jacopo. "Mattarella convoca il Consiglio Supremo di Difesa contro la guerra ibrida: passo avanti per l'Italia." *Il Riformista*, 12 novembre 2025. https://www.ilriformista.it/mattarella-

Ad oggi, Roma non ha un documento strategico ufficiale che codifica la strategia italiana nel contrasto alla guerra ibrida. Tuttavia, l'attuale Ministro della Difesa, Guido Crosetto, ha redatto e pubblicato il non-paper "Il contrasto alla guerra ibrida: una strategia attiva". Nonostante la natura informale e non vincolante del documento, il non-paper disamina dettagliatamente il concetto di guerra ibrida trattando ampiamente il tema della manipolazione informativa e delle tecniche di disinformazione da parte di attori ostili, in primis la Russia[44]. Il documento si sviluppa in tre direzioni — che cos'è, dove e come — e pone come priorità la circoscrizione di un cyberspazio di interesse nazionale e di un'armata cyber composta da 1200-1500 unità. Inoltre, il documento sottolinea la necessità di istituire un centro nazionale per il contrasto alla guerra ibrida e della cooperazione in ambito Ue, NATO e G7.

Tuttavia, l'azione italiana è ancora condizionata da una frammentazione istituzionale che non permette al decisore politico di avere una visione olistica della situazione. Difatti, in Italia, ci sono sette diverse istituzioni che si occupano di contrastare le minacce ibride nonché varie unità si occupano di contrasto alla disinformazione[45]. Il centro nazionale proposto da Crosetto può essere una soluzione a condizione che esso riesca a unificare e uniformare la risposta alle minacce ibride. Altro limite fondamentale della risposta italiana riguarda ancora la carenza di una cultura politica condivisa della minaccia ibrida data da un'alta

convoca-il-consiglio-supremo-di-difesa-contro-la-guerra-ibrida-passo-avanti-per-litalia-488775/.

[44] Crosetto, Guido. Il contrasto alla guerra ibrida: una strategia attiva. Ministero della Difesa, 2025.

[45] Pugliese, Matteo. "Superare la frammentazione istituzionale per combattere la disinformazione in Italia." *Geopolitica.info*, 10 marzo 2025. https://www.geopolitica.info/disinformazione-italia/.

frammentazione politica nonché la mancanza di strumenti vincolanti che permettano di affrontare minacce non convenzionali in maniera coerente[46].

Rispetto all'Italia, la Slovacchia ha precocemente inquadrato il tema della disinformazione russa come minaccia alla sicurezza nazionale e presenta minor frammentazione istituzionale. Tuttavia, il suo sviluppo risulta fortemente condizionato dalla riluttanza dei governi Smer, dal 2010 a oggi, ad affrontare la questione seriamente, per evitare di compromettere i rapporti con la Federazione Russa[47]. Tuttavia, è presente materiale strategico sia durante i periodi dei governi Smer sia nell'interregno politico del centrodestra. Inoltre, va premesso che a livello di elaborazione dei documenti strategici nazionali sulla sicurezza (*Security Strategy*) si registra un gap temporale marcato con un documento del 2005 e il successivo solo nel 2021 mentre nel 2017, il Parlamento non approvò un aggiornamento intermedio.

I documenti del 2017 hanno avuto come scopo quello di circoscrivere nello specifico il tema della disinformazione. Il *Security Strategy* abortito aveva già evidenziato che le azioni propagandistiche di attori interni ed esterni — con particolare riferimento alla Russia — siano una minaccia per le relazioni del Paese con la NATO e l'Ue e per la fiducia domestica alle istituzioni pubbliche[48]. Al contempo, il Consiglio di Sicurezza della Repubblica Slovacca (BRSR[49]) ha

[46] Carrer, Gabriele, Teresa Coratella, e Silvia Samorè. "Democratic defence: How Italy can lead the fight against Russian disinformation," *European Council on Foreign Relations*, 5 luglio 2023. https://ecfr.eu/publication/democratic-defence-how-italy-can-lead-the-fight-against-russian-disinformation/.

[47] Bučka, Pavel, e Miroslav Žentek. "Predstavuje Rusko bezpečnostnú hrozbu pre Slovenskú republiku?" In *Bezpečnostné fórum 2019: Zborník vedeckých príspevkov*, 16–25. Banská Bystrica: Interpolis, 2019.

[48] "LP/2017/627: Návrh Bezpečnostná stratégia Slovenskej republiky." Ministry of Foreign and European Affairs of the Slovak Republic, 31 agosto 2017. https://www.slov-lex.sk/legislativne-procesy/SK/LP/2017/627.

[49] Bezpečnostná Rada Slovenskej Republiky.

approvato il "Dizionario terminologico della Gestione delle Crisi". Il documento è un glossario tecnico finalizzato all'armonizzazione concettuale e operativa dei termini inglesi in lingua slovacca. Lo scopo è quello di operativizzare i termini nell'ambito del diritto, nello sviluppo dei documenti strategici e nelle attività pratiche di gestione delle crisi[50]. Nel Dizionario non viene definito direttamente il concetto di disinformazione ma è ricompreso nel concetto di *information warfare*[51], intesa come manipolazione del pensiero e del comportamento degli individui a fini di vantaggio strategico.

Il 2021 segna una svolta nello sviluppo strategico slovacco con la pubblicazione di tre documenti importanti: la "Strategia Nazionale di Cybersicurezza 2021-2025" e la revisione della *Security Strategy* e quella della *Defence Strategy*. Il primo, pubblicato dall'Ufficio Nazionale per la Sicurezza (NBÚ[52]), riconosce che lo spazio digitale comprende anche attività virtuali, quali propaganda, estremismo e disinformazione, capaci di produrre effetti di sicurezza che travalicano il dominio cyber[53]. Il documento delinea una serie di obiettivi strategici tra cui: migliorare le capacità nazionali ed uniformare i processi legali, diplomatici e cyber; aumentare l'efficienza nell'individuazione e nell'attribuzione del cybercrimine; rendere il settore privato e pubblico più resiliente; rafforzare le partnership internazionali; aumentare la resilienza sociale tramite la sensibilizzazione pubblica; e aumento delle capacità di ricerca e sviluppo nel campo della cybersicurezza.

[50] BRSR. "Terminologický slovník krízového riadenia a zásady jeho používania." 2017. https://www.reserves.gov.sk/wp-content/uploads/2019/10/Terminologický-slovník-krízového-riadenia.pdf.
[51] Informačná vojna.
[52] Národný Bezpečnostný Úrad.
[53] NBÚ. *The National Cybersecurity Strategy 2021–2025.* 2021. https://www.nbu.gov.sk/wp-content/uploads/cybersecurity/National_cybersecurity_strategy_2021.pdf.

Il Parlamento slovacco ha approvato una nuova Strategia di Sicurezza Nazionale che riconosce esplicitamente la disinformazione come minaccia alla sicurezza interna ed esterna, attribuendo in larga parte le tensioni regionali alla Russia. Il documento prevede interventi sul piano educativo e dell'alfabetizzazione mediatica (punto 54) e promuove una comunicazione strategica coordinata tra istituzioni e *think tank* (punto 55)[54]. Tale impostazione è rafforzata dalla *Defence Strategy*, che assegna alle istituzioni pubbliche un ruolo attivo nel contrasto alla propaganda, collegando la resilienza informativa alla difesa nazionale e all'appartenenza della Slovacchia a NATO e UE[55].

A seguito dei tre documenti, viene pubblicato nel 2022 il "Piano d'azione per il coordinamento della lotta contro le minacce ibride 2022–2024" (APHH)[56]. Il Piano calendarizza una serie di misure con relativa scadenza temporale e definizione dei soggetti istituzionali che devono mettere in pratica le misure. L'APHH definisce le priorità in sei capitoli. Il primo, detto "Compiti generali", definisce l'architettura istituzionale e procedurale per il coordinamento della risposta slovacca alle minacce ibride. Il secondo, chiamato "Misure sistemiche", si occupa di miglioramento delle capacità analitiche dello stato e di sviluppo di strumenti strategici. I restanti affrontano specifiche tematiche quali la comunicazione strategica e disinformazione, il rafforzamento della resilienza della popolazione, la protezione dei processi elettorali e di contrasto all'influenza straniera.

---

[54] "Security Strategy of the Slovak Republic." *Ministry of Foreign and European Affairs of the Slovak Republic*, 2021. https://www.mzv.sk/documents/30297/4638226/security-strategy-of-the-slovak-republic.pdf

[55] "Defence Strategy of the Slovak Republic." *Ministry of Defence of the Slovak Republic*, 2021. https://www.mosr.sk/data/files/4291_defence-strategy-of-the-slovak republic-2021.pdf.

[56] "Akčný plán koordinácie boja proti hybridným hrozbám". *Ministerstvo Obrany Slovenskej Republiky*, 2022. https://www.hybridnehrozby.sk/wp-content/uploads/2023/08/APHH-2022.pdf.

Infine, sebbene l'attuale governo sia meno volenteroso ad agire nei confronti della Russia, lo sviluppo strategico della questione è continuato. In tal senso, due sono i documenti rilevanti: il "Concetto di Comunicazione Strategica" e la "Strategia Nazionale di Cybersicurezza 2026-2030". Il primo, pubblicato nel 2024, inquadra la comunicazione strategica come uno strumento volto a rafforzare la fiducia nelle istituzioni, garantire un'informazione trasparente e coerente e aumentare la resilienza della società slovacca nello spazio informativo[57]. Sul piano organizzativo, il coordinamento è affidato all'Ufficio del Governo della Repubblica Slovacca[58], che attraverso un'unità dedicata garantisce l'unitarietà del messaggio istituzionale, lasciando ai singoli ministeri l'attuazione operativa della comunicazione pubblica.

Il secondo, pubblicato il 6 febbraio 2026, delinea uno sforzo più onnicomprensivo nei confronti delle minacce ibride riconoscendo che l'accresciuta pericolosità dello scenario internazionale espone il Paese ad interferenze straniere. Il documento definisce cinque pilastri: la protezione dello spazio cyber nazionale in riferimento a cittadini e delle imprese; sviluppo di capacità nazionali; preparazione di prodotti e servizi digitali sicuri e innovativi; sviluppo di capacità e competenze in materia di consapevolezza e istruzione; nonché sviluppo di partenariati internazionali[59].

Infine, tenendo conto delle peculiarità dei due Paesi, è possibile tracciare brevemente possibili spazi di cooperazione. Attualmente Italia e Slovacchia sviluppano la loro cooperazione sul tema attraverso la loro partecipazione a spazi

[57] "Koncepcia strategickej komunikácie Slovenskej republiky", *Centre for Countering Hybrid Threats*, 2024. https://www.hybridnehrozby.sk/wp-content/uploads/2024/07/Koncepcia-strat.-komunikacie-2024.pdf.
[58] Úrad Vlády Slovenskej Republiky.
[59] NBÚ, *Národná stratégia kybernetickej bezpečnosti na roky 2026 až 2030*. 2026. https://irp.cdn-website.com/93da658b/files/uploaded/03_Vlastny_material_Strategia_KB+schvalena.pdf

di cooperazione multilaterali. Entrambi i Paesi sono membri dell'Ue, della NATO e del Centro Europeo di Eccellenza per le Minacce Ibride partecipando ai loro progetti ed agenzie. In queste piattaforme, i due Paesi contribuiscono a rafforzare gli sforzi regionali e da questi ultimi possono trarre indicazioni e condivisione di buone pratiche. Ciononostante, Roma e Bratislava dovrebbero dimostrare maggior volontà politica andando oltre al semplice inquadramento della minaccia. Ad oggi, la materia non è sul tavolo data la diversità delle visioni sul dossier Ucraina mentre gli ultimi incontri hanno riguardato altre tematiche quali difesa, energia nucleare, e lotta all'immigrazione clandestina[60].

Conclusione

Nel complesso, i casi studiati dimostrano come la propaganda russa non operi secondo uno schema uniforme ma si mimetizza nel tessuto sociale, culturale ed istituzionale in cui opera. La polarizzazione crescente domestica è un elemento comune tra i due casi ma i fattori endogeni sono differenti. Da un lato, nel caso italiano, la Russia fa leva sull'ambiguità ideologica di parte delle élite culturali e politiche situate agli estremi dello spettro politico. Le narrative si diffondono all'interno di un sistema mediatico in costante crisi finanziaria e concentrato attorno a centri di potere economico-politico. Dall'altro lato, nel caso slovacco, Mosca si inserisce in fratture identitarie mai sanate completamente, in un contesto storico legato alla transizione post-socialista e alla dissoluzione della Cecoslovacchia. A ciò si aggiunge un sistema mediatico in progressivo

[60] Governo Italiano. "Incontro del Presidente Meloni con il Presidente della Repubblica Slovacca." *Presidenza del Consiglio dei Ministri*, 14 gennaio 2025. https://www.governo.it/it/articolo/incontro-del-presidente-meloni-con-il-presidente-della-repubblica-slovacca/27474 ; Governo Italiano. "Joint press release of the President of the Council of Ministers of the Italian Republic, Giorgia Meloni, and the Prime Minister of the Slovak Republic, Robert Fico". *Presidenza del Consiglio dei Ministri*, 3 giugno 2025. https://www.governo.it/sites/governo.it/files/Joint_Press_Release_ITA-SLO_20250603.pdf

scivolamento verso dinamiche di *state capture*, accompagnato dalla preesistente proliferazione di media alternativi compiacenti verso Mosca.

Oltre a questi elementi, vanno evidenziati anche caratteristiche esogene determinanti nello spiegare la diversità delle narrazioni pro-Cremlino e la loro permeabilità tra i due Paesi e la differente risposta alla minaccia. Roma è un Paese fondatore dell'Ue e della NATO nonché una media potenza fortemente attiva e coinvolta nei principali tavoli internazionali. Ciononostante, la sua distanza geopolitica e geografica rispetto ad una periferia incandescente come quella del Fronte Orientale rende il Paese vulnerabile all'infiltrazione delle narrative russe. Al contempo, gli ultimi sviluppi strategici stanno tentando di colmare questa lacuna.

Di contro, Bratislava si configura come piccola potenza periferica integrata nello spazio euro-atlantico e con margini di manovra limitati nei principali dossier geopolitici. Confinando direttamente con l'Ucraina, la Slovacchia è stata maggiormente bersagliata dalle narrative pro-Cremlino portando il Paese a sviluppare risposte strategiche ben prima rispetto all'Italia.

L'analisi comparata evidenzia che l'appartenenza comune a framework multilaterali non costituisce di per sé una garanzia di resilienza. La capacità di rispondere dipende dalla continuità dell'impegno politico. Tra i due Paesi, quello che attualmente dimostra maggior attenzione alla minaccia russa è sicuramente l'Italia tenendo conto che il 2025 è stato un anno molto negativo nei rapporti con Mosca. Tale tendenza è riconducibile all'evoluzione del conflitto in Ucraina, che ha congelato rapporti fino ad allora relativamente positivi nel periodo precedente al 2022. D'altro canto, la Slovacchia continua a perseguire una politica estera ambigua per difendere specifici interessi nazionali. Tuttavia, i costi reputazionali sono elevati in quanto Bratislava viene percepita dalle

principali cancellerie europee come irrilevante e inaffidabile. Perciò, non è pronosticabile, almeno nel breve-medio termine, un coordinamento strategico tra i due Paesi.

Cyberspazio e guerra ibrida: attori, tendenze e strategie di difesa nel dominio digitale europeo

di Anna Calabrese

Introduzione

Nel contesto della competizione strategica contemporanea, la nozione di minaccia ibrida ha progressivamente ampliato la portata dei discorsi sulla sicurezza oltre la dimensione strettamente militare, includendo azioni sinergiche e parallele nei domini fisici, digitali e cognitivi. Spesso condotte da attori statuali attraverso proxy non statali, queste operazioni hanno l'obiettivo di erodere la resilienza e la stabilità democratica degli avversari. In questo quadro, il conflitto si manifesta sempre più come una combinazione di ostilità convenzionale e strumenti non cinetici, confermando la centralità dello spazio cibernetico quale quinto dominio operativo, come sancito dal NATO Summit di Varsavia del 2016.

I dati più recenti confermano la rilevanza del fenomeno, in allarmante aumento a partire dai prodromi dell'invasione dell'Ucraina: secondo il Microsoft Digital Defense Report 2025, la Russia ha aumentato del 25% gli attacchi informatici contro gli Stati NATO nell'ultimo anno, colpendo in particolare settori governativi, infrastrutture critiche e servizi essenziali. L''Italia risulta tra i Paesi maggiormente bersagliati, con un incremento del 53% degli attacchi nel primo semestre 2025 rispetto all'anno precedente. In particolare, secondo la relazione

annuale del DIS relativa agli scenari futuri per la sicurezza nazionale, tra il 2024 e il 2025 gli attacchi contro il settore pubblico sono aumentati del 18%[1].

I recentissimi episodi come l'intrusione mirata nei sistemi del Ministero dell'Interno italiano che ha comportato l'esfiltrzione dei dati relativi a circa 5mila agenti della Digos[2], attribuito secondo alcune fonti a gruppi filo-cinesi, giustificano e spiegano la crescente preoccupazione sia a livello multilaterale che nazionale.

Da un lato diverse dichiarazioni rivelano un'incisività e assertività senza precedenti, come quella della Presidente della Commissione Europea Ursula von der Leyen che ad ottobre 2025 ha affermato che le azioni intraprese della Russia nei confronti dell'Europa fanno parte di "una campagna coerente e in *escalation* per destabilizzare i cittadini, mettere alla prova la nostra determinazione, dividere la nostra Unione", qualificandola con allarmante lucidità come una vera e propria guerra ibrida su vasta scala. Dall'altro, gli Stati Membri di Unione Europea e NATO avanzano riflessioni circa le proprie capacità e elaborano strategie per rispondere in maniera adeguata e resiliente alle cangianti forme della minaccia ibrida odierna. In questo solco si inserisce il Non-Paper presentato dal Ministro della Difesa Guido Crosetto di fronte al Consiglio Supremo di Difesa a novembre 2025, il quale si propone di identificare e analizzare i caratteri, i vettori e gli strumenti della minaccia sottosoglia nonché

[1] Presidenza del Consiglio dei Ministri, Dipartimento delle informazioni per la sicurezza, Relazione annuale sulla politica dell'informazione per la sicurezza, 2026, https://www.sicurezzanazionale.gov.it.

[2] Crescenzi, Chiara. "Attacco hacker cinese al Viminale: una violazione mirata per esfiltrare identità di agenti Digos." *Cybersecurity360*, 2026. https://www.cybersecurity360.it/cybersecurity-nazionale/attacco-hacker-cinese-al-viminale-una-violazione-mirata-per-esfiltrare-identita-di-agenti-digos/.

le debolezze del Sistema Paese al fine di rafforzare la postura strategica ma anche operativa della difesa italiana verso un approccio proattivo.

Il presente lavoro, muovendo dalla consapevolezza di estrema mutevolezza e ambiguità che aleggia attorno al concetto di minaccia ibrida, vuole allora indagarne le manifestazioni nello spazio cibernetico. Fornendo punti di riferimento circa le forme, gli attori e le nuove tendenze e delineando lo stato dell'arte della difesa cibernetica europea, si discuteranno altresì le questioni - operative ma anche dottrinali - ancora aperte, come la necessità di sviluppare capacità offensive di deterrenza e l'inquadramento giuridico della minaccia.

Inquadrare il fenomeno: le minacce cyber alla luce del rapporto ENISA 2025

L'ENISA (European Union Agency for Cybersecurity), agenzia che dal 2004 supporta Stati membri e istituzioni nel rafforzare la sicurezza informatica, la resilienza delle infrastrutture digitali e le capacità di risposta agli incidenti cyber, elabora annualmente una panoramica puntuale delle principali minacce cibernetiche in Europa. Essa mira ad individuare trend, attori e settori più colpiti e offrendo valutazioni e raccomandazioni operative per rafforzare la risposta nazionale e comune. Il Threat Landscape 2025 è stato redatto sulla base dei circa 4.900 incidenti che hanno colpito l'Unione tra luglio 2024 e giugno 2025 e riflette come il contesto delle minacce informatiche stia evolvendo verso pressioni di carattere misto e potenzialmente convergenti, con ridotti incidenti singoli ad alto impatto e campagne invece più continue e diversificate che, in perfetta linea con le manifestazioni della minaccia sottosoglia, erode la resilienza più che destabilizzare in maniera dirompente. Se sin dalle prime fasi dell'invasione russa dell'Ucraina nel 2022 e tra il 2022 e il 2024 si è assistito a una pluralità di attacchi informatici DDoS (Distributed Denial of Service), ransomware, defacement e sabotaggi contro infrastrutture critiche ucraine dal settore

energetico a quello dei trasporti e delle telecomunicazioni, con un incremento dalla prima alla seconda metà del 2024 del 48%[3], nel 2025 l'introduzione di nuovi elementi di minaccia e ostilità cibernetica sono una innegabile manifestazione di una distinzione tra spazio militare e civile che diventa sempre più labile e sfumata e in cui lo spazio geografico, specialmente nell'ambito cyber, non è più un limite bensì consente di trarre opportunità dall'a-territorialià. Sebbene si riconosca un incremento dei livelli di ostilità informatica legata al conflitto tra Kiev e Mosca e si affermi che nell'ultimo anno la Russia abbia aumentato del 25% gli attacchi informatici contro gli Stati NATO, con particolare attenzione al settore governativo e alle infrastrutture critiche[4], le conseguenze dell'attività informatica malevola si estendono ben oltre le sole contingenze conflittuali di specie. L'Europa è infatti costantemente presa di mira da gruppi di minaccia diversi ma convergenti[5], con l'Italia che si attesta circa il 10% di attacchi a livello globale, posizionandosi come una delle nazioni più colpite nei settori difesa e istituzioni pubbliche[6] [7].

L'origine della minaccia: una panoramica delle *state-aligned activities*

Negli ultimi trent'anni l'incremento esponenziale dell'accesso a Internet ha interessato anche le periferie globali, riducendo le distanze e conducendo a una

[3] State Service for Special Communications and Information Protection of Ukraine, "Russian Cyber Operations: Attack Automation, Espionage Against Defence Sector, and New Tactics—Analysis for the Second Half of 2024," April 30, 2025

[4] Microsoft Corporation, *Microsoft Digital Defense Report 2025: Safeguarding Trust in the AI Era*, (Redmond, WA: Microsoft Corporation, 2025), https://cdn-dynmedia-1.microsoft.com

[5] European Union Agency for Cybersecurity, "EU Consistently Targeted by Diverse yet Convergent Threat Groups," *ENISA*, 1 ottobre 2025, https://www.enisa.europa.eu/news/etl-2025-eu-consistently-targeted-by-diverse-yet-convergent-threat-groups

[6] "In Italia il 10,2% degli attacchi cyber mondiali. Difesa e istituzioni: +600% di attacchi in un anno." *Cybersec Italia*, 5 novembre 2025. https://www.cybersecitalia.it/in-italia-il-102-degli-attacchi-cyber-mondiali-difesa-e-istituzioni-600-di-attacchi-in-un-anno/54113/

[7] CLUSIT – Associazione Italiana per la Sicurezza Informatica. *Rapporto Clusit 2025 sulla cybersecurity in Italia e nel mondo*. Milano: CLUSIT, 2025. https://www.cybersecitalia.it/wp-content/uploads/2025/03/Rapporto_Clusit_03-2025_web.pdf.

progressiva “democratizzazione” delle competenze digitali[8]. Se in passato le competenze e le infrastrutture tecnologico-informatiche dipendevano da una sorta di “monopolio” statale, oggi la governance frammentata[9] e la struttura stessa del cyberspazio come mercato aperto consentono spazi di azione e opportunità a una diversità di attori, che in questo contesto vengono definiti Cyber Non State Actors (CNSA). Con questo termine si designano tipicamente individui ed altre entità che possono prendere forma di organizzazioni e istituzioni a livello globale, regionale o locale e che operano in maniera indipendente[10]. Se negli anni ‘80 e ‘90 gli incidenti cyber erano prevalentemente riconducibili a entità individuali non connesse ad autorità e responsabilità statale, il cyberspace è diventato progressivamente arena di confronto essenziale per la sovranità e la sicurezza nazionale. Il primo caso di “guerra digitale”[11] in Kosovo, dove azioni di gruppi come Black Hand[12] corruppero siti kosovo-albanesi e minacciarono il sabotaggio dell’infrastruttura informatica dei membri NATO, dimostra l’inizio di una tendenza di convergenza tra l’uso malevolo dello spazio cyber da parte dei CNSA e ambizioni strategiche nonché conflittuali degli Stati sovrani, poi culminatasi con gli attacchi in Estonia o il famoso Stuxnet, a presunta responsabilità statunitense e israeliana. Coerentemente, il Threat Landscape 2025 evidenzia infatti come anche per l’Europa le attività state-aligned rappresentino il segmento più sofisticato della minaccia cyber. Secondo

[8] Calabrese, A., Cyberwar e diritto internazionale: la frontiera digitale del conflitto armato tra principi umanitari, responsabilità e protezione dei civili, Università degli Studi di Torino, 2025.
[9] E-IR (Editorial Intelligence), “Global Cybersecurity Governance Is Fragmented—Get Over It”, online, 2021, disponibile su: e-ir.info
[10] COMITATO INTERNAZIONALE DELLA CROCE ROSSA (CICR), Glossario “Exploring Humanitarian Law (IHL)", Ginevra, 2021, disponibile su: icrc.org.
[11] Conoscenti, M., “Language Engineering and Media Management Strategies in Recent Wars”, Bulzoni, 2004, pp.1-22.
[12] Denning D.E., "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", Global Problem Solving Information Technology and Tools, December 10, 1999, nautilus.org.

ENISA, tra luglio 2024 e luglio 2025 il 7,2% degli incidenti associati a gruppi allineati a Stati ha colpito membri dell'UE, con una percentuale più elevata (32%) attribuibile alla Russia, seguita da Cina (24%), Corea del Nord (12%) e Iran (5.3%)[13]. Pur presentando similitudini e tratti comuni, le attività dei principali attori statuali mostrano pattern operativi differenziati per obiettivi e tecniche.

Gli intrusion sets riconducibili al nesso russo sono segnalati come più attivi nel periodo di riferimento, sintomo dell'attivismo informatico legato al conflitto in Ucraina. I settori più colpiti sono la pubblica amministrazione, con una sovrarappresentazione delle entità governative, diplomatiche, militari e dell'infrastruttura della difesa e digitale. Così come i target, anche la diffusione geografica dell'attività ricondotta a gruppi filo-russi evoca un chiaro collegamento delle ostilità informatiche al conflitto cinetico russo-ucraino e al sostegno degli Stati membri UE a Kiev: il targeting sembra infatti essere concentrato su Polonia, Francia, Germania e Belgio, paesi in prima linea per il supporto alla causa ucraina, con Berlino che si attesta il secondo posto per allocazione di armi pesanti dopo gli Stati Uniti[14] e Varsavia che gioca un ruolo cruciale come hub logistico, energetico e militare oltre che umanitario, spendendo circa il 7.54% del PIL per l'accoglienza di rifugiati[15].

Quanto alla Cina, il quadro indica una focalizzazione sui settori della PA, dei trasporti, della società civile e dell'infrastruttura digitale, con una particolare concentrazione su governi ed entità diplomatiche, industrie aeronautiche e marittime, ONG e organizzazioni per i diritti umani, nonché telecomunicazioni.

---

[13]European Union Agency for Cybersecurity, *ENISA Threat Landscape 2025* (Attica: ENISA, 2025), https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.

[14] Arianna Antezza et al., *Ukraine Support Tracker Data* (Kiel: Kiel Institute for the World Economy, dicembre 2025), https://www.kielinstitut.de/publications/ukraine-support-tracker-data-6453/.

[15]Ibidem.

Tale focus potrebbe spiegarsi con una strategia volta allo spionaggio, raccolta di dati strategici (si pensi alla già citata infiltrazione ai danni del DIS italiano) e furto di proprietà in linea con il Made in China 2025, programma decennale inaugurato nel 2015 che mira a porre fine alla dipendenza dalla tecnologia internazionale e potenziare la propria capacità industriale e la produzione intelligente, in settori chiave come robotica, attrezzature aerospaziali e aeronautiche; attrezzature per l'ingegneria oceanica e la navigazione ad alta tecnologia, veicoli a risparmio energetico[16]. Le campagne di cyberspionaggio sembrano essere concentrate in Italia, Germania, Francia e Belgio, realtà particolarmente interessanti per l'acquisizione tecnologica (manifattura avanzata europea, automotive, aerospazio e supply chain UE) e nodi logistici cruciali per la Belt and Road initiative (porti mediterrranei, hub aeroportuali come Anversa e reti ferroviarie e industriali europee).

Per quanto concerne gli intrusion set riconducibili alla Corea del Nord, in Europa essi sembrano orientati nuovamente in Belgio, Italia, Germania e Francia, con un forte interesse di gruppi parastatali come Lazarus e Famous Chollima nei confronti del settore privato e dei servizi finanziari, nonché delle criptovalute e asset tecnologici ad alto valore aggiunto. Si osserva un'insolita concentrazione dell'attività malevola di Pyongyang in Lussemburgo, il che sottolinea l'interesse prevalentemente finanziario dei target coreani: principale centro finanziario europeo e hub tecnologico oltre che sede delle maggiori banche internazionali e fondi di investimento, il Paese è un bersaglio appetibile per campagne di cyber-spionaggio e operazioni orientate alla generazione di entrate. La peculiarità dell'attività cibernetica nordcoreana risiede in una duplice logica: da un lato, la raccolta di intelligence e dati tecnologici di valore viene implementata attraverso

[16] Institute for Security and Development Policy, "Made in China 2025," *ISDP Backgrounder*, giugno 2018, https://www.isdp.eu/publication/made-china-2025/.

sofisticate campagne di social engineering e di infiltrazione professionale, attraverso le quali operatori legati al gruppo *Famous Chollima* cercano di ottenere impiego come sviluppatori o tecnici IT presso aziende occidentali, incluse imprese europee operanti nei settori della difesa o collegate ad enti governativi. Dall'altro, la generazione di risorse finanziarie[17] è direttamente collegato all'isolamento economico prodotto dal regime di sanzioni internazionali[18] e alla necessità di finanziare programmi strategici, in particolare missilistici e nucleari[19].

Infine, oltre ai principali attori sopracitati, il rapporto ENISA evidenzia attività cyber offensive riconducibili anche ad altri Paesi, tra cui India, Iran e attori privati offensivi (*private sector offensive actors*). Nel complesso, l'analisi delle attività cyber riconducibili ai diversi attori statuali evidenzia come ciascuno di essi tenda a orientare le proprie operazioni in funzione di priorità strategiche specifiche, sfruttando al contempo vulnerabilità settoriali e tecnologiche degli obiettivi individuati: i gruppi legati all'India, come *Bitter* e *SideWinder*, hanno condotto campagne di spear-phishing contro ambasciate dell'UE, probabilmente con l'obiettivo di raccogliere informazioni sulle posizioni europee in materia di sicurezza marittima, cooperazione nell'Indo-Pacifico e trasferimento tecnologico. Le attività riconducibili all'Iran risultano invece più limitate e concentrate su società civile, ONG e amministrazioni pubbliche, spesso per

---

[17] Sunha Bae, "Deterrence Under Pressure: Sustaining U.S.–ROK Cyber Cooperation Against North Korea," *Center for Strategic and International Studies (CSIS)*, 1 aprile 2025, https://www.csis.org/analysis/deterrence-under-pressure-sustaining-us-rok-cyber-cooperation-against-north-korea.

[18] United Nations Security Council, *Final Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)* (New York: United Nations, 2 marzo 2020), https://www.ncnk.org/sites/default/files/n2006067.pdf.

[19] GAID, "North Korea Funds Weapons With Cybercrime, U.N. Report Says," *GAID News*, 2025, https://www.gaid.org/news/news-blockchain-and-cryptocurrency/north-korea-funds-weapons-with-cybercrime-u-n-report-says .

monitorare opposizione[20] politica e dissidenti. Dunque, la profilazione degli attori riflette una logica di targeting mirato che combina interessi strategici, opportunità operative e vulnerabilità strutturali dei sistemi colpiti, rendendo l'analisi di tali pattern rilevante per anticipare minacce e rafforzare strategie di resilienza differenziate sulla base dei vettori di provenienza della minaccia.

Nuovi trend: integrazione dell'intelligenza artificiale, *supply chain* e vulnerabilità del *cloud*

Nonostante gli sforzi intrapresi negli ultimi anni e l'attenzione posta alla cyber sicurezza nella governance europea, nuovi trend di minaccia stanno ridefinendo il panorama della cyber defence. In primo luogo, l'Intelligenza Artificiale è diventata un elemento caratterizzante delle minacce cyber nel continente: lo sfruttamento dell'AI non si limita più al semplice supporto operativo, ma si configura come un elemento strutturale delle operazioni offensive, integrandosi in tutte le fasi della Cyber Kill Chain e fungendo da catalizzatore degli attacchi informatici, fino ad arrivare a generarli in modo autonomo. Secondo ENISA 2025, infatti, le campagne di phishing supportate dall'IA hanno rappresentato oltre l'80 %[21] delle attività di ingegneria sociale osservate all'inizio dell'anno. Inoltre, modelli commerciali di LLM vengono utilizzati ed addestrati per il supporto e l'assistenza per tecniche di ingegneria sociale. Ulteriore forma che lo sfruttamento cyber dell'IA assume è poi quella dell'automazione dei processi di individuazione delle gerarchie operative, protocolli e vulnerabilità dei target, particolarmente problematica per la tutela delle infrastrutture critiche, fino alla generazione di malware in grado di adattarsi in tempo reale alle difese

[20] Microsoft Threat Intelligence, "Iran Turning to Cyber-Enabled Influence Operations for Greater Effect," *Microsoft Security Insider*, 2 maggio 2023, https://www.microsoft.com/security/security-insider/intelligence-reports/iran-turning-to-cyber-enabled-influence-operations-for-greater-effect.

[21] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2025* (Attica: ENISA, 1 ottobre 2025), https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

(autonomous malware), reindirizzando i canali di *command and control* o riscrivendo automaticamente i *payload* per eludere i sistemi[22].

Il punto di svolta rappresenta però l'inserimento delle tecniche di automazione nelle fasi di delivery e attacco: l'uso dell'AI non si limita più all'assistenza decisionale, ma introduce un cambio di paradigma operativo, in cui sistemi intelligenti possono condurre autonomamente segmenti rilevanti degli attacchi informatici, relegando l'operatore umano a un ruolo marginale di supervisione: secondo le analisi, l'80–90% dell'intera campagna di *hacking* sarebbe stato gestito dall'AI, con l'essere umano coinvolto solo in pochi snodi decisionali critici (circa 4–6 per campagna)[23]. Un malware generato dall'IA, polimorfico e adattivo, modifica autonomamente il proprio codice in funzione del contesto operativo, elude i meccanismi di difesa, varia in tempo reale le tecniche di attacco e migliora progressivamente la propria efficacia; sebbene utilizzi tecniche familiari, la sua capacità di adattarsi rapidamente dopo un fallimento sposta significativamente l'equilibrio a favore degli attaccanti, complicando i processi di rilevamento, attribuzione e risposta difensiva.

Ulteriore tendenza che suggerisce un'urgente riflessione è il massiccio sfruttamento dell'interconnessione degli ecosistemi digitali moderni. Attacchi sempre più sofisticati mirano a minare la fiducia verso fornitori di servizi MSP (Managed Service Providers), soluzioni di monitoraggio e gestione remota, cloud e altri provider di servizi di terze parti[24]. L'obiettivo degli attaccanti è ottenere

---

[22] Timothy R. Dubber and Seth Lazar, "Military AI Cyber Agents (MAICAs) Constitute a Global Threat to Critical Infrastructure," arXiv, June 2025, https://arxiv.org.

[23] Anthropic, *Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign* (San Francisco: Anthropic, novembre 2025), https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf.

[24] Microsoft Corporation, *Microsoft Digital Defense Report 2025: Safeguarding Trust in the AI Era*, (Redmond, WA: Microsoft Corporation, 2025), https://cdn-dynmedia-1.microsoft.com.

accesso attraverso sistemi IT comunemente utilizzati e ritenuti affidabili, trasformando in punti di ingresso ciò che è percepito come infrastruttura sicura. La globalizzazione e la decentralizzazione delle supply chain, pur essendo vantaggiose sotto il profilo economico e della resilienza, diventano moltiplicatori di rischio. La distribuzione delle vulnerabilità, combinata con l'eterogeneità tecnologica (oltre che normativa), permette agli attacchi di propagarsi lungo tutta la catena, generando effetti a cascata che colpiscono sistemi critici e infrastrutture cloud interconnesse, la cui responsabilità è spesso impossibile da rintracciare. Gli aggressori sfruttano queste dinamiche per identificare i cosiddetti *points of failure*, massimizzando l'impatto delle loro operazioni.

Proprio per questo motivo, il cloud è diventato un'infrastruttura strategica estremamente concreta e "materiale". I recenti sviluppi della guerra in Iran offrono un esempio concreto: durante l'offensiva cinetico-cyber condotta da Stati Uniti e Israele ad inizio marzo, la temporanea interruzione di data center Amazon Web Services negli Emirati Arabi Uniti e in Bahrain[25] ha mostrato quanto un attacco fisico possa avere ripercussioni economiche e operative immediate, non solo nella regione colpita, ma anche sulle piattaforme globali che dipendono da queste infrastrutture. Questo episodio evidenzia come la resilienza del cloud e la continuità dei servizi critici siano direttamente collegate alla sicurezza nazionale e alla stabilità geopolitica. L'Unione Europea, in linea con la propria volontà politica di costruire un ecosistema di autonomia strategica su più fronti, ha certamente percepito la centralità del tema della sovranità digitale alla luce delle minacce a cui è sottoposta. Secondo diverse stime il 97,2% dei servizi cloud infrastrutturali e di piattaforma utilizzati nel mondo è erogato da

[25] Reuters, "Amazon Cloud Unit Flags Issues at Bahrain, UAE Data Centers Amid Iran Strikes," *Reuters*, March 2, 2026, https://www.reuters.com/world/middle-east/amazon-cloud-unit-flags-issues-bahrain-uae-data-centers-amid-iran-strikes-2026-03-02/.

hyperscaler statunitensi (83,7%) o cinesi (13,5%). I provider europei restano marginali, con una quota globale che non supera il 2,8%[26]. La Commissione europea ha quindi avviato iniziative per rafforzare la sovranità digitale del continente, promuovendo investimenti in data center, standard di interoperabilità e lo sviluppo di infrastrutture cloud sicure per la pubblica amministrazione e i dati critici. Nel 2025 Bruxelles ha infatti proposto un piano per triplicare la capacità dei data center UE, puntando su sostenibilità, sicurezza e riduzione della dipendenza dagli hyperscaler extra-UE[27]. Nonostante l'attivismo di Bruxelles e diverse stime che prevedono per le organizzazioni europee un raddoppio di spesa per IaaS (Infrastructure as a Service) nel cloud sovrano tra il 2025 e il 2026[28], le aziende hyperscale stanno adottando soluzioni per mantenere le proprie quote di mercato. AWS ha ad esempio promosso nel gennaio 2026[29] l'AWS European Sovereign Cloud, un'infrastruttura presentata come allineata alle esigenze europee di sovranità e autonomia, fisicamente localizzata nell'Unione Europea, con un primo nucleo in Germania, operata da personale europeo e dotata di una governance separata rispetto alle altre regioni AWS[30].

---

[26] Emanuele Villa, "Cloud europeo, tra sovranità digitale e sfida alle big tech," *Agenda Digitale*, 24 novembre 2025, https://www.agendadigitale.eu/infrastrutture/cloud-europeo-tra-sovranita-digitale-e-sfida-alle-big-tech/.

[27] European Commission, *AI Continent Action Plan*, Comunicazione COM(2025)165, 9 aprile 2025, https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan. (digital-strategy.ec.europa.eu).

[28] Maguire, J., "Gartner Forecasts Sharp Rise in Sovereign Cloud Investment, Led by Europe." *TechStrong IT*, 10 febbraio 2026. https://techstrong.it/featured/gartner-forecasts-sharp-rise-in-sovereign-cloud-investment-led-by-europe/.

[29] Amazon Web Services, "AWS Launches AWS European Sovereign Cloud and Announces Expansion Across Europe," *About Amazon Press Center*, 14 gennaio 2026, https://press.aboutamazon.com/aws/2026/1/aws-launches-aws-european-sovereign-cloud-and-announces-expansion-across-europe.

[30] Parravicini, F., "Sovranità digitale, AWS: 'European Sovereign Cloud modello di autonomia operativa'." *Corriere Comunicazioni*, 13 marzo 2026.

Alla stessa logica risponde l'EU Data Boundary di Microsoft[31]. La questione solleva però intricati nodi giuridici: sebbene l'infrastruttura sia formalmente sottoposta al diritto europeo, inclusi il Regolamento generale sulla protezione dei dati (GDPR)[32] e le normative nazionali degli Stati membri, il provider rimane una società statunitense. Questo introduce il potenziale conflitto con il U.S. CLOUD Act[33], la normativa americana che consente alle autorità statunitensi di richiedere dati a società con sede negli Stati Uniti anche se tali dati sono conservati all'estero. Nel corso di un'audizione davanti al Senato francese, il direttore legale di Microsoft Francia ha infatti riconosciuto che la società non può garantire in modo assoluto che i dati europei siano immuni da eventuali richieste delle autorità statunitensi.

Risposta europea: stato dell'arte e lacune

Di fronte a queste trasformazioni del panorama delle minacce, che mirano non solo a individui o organizzazioni, ma direttamente alla struttura digitale su cui si fondano le società moderne, emerge quindi la necessità di interrogarsi su quanto l'Unione Europea abbia già fatto in materia di cybersecurity e su quali ulteriori misure siano necessarie per rafforzare la propria capacità di difesa nel dominio digitale. Nell'ultimo decennio l'Unione Europea ha compiuto passi significativi verso una cyber governance più assertiva e integrata. A partire dalla direttiva NIS

---

https://www.corrierecomunicazioni.it/digital-economy/cloud/la-strategia-di-aws-per-coniugare-sovranita-europea-e-innovazione-globale/

[31] "Microsoft mette al sicuro i dati europei: completato l'EU Data Boundary," *HDblog*, 28 febbraio 2025, https://www.hdblog.it/microsoft/articoli/n610443/microsoft-eu-data-boundary-sicurezza-dati/.

[32] European Union, *Regolamento generale sulla protezione dei dati (GDPR)*, Regolamento (UE) 2016/679, 27 aprile 2016, EUR-Lex, https://eur-lex.europa.eu/IT/legal-content/summary/general-data-protection-regulation-gdpr.html.

[33] United States, *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, Division V of the *Consolidated Appropriations Act, 2018*, Public Law 115-141, 115th Cong., March 23, 2018, https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf.

del 2016[34], rafforzata con la NIS2 nel 2022, l'UE ha imposto requisiti minimi di sicurezza e obblighi di notifica per operatori di servizi essenziali e fornitori digitali, promuovendo una gestione del rischio più uniforme. La legislazione successiva, dal Cybersecurity Act del 2019 al Cyber Resilience Act, ha consolidato un approccio preventivo, estendendo obblighi di sicurezza "by design" a prodotti e servizi digitali, mentre strumenti come il Cyber Blueprint e le strategie settoriali hanno integrato aspetti tecnologici, industriali e di difesa. La visione di una cyber governance integrata è stata poi formalizzata nella "Strategia UE per la cybersicurezza nel decennio digitale"[35] presentata dalla Commissione nel 2020 e che propone un approccio unitario alla sicurezza digitale integrando dimensioni tecnologiche, industriali, normative e di difesa e ponendo al centro il concetto di cyber resilience, essenziale per garantire autonomia, legittimità e fiducia nel mercato digitale unico europeo. Parallelamente, la Commissione ha rafforzato la resilienza attraverso investimenti con Digital Europe, l'European Defence Fund e la promozione di standard comuni, consolidando il ruolo di ENISA nella supervisione e nel monitoraggio della sicurezza digitale europea.

Tuttavia, oltre la già citata vulnerabilità proveniente dalla dipendenza da fornitori extra UE per tecnologie strategiche[36], l'UE soffre dell'assenza di un vero approccio alla deterrenza. La postura comunitaria, infatti, resta ancora fortemente improntata alla reattività, mentre lo scenario operativo attuale

---

[34] European Commission. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union L 194/1 (19 July 2016).

[35] European Union, *Strategia dell'UE per la cibersicurezza*, Shaping Europe's Digital Future, 1 luglio 2025, https://digital-strategy.ec.europa.eu/it/policies/cybersecurity-strategy. (digital-strategy.ec.europa.eu).

[36] European Parliament, *Report on European technological sovereignty and digital infrastructure (A 10-0107/2025)*, European Parliament, 2025, https://www.europarl.europa.eu.

necessiterebbe una strategia programmatica e attiva-offensiva[37]. Anche il Libro Bianco sulla Difesa Europea dimostra tale consapevolezza sancendo che "Both defensive and offensive cyber capabilities are needed to ensure the protection and freedom of manoeuvre in cyberspace"[38], riconoscendo, in un'ottica odierna di militarizzazione del cyberspace, che la sola difesa non è sufficiente per proteggere gli interessi strategici dell'Unione e per mantenere credibilità e deterrenza nel dominio digitale. A livello degli Stati membri si osservano segnali concreti di evoluzione in tale direzione. La Germania, tradizionalmente cauta nelle operazioni offensive, sta rivedendo la propria postura di sicurezza digitale, con dichiarazioni politiche che prospettano la possibilità di colpire gli attaccanti e di adottare misure di risposta attiva nel cyberspazio contro minacce esterne, incluse azioni legislative per consentire interventi più proattivi contro hacker stranieri[39]. Anche Francia[40] e Paesi Bassi[41] hanno recentemente incluso capacità informatiche offensive nelle loro recenti strategie di sicurezza informatica, mentre il dibattito in Italia ha preso forma nell'ultimo anno. La strategia delineata dal Ministro della Difesa a fine 2025[42], si impernia attorno alla costruzione di una "arma cyber" articolata su un organico misto civile-militare,

---

[37] "From reactive to proactive: Europe's strategic shift in cyber defense," Benoît Chatelain, *Sopra Steria Defence & Security Blog*, June 20 2025, https://www.soprasteria.be.

[38] European Commission, *White Paper for European Defence – Readiness 2030* (Bruxelles: European Commission, 19 marzo 2025).

[39] POLITICO Europe, "Germany Prepares to Authorize Offensive Cyber Operations, or 'Hack-Back' Against Cyber Enemies," *POLITICO Europe*, 9 febbraio 2026, https://www.politico.eu/article/germany-prepares-hack-back-cyber-enemies/.

[40] Laudrain, A. P. B., "France's New Offensive Cyber Doctrine." *Lawfare*, 26 febbraio 2019. https://www.lawfaremedia.org/article/frances-new-offensive-cyber-doctrine.

[41] Netherlands Ministry of Defence. *Defensie Cyber Strategie 2025*. Den Haag: Ministerie van Defensie, 3 ottobre 2025. https://www.defensie.nl/documenten/2025/10/03/defensie-cyber-strategie-2025.

[42] *Il Sole 24 Ore*. "Dall'esercito cyber a un centro di guerra: ecco il piano di Crosetto contro le minacce ibride." *Il Sole 24 Ore*, 13 novembre 2025. https://www.ilsole24ore.com/art/dall-esercito-cyber-un-centro-guerra-ecco-piano-crosetto-contro-minacce-ibride%E2%80%91AHx11QiD.

con l'obiettivo di integrare capacità difensive e offensive in sinergia con alleati europei e NATO, riflettendo una visione che supera la pura reattività in favore di una deterrenza più efficace. L'auspicata e rinnovata postura italiana prevede non solo l'adozione di structuri operative specializzate (circa 1.200-1.500 unità operative) ma anche la necessità di un assetto normativo e di governance chiaro e flessibile, capace di accompagnare lo sviluppo tecnico-operativo e di assicurare coerenza e unità d'azione nelle capacità offensive, difensive e di resilienza nazionale[43].

Conclusioni

L'analisi condotta evidenzia come le minacce ibride contemporanee nel contesto cyber e le loro tendenze più attuali, dall'uso offensivo dell'intelligenza artificiale alla vulnerabilità delle supply chain e delle infrastrutture cloud, abbiano reso obsoleta una strategia di risposta puramente difensiva e reattiva. Nonostante i progressi normativi e operativi dell'UE negli ultimi anni, permangono lacune significative. L'Unione resta largamente dipendente da fornitori extra-europei per infrastrutture critiche e tecnologie strategiche basate sull'AI, e le capacità offensive integrate sono ancora limitate. Il Libro Bianco sulla Difesa Europea sottolinea la necessità di sviluppare capacità sia difensive sia offensive, per garantire libertà di manovra, deterrenza e proiezione di potenza nel cyberspazio. Questa sfida si estende in modo cruciale all'intelligenza artificiale, strumento dual-use la cui applicazione offensiva o difensiva può determinare l'equilibrio strategico nel dominio digitale. Per l'Europa, sviluppare piattaforme di threat detection e sistemi decisionali basati su IA europea significa costruire sovranità digitale e algoritmica, riducendo la dipendenza da tecnologie esterne e

[43] Calabrese, A., "Verso un'arma cyber nazionale: la strategia del Min. Crosetto nel contesto europeo." *Geopolitica.info*, 14 novembre 2025. https://www.geopolitica.info/strategia-cyber-crosetto/.

aumentando la resilienza complessiva. Se è realistico riconoscere che l'autonomia completa, ad esempio un cloud europeo totalmente indipendente, richiederà ancora tra i 10 e i 20 anni, diventa dunque fondamentale procedere con consapevolezza, assumendo il controllo delle proprie interdipendenze critiche e sviluppando un ecosistema digitale strategicamente autonomo, resiliente e interoperabile e supportato da una governance normativa flessibile e condivisa.

Allo stesso tempo, la leadership normativa dell'UE costituisce una sfida duplice: se da un lato essa posiziona l'Europa come standard setter globale, dall'altro la rende un bersaglio strategico: campagne malevole hanno sfruttato il brand e la percepita legittimità delle istituzioni europee, ENISA compresa, impersonando funzionari o eventi ufficiali per aumentare l'efficacia di phishing e malware mirati. Colpire sistemi regolamentati e formalmente affidabili amplifica l'impatto degli attacchi e mina la fiducia internazionale, rendendo la regolamentazione una doppia sfida. Per quanto necessaria, quest'ultima non deve quindi diventare vincolo: occorre conciliare l'autonomia tecnologica con quadri normativi flessibili, capaci di sostenere posture adattabili, garantendo così risposte efficaci in uno spazio cibernetico sempre più ibrido, competitivo e sofisticato.

La cyber difesa europea non può allora limitarsi ai tradizionali e convenzionali meccanismi e strumenti di protezione, che diventano velocemente obsoleti. Per trasformare la resilienza in reale capacità operativa nello spazio digitale, è indispensabile sviluppare infrastrutture sovrane, capacità tecnologiche autonome e sistemi di intelligenza artificiale europei, strumenti che garantiscano sicurezza, sovranità e proiezione strategica in un dominio ormai indispensabile alla competizione globale. A tale sviluppo deve affiancarsi un

quadro normativo chiaro e flessibile, che sostenga l'azione e la cooperazione europea senza limitarne l'efficacia di fronte a minacce ibride in continua evoluzione

Il fronte geo-economico della guerra ibrida: la filiera delle terre rare

di Lorenzo Rossi

Introduzione

Il *Non-Paper* del Ministro della Difesa Guido Crosetto, pubblicato nel novembre 2025, riconosce nella coercizione geo-economica uno delle modalità in cui la minaccia ibrida si manifesta, nonché riconducibile a quelle "azioni coordinate in più domini condotte da attori statuali e non-statuali, al di sotto della soglia del conflitto armato e spesso non attribuibili, mirate a danneggiare, destabilizzare o indebolire"[1].

Secondo il documento, la coercizione geo-economica "si manifesta attraverso l'uso di strumenti economici come leve di pressione politica e strategica"[2], ai quali uno Stato può ricorrere come leve di diplomazia coercitiva al fine di influenzare le scelte sovrane di un altro Stato.

I casi di pressione economica sono accomunati da due elementi ricorrenti*: in primis*, lo sfruttamento delle dipendenze economiche di uno Stato, sia esso economicamente *import* o *export-oriented*. In secondo luogo, il ricorso agli strumenti di politica commerciale come gli *export controls* a fini coercitivi[3].

---

[1] Crosetto, G. "Il contrasto alla guerra ibrida: una strategia attiva". Non-Paper del Ministro della Difesa Guido Crosetto, edizione novembre 2025, p. 1. https://www.difesa.it/assets/allegati/83696/nonpaper_il_contrasto_alla_guerra_ibrida.pdf

[2] *Ivi*, p. 34

[3] Frandi, N. "Coercizione economica: definizioni, casi reali e nuove prospettive nelle relazioni internazionali". Affari Internazionali, 16 settembre 2024. https://www.affarinternazionali.it/coercizione-economica-definizioni-casi-reali-e-nuove-prospettive-nelle-relazioni-internazionali/

In questo dominio, la Cina emerge come principale attore in grado di esercitare pressione, specie in settori vitali come la filiera delle terre rare. Negli ultimi tre decenni Pechino ha acquisito *de facto* il monopolio nell'estrazione e nella raffinazione dei minerali critici, ottenendo un controllo a monte della *supply chain*[4].

Questo garantisce al Dragone strumenti di influenza economica notevoli, dal momento che le terre rare costituiscono la spina dorsale di molti settori industriali, primo fra tutti quello dei semiconduttori: la prospettiva di un ipotetico e potenziale blocco, anche parziale, delle esportazioni risulterebbe pericoloso per svariati settori dell'economia.

Il ricorso a strumenti come gli *export controls*, la tentata acquisizione di *asset* strategici europei e la penetrazione in Africa rende Pechino il principale *competitor* economico-industriale dell'Italia e dell'Unione Europea.

Il presente elaborato propone una disamina sul vantaggio comparato della Cina nel settore delle terre rare attraverso le lenti della guerra ibrida e della coercizione geo-economica.

L'analisi verterà sulla vulnerabilità economico-strategica dell'Unione Europea nei confronti di Pechino, e di come l'organizzazione di una *supply chain* sicura per le terre rare costituisca una delle chiavi di volta dell'Autonomia Strategica Europea (ASE). Pertanto, verranno presi in considerazione i progetti e gli atti normativi varati in sede comunitaria al fine di comprendere la direzione intrapresa dai ventisette per fronteggiare tali fragilità e dipendenze strutturali.

[4] Rossi, L. "L'industria dei semiconduttori nell'era di Donald Trump: tra economia e sicurezza nazionale". Geopolitica.info, 7 aprile 2025. https://www.geopolitica.info/semiconduttori-usa-trump/

Terre rare e monopolio cinese: rischi e vulnerabilità strategiche per l'UE

L'industria e l'economia contemporanea non possono prescindere dall'utilizzo delle cosiddette "terre rare" o *Rare Earth Elements* (*REEs*), minerali che trovano applicazione in un ventaglio di attività manifatturiere che spazia dall'energia alla microelettronica.

Per "terre rare" si intende un gruppo di diciassette elementi, con particolari proprietà fisiche e chimiche, che li rendono adatti per la fabbricazione di componenti come magneti e microchip[5]. Tuttavia, l'aggettivo "rare" non implica la scarsità di questi elementi. Al contrario, sono presenti in grandi quantità nel sottosuolo terrestre. Ciò che conferisce il connotato della rarità è l'estrema difficoltà nei processi di estrazione e raffinazione, nonché gli ingenti costi a livello economico e ambientale. L'estrazione delle terre rare costituisce la fase iniziale di importanti filiere come quella dei semiconduttori: elementi come neodimio e disprosio sono indispensabili, ad esempio, per produrre microelettronica avanzata.

La filiera dei semiconduttori è estremamente complessa e frammentata: si parte dall'estrazione dei minerali critici, che avviene principalmente in Cina; la progettazione dei chip più avanzati avviene negli Stati Uniti e la loro fabbricazione a Taiwan, utilizzando macchinari di produzione olandese[6].

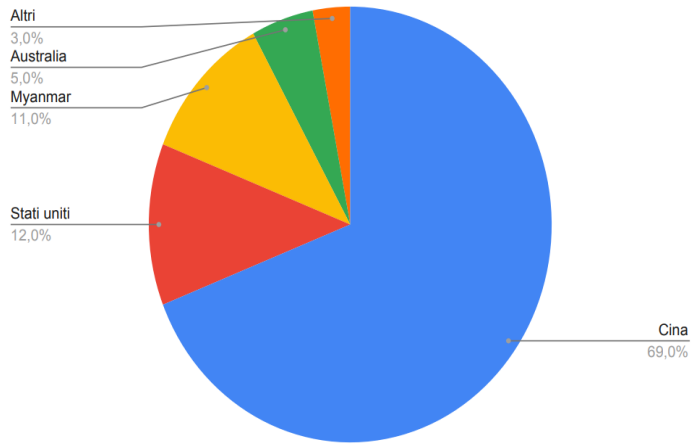
I processi di estrazione e raffinazione di *REEs* sono oggi un monopolio *de facto* di un singolo Paese: la Cina. Pechino controlla infatti una quota rilevante della lavorazione di questi minerali: nello specifico, il 69% dei processi di estrazione e

[5] American Geoscience Institute. "What are rare earth elements, and why are they important?". https://profession.americangeosciences.org/society/intersections/faq/what-are-rare-earth-elements-and-why-are-they-important/.

[6] Domizio L., Ribichini A. (a cura di). "Il Mondo e gli Occidenti: Sfide Globali alla Sicurezza Europea nel XXI secolo". Geopolitica.info, 16 giugno 2025, pp. 216-218 (Lorenzo Rossi). https://www.geopolitica.info/geopolitical-brief-51-il-mondo-e-gli-occidenti-sfide-globali-alla-sicurezza-europea-nel-xxi-secolo/.

il 90% di quelli di raffinazione[7]. A titolo di paragone, nel 2023 gli Stati Uniti si posizionavano al secondo posto per produzione di terre rare, ma con una quota di mercato globale del solo 12%, mentre altri Paesi occidentali, come l'Australia, si fermavano al 5%[8].

La notevole capacità produttiva è stata ottenuta grazie a decenni di politiche governative mirate e basso costo della manodopera, nonché di regolamentazioni ambientali lassiste e meno stringenti di quelle dei Paesi occidentali[9]. La celebre frase pronunciata da Deng Xiaoping nel 1992 esemplifica la direzione già da allora intrapresa dal Partito Comunista Cinese: "Il Medio Oriente ha il petrolio, la Cina ha le terre rare"[10].



Paesi produttori di terre rare, 2023. Fonte: Polytechnique Insights[11].

[7] European Parliament Think Thank. "China's rare earth export restrictions". 24 novembre 2025. https://epthinktank.eu/2025/11/24/chinas-rare-earth-export-restrictions/.
[8] Xémard, M. " China has a monopoly on rare earth materials". Polytechnique Insights, 29 gennaio 2025. https://www.polytechnique-insights.com/en/columns/geopolitics/china-has-a-monopoly-on-rare-earths/
[9] Feng, E. "How China came to rule the world of rare earth elements". NPR, 23 luglio 2025. https://www.npr.org/2025/07/23/nx-s1-5475137/china-rare-earth-elements.
[10] Hearty, Alam. "Rare earths: Next Element in the trade war?". Center for Strategic & International Studies (CSIS), 20 agosto 2019. https://www.csis.org/analysis/rare-earths-next-element-trade-war.
[11] Xémard, M. " China has a monopoly on rare earth materials". Polytechnique Insights, 29 gennaio 2025. https://www.polytechnique-insights.com/en/columns/geopolitics/china-has-a-monopoly-on-rare-earths/.

Se fino agli anni ’80 gli Stati Uniti detenevano il primato nell’estrazione dei minerali critici, questo è stato perso a favore della Cina negli anni ’90 a causa della concorrenza aggressiva e del *dumping* sui prezzi[12]. Simbolo del sorpasso è stata la chiusura della miniera di Mountain Pass in California nel 2002, con la parentesi di riapertura nel 2017 per tentare di recuperare il divario strategico e produttivo[13].

Il rafforzamento dell’industria estrattiva è stato incluso anche nel piano industriale quinquennale *Made in China 2025*, lanciato nel 2015 con l’obiettivo di rendere la Cina autosufficiente nella produzione di componenti ad alta tecnologia[14]. Se, a distanza di un decennio, il *core goal* del progetto non può dirsi raggiunto (la Cina è lontana dall’autosufficienza produttiva e tecnologica, specie per i microchip di ultima generazione, per i quali gli Stati Uniti detengono ancora il primato della progettazione e Taiwan della produzione)[15], lo stesso non può dirsi per la lavorazione delle terre rare.

Il quadro appena descritto delinea chiaramente un vantaggio comparato cinese in questo settore, il quale, prendendo in considerazione le esigue capacità produttive dei *competitor*, assume le vesti di un monopolio economico. Le ripercussioni di tale asimmetria non si limitano però alla mera sfera economica. Una situazione di monopolio garantisce senza dubbio vantaggi nella fissazione dei prezzi e nella gestione dell’offerta, ma influisce in larga parte sulle dinamiche

[12] Ibidem
[13] MP Materials. “Mountain Pass History”. https://mpmaterials.com/history/.
[14] Crebo-Rediker, Khan. “Leapfrogging China’s critical minerals dominance”. Council of Foreign Relations (CFR), febbraio 2026. https://www.cfr.org/reports/leapfrogging-chinas-critical-minerals-dominance.
[15] Domizio L., Ribichini A. (a cura di). “Il Mondo e gli Occidenti: Sfide Globali alla Sicurezza Europea nel XXI secolo”. Geopolitica.info, 16 giugno 2025, p. 222 (Lorenzo Rossi). https://www.geopolitica.info/geopolitical-brief-51-il-mondo-e-gli-occidenti-sfide-globali-alla-sicurezza-europea-nel-xxi-secolo/.

di potere nelle relazioni internazionali, costituendo uno strumento di coercizione geopolitica alternativo alla forza militare.

Negli ultimi due decenni si è assistito ad una deriva securitaria dei rapporti commerciali globali, comportando un legame sempre più stretto tra economia e sicurezza nazionale[16] e introducendo un paradigma opposto a quello affermatosi durante la globalizzazione del 1945-1989 e della successiva 1989-2008. Il *trend* dominante infatti non risulta più essere l'apertura dei mercati, ma la corsa alla messa in sicurezza delle *supply chain* e il disaccoppiamento delle catene globali del valore.

La filiera delle terre rare è esemplare in questo senso: senza questi minerali le industrie della difesa verrebbero paralizzate, con conseguenze esiziali per le capacità militari dei Paesi colpiti. Per tale motivo i maggiori Paesi avanzati stanno cercando di ridurre le proprie dipendenze dalle filiere globali, dalla Cina e dai suoi minerali *in primis*, specie dopo casi di *weaponization* del commercio attuati da Pechino negli anni passati[17].

Il caso più noto è sicuramente la crisi sino-giapponese del 2010, scoppiata in seguito all'arresto di due membri dell'equipaggio di un peschereccio cinese da parte della Guardia Costiera nipponica al largo delle isole Senkaku, sotto sovranità di Tokyo ma reclamate da Pechino. In reazione all'arresto, la Cina bloccò l'export di terre rare verso il Giappone, causando seri danni economici. Di conseguenza, le autorità nipponiche furono costrette a rilasciare i marinai

[16] Frandi, N. "Coercizione economica: definizioni, casi reali e nuove prospettive nelle relazioni internazionali". Affari Internazionali, 16 settembre 2024. https://www.affarinternazionali.it/coercizione-economica-definizioni-casi-reali-e-nuove-prospettive-nelle-relazioni-internazionali/.

[17] Domizio L., Ribichini A. (a cura di). "Il Mondo e gli Occidenti: Sfide Globali alla Sicurezza Europea nel XXI secolo". Geopolitica.info, 16 giugno 2025, pp. 224-226 (Lorenzo Rossi). https://www.geopolitica.info/geopolitical-brief-51-il-mondo-e-gli-occidenti-sfide-globali-alla-sicurezza-europea-nel-xxi-secolo/.

cinesi[18]. Nel fatto possono essere rintracciati i due connotati della coercizione geo-economica: esercizio di pressione politica e diplomatica tramite strumenti di politica commerciale sfruttando le dipendenze di un Paese.

Il caso più recente di ricorso alla leva geo-economica è invece l'introduzione nel 2025 di due pacchetti di controlli sull'esportazione di terre rare verso gli Stati Uniti, in risposta ai dazi imposti dall'Amministrazione Trump. In particolare, con l'introduzione dei controlli gli esportatori sono obbligati ad ottenere una licenza e a rilasciare informazioni, spesso ritenute sensibili, sugli utilizzatori finali dei minerali. Inoltre, il governo di Pechino ha esteso l'obbligatorietà di licenza anche per tutte quelle aziende che fabbricano prodotti utilizzando minerali critici (perlopiù magneti) per la vendita finale. Risulta chiaro che ciò implicherebbe l'extraterritorialità della legge cinese e un controllo capillare della filiera da parte di Pechino[19].

Sebbene queste misure non si configurino come un blocco vero e proprio, garantiscono di fatto alla Cina un controllo ancora più esteso sulla filiera, con la possibilità di accedere a informazioni sensibili o escludere direttamente un'azienda dalle fonti di approvvigionamento.

Pechino potrebbe sfruttare la propria posizione per ottenere concessioni di natura commerciale e tecnologia, incentivando le aziende specializzate nelle *cutting-edge technologies* a trasferirsi in Cina per garantirsi l'accesso alle forniture[20].

---

[18] Terazawa, T. "How Japan solved its rare earth minerals dependency issue". World Economic Forum, 13 ottobre 2023. https://www.weforum.org/stories/2023/10/japan-rare-earth-minerals/.

[19] European Parliament Think Thank. "China's rare earth export restrictions". 24 novembre 2025. https://epthinktank.eu/2025/11/24/chinas-rare-earth-export-restrictions/.

[20] Dans, E. "How to loosen China's strangehold on Rare Earths". Center for European Policy Analysis, (CEPA), 14 ottobre 2025. https://cepa.org/article/how-to-loosen-chinas-stranglehold-on-rare-earths/.

La dipendenza dalle terre rare prodotte in Cina rientra, dunque, nel concetto di minaccia ibrida, intesa come azione ostile al di sotto della soglia armata per arrecare danni a un Paese, in questo caso sotto la sfera della sicurezza economica, industriale e, per estensione, quella militare.

Sicurezza delle *supply chain*: i piani strategici dell'Unione Europea

Il monopolio cinese sulle terre rare e il rischio di *weaponization* della filiera pongono dei seri rischi per la sicurezza economica dell'Unione Europea, il cui tessuto produttivo risulta essere quasi totalmente dipendente dalle importazioni di minerali critici da Pechino.

Stando alle cifre più recenti, l'Unione Europea importa l'85% delle terre rare pesanti e leggere dalla Cina, oltre al 90% dei magneti[21]. L'economia europea è fortemente integrata con le catene globali del valore delle terre rare e dei semiconduttori: da uno studio della BCE[22] emerge come l'80% delle grandi aziende continentali sia collegata da meno di tre interlocutori ai produttori cinesi di *REEs*.

Questa forte integrazione pone i Paesi UE in una posizione di forte vulnerabilità in settori vitali per il tessuto produttivo europeo come l'*automotive*, l'energia, l'elettronica e soprattutto l'industria della difesa. Le materie prime critiche contribuiscono a 3,9 trilioni di euro di produzione industriale, il 22% del PIL dell'Unione Europea[23].

---

[21] European Parliament Think Thank. "China's rare earth export restrictions". 24 novembre 2025. https://epthinktank.eu/2025/11/24/chinas-rare-earth-export-restrictions/.
[22] Ibidem
[23] Iren. "Materie prime critiche: con un 2,6 miliardi di euro di investimenti l'Italia coprirebbe il 66% del fabbisogno nazionale. L'inserimento nel Piano Mattei di progetti di riciclo RAEE porterebbe una valorizzazione delle materie prime critiche per altri 2,5 miliardi di euro". 5

A Pechino basterebbe un'intensificazione degli *export-controls* per creare seri disagi alla filiera e all'economia, provocando un aumento dei prezzi e ritardi di consegna, complice le esigue riserve di materiali da parte delle grandi aziende europee[24]. Una tale configurazione metterebbe a rischio la transizione *green* e digitale, il riarmo e, in ultima istanza, il conseguimento di una reale e completa Autonomia Strategica Europea (ASE).

I rischi derivanti la dipendenza pressoché totale dall'*import* cinese hanno portato le istituzioni europee all'elaborazione di piani strategici per limitare le vulnerabilità e l'esposizione dell'economia continentale a interruzioni della *supply chain* e a *shock* geopolitici.

La *policy* comunitaria ruota attorno a tre progetti: la *European Raw Materials Alliance* (ERMA, 2020), il *Critical Raw Materials Act* (CRMA, 2024), e il programma *RESourceEU* (2025)[25].

Il CRMA, oltre a identificare i minerali critici, definisce il quadro degli obiettivi che l'Unione Europea intende conseguire entro il 2030 per mitigare la propria dipendenza dalla filiera dei *REEs*. Nel dettaglio, il regolamento fissa dei *benchmark* per le materie prime strategiche, ponendo obiettivi come l'estrazione di un minimo del 10% del fabbisogno di minerali critici sul suolo europeo, il riciclo di una quota del 25% e soprattutto che non più del 65% delle terre rare provenga da un singolo Paese. Oltre a ciò, il CRMA mira a diversificare le fonti di approvvigionamento tramite accordi commerciali e *partnership* strategiche[26].

———

novembre 2025. https://www.gruppoiren.it/it/media/comunicati-stampa/2025/Materie-prime-critiche-2,6-miliardi-di-euro-di-investimenti-per-coprire-il-fabbisogno-italiano.html.

[24] European Parliament Think Thank. "China's rare earth export restrictions". 24 novembre 2025. https://epthinktank.eu/2025/11/24/chinas-rare-earth-export-restrictions/.

[25] Ibidem.

[26] European Commission. "Critical Raw Materials act". https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials/critical-raw-materials-act_en.

Il CRMA funge da politica industriale di coordinamento, atta a fissare obiettivi e standard comuni, mentre il programma *RESourceEU* (lanciato a fine 2025) è l'*action plan* che prevede lo stanziamento di fondi strutturali necessari al raggiungimento di tali obiettivi. Fondi che ammonterebbero a tre miliardi di euro per finanziare i progetti strategici[27].

Secondo la lettura di McNamara, il varo di simili piani strategici orientati a obiettivi geopolitici ha segnato un cambiamento nell'approccio delle istituzioni europee in economia, ossia l'abbandono dell'approccio neoliberale a favore di strumenti tipici della politica industriale con il fine di rendere l'UE un attore *market-maker* attivo e non solo un soggetto regolatore del mercato[28].

Infine, un meccanismo di difesa fondamentale in campo economico è rappresentato dallo strumento anti-coercizione (ACI), entrato in vigore nel 2023 e definito informalmente "*bazooka* economico". L'ACI permetterebbe di adottare contromisure (come restrizioni all'ingresso nel mercato unico di determinate merci) al fine di reagire a eventuali tentativi di coercizione economica. Nell'eventualità che la Cina minacci o introduca restrizioni all'export di terre rare per danneggiare i Paesi UE, l'uso del *bazooka* è una delle opzioni sul tavolo[29].

---

[27]European Commission. "RESourceEU Action Plan". https://single-market-economy.ec.europa.eu/document/download/e9ac2181-0dc7-4e61-a964-ba0a39c2aea8_en.

[28] Simoni, M. "Il ritorno della politica industriale in Italia e in Europa: questioni aperte di *political economy*". Confindustria, Rivista di politica economica, Sistema Italia 2025, pp. 136-137. https://public.confindustria.it/repository/2025/06/30122212/rivista-sistema-italia-2025-rivista-sistema-italia_VII_simoni.pdf.

[29] Wunnerlich, Wright. "The EU's anti coertion system". German Marshall Fund (GMF), 3 febbraio 2026. https://www.gmfus.org/news/eus-anti-coercion-instrument#:~:text=Discussions%20about%20an%20ACI%20first,not%20to%20use%20Lithuanian%20components.

Nonostante rappresentino uno spartiacque importante, i piani UE hanno suscitato perplessità circa l'efficacia e la probabilità di raggiungere gli obiettivi fissati entro il 2030.

Secondo un *report* della *European Court of Auditors* (ECA)[30], né i tentativi di disaccoppiamento né quelli di diversificazione hanno finora mostrato evidenze di successo.

Le capacità di riciclaggio rimangono al di sotto del 5% del fabbisogno, mentre il *target* fissato è del 25%. I finanziamenti erogati dall'Unione restano insufficienti per sviluppare progetti strutturali dedicati all'estrazione, alla raffinazione e al riciclaggio, con conseguenti ritardi[31].

La scoperta del più grande giacimento di terre rare a Kiruna, in Svezia, nel 2023 rappresenta certamente un'occasione per gli obiettivi concernenti l'estrazione, ma affinché entri in funzione occorreranno tra i dieci e i quindici anni, ben al di là della *deadline* fissata dal CRMA[32].

L'agenda europea parte dunque in salita, a causa di lacune strutturali e dipendenze di radice pluriennale dalle catene globali del valore, che espongono gli Stati membri a *shock* geopolitici e ricatti economici. Contemporaneamente, la domanda di minerali critici tenderà ad aumentare nei prossimi anni a causa dei processi di transizione verde e di riarmo. La diversificazione e il rafforzamento

---

[30] Nikolov. K. "EU vulnerable to critical raw materials shock despite flagship law, auditors warn". EUalive, 9 febbraio 2026. https://eualive.net/eu-vulnerable-to-critical-raw-materials-shock-despite-flagship-law-auditors-warn/#:~:text=The%20Critical%20Raw%20Materials%20Act,%2C%20barite%2C%20tungsten%20and%20others.

[31] Ibidem.

[32] LKAB Minerals. "Delivering critical materials and rare earth elements – a realistic vision?". 29 settembre 2023, https://www.lkabminerals.com/news/critical-minerals/#:~:text=How%20do%20we%20get%20started,and%20create%20modern%2C%20safe%20mines.

delle *supply chain* rimangono essenziali per ridurre la vulnerabilità del continente.

Secondo il Jacques Delors Centre[33], la Commissione dovrebbe puntare ulteriormente su *partnership* strategiche e progetti in collaborazione con Paesi partner, finanziando progetti sulla scia del progetto *Global Gateway*. Inoltre, andrebbero rafforzate le reti di investimento e i fondi a disposizione per realizzare progetti, che sono per loro natura *capital intensive*.

Infine, risulta fondamentale il dialogo tra istituzioni e grandi aziende, per spingere queste ultime a diversificare le proprie fonti di approvvigionamento. A titolo di esempio, i produttori europei importano oggi il 98% delle terre rare dalla Cina, nonostante la presenza di fonti alternative. La ricerca di partner alternativi è un passo decisivo verso il *derisking*[34]. Nel 2025 la Commissione Europea[35] ha redatto una lista di 13 progetti strategici, identificando potenziali partner funzionali alla diversificazione delle catene di approvvigionamento delle materie prime. Nei fornitori ipotetici di terre rare rientrano Paesi come il Canada per il Gallio, materiale importato per il 73% dalla Cina nel 2023[36].

I progetti europei hanno portato l'Italia a muoversi verso una politica coerente sulle materie prime critiche. Sulla scia del CRMA, il Comitato Interministeriale per la Transizione Ecologica (CITE) ha varato il Piano Nazionale di Esplorazione

---

[33] Findeisen, Wernert. "Meeting the costs of resilience: the EU's critical raw materials strategy must go to the extra kilometer". Hertie School, Jacques Delors Centre. https://www.delorscentre.eu/en/publications/eu-critical-raw-materials.

[34] Ibidem.

[35] European Commission. "Commssion selects 13 Strategic Projects in third countries to secure access to raw materials and to support local value creation". 4 giugno 2025. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1419.

[36] Eurostat. "International trade in critical raw materials". Giugno 2025. https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=655661&utm_source=chatgpt.com#:~:text=For%20its%20imports%20of%20gallium,Antimony.

mineraria (PNE), con l'obiettivo di fissare una strategia mineraria italiana e sfruttare le potenzialità del sottosuolo nazionale. L'iniziativa è stata finanziata con 3,5 milioni di euro, si articola in 14 progetti e si concentra sulle materie critiche individuate dall'Unione Europea[37]. Per l'Italia, la via verso il rafforzamento della filiera passa soprattutto attraverso i processi di recupero delle terre rare dai rifiuti elettronici: con un investimento di circa 2,6 miliardi di euro nella filiera del riciclaggio l'Italia potrebbe coprire il 66% del fabbisogno di nazionale di materie prime critiche. Attraverso il Piano Mattei l'Italia potrebbe sfruttare la notevole quantità di rifiuti elettronici prodotti in Nord Africa (42% dell'intero continente), per un valore prodotto di circa 2,5 miliardi di euro. Per l'Italia un disegno strategico coerente con quello europeo si rivela fondamentale soprattutto alla luce del contributo delle materie prime critiche e delle tecnologie derivate al PIL nazionale, cifra stimata attorno al 31%[38].

La posizione italiana sui minerali critici trova l'appoggio della Germania: in un documento strategico inviato alla Commissione Europea nel febbraio 2026, firmato dal Ministro degli Esteri Tajani e dall'omologo tedesco Wadephul, si sottolinea l'importanza della collaborazione dell'UE con gli Stati Uniti, con i partner africani, dell'America Latina e dell'Indo-Pacifico per costruire partenariati vantaggiosi e rafforzare le capacità di stoccaggio, riciclo e innovazione tecnologica in Europa[39].

---

[37] Petrone, A. "Miniere in Italia: parte il Programma Nazionale di Esplorazione". Rinnovabili, 1° luglio 2025. https://www.rinnovabili.it/mercato/politiche-e-normativa/miniere-in-italia-programma-nazionale-di-esplorazione/.

[38] Iren. "Materie prime critiche: con un 2,6 miliardi di euro di investimenti l'Italia coprirebbe il 66% del fabbisogno nazionale. L'inserimento nel Piano Mattei di progetti di riciclo RAEE porterebbe una valorizzazione delle materie prime critiche per altri 2,5 miliardi di euro". 5 novembre 2025. https://www.gruppoiren.it/it/media/comunicati-stampa/2025/Materie-prime-critiche-2,6-miliardi-di-euro-di-investimenti-per-coprire-il-fabbisogno-italiano.html.

[39] Ministero degli Affari Esteri e della Cooperazione Internazionale. "Minerali critici: documento strategico di Italia e Germania alla Commissione UE". 3 febbraio 2026.

Conclusioni

L'ultimo decennio ha visto un'inversione dei processi di apertura dei mercati e dell'integrazione delle economie globali, un fenomeno noto come *deglobalisation*[40]. Economia e sicurezza nazionale non vengono più considerate come sfere separate, e uno dei fattori che ha comportato questo cambio di paradigma sono le minacce geo-economiche.

La coercizione geo-economica, rientra tra le forme assunte dalla cosiddetta minaccia ibrida in quanto utilizza strumenti non convenzionali e sotto la soglia tradizionale di forza (restrizioni commerciali, controlli alle esportazioni, sanzioni mirate o manipolazione delle catene di approvvigionamento) per perseguire finalità strategiche e geopolitiche, ottenendo effetti destabilizzanti e profondi paragonabili a quelli di minacce più convenzionali e incidendo su stabilità economica, tenuta sociale e sicurezza dei soggetti statali colpiti.

I processi di *outsourcing* e *offshoring* hanno reso i Paesi avanzati vulnerabili alla notevole capacità produttiva della Cina nel settore dei minerali critici, essenziali per il tessuto economico-industriale, per l'innovazione e l'intelligenza artificiale. Un'interruzione delle forniture, un blocco parziale o ritardi di consegna getterebbero nel *caos* le economie colpite, con ricadute in settori collegati come la difesa. Questo comporta una compromissione delle capacità di risposta ad una minaccia, nonché la difficoltà nel raggiungimento dell'autonomia strategica, centrale nell'agenda europea.

A partire dal 2020, poi con la guerra in Ucraina e con la crescente aggressività cinese le istituzioni europee sono state costrette a ripensare il proprio ruolo: da

---

https://www.esteri.it/it/sala_stampa/archivionotizie/comunicati/2026/02/minerali-critici-documento-strategico-di-italia-e-germania-alla-commissione-ue/.

[40] Keller, Malord. "Deglobalisation: what you need to know". World economic Forum, 17 gennaio 2023. https://www.weforum.org/stories/2023/01/deglobalisation-what-you-need-to-know-wef23/.

regolatore di mercato a promotore di politiche industriali *mission-oriented* al fine di mutare la struttura dell'economia a favore di una maggiore resilienza e una dipendenza mitigata da Pechino.

Nonostante ciò, i piani strategici di Bruxelles presentano lacune non trascurabili, a partire dall'insufficienza di fondi e la mancata diversificazione delle fonti di approvvigionamento.

Un'azione più decisa da parte della Commissione e delle istituzioni può, senza dubbio, accelerare il processo di *derisking* e messa in sicurezza delle *supply chain* e, in ultima istanza, giocare da tassello fondamentale per l'Autonomia Strategica Europea.

L'Underwater come dimensione della sicurezza nazionale

di Alessandro Paolinelli e Annalaura Di Michele

Introduzione

Il mare è uno spazio di opportunità e una risorsa vitale per la prosperità e la sicurezza di un Paese. Oggi questo spazio politico non può più essere considerato separato dalle dinamiche relative alla sicurezza nazionale, poiché esso si sta progressivamente configurando come uno strumento integrante della *Grand Strategy*. In questo scenario, la difesa deve evolvere per contrastare non solo minacce convenzionali, ma anche aggressioni non convenzionali nel quadrante subacqueo. La presente analisi intende dunque esaminare la natura delle operazioni ibride nel dominio *underwater*, evidenziando come lo spazio sottomarino sia divenuto un fronte critico per la sicurezza dello Stato.

Nella prima sezione verrà analizzato l'ambiente marittimo, ponendo particolare attenzione ai suoi elementi costitutivi e alle caratteristiche che lo rendono un dominio strategico. Il *maritime domain* rappresenta infatti uno dei principali ambiti nei quali lo Stato ha il dovere di garantire sviluppo, protezione e sicurezza dei propri *asset*. Verrà inoltre illustrato come la difesa marittima contribuisca non solo alla sicurezza nazionale, ma anche alla tutela delle attività economiche legate al mare, generando un flusso di protezione e di ricchezza che può essere inteso come un ponte tra resilienza e sviluppo economico. In questo quadro, il dominio marittimo emerge come un vero e proprio fronte di competizione ibrida.

Nella seconda sezione l'analisi si concentrerà sul ruolo delle infrastrutture critiche connesse all'ambiente subacqueo, quali i cavi sottomarini in fibra ottica, le piattaforme energetiche *offshore* e i *terminal* portuali. Queste infrastrutture costituiscono l'ossatura del funzionamento di un Paese, ma al tempo stesso

rappresentano obiettivi privilegiati per le minacce ibride. Il loro danneggiamento o la loro compromissione possono infatti generare effetti significativi sulla sicurezza, sull'economia e sul benessere complessivo del Sistema Paese. L'analisi prenderà in esame i contesti strategici in cui tali infrastrutture sono inserite, nonché le sfide tecnologiche e industriali legate alla loro protezione negli abissi marini e alle risorse ad esse associate.

Delineato il quadro teorico e funzionale dell'*underwater domain*, l'analisi si focalizza sulle modalità di sabotaggio delle infrastrutture sommerse condotte secondo il paradigma della *plausible deniability*. Attraverso l'esame di vettori eterogenei, dalle *backdoors* informatiche e le compromissioni della *supply chain*, fino ai danneggiamenti fisici tramite reti a strascico, si intende mappare i fattori che trasformano un incidente tecnico in un atto di *guerra ibrida*. L'obiettivo non è fornire soluzioni univoche, bensì inquadrare l'opacità dell'ambiente sottomarino come un *battlespace* in cui il confine tra coincidenza e aggressione deliberata risulta strategicamente sfumato.

I restringimenti del traffico per mare segnano passaggi di significativo valore geostrategico anche al di sotto dello specchio d'acqua. Ci impegniamo qui ad esaminare quali siano le possibili modalità attraverso cui le strozzature del commercio marittimo internazionale, attraverso le loro peculiarità correlate ai fondali, siano elementi di proiezione di una sovranità sottomarina verso la superficie e gli Stati rivieraschi. Così lo spazio subacqueo appare come una nuova frontiera degli equilibri e dei rapporti con l'Oriente se si pensa all'iniziativa *IMEC* in controbilanciamento della *Belt and Road Initiative* cinese. Un particolare occhio di riguardo si rivolge anche alle rotte artiche.

Il dominio marittimo quale nuova frontiera della competizione ibrida

Oggigiorno l'ambiente marittimo si presenta come uno dei domini strategicamente più rilevanti dello scenario contemporaneo, strettamente connesso al fronte cibernetico. Non a caso, il mare è oramai sempre più inteso come uno spazio di guerra illimitata che si apre al *cyber*. Come direbbe Carl Schmitt, il mare non ha confini[1], e questo concetto, attualizzato all'età contemporanea, produce una condizione di guerra permanente e normalizzata in cui diritto internazionale si svuota di peso e di significato.

In ottica contemporanea, il mare si prefigura come un ecosistema ibrido in cui si è realizzata una sovrapposizione dei domini, in cui gli schemi tradizionali si sono fusi perfettamente con le attuali minacce ibride nel campo cyber, in quanto anche il mare dipende dalle tecnologie non convenzionali e *dual use*. L'ambiente marittimo è composto dallo spazio fisico, dalle risorse naturali essenziali per la sicurezza energetica e alimentare degli Stati, dalle infrastrutture critiche da esso ospitate e dagli attori, statali o non statali. La complessità dell'ambiente marittimo rende il suo dominio esclusivo difficilmente praticabile, ma al tempo stesso essenziale per la proiezione di potere e per la prosperità economica.

Il mare è strategico perché consente un'elevata mobilità. Infatti, oltre l'80% del commercio mondiale viaggia via mare. Controllare o proteggere le rotte significa garantire la continuità delle catene di approvvigionamento[2]. Tuttavia, gli attacchi alle rotte del Mar Rosso e l'instabilità strutturale del Mediterraneo dimostrano come la libertà dei traffici marittimi sia in parte compromessa. Questo avviene perché gli attori europei non dispongono ancora di strumenti adeguati a proiettare la propria potenza oltre il raggio delle proprie basi. Infatti, le ambizioni

[1] Schmitt, Carl, *Il nomos della terra*, Adelphi, 1991.
[2] *Sicurezza Marittima*, Consiglio dell'Unione Europea, https://www.consilium.europa.eu/it/policies/maritime-security.

navali europee devono fare i conti con problemi strutturali quali: unità navali insufficienti e un budget militare limitante. Un esempio è dato dalla Marina dell'Esercito Popolare di Liberazione (PLAN) rappresentante oggi la più grande flotta al mondo per numero di unità da combattimento, con oltre 350 navi tra cacciatorpediniere, fregate, corvette e unità anfibie, sostenute da una capacità cantieristica industriale senza equivalenti e da un ritmo di costruzione continuo[3]. Le marine europee, considerate nel loro insieme (Regno Unito, Francia, Italia, Spagna, Germania e altre flotte UE e NATO), dispongono invece di circa 200–230 unità da combattimento principali e di una componente subacquea complessivamente comparabile in termini numerici a quella cinese, ma distribuita tra più Stati e catene di comando[4]. Sul piano qualitativo, l'Europa mantiene un elevato livello tecnologico medio: piattaforme come cacciatorpediniere di difesa aerea, fregate multiruolo di ultima generazione e gruppi portaerei con significativa esperienza operativa conferiscono alle flotte europee una forte capacità *expeditionary* e di integrazione interforze, soprattutto in ambito NATO. Tuttavia, questa superiorità qualitativa è attenuata dalla mancanza di un comando navale unitario e da bilanci della difesa meno orientati alla crescita quantitativa della flotta.

L'insufficiente quantità di unità navali attualmente disponibili in Europa rappresenta una conseguenza diretta di una tendenza inaugurata negli anni '90[5]. Dalla fine della Guerra fredda, infatti, il budget militare di tutti i paesi europei è sceso drasticamente, raggiungendo i minimi storici nel decennio compreso tra gli anni 2000-2010. Tuttavia, questa tendenza è stato interrotto dal conflitto

[3] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China*, Washington, D.C., Annual Report to Congress, 2023.
[4] IISS, *The Military Balance 2024*, sezioni: "Europe – Naval Forces" e "China – Naval Forces".
[5] Mazziotti di Celso, M., Il ritorno della guerra convenzionale sul mare. Le capacità delle flotte europee e gli ostacoli da superare, *Rivista Marittima*, Dicembre 2022.

russo ucraino: nel 2024 gli investimenti nel settore della difesa hanno registrato una crescita senza precedenti, con gli Stati membri che hanno superato il parametro di riferimento collettivo per la difesa del 20%, destinando il 31% della spesa complessiva per la difesa - la percentuale più alta mai registrata[6]. La comunità internazionale ha registrato livelli record di spesa militare, anche se ciò lo si deve all'impulso fornito dall'industria bellica statunitense. Infatti, come emerge dal Documento Programmatico della Difesa (DPP 2025-2027) si riscontrano stanziamenti dettagliati per piattaforme navali specifiche[7]: circa 1 miliardo di euro nel 2025 per cacciamine di nuova generazione; oltre 355 milioni nel 2025 e ulteriori 3,9 miliardi entro il 2040 per le *FREMM*; oltre 103 milioni nel 2025 e ulteriori 2,5 miliardi entro il 2035 per nuovi pattugliatori e programmi di rinnovamento della linea operativa.

La frontiera della competizione ibrida marittima ha come obiettivi primari le infrastrutture sensibili, poiché il danno non si limiterebbe alla dimensione materiale, ma eroderebbe, oltre che le capacità strategiche, anche la fiducia dell'opinione pubblica nelle istituzioni. In tale contesto, il dominio marittimo assume il ruolo di vettore strategico: un impiego limitato di mezzi cinetici è sufficiente a generare effetti sproporzionati sulla sfera cognitiva e politica, poiché l'obiettivo primario della guerra non convenzionale contemporanea è l'influenza delle percezioni e dei processi decisionali.

---

[6]La difesa dell'UE in cifre, Consiglio dell'Unione Europea, https://www.consilium.europa.eu/it/policies/defence-numbers/#:~:text=Promuovere%20la%20competitivit%C3%A0.

[7] Marrone, A., Ravazzolo, G., Il Documento Programmatico della Difesa 2025-2027: priorità, budget e domini operativi, Istituto Affari Internazionali, 2025, https://www.affarinternazionali.it/il-documento-programmatico-della-difesa-2025-2027-priorita-budget-e-domini-operativi.

L'opacità del mare profondo è allora un punto vulnerabile del Sistema Paese, per questo motivo si sta manifestando la necessità di definire un nuovo dominio, quello dell'*underwater*. Quest'ultimo comprende tutte le attività civili e militari che si svolgono sui fondali. Esse vengono categorizzate in base alle loro funzioni specifiche quali: il controllo e la negazione dello spazio subacqueo, la protezione delle infrastrutture critiche dei fondali, la deterrenza strategica e la raccolta informativa e la sensoristica dei dati. Non è un caso che i cavi sottomarini, le condotte di idrocarburi o le testate di pozzi *deep water*[8], siano oggi al centro del contrasto cinetico e risultino essere i principali bersagli delle *hybrid threats*, all'interno di una condizione di crescente competitività.

Per il controllo e la negazione dello spazio subacqueo le potenze effettuano costanti e vigili attività di pattugliamento dello spazio sottomarino, cercando di individuare e neutralizzare possibili unità avversarie o di impedire l'accesso a determinate aree marittime ai competitor. La sorveglianza è invece effettuata attraverso sottomarini, navi dotate di sonar e reti acustiche fisse come il sistema *Sound Surveillance System* (SOSU), sviluppato durante la Guerra fredda[9] e che rappresenta ancora oggi il modello principale delle reti di sorveglianza subacquea.

Relativamente alla protezione delle infrastrutture critiche dei fondali, pienamente esplicativo è il caso del sabotaggio dei gasdotti Nord Stream 1 e 2 nel

[8] I pozzi di *deep water* (acque profonde) sono installazioni di perforazione offshore progettate per l'esplorazione e l'estrazione di idrocarburi situati sotto il fondale marino. Si parla di *deepwater* quando la profondità dell'acqua supera i 300-500 metri. Quando invece la profondità supera i 1.000-1.500 metri, si parla più specificamente di *ultra-deepwater*. I pozzi *deep water* richiedono mezzi mobili specializzati, come navi di perforazione (*drillships*) o piattaforme semisommergibili, dotate di sistemi di posizionamento dinamico per restare ferme sopra il pozzo.

[9] Weir, Gary E., The American sound surveillance system: using the ocean to hunt soviet submarines, 1950-1961, International Journal of Naval History, 2006.

Mar Baltico nel 2022[10]. L'evento ha evidenziato la vulnerabilità delle reti energetiche e comunicative nonché l'importanza del pattugliamento e del monitoraggio subacqueo.

In merito alla deterrenza strategica, essa mira a disporre di armamenti quali i sottomarini lanciamissili balistici (SSBN), come gli *Ohio-class Ballistic Missile Submarine*[11] statunitensi o i *Borei-class submarine* russi[12], per garantire una capacità di reazione istantanea grazie alla loro invisibilità. Sono strumenti altamente innovativi che permettono di esercitare un'elevata proiezione di potenza di lungo raggio nell'ambiente marittimo.

Quanto alla raccolta informativa dei dati e la sensoristica (ISR), l'obiettivo è quello di definire una mappatura quanto più completa possibile dei fondali, tramite sonar e reti acustiche, oppure per opera di tecnologie che utilizzano le onde sonore per ottenere informazioni dettagliate, trasformando così l'acustica in uno strumento di osservazione. I sonar scientifici, come gli *echosounder*, emettono impulsi acustici che rimbalzano sul fondale e sugli oggetti circostanti per creare mappe tridimensionali[13]. Le reti di sensori acustici localizzati negli abissi permettono di registrare segnali persistenti del traffico marino, trasformando questi segnali in dataset utili per il monitoraggio ambientale e la protezione delle infrastrutture sensibili. Ulteriori approfondimenti a riguardo sono presenti nella quarta sezione.

---

[10] *The Nord Stream Incident: open breafing*, Security Council Report, 2025.https://www.securitycouncilreport.org/whatsinblue/2025/08/the-nord-stream-incident-open-briefing-2.php.

[11] *Ohio-Class Submarines*,General Dynamics mission systems, https://gdmissionsystems.com/submarine-systems/ohio-class

[12] *Russia Submarine Capabilities*, NTI, 2024, https://www.nti.org/analysis/articles/russia-submarine-capabilities/.

[13] *Undersea Sensor Grinds & Seabed Infrastructures*, Envisioning, https://www.envisioning.com/research/aegis/undersea-sensor-grids.

Strategicità e vulnerabilità delle infrastrutture marittime

La dimensione securitaria marittima storicamente si fondava principalmente sulla proiezione militare a lunga distanza come forma di deterrenza e capacità di risposta alle crisi. In questo quadro, l'Italia si configura come una media potenza marittima dotata di piena autonomia d'azione in scenari *expeditionary* e di interdizione[14]. Il pilastro di tale capacità risiede nella sinergia tra la portaerei Cavour e la nuova LHD Trieste: quest'ultima, integrando i velivoli di quinta generazione F-35B Lightning II, allinea l'Italia a un ristretto gruppo di nazioni (con Stati Uniti e Regno Unito) capaci di esprimere una proiezione aerea e logistica di tale sofisticatezza[15] .

La difesa marittima svolge una funzione portante nel sistema Paese, un ambiente marittimo sicuro riduce il rischio operativo per gli attori economici, incentivando gli investimenti e garantendo la continuità delle catene di approvvigionamento, centrali per la stabilità nazionale.

L'interconnessione tra sicurezza ed economia guida la ristrutturazione dei principali hub portuali italiani (Genova, Trieste, Livorno, Gioia Tauro), i quali hanno integrato tecnologie avanzate — come sistemi SCADA, VTS, AIS e piattaforme IoT — per il monitoraggio e la gestione automatizzata dei flussi[16]. Tale evoluzione ha trasformato il porto in un ecosistema ibrido in cui sviluppo industriale e sicurezza sono interdipendenti. Tuttavia, la persistenza di vulnerabilità strutturali espone questi nodi critici a minacce ibride, con

[14] Leoni, R., Più navi e più potenza di fuoco. Il futuro della Marina Militare italiana, Formiche, 2024, https://formiche.net/2024/10/piu-navi-e-piu-potenza-di-fuoco-il-futuro-della-marina-militare-italiana/#content.

[15] Peruzzi, L., La LHD Trieste sarà equipaggiata con sky-jump per l'impiego degli F-35B, Analisi Difesa, 2019, https://tinyurl.com/b43c6349.

[16] Di Silvio, C., *Cyberminacce alle infrastrutture portuali italiane: vulnerabilità strategiche e risposta operativa nel dominio marittimo*, CeSI, 2025, https://www.cesi-italia.org/it/articoli/cyberminacce-alle-infrastrutture-portuali-italiane-vulnerabilita-strategiche-e-risposta-operativa-nel-dominio-marittimo.

particolare riferimento ad attacchi cibernetici sofisticati quali *Advanced Persistent Threat* (APT), *ransomware* e operazioni di cyberspionaggio condotte da attori statali o criminali specializzati. Il caso *WannaCry* (2017) rappresenta un esempio paradigmatico di *ransomware* evoluto. Si trattò di un *malware worm-based* capace di propagarsi automaticamente su scala globale che colpì in pochi giorni oltre 150 Paesi, compromettendo alcune infrastrutture critiche, tra cui il sistema sanitario britannico (NHS)[17]. L'attacco, attribuito da diverse autorità al gruppo Lazarus legato probabilmente alla Corea del Nord, evidenziò il passaggio da forme tradizionali di cybercriminalità a operazioni cibernetiche altamente sofisticate, tali da collocare il *ransomware* evoluto tra criminalità organizzata e strumenti di pressione strategica nel dominio cibernetico.

Dunque, la *cyber security* propone continuità operative contro attori non necessariamente politici o istituzionalizzati. Si parla, infatti, della c.d. attribuzione opaca e risposta asimmetrica, per riferirsi a questa nuove forme di competizione che rendono difficile distinguere nettamente tra pace e conflitto. Concetto meglio conosciuto attraverso l'espressione *plausibile deniability:* la nazione attaccante può disconoscere la paternità delle azioni condotte dai suoi *proxy* – termine che comprende entità non statuali, Stati falliti, organizzazioni terroristiche e criminali, gruppi economici e finanziari, pirati informatici e agenti – mantenendo il conflitto sotto la soglia della guerra aperta[18].

Una maggiore strategicità degli asset li espone consequenzialmente a un più alto rischio di vulnerabilità, ed è proprio questo il caso delle infrastrutture critiche.

---

[17] Europol, Internet Organised Crime Threat Assessment 2017, L'Aia, 2017; ENISA, Threat Landscape Report 2017; UK National Cyber Security Centre, WannaCry Cyber Attack and the NHS, 2017; U.S. DHS-CISA, Alert TA17-132A, 2017; The White House, Statement on WannaCry Attribution, 19 dicembre 2017.

[18] Serino, P., *Come difendersi nella guerra ibrida, Istituto Affari Internazionali*, 2025, https://www.huffingtonpost.it/blog/2025/12/23/news/difendersi_dalla_guerra_ibrida-20813526/.

Lungo i cavi sottomarini non transita solo il 95% dei dati, ma potere economico, capacità decisionale e vantaggio strategico. Parliamo di infrastrutture che sostengono la finanza globale, i sistemi di difesa e intelligence, la gestione delle *smart grid* energetiche e, sempre più spesso, collegano anche parchi eolici *offshore* e *data center* marini[19]. Per ragioni di sicurezza, non è possibile rendere nota la localizzazione di questi sistemi poiché genererebbe un'estrema vulnerabilità per la stabilità e la sicurezza nazionale. Infatti, il danneggiamento anche solo di uno di questi sistemi rallenterebbe il sistema delle connessioni, produrrebbe significative perdite economiche, ma ancor più grave sarebbe il danno prodotto a livello d'immagine per la resilienza del Paese. Per effettuare delle stime, TeleGeography sostiene che in Italia si trovano circa 25 cavi sottomarini noti[20].

La rete europea, pur disponendo di oltre 300 stazioni di atterraggio, persegue una strategia di diversificazione dei *landing points* volta a mitigare l'eccessiva concentrazione geografica. Nonostante tale sforzo, permane una criticità sistemica dovuta alla dipendenza da specifici corridoi: il Mar Rosso, in particolare, rappresenta un *bottleneck* imprescindibile dove transita circa il 90% del traffico dati tra Europa e Asia[21]. Per contrastare tale fragilità, alcuni hub strategici come Marsiglia e Sines sono stati potenziati secondo criteri di ridondanza geografica**.** L'attacco del ottobre 2022[22] ai cavi nel sud della Francia — attribuito a un'azione di sabotaggio e capace di degradare la connettività

[19] Fabbri, F., Cavi sottomarini, mercato mondiale stimato a 59 miliardi di dollari entro il 2032, Key4biz, 2025, https://www.key4biz.it/cavi-sottomarini-mercato-mondiale-stimato-a-59-miliardi-di-dollari-entro-il-2032.

[20] Brugnoni, S., *La mappa dei cavi sottomarini in Italia: dove si trovano e perché sono importanti*, 2025, https://www.geopop.it/la-mappa-dei-cavi-sottomarini-in-italia-dove-si-trovano-e-perche-sono-importanti/.

[21] *Relazione sulla sicurezza e la resilienza delle infrastrutture di cavi sottomarini dell'UE*, Commissione Europea, 2025, https://digital-strategy.ec.europa.eu/it/library/report-security-and-resilience-eu-submarine-cable-infrastructures.

[22] Redazione, *Cavi internet tranciati a Marsiglia*, Resilience Engineering, 2022, https://ingegneriadellaresilienza.it/cavi-internet-tranciati-al-largo-di-marsiglia/.

globale — conferma come la resilienza di questi punti logistici non sia più solo un'esigenza tecnica, ma una priorità di sicurezza nazionale e internazionale a fronte di minacce ibride[23].

Oltre al transito dei dati, tra le infrastrutture sensibili è bene sottolineare anche il ruolo delle piattaforme *offshore*: ampie strutture che raccolgono gli impianti necessari alla perforazione del fondo marino per l'esplorazione, lo stoccaggio e la lavorazione del petrolio e gas naturale. Secondo quanto dichiarato dal ministero dello Sviluppo economico, in Italia ci sono all'incirca centocinquanta piattaforme *offshore*, maggiormente collocate nell'Adriatico, ma presenti anche nel canale di Sicilia[24]. Un'azione offensiva contro una tale piattaforma non significa solamente ledere gli interessi di un singolo attore, ma rappresenta un attacco diretto all'economia e alla stabilità sociale del Paese. Il fine di esercitazioni antiterroristiche, come la *Gold Finger* dei reparti speciali della Marina Militare, è di riprendere il controllo delle infrastrutture in tempi rapidissimi, minimizzando i rischi per il personale civile e prevenendo disastri ambientali o blocchi energetici[25].

I tentativi e le modalità di sabotaggio nel dominio sottomarino: una panoramica teorica *cross domain*

Ripartendo da Schmitt, il termine "tentare" ci rimanda al greco πειράω (peiràō), per l'appunto "tentare, provare", da cui il termine πειρατής (peiratès): pirata. In

---

[23] Per completezza del discorso, è necessario ricordare che i dati non transitano solamente lungo i fondali marini, ma anche attraverso dorsali terrestri in fibra ottica (*backbone* nazionali e transfrontalieri), corridoi lungo cui si concentra il traffico dei dati prima e dopo l'innesto nei sistemi sottomarini.

[24] *Alla scoperta delle piattaforme offshore*, Mariter, 2024, https://maritersrl.com/alla-scoperta-delle-piattaforme-offshore/.

[25] Lugano, F., *COMSUBIN: lo Scudo sulle Infrastrutture Strategiche Italiane. Esercitazioni Speciali per Affrontale le Nuove Minacce*, Scenari Economici, 2026, https://scenarieconomici.it/comsubin-lo-scudo-sulle-infrastrutture-strategiche-italiane-esercitazioni-speciali-per-affrontare-le-nuove-minacce/.

ottica schmittiana, la *plausible deniability* è correlabile alla cosiddetta "analogia piratica"[26]: siamo fuori dalla sfera del civile, delle regole, del diritto.

Il fine è complicare e rallentare il processo decisionale dell'avversario[27]. La discriminante, infatti, è proprio il fattore temporale. Che si parli di resilienza[28], *risk assessment* o previsione, il tempo detta le regole dell'entità di un danno economico (e non) al Sistema Paese. Il sabotaggio del *Nord Stream* è stato sicuramente un evento spartiacque nella letteratura sul tema[29]. Tuttavia ad oggi le infrastrutture che sembrano darci una più attuale declinazione dell'azione sotto la soglia di violenza nel dominio marittimo sono proprio i cavi sottomarini.

Il cavo sottomarino ha nel suo DNA costitutivo tutti i cinque domini sopracitati: tellurico (stazioni di approdo), marittimo (fondali e *underwater*), aereo (dominio vettore di sorveglianza con UAV e protezione delle flotte posacavi), spazio esoatmosferico (sincronizzazione temporale e *backup* delle comunicazioni) e *cyber* (flusso dei dati e vulnerabilità alle intercettazioni). Si evince dunque la ragione per cui i tentativi di compromissione possano seguire infinite vie. Si pensi che alcuni danneggiamenti avvengono attraverso il trascinamento delle ancore di pescherecci sui fondali più bassi, pertanto con l'impiego di elementi cinetici direttamente rivolti all'obiettivo fisico. Già dal Febbraio 2023, a titolo di esempio, fu noto che mercantili cinesi avessero danneggiato dei cavi tra Taiwan e le isole Matsu[30].

---

[26] Cfr. Scuccimarra, Luca (a cura di), *La metamorfosi della pirateria*, Quodlibet, 2023.
[27] Cfr. Zampieri, Francesco, Dalla geografia militare alla geostrategia marittima, Nuova Cultura, 2026.
[28] Paolinelli, A., *Minacce cyber verso le infrastrutture critiche in aumento in Europa: la resilienza e il ruolo di NIS2 e la CER*, Geopolitica.info, 2025, https://www.geopolitica.info/minacce-cyber-verso-infrastrutture-europee/.
[29] Fabbri, V. *La guerra in superficie e quella in fondo al mare*, *Geopolitica.info*, 2023, https://www.geopolitica.info/guerra-superficie-mare/.
[30] Mariotti, M. Washington non molla Taiwan, Domino, Luglio 2025.

Un'altra possibilità che si apre, forse più complessa, è il sabotaggio non cinetico e pertanto l'interruzione del servizio che l'infrastruttura fornisce per vie informatiche. In questo contesto, esempi significativi sono gli attacchi cibernetici ai *Network Management Systems*, ossia i sistemi di gestione del traffico dati all'interno dei cavi (si pensi al caso delle Hawaii del 2022[31]). Un report *ENISA 2025* evidenzia l'importanza delle vulnerabilità in API (*Application Programming Interface[32]).* Se immaginiamo i cavi sottomarini come un "sistema nervoso sottomarino": le API sono un "ponte digitale" che permette ai *software* di gestione a terra di comunicare con l'*hardware* fisico posato sul fondale[33]. Se queste non sono sicure per i fornitori di posizionamento e manutenzione dei cavi, possono permettere ad attori ostili di eseguire il r*e-routing* (reindirizzamento) del traffico regionale per attività di intercettazione di massa senza interrompere il servizio[34].

Ulteriore e conclusivo esempio di compromissione non cinetica è il GNSS (*Global Navigation Satellite System*) *Spoofing e Jamming***.** Queste minacce non cinetiche sono state tra le più impiegate nel 2024-2025 per "accecare" o ingannare le navi che pattugliano o riparano le infrastrutture. Il picco si è verificato nel Mar Baltico[35] (2025): più di 3.000 navi hanno riportato interferenze simultanee ai segnali GPS/GNSS. Lo *spoofing*[36] (invio di segnali falsi) è stato usato per nascondere i movimenti di "navi ombra" impegnate in attività sospette vicino ai cavi o per

[31] Carrer, V., Chi c'è dietro all'attacco contro un cavo sottomarino alle Hawaii, Formiche, 2022, https://formiche.net/2022/04/attacco-cavo-sottomarino-hawaii/#content.
[32] Cos'è un'API (application programming interface)?, IBM, https://www.ibm.com/it-it/think/topics/api
[33] Submarine Cable Networks, https://www.submarinenetworks.com/en/stations.
[34] *ENISA threat landscape*, ENISA, https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA Threat Landscape 2025 Booklet.pdf.
[35] 2025 Was a Stress Test & Maritime AI™ Is the Only Way to Pass, Windward, https://windward.ai/blog/2025-maritime-stress-test/.
[36] *Spoofing*, SBG Systems, https://www.sbg-systems.com/it/glossary/spoofing-definition/.

indurre errori di navigazione in unità di sorveglianza. La criticità che si coniuga al fattore temporale, si riscontra poi attraverso l'impatto sulle riparazioni ai cavi compromessi: senza un segnale GPS preciso, le navi posacavi non possono stazionare con precisione millimetrica sopra il guasto, ritardando i tempi di ripristino da giorni a settimane e facendo proseguire il disservizio.

Pertanto possiamo concludere che il tentativo di compromissione di un'infrastruttura sottomarina, in particolare riguardo ai cavi e ai differenti *provider*, sia spesso riconducibile ad attori che fanno della difficoltà nell'identificazione della natura della minaccia, proveniente da ambienti diversi e in modalità diverse, il loro punto di forza. Questo, ad oggi, rappresenta uno degli scenari più complessi a cui dover far fronte nel campo della difesa e dell'intelligence.

Un teatro complesso sotto la superficie: dai *chockepoints* alla batimetria

Se l'ambiguità è il metodo, i *chokepoints*, già citati nelle precedenti sezioni, possono esserne il teatro elettivo. Ma cos'è precisamente un *chokepoint*? Anche detto "collo di bottiglia", è una strettoia naturale o artificiale, sia essa uno stretto o un canale, che costituisce un passaggio obbligato per le imbarcazioni in uno spazio che ha come peculiarità quella di costituire una "strozzatura" del passaggio marittimo con tutte le sue conseguenze sul piano commerciale e militare. E' importante comprendere questo dettaglio a pieno poiché una strettoia corrisponde a un rallentamento, e rallentamento corrisponde ad una erosione del fattore tempo che nelle migliori strategie ibride, dilatando la persistenza del danno, fa la differenza.

Come si è potuto apprendere fino ad ora, la vulnerabilità di superficie si riflette verticalmente sul fondale. Se un *chokepoint* è bloccato o instabile, la manutenzione dei cavi in quell'area diventa impossibile (si veda la crisi degli

Houthi nel Mar Rosso che ha rallentato le riparazioni dei cavi tranciati nel 2024)[37][38]. I cinque più rilevanti per il commercio marittimo sono lo Stretto di Malacca, lo Stretto di Hormuz, lo Stretto di Bab El Mandeb, il Canale di Panama e il Canale di Suez. Malacca è una strettoia tra Indonesia e Malesia; Hormuz, tra Iran e Oman collega il golfo persico al Golfo di Oman ed è vitale per il transito globale di petrolio e gas; Bab El Mandeb è ubicato tra Yemen e Corno d'Africa e collega il Golfo di Aden al Mar Rosso: *Bab* (باب) in lingua araba significa appunto "porta"; il Canale di Panama è una strettoia nell'omonima Repubblica che rappresenta un passaggio tra Caraibi e Oceano Pacifico; il Canale di Suez, in Egitto, è il passaggio tra Mar Rosso e Mar Mediterraneo. Risulta inadeguato non considerare questi restringimenti del traffico marittimo come una realtà multidimensionale. La questione è ben più complessa se si analizza il collo di bottiglia come un caso studio su più livelli (dalla superficie al fondale e viceversa). Restringere il mare non significa solo restringere il traffico in superficie, ma anche condensare in un unico punto il passaggio di più cavi sottomarini, creando la sopracitata correlazione tra superficie e fondale, e pertanto anche una vulnerabilità sistemica.

Manifestazione concreta del parallelismo semantico pocanzi proposto sull'analogia piratica, è il sabotaggio ad opera degli *Houthi* nel 2024 con il danneggiamento del cavo (*Asia-Africa-Europe 1*), avvenuto nello stretto di Bab El Mandeb in un clima geopolitico di incertezza che ci riconduce al già noto

[37] Proietti, L., Cavi sottomarini, la poca sicurezza del Mar Rosso mette in crisi i progetti di Google e Meta, Cybersecitalia, 2025, https://www.cybersecitalia.it/cavi-sottomarini-la-poca-sicurezza-del-mar-rosso-mette-in-crisi-i-progetti-di-google-e-meta/54906/.

[38] Gandelli, S. (a cura di), La mappa dei 4 cavi sottomarini che gli Houti avrebbero sabotato tra Europa e Asia, Geopop, 2024, https://www.geopop.it/la-mappa-dei-4-cavi-sottomarini-che-gli-houthi-avrebbero-sabotato-tra-europa-e-asia/.

concetto di *plausible deniability*[39]. Gli *Houthi* non hanno inviato un sottomarino o dei sommozzatori a tagliare i cavi con delle cesoie (un'operazione tecnicamente complessa e palesemente intenzionale), ma hanno creato le condizioni affinché una nave alla deriva facesse il "lavoro sporco" per loro. In questo contesto, il sabotaggio ha più di un obiettivo. Alla radice c'è il fattore ideologico e politico: sabotare un'infrastruttura in un settore del conflitto israelo-palestinese ha un significato che esula dalla sola compromissione. Tra le altre ragioni, vi è il traffico marittimo di navi statunitensi, israeliane e britanniche, divenute bersagli degli attacchi degli *Houthi*[40]. La conseguenza è stata un'interruzione persistente del servizio fornito dai tre cavi compromessi.

Soffermiamoci in particolare sul significato di un attacco all'*AAE-1.* Si consideri un cavo di circa 25000km che collega dal Sud Est Asiatico all'Europa passando per l'Egitto e connettendo Hong Kong, Vietnam, Cambogia, Malesia, Singapore, Thailandia, India, Pakistan, Oman, Emirati Arabi Uniti, Qatar, Yemen, Djibouti, Arabia Saudita, Grecia, Italia e Francia[41]. Abbiamo diverse ragioni per credere che il messaggio sia principalmente rivolto ad attori europei e Stati parti degli Accordi Abramo con il fine di "scollegarli" dall'Oriente.

Il danno principale torna tuttavia ad essere legato al fattore temporale. Il *chokepoint* diventa un'arma ibrida nel momento in cui si rallenta significativamente la riparazione dell'infrastruttura lesa. Le navi posacavi sono grandi, lente e vulnerabili e se l'area di superficie è sotto attacco missilistico o se

---

[39] Leccese, G. Chokepoint Above and Below the Surface: The Red Sea's Emerging Infrastructure Challenge, Istituto Affari Internazionali (IAI), 2025, https://www.iai.it/it/pubblicazioni/c41/chokepoint-above-and-below-surface-red-seas-emerging-infrastructure-challenge.

[40] Madory, D., *What Caused the Red Sea Submarine Cable Cuts?*, Kentik, 2024, https://www.kentik.com/blog/what-caused-the-red-sea-submarine-cable-cuts/.

[41] Submarine Cable Networks, *AAE-1,* https://www.submarinenetworks.com/en/systems/asia-europe-africa/aae-1/.

è un settore di un teatro di operazioni, il risultato è un potenziale blackout prolungato che logora l'economia degli Stati rivieraschi, la stabilità del commercio dei paesi colpiti e tutto ciò senza l'uso di testate nucleari o invasioni terrestri. Ciò si va a incastonare in un più esteso teatro di guerra che rende la complessità ben più elevata di un banale sabotaggio come fosse un "dispetto" da parte di uno Stato ad un altro. Qui è racchiusa la natura *cross domain* di un *chokepoint* che, coniugata a quella precedentemente esposta del cavo sottomarino, crea un quadrato di complessità tale da ridurre esponenzialmente la rapidità di ogni intervento e pertanto viene meno quel ritorno allo stato di funzionamento che il termine "resilienza" ci richiede. Inoltre, in questa situazione più che in altre è ancora più complesso andare a comprendere la soglia che divide il civile dal militare.

Infine, alla complessità dei *chokepoints* si lega quella di rotte infrastrutturali alternative come *IMEC* e le rotte Artiche. Se un Paese non può garantire la sicurezza del fondale nei propri colli di bottiglia di riferimento, il rischio è la perdita della propria sovranità digitale, informatica, energetica, economica e commerciale. In un'ottica volta al futuro, troviamo importante rivolgere maggiore attenzione all'Artico e al GIUK *Gap* (*Greenland*, *Iceland*, *UK*). Per GIUK *Gap* si intendono due restringimenti situati rispettivamente a sud-est della Groenlandia e tra Islanda e Gran Bretagna. La posizione è tra i primi elementi precipui. La vicinanza alla Groenlandia e quello che oggi vediamo apparire come uno "schermo" NATO che crea un argine contro il movimento russo verso l'Artico, sono due fattori che mettono in luce come quest'ultimo abbia un significativo valore strategico. Qui non ci soffermiamo sulla rilevanza di questo passaggio per le rotte artiche, ma non è di minore importanza lo svolgimento di uno studio approfondito della batimetria di questi restringimenti.

Perché lo studio batimetrico è così importante? Lo studio dei fondali sottomarini permette di comprendere dove possono passare o meno cavi ed eventuali mezzi subacquei poiché i fondali possono essere bassi, frastagliati, o presentare in generale elementi ostili al passaggio; il secondo elemento di complessità invece è correlato al diritto internazionale del mare. Esistono infatti porzioni sottomarine la cui sovranità risponde alle logiche della Convenzione di *Montego Bay* sul diritto dell'Alto Mare con particolare riguardo alla Piattaforma Continentale (Art. 76)[42]. In parole più semplici: immaginiamo che due Stati rivieraschi, uno ad est e uno ad ovest siano separati dal mare. Sott'acqua, la loro "terra" si estende al di là della linea di costa per svariate miglia, ergo è possibile che le due possano anche convergere in uno stesso punto. La sovranità che si esercita su un fondale, che si estende per svariate miglia, rischia di avviare un conflitto di interessi tra Stati per il controllo di una sua parte e può fare la differenza in campo commerciale, di estrazione di materie prime critiche e di posizionamento delle infrastrutture. Ad oggi questa è materia di studio della Commissione sui Limiti della Piattaforma Continentale[43]. Nel contesto del conflitto ibrido, possiamo riscontrare un caso interessante di *Lawfare* (guerra attraverso le norme) ossia usare le procedure UNCLOS per invalidare le pretese territoriali degli avversari per sottrarre materie prime critiche o aree di interesse.

Che vi passino cavi o meno, l'esame batimetrico dei fondali ci fornisce un dato fondamentale che risponde alla domanda "dove può passare un mezzo subacqueo per studiare o compromettere un'infrastruttura nazionale?", e non solo. Assai più complessa si fa la questione ibrida ove le norme atte ad arginare

[42] *La Convenzione delle Nazioni Unite sui diritti del mare*, https://www.carteinregola.it/wp-content/uploads/2019/07/Convenzione_Diritti1982-Montego-Bay.pdf.
[43] *Oceans and Law of the Sea*, United Nations, https://www.un.org/Depts/los/index.htm.

una minaccia non “coprano” ogni aspetto possibile. Questa sfida per i *policymakers* è ancora aperta[44].

Conclusioni

L’analisi condotta evidenzia come la dimensione *underwater* rappresenti oggi una nuova frontiera della sicurezza nazionale, un dominio dove la distinzione tra pace e conflitto si dissolve nell'opacità degli abissi. Non è più possibile considerare il mare come una superficie di transito; esso è un ecosistema integrato la cui stabilità è condizione necessaria per la sopravvivenza economica e digitale dello Stato.

Le infrastrutture critiche sottomarine sono passate dall'essere "*asset* invisibili" a "bersagli primari" della guerra ibrida. Come dimostrato dal caso dei cavi in fibra ottica e delle piattaforme energetiche, la loro vulnerabilità non è solo fisica, ma sistemica. Il sabotaggio non mira necessariamente alla distruzione totale, ma all’uso del tempo come arma: rallentare le riparazioni, creare incertezza nell'attribuzione e logorare la fiducia dei mercati. In questo contesto, la *plausible deniability* diventa lo scudo dietro cui attori statali e non statali operano per ridefinire gli equilibri di potere senza scatenare una risposta convenzionale.

I "colli di bottiglia" marittimi agiscono come moltiplicatori di vulnerabilità. La sovrapposizione tra rotte commerciali di superficie e corridoi infrastrutturali sottomarini crea dei punti di pressione dove il controllo della batimetria e della tecnologia *underwater* diventa sinonimo di sovranità geopolitica. Il rischio è chiaro: l’incapacità di proteggere questi restringimenti non comporta solo un

[44] Di Francesco, G., *Il ritorno dell’Artico e il controllo del GIUK Gap*, Opinio Juris, https://www.opiniojuris.it/wp-content/uploads/2018/09/IL-RITORNO-DELLARTICO-E-IL-CONTROLLO-DEL-GIUK-GAP.pdf.

danno economico, ma una vera e propria "eclissi di sovranità" a favore di chi possiede i mezzi per monitorare o interdire i fondali.

L'emergere di rotte alternative e l'evoluzione tecnologica (tecnologie quantistiche, droni *AI-driven*) impongono un cambio di paradigma. La difesa nazionale deve evolvere verso una “postura *cross-domain*”, capace di integrare la sorveglianza satellitare, la *cybersecurity* delle reti di gestione e la presenza militare sottomarina. L’Italia, come media potenza marittima e hub centrale del Mediterraneo, si trova dinanzi a una sfida legislativa e operativa: colmare i vuoti del diritto internazionale per rispondere a minacce che operano nella "zona grigia" e investire in una “resilienza subacquea” che sia al contempo tecnologica, industriale e normativa.

La riscoperta del dominio elettromagnetico: lezioni dal conflitto russo-ucraino tra asimmetrie euro-atlantiche e dipendenze capacitive

di Anna Calabrese

Introduzione

La guerra tra Russia e Ucraina si è imposta come momento spartiacque degli studi strategici moderni, stravolgendo il modo di comprendere e contrastare le minacce dell'ambiente bellico contemporaneo. In un contesto segnato da mutevoli ostilità che agiscono sotto la soglia tradizionale di conflitto armato come tipicamente inteso, le nazioni occidentali, l'Unione Europea e la NATO si stanno interrogando circa le proprie capacità e *gap* da colmare per rispondere alle diverse forme che assume la cosiddetta "minaccia ibrida".

Per l'Italia, il Non Paper diffuso dal Ministero della Difesa lo scorso novembre rappresenta il tentativo di offrire una visione d'insieme della minaccia e delle sue articolazioni e origini, insieme alla definizione delle capacità da rafforzare per agire assertivamente in un ambiente strategico asimmetrico. Tra gli strumenti e i "domini d'azione" che il documento tratta, figura anche lo spazio elettromagnetico. A partire dal 2018[1], il settore dell'aviazione civile ha assistito a un aumento esponenziale di incidenti di *jamming* e *spoofing*, livelli di interferenza a lungo associati al settore militare ma oggi impiegati senza distinzione nell'ambiente aereo ed elettromagnetico civile e commerciale, traducendosi nella perfetta logica *dual-use* che caratterizza la minaccia ibrida del XXI° secolo e

[1] Safran. "Meeting the Challenges of 'Jamming' and 'Spoofing' in Civil Aviation" *Safran Group*, 15 gennaio 2025 https://www.safran-group.com/news/meeting-challenges-jamming-and-spoofing-civil-aviation-2025-01-15.

che riduce la labile soglia tra civile e militare. Se ad agosto 2024 sono stati registrati fino a 1500 casi di *spoofing* al giorno principalmente per aerei di linea in aree di conflitto come in Medio Oriente, per l'Europa è riscontrabile un aumento considerevole di interferenze del GNSS (Global Navigation Satellite System) a partire dall'invasione dell'Ucraina nel febbraio 2022[2] con incidenti a navi e aerei sul fianco orientale, dalla Finlandia a Cipro fino in Bulgaria. A titolo di esempio, in Estonia l'85% dei voli è stato interessato da interferenze GPS, mentre in Polonia sono stati registrati 2.732 casi nel gennaio 2025[3]. Inoltre, il presunto attacco mirato all'aereo della Presidente della Commissione UE Ursula Von der Leyen dello scorso 2 settembre [4] ha suscitato forte preoccupazione a livello nazionale e internazionale e ha riacceso, così, diverse riflessioni su quali strumenti adottare per migliorare la sicurezza aerea nel contesto di guerra ibrida. Il crescente numero degli incidenti registrati, spesso è riconducibile all'attività russa[5] che dispone di basi di disturbo lungo i confini degli Stati baltici e lungo i confini con l'Ucraina. Alla luce di ciò, i ministri europei si sono riuniti il 4 giugno scorso e hanno sottolineato l'urgente necessità di nuove azioni di risposta e contrasto verso le minacce comuni di *jamming* e *spoofing*.

Del resto, anche a livello nazionale avanzano le riflessioni su questo fronte; eppure, facendo riferimento al Non paper ministeriale di novembre si nota la

---

[2] Euronews, "What Can Europe Do to Better Defend Against GPS Interference from Russia?" *Euronews*, 2 settembre 2025. https://www.euronews.com/my-europe/2025/09/02/what-can-europe-do-to-better-defend-against-gps-interference-from-russia.

[3] Amandine Hess, "Le interferenze ai sistemi Gps sono in aumento in Europa," Euronews, 2 settembre 2025, https://it.euronews.com/my-europe/2025/09/02/le-nterferenze-ai-sistemi-gps-sono-in-aumento-in-europa.

[4] Proietti, Lorenzo, "Volo von der Leyen, il Governo italiano corre ai ripari. Crosetto: 'Nella cyber war episodi così sono centinaia al giorno'" *Cybersecitalia.it*, 2 settembre 2025. https://www.cybersecitalia.it/volo-von-der-leyen-il-governo-italiano-corre-ai-ripari-crosetto-nella-cyber-war-episodi-cosi-sono-centinaia-al-giorno/50794/.

[5] Consiglio dell'Unione europea, "Call for Common Actions in Response to Global Satellite Navigation Systems (GNSS) Jamming and Spoofing Threats" *Council of the European Union*, 4 giugno 2025. https://data.consilium.europa.eu/doc/document/ST-9188-2025-REV-1/en/pdf.

mancanza di uno spazio di analisi unicamente dedicato alla guerra elettronica e allo sfruttamento malevolo dello spettro elettromagnetico, analizzato invece congiuntamente alla minaccia cibernetica.

Sebbene alcuni tra i Paesi occidentali che stanno revisionando la propria struttura e organizzazione interna del comparto difesa oggi non separano guerra elettronica e guerra cyber, facendole convergere in un'unica struttura di comando, si pensi al *Mando Conjunto del Ciberespacio* (MCCE) in Spagna, il *Cyber & ElectroMagnetic Command* (CEMC) britannico, il *Cyber and Information Domain Service* (CIDS) tedesco, oggi si parla di una sostanziale convergenza di capacità informatiche e elettroniche, fondando l'argomento su un'intersezione funzionale, operativa e tecnologica a più livelli. Oltre a colpire gli stessi bersagli con vettori diversi (rispettivamente logica interna e mezzo fisico di trasmissione), gli strumenti cibernetici e elettronici offensivi agiscono in maniera dinamica, con azioni EW che abilitano attacchi cyber e, viceversa, azioni cibernetiche che degradano capacità elettroniche. E' fondamentale comprendere che i sistemi informatici odierni dipendono strutturalmente dallo spettro elettromagnetico: trattare il secondo in maniera dedicata è allora essenziale per comprendere lo stato dell'arte della strategia e della capacità tecnologica europea per difendersi dalle minacce ibride nella loro varietà. Questo contributo muove da questa consapevolezza, indagando come il nuovo panorama di minaccia e sfruttamento nello spazio elettromagnetico nonché il caso russo-ucraino forniscano spunti di riflessione per colmare gap e asimmetrie dei paesi europei di fronte al ridimensionamento delle alleanze occidentali.

Definire lo spazio elettromagnetico

Lo sfruttamento delle capacità elettroniche è un aspetto della guerra moderna che sfida la comprensione delle dinamiche di forza tradizionali a causa della sua natura tecnica e cangiante. L'aumento della sofisticazione di tali capacità e delle *multidomain operations*, tuttavia, richiedono di definire i confini, il potenziale e le implicazioni dell'Electronic Warfare (EW).

La Commissione Europea riconosce il carattere strategico dell'EW che agisce come "vero e proprio moltiplicatore di forza"[6] terrestre, aerea, marittima, spaziale e cibernetica, domini che dipendono da un accesso sicuro allo spazio elettromagnetico. Essa fornisce una *real-time situational awareness*, rafforza il comando e il controllo, migliorando la precisione di puntamento e, garantendo al contempo la resilienza operativa in ambienti contesi in cui le comunicazioni, i radar e i sistemi di navigazione satellitare sono esposti a interruzioni o blocchi[7]. Lo scopo della guerra elettronica è allora la negazione del vantaggio derivante dall'utilizzo dello spettro elettromagnetico all'avversario[8], combinando capacità offensive, difensive e di supporto. L'attività nello spettro elettromagnetico può infatti assumere la forma ausiliaria con il supporto elettromagnetico (ES - oppure, secondo la terminologia NATO, Misure di Supporto Elettronico/ESM): la fornitura di intelligence militare tramite rilevamento, localizzazione, intercettazione, identificazione e analisi dei segnali radar e di comunicazione[9] al fine di riconoscere minacce, e supportare la fase di *targeting* la pianificazione e

[6] Commissione europea, "Electronic Warfare" *European Commission – Directorate-General for Defence Industry and Space*, dicembre 2025. https://defence-industry-space.ec.europa.eu/system/files/2025-12/Factsheet-Electronic-Warfare.pdf.
[7] Ibidem.
[8] NATO, "Electromagnetic warfare" *NATO*, 22 marzo 2023. https://www.nato.int/en/what-we-do/deterrence-and-defence/electromagnetic-warfare.
[9] Rohde & Schwarz, "Electromagnetic warfare", https://www.rohde-schwarz.com/it/soluzioni/aerospace-and-defense/multi-domain/sigint-ew/electromagnetic-warfare/electromagnetic-warfare_233140.html.

la condotta di operazioni in altri domini. La forma offensiva dello sfruttamento dell'EMS concerne invece l'attacco elettromagnetico (EA), che mira ad interrompere e negare capacità, degradare o distruggere[10] infrastrutture delle forze nemiche attraverso l'uso strategico di armi elettromagnetiche o a energia diretta. Esempi pratici di tale capacità possono essere il *jamming* di segnali nemici che ostacolano le capacità di difesa aerea o navale (radio, radar e GPS), lo *spoofing* attraverso la trasmissione di segnali falsificati per ingannare i sensori nemici, l'uso di *High-speed Anti-Radiation Missile* per rilevare, colpire e distruggere gli emettitori radar nemici - uno strumento chiave nelle operazioni di soppressione/distruzione della difesa aerea nemica (SEAD/DEAD)[11]. Non da ultimo, le contromisure all'attività offensiva nello spettro elettromagnetico pertengono alla protezione elettromagnetica che, come suggerisce il nome, implica la protezione delle capacità proprie e alleate di utilizzare lo spettro elettromagnetico[12] e operarvi indipendentemente dalle condizioni, tra cui contestazione, congestione, accesso negato[13]. Le misure di protezione elettronica sono incluse nei sistemi dipendenti dallo spettro: alcuni esempi di tale utilizzo sono la bassa probabilità di intercettazione o rilevamento (LPI/LPD, tecniche che rendono i segnali radar meno soggetti a intercettazione[14]), l'*anti-jamming* e il salto di frequenza (tecnica di trasmissione radio in cui il segnale trasmette cambiando

[10] Lockheed Martin, "Electronic Warfare" *Lockheed Martin*, 2025. https://www.lockheedmartin.com/en-us/capabilities/electronic-warfare.html.
[11] Kass, Harrison, "The AGM-88 HARM Is Still an Important Part of the Nation's Air Defenses" *The National Interest*, 5 dicembre 2025.
[12] Congressional Research Service, "Defense Primer: Electronic Warfare" *Congressional Research Service*, 26 febbraio 2019. https://sgp.fas.org/crs/natsec/IF11118.pdf.
[13] Dirk A. D. Smith e Steve Tourangeau, "Electronic Protective Measures" *Joint Air & Space Power Conference 2021 Read Ahead, Joint Air Power Competence Centre*, maggio 2021. https://www.japcc.org/essays/electronic-protective-measures/.
[14] Fuller, K. L., "To See and Not Be Seen" *IEE Proceedings F Radar and Signal Processing* 137, no. 1, giugno 2010.

rapidamente la frequenza portante, seguendo una logica di passaggio predefinita, pseudocasuale e nota solo al sistema trasmettitore e ricevitore).

Capacità russe e mutamento dell'equilibrio nello spettro elettromagnetico

Benché non rappresenti una novità, è con la guerra in Ucraina che la guerra elettronica è tornata al centro dell'attenzione, assumendo un ruolo primario nella gestione dei conflitti contemporanei e riportando al centro della competizione globale lo spazio elettromagnetico dopo anni di supremazia occidentale riscontrabile in Afghanistan[15] e Iraq[16], ambienti a bassa contestazione nemica. Una delle prime delle prime applicazioni[17] dello spazio elettromagnetico a fini militari si registrò infatti durante la guerra russo-giapponese. Divenuto decisivo tra le due guerre e in particolare nella Seconda Guerra mondiale[18], lo sfruttamento dello spettro consentì ad esempio alla Gran Bretagna[19], all'inizio degli anni '30, di rispondere alla crescente potenza aerea tedesca attraverso l'efficace sistema di allerta precoce Chain Home Low, grazie al quale fu possibile per la Royal Air Force captare le onde radio riflesse dagli aerei nemici e intercettare i tedeschi. Più tardi il successo della guerra elettronica americana durante la Guerra del Golfo dimostrò che la EW, se pianificata e integrata a livello sistemico e dottrinale, è un moltiplicatore decisivo della

---

[15] Von Spreckelsen, Malte, op.cit.

[16] DesertStorm30 — Electric Avenue: Electronic Warfare and the Battle Against Iraq's Air Defences During Operation Desert Storm", op.cit.

[17] Von Spreckelsen, Malte, "Electronic Warfare – The Forgotten Discipline" Joint Air Power Competence Centre Journal Edition 27, dicembre 2018, https://www.japcc.org/articles/electronic-warfare-the-forgotten-discipline/.

[18] Thurbon, M. T., "The Origins of Electronic Warfare" *The RUSI Journal* 122, no. 3 (1977): 56-63, https://www.tandfonline.com/doi/pdf/10.1080/03071847709428739.

[19] Garcia-Atutxa, Igor, Hodei Calvo-Soraluze, Ekaitz Dudagoitia Barrio e Francisca Villanueva-Flores, "The Strategic and Technological Impact of Radar in World War II" *History of Science and Technology* 15, no. 1 (giugno 2025): 62-78, https://www.researchgate.net/publication/392910567_The_strategic_and_technological_impact_of_radar_in_World_War_II.

potenza militare che garantisce la superiorità. Quest'ultima rimase però a lungo incontestata, riducendo la centralità percepita delle capacità elettroniche alleate mentre la diffusione di tecnologie commerciali e l'emergere di attori dotati di capacità avanzate hanno reso l'ambiente elettromagnetico sempre più conteso.

In questo senso è rilevante il rapido emergere di capacità avversarie di Russia e Cina[20] che hanno saputo sfruttare l'ambiente permissivo creato da una sostanziale inerzia occidentale e soprattutto statunitense, complice del passaggio da una strategia di supremazia e contestazione dei domini, ad un'altra nello scenario post-Guerra Fredda imperniato sulla controinsurrezione[21] e su teatri asimmetrici a bassa intensità tecnologica.

A differenza dell'Occidente, in particolare la Russia post-91 ha sviluppato uno degli arsenali di guerra elettronica più avanzati e sofisticati per sopperire e offrire una soluzione asimmetrica ai limiti cinetici rispetto alle operazioni di attacco di precisione della NATO, in modo da disturbare e interrompere il C4ISR[22] (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance), sfruttando lo spettro come un vero moltiplicatore di forza e un formidabile asset di supporto al combattimento.

---

[20] Magnuson, Stew, "Daily Fight for Ukraine Spectrum Superiority Puts Electronic Warfare Front, Center" *National Defense Magazine*, 8 marzo 2024, https://www.nationaldefensemagazine.org/articles/2024/3/8/daily-fight-for-ukraine-spectrum-superiority-puts-electronic-warfare-front-center.

[21] Gargasson, Clara, e Black, James, "Electromagnetic Warfare: NATO's Blind Spot Could Decide the Next Conflict" RAND Corporation, 24 novembre 2025, https://www.rand.org/pubs/commentary/2025/11/electromagnetic-warfare-natos-blind-spot-could-decide.html.

[22] Reach, Clint, Demus, Alyssa, Grisé, Michelle, Holynska, Khrystyna, Lynch, Christopher, Massicot, Dara, e Woodworth, David, "Russia's Evolution Toward a Unified Strategic Operation: The Influence of Geography and Conventional Capacity", RAND Corporation RR-A1233-8, 2023, https://www.rand.org/pubs/research_reports/RRA1233-8.html.

A partire dal 2008 e dalla riforma delle Forze Armate del Cremlino, che ha portato l'organizzazione a strutturarsi da un sistema divisionale a uno basato su brigate di manovra, ogni una di esse è stata integrata con delle unità di guerra elettronica (unità EW). Una caratteristica saliente delle forze terrestri russe, infatti, è l'organicità di questo inserimento, in quanto una simile struttura implica che le forze russe non conducano operazioni senza il necessario supporto elettronico. Sintomo della centralità dedicata alle capacità EW è poi la riorganizzazione delle singole unità a livello operativo e strategico: nel 2009 e nel 2015 sono state costituite due nuove brigate, la 15° e la 19°, rispettivamente nei distretti militari occidentale e meridionale, nell'Oblast di Tula e a Rassvet[23].

Ad oggi, almeno 14 unità militari di guerra elettronica russe sono supportate da oltre quattrocento siti radar distribuiti nei suoi territori e in quelli alleati e sono organizzate e distribuite geograficamente come mostrato nella Fig. 1

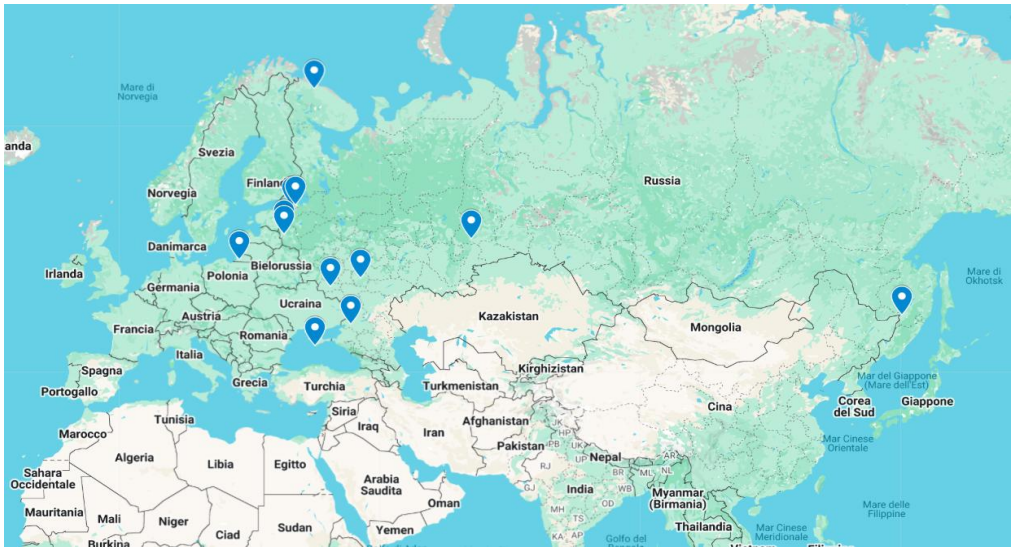


Fig. 1. Siti radar russi. Elaborazione dell'autore.

[23] McDermott, Roger N., "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum", International Centre for Defence and Security, settembre 2017, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

La logica di integrazione delle capacità specifiche di EW su tutta la catena operativa si evince dall'organizzazione: cinque delle unità sopracitate fanno riferimento al GS (General Staff), quattro alle Ground Forces (GF), tre alla Marina, tre alle forze aerospaziali (VKS-*Vozdušno-kosmičeskie sily*) e due alle forze strategiche missilistiche o *Raketnye Vojska Strategičeskogo Naznačenija*, RVSN e qui note come SRF (*strategic rocket forces*)[24].

E' interessante sottolineare come la maggior parte delle unità sia dotato del sistema Murmansk-BN, *jammer gound-based* di potenza 400-kw progettato specificamente per bloccare le comunicazioni satellitari militari ad alta frequenza statunitensi e della NATO. Dotato di un raggio d'azione di circa 5,000-8,000 km[25], infatti, viene utilizzato per condurre ricognizioni radio, intercettare e sopprimere i segnali nemici nell'intera gamma delle onde corte con frequenze da 3 a 30 MHz comunemente utilizzate da navi da guerra e aerei. Sul teatro europeo, i principali siti HF Global Communications System (HFGCS) si trovano presso la base di Sigonella in Sicilia e la base della Royal Air Force di Croughton, nel Regno Unito.

Secondo le stime sul "minimum jamming range"[26], cioè la distanza minima alla quale il jammer deve trovarsi rispetto al ricevitore per risultare efficace, in funzione della distanza tra l'emittente HF e il ricevitore, affinché il Murmansk

---

[24] McDermott, Roger N., Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum International Centre for Defence and Security, settembre 2017, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

[25] Army Recognition, "Murmansk-BN Electronic Warfare Communications Jamming System" *Army Recognition*, 9 agosto 2024, https://www.armyrecognition.com/military-products/army/electronic-warfare/murmansk-bn-electronic-warfare-communications-jamming-system-data?highlight=WyJydXNzaWEiXQ%3D%3D.

[26] Reach, Clint, Demus, Alyssa, Grisé, Michelle, Holynska, Khrystyna, Lynch, Christopher, Massicot, Dara, e Woodworth, David, "Russia's Evolution Toward a Unified Strategic Operation: The Influence of Geography and Conventional Capacity", RAND Corporation RR-A1233-8, 2023, https://www.rand.org/pubs/research_reports/RRA1233-8.html.

possa operare fino a un raggio massimo di 5.000 km, è necessario che trasmettitore e ricevitore si trovino ad almeno 500 km l'uno dall'altro.

La Fig. 2 mostra i siti HFGCS statunitensi/NATO accompagnati da un cerchio blu che rappresenta circa 500km di distanza.

Fig. 2. Siti HFGCS USA/NATO. Elaborazione dell'autore.

Pertanto, quando gli HFGCS comunicano con sistemi localizzati fuori dal perimetro massimo dei 500 km, ovvero al di fuori dal sud Italia e dalle vicinanze del Regno Unito, il Murmansk raggiunge la sua massima portata e le comunicazioni HF possono essere compromesse o interrotte completamente, costringendo la NATO a ricorrere ad architetture alternative o al SATCOM.

A seconda della specificità del conflitto, la perdita delle comunicazioni ad alta frequenza sarebbe tuttavia rilevante in quanto tali sistemi non sono completamente sostituibili da architetture satellitari. Le comunicazioni HF, infatti, rappresentano una capacità indipendente dai satelliti e possono operare anche in contesti *GNSS-denied o space-denied* in cui i sistemi SATCOM sono

vulnerabili al rilevamento e interferenze[27], pertanto la loro degradazione o negazione costituisce comunque un problema operativo significativo, poiché in grado di limitare la flessibilità e la resilienza delle operazioni NATO.

Dipendenze e asimmetrie capacitive: vulnerabilità dell'Alleanza nello spettro elettromagnetico.

L'evoluzione delle capacità russe e l'integrazione delle capacità elettroniche dimostrata durante il conflitto russo-ucraino risulta ancor più allarmante se inserita nel più ampio quadro di riflessione circa le vulnerabilità strutturali dell'Alleanza Atlantica. Nonostante il ritorno della centralità dello spettro elettromagnetico nei conflitti odierni, la sua dipendenza verso gli strumenti essenziali per le strategie di guerra ibrida e l'aumento di investimenti e sforzi, la NATO oggi presenta vulnerabilità derivanti dalla forte dipendenza capacitiva dai sistemi statunitensi nei settori chiave del C4ISR, del SATCOM, della protezione elettronica e delle capacità avanzate di EW. In un contesto caratterizzato da incertezza rispetto all'impegno statunitense verso gli alleati europei, esacerbato dalle rinnovate richieste di maggiore assunzione di responsabilità e carico degli oneri finanziari, tale dipendenza si traduce in una vulnerabilità sistemica, obbligando la NATO a riflettere a un necessario cambio di paradigma[28].

La succitata dipendenza riguarda soprattutto la raccolta, la distribuzione e la capacità analitica ELINT (*electronic intelligence*)[29] e risultanti dati, gestione e

[27] Rohde & Schwarz, "HF Communications" Rohde & Schwarz, https://www.rohde-schwarz.com/lat/soluciones/aerospace-and-defense/sea/naval-systems/communications-systems/hf-communications_255935.html.

[28] Tim Martin, "NATO requires an electronic warfare 'paradigm shift' to beat Russia, says alliance official," *Breaking Defense*, 12 maggio 2025, https://breakingdefense.com/2025/05/nato-requires-an-electronic-warfare-paradigm-shift-to-beat-russia-says-alliance-official/.

[29] La raccolta ELINT (Electronic Intelligence, o Intelligenza Elettronica) è la raccolta e analisi di segnali elettronici non di comunicazione, come quelli provenienti da radar, sistemi d'arma o sensori, per identificare le capacità, le posizioni e le attività di un avversario nello spettro elettromagnetico, fornendo informazioni cruciali per la difesa e la pianificazione strategica. È una sottocategoria della SIGINT (Signals Intelligence) e differisce da essa perché si concentra

centralizzazione delle librerie delle minacce[30] e di conseguenza la soppresione elettronica delle difese aeree nemiche SEAD e jamming, che si appoggiano in maniera sostanziale e fondamentale alle prime. In effetti, l'esercito USA gestisce[31] di gran lunga la flotta più grande e diversificata di risorse ISR (*Intelligence, Surveillance, and Reconnaissance*) aeree e orbitali dell'Alleanza, nonché alcune piattaforme di raccolta ELINT non tradizionali più efficienti. A ciò si aggiunge anche il monopolio della gestione del Dinstributed Common Ground System[32], un'architettura di rete globale in cui i dati provenienti dalle piattaforme ISR possono essere caricati, trasmessi alle entità militari e alle agenzie di intelligence competenti del governo degli Stati Uniti e del Dipartimento della Difesa di Washington per essere analizzati e sfruttati, e successivamente redistribuiti come prodotti di intelligence ai gruppi di utenti attivi in prima linea.

Gli Stati Uniti mantengono anche le librerie di minacce più complete e aggiornate della NATO e su cui molti alleati fanno affidamento, sia attraverso l'accesso diretto (ove gli accordi di sicurezza lo consentono), sia attraverso gli

---

sui segnali di macchine e non su quelli di comunicazione umana. ELINT è l'informazione derivata principalmente da segnali elettronici che non contengono voce o testo (che sono considerati COMINT)

[30] Una libreria delle minacce di guerra elettronica (EW) è un database sicuro e curato che raccoglie le caratteristiche degli emettitori nemici identificati—come frequenze radar, modulazione e schemi di impulsi—utilizzato dalle forze armate per rilevare, classificare e contrastare segnali ostili in tempo reale. Queste librerie supportano le operazioni di supporto elettronico (ES) e di attacco elettronico (EA), fornendo informazioni a sistemi come i Radar Warning Receiver (RWR).

[31]Justin Bronk, Airborne Electromagnetic Warfare in NATO: A Critical European Capability Gap, RUSI, 2025, https://static.rusi.org/airborne-electronic-warfare-in-nato_0.pdf.

[32] U.S. Air Force, "Air Force Distributed Common Ground System," U.S. Air Force Fact Sheets, s.d., https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104525/air-force-distributed-common-ground.

aggiornamenti dei dati di missione forniti dagli Stati Uniti per i sistemi d'arma di fabbricazione americana come l'F-35 e l'F-16[33].

Tuttavia, non si può parlare di dipendenza totale dagli USA in quanto alcuni paesi europei dell'alleanza dispongono di capacità nei campi di raccolta, PED (Processing, Exploitation, and Dissemination) e nella generazione e sfruttamento dei dati di missione. Parigi e Stoccolma, ad esempio, producono ECM (Electronic Countermeasures) altamente efficienti per i caccia Rafale (francesi) e Gripen (svedesi) oltre a disporre di capacità nazionali di produzione di aggiornamenti dei dati di missione per tali sistemi d'arma e raccolta ELINT. Anche Italia e Germania possono contare su capacità di ESM (Electronic Support Measures) e ECM a supporto dei prossimi programmi Eurofighter EK e EA-37b. In questo senso, è essenziale sottolineare il ruolo chiave della cooperazione industriale europea nello sviluppo di sistemi che efficientino le capacità di EW comuni. Il consorzio EuroDASS composto dalle italiane Leonardo ed ELT Group, la spagnola Indra e la tedesca Hensoldt ha reso noto, a fine 2024, un nuovo sistema di guerra elettronica di nuova generazione per il caccia Eurofighter Typhoon. Questo sistema è progettato per proteggere e far sopravvivere l'aereo contro minacce moderne e future senza richiedere modifiche alla struttura esterna dell'aereo, attraverso l'uso congiunto di tecnologie radio, AI e machine learning[34].

Nel 2022, l'Italia è inoltre diventata la nuova nazione partner dell'F-35 Partner Support Complex (PSC) a completare da sola il suo primo Mission Data File (MDF) a supporto della flotta F-35 Lightning II dell'Aeronautica Militare Italiana,

[33] I file di dati di missione (MDF) sono "enciclopedie di combattimento" digitali contenenti informazioni vitali sulle minacce (radar nemici, SAM) per gli aerei, ne sono un esempio quelle esistenti per gli F-35 e F-16

[34] ELT Group, "Revealed: The next generation electronic warfare system for Eurofighter Typhoon that won't require updates to its airframe," *Press release*, 20 novembre 2024, https://www.eltgroup.net/media/press-release/revealed-the-next-generation-electronic-warfare-system-for-eurofighter-typhoon-that-wont-require-updates-to-its-airframe/ .

segnando un fondamentale e necessario passo avanti per la piena capacità operativa della flotta italiana.

Un'altra delle principali aree di dipendenza strutturale dalla NATO risiede nelle capacità di *airborne electronic attack* (EA), in particolare il *support jamming*. Attualmente, quasi l'intera capacità dell'Alleanza in questo ambito risiede negli EA-18G Growler[35] della US Navy, affiancati in misura minore dagli assetti EC-130H e EA-37B Compass Call dell'US Air Force. Al di fuori degli Stati Uniti, non esistono capacità equivalenti nelle aeronautiche NATO, con la sola eccezione parziale dell'Italia, che ha ordinato due EA-37B[36] destinati a entrare in servizio nella seconda metà degli anni 2020. Gli assetti europei attualmente disponibili, come gli F-16CM statunitensi basati in Europa, i Tornado ECR italiani e tedeschi, sono principalmente piattaforme SEAD dotate di avanzate capacità di ESM e di ECM difensivo, ma incapaci di fornire *escort jamming* dedicato paragonabile a quello assicurato dai Growler. Il programma Eurofighter EK tedesco, destinato a sostituire i Tornado ECR, migliorerà le capacità di SEAD stand-off entro il 2030, ma l'introduzione di una reale capacità di *airborne* EA di supporto rimane confinata a una fase di pianificazione ("Step 2") e non sarà operativa prima dei primi anni 2030.

Al di fuori dei casi sopra menzionati che rappresentano delle eccezioni, la maggior parte dei membri europei dell'Alleanza non dispone di capacità dedicate a raccolta ed analisi profonda ELINT in quanto è complesso sviluppare e mantenere queste aree di specializzazione in forze armate di piccole e medie

[35] Bronk , J., Watling, J., *Rebalancing European Joint Fires to Deter Russia*, Occasional Paper (London: Royal United Services Institute for Defence and Security Studies, aprile 2025), https://static.rusi.org/rebalancing-european-joint-fires-to-deter-russia.pdf.
[36] "L'EA-37B ha effettuato il primo volo addestrativo," *Rivista Italiana Difesa (RID)*, 15 maggio 2025, https://www.rid.it/shownews/7293/l-rsquo-ea-37b-ha-effettuato-il-primo-volo-addestrativo.

dimensione che non godono delle dinamiche di economie di scala. In questo senso, appare necessario e potenzialmente vantaggioso per i membri europei della NATO promuovere una maggiore integrazione degli sforzi a livello comunitario, sviluppando capacità ELINT e EW condivise che consentano di superare i limiti strutturali delle singole forze armate nazionali. In particolare, la cooperazione europea potrebbe concentrarsi sulla creazione di architetture comuni per la raccolta, l'archiviazione e l'analisi dei dati elettromagnetici, nonché sullo sviluppo congiunto di file di missione, librerie di segnali, registri ELINT ed ecosistemi di data fusion, riducendo la dipendenza da assetti e *know-how* statunitensi e rafforzando, al contempo, l'autonomia strategica europea anche nel dominio elettromagnetico.

Resilienza e adattamento nel dominio elettromagnetico: il caso ucraino

Il recente conflitto in Ucraina ha rappresentato un punto di svolta nella percezione della guerra elettronica, sottolineando la rilevanza operativa del dominio elettromagnetico, obbligando la NATO ad una rinnovata consapevolezza delle proprie carenze e dipendenze di fronte all'attivismo della Russia e del rapido adattamento capacitivo dell'Ucraina. Vi sono infatti segnali che questo divario di capacità sia stato recepito dagli Alleati: ad aprile scorso[37] dieci nazioni NATO e l'Ucraina hanno inaugurato la Coalizione per la guerra elettronica[38]. Il quadro di cooperazione, analogamente alle coalizioni già esistenti nei settori della guerra aerea, artiglieria e droni, è volto a formalizzare lo scambio di conoscenze e equipaggiamenti tra i firmatari (Germania, Francia, Repubblica

[37]J. Knowles, "European Nations Establish EW Coalition," *Journal of Electromagnetic Dominance (JED)*, 18 aprile 2025, https://www.jedonline.com/2025/04/18/european-nations-establish-ew-coalition/.

[38]Ministry of Defence of Ukraine, "Ramstein: What the Ukraine Defense Contact Group Meetings Delivered for Ukraine in 2025," *Ministry of Defence of Ukraine*, 2025, https://mod.gov.ua/en/news/ramstein-what-the-ukraine-defense-contact-group-meetings-delivered-for-ukraine-in-2025.

Ceca, Danimarca, Lettonia, Lituania, Norvegia, Polonia, Regno Unito) e l'Ucraina. L'Italia ha raggiunto[39] la Coalizione qualche mese dopo, insieme a Belgio, Estonia e Svezia. Questa accelerazione e approfondimento nella cooperazione tra Ucraina e membri NATO muove dal fatto che le dinamiche del conflitto tra Kiev e Mosca hanno scardinato l'assunto per cui la superiorità quantitativa e qualitativa nel dominio elettromagnetico garantirebbe automaticamente il controllo dello spettro. Pur partendo da una posizione di marcata inferiorità rispetto alla Federazione Russa, l'Ucraina ha infatti dimostrato una capacità di adattamento rapida e in larga parte inattesa, risultato reso possibile dalla combinazione di tecnologie di origine occidentale, integrazione in soluzioni native e operazioni decentralizzate[40]. Uno degli elementi fondamentali della risposta ucraina è stata la protezione e garanzia di continuità delle comunicazioni C2 in un ambiente altamente contestato dal *jamming* russo grazie all'impiego di radio a salto di frequenza fornite dagli USA e l'utilizzo dei terminali Starlink[41]. Accanto al supporto occidentale Kiev ha anche sviluppato soluzioni innovative a basso costo, spesso appoggiandosi a tecnologie commerciali[42], tra cui il Bukovel-AD[43] anti-drone, *jammer* portatili e droni dotati di intelligenza

[39]Robert Wall, "Ukraine Electronic Warfare Coalition Expands With More NATO Members," *Aviation Week & Space Technology*, 9 giugno 2025, https://aviationweek.com/defense/sensors-electronic-warfare/ukraine-electronic-warfare-coalition-expands-more-nato-members.

[40] Brig Jaideep Agarkar, "Russia-Ukraine War: Lessons from an Electronic Warfare (EW) Perspective," *Centre for Land Warfare Studies (CLAWS)*, 31 maggio 2025, https://claws.co.in/russia-ukraine-war-lessons-from-an-electronic-warfare-ew-perspective/.

[41] Valentina Chabert, Guerre spaziali. Conflitti e competizione per le risorse nell'era delle società private (Milano: Ledizioni, 2025).

[42]Aosheng Pusztaszeri e Emily Harding, "Technological Evolution on the Battlefield," in War and the Modern Battlefield: Insights from Ukraine and the Middle East, CSIS Defense and Security Department, 16 settembre 2025, https://www.csis.org/analysis/chapter-9-technological-evolution-battlefield.

[43] Vadim Kushnikov, "Ukrainian *Bukovel-AD* EW system 'landed' Russian ZALA 421-16E2 UAV," *Militarnyi*, 16 marzo 2023, https://militarnyi.com/en/news/ukrainian-bukovel-ad-ew-system-landed-russian-zala-421-16e2-uav/.

artificiale in grado contrastare e contrattaccare il disturbo elettromagnetico russo[44].

Le capacità ucraine nel dominio elettromagnetico rappresentano oggi un caso di studio di valore strategico per la NATO, non solo per ciò che riguarda le tecnologie impiegate, ma soprattutto per l'approccio adottato osservato. L'integrazione di equipaggiamenti occidentali, soluzioni commerciali e innovazioni locali ha dimostrato che è possibile bilanciare una superiorità EW avversaria attraverso resilienza e agilità. L'esperienza ucraina non va però compresa limitatamente come un insieme di contromisure tattiche, bensì essa rappresenta l'espressione di un modello di adattamento sistemico in cui le capacità militari e tecnologiche si uniscono ad un'architettura statale che accoglie l'innovazione in maniera flessibile, convergendo in un ecosistema resiliente e reattivo[45] e costituendo, pur riconoscendo le specificità del caso, un modello esportabile di integrazione tra EW, obiettivi strategici e governance dell'innovazione. Il processo di trasformazione digitale ucraina in tempo di guerra ha visto un ruolo dello Stato tutt'altro che centralizzante e gerarchico, bensì come facilitatore di sinergie distribuite tra forze armate, settore privato[46] e collaborazione occidentale che ha ridotto drasticamente i tempi di reazione e adattamento con contromisure adeguate. Per la NATO e soprattutto per gli alleati

[44] Nataliia Kushnerska, "Missiles, AI, and drone swarms: Ukraine's 2025 defense tech priorities," Atlantic Council, January 2, 2025, https://www.atlanticcouncil.org/blogs/ukrainealert/missiles-ai-and-drone-swarms-ukraines-2025-defense-tech-priorities/.
[45]Digital State UA, "ІІІІ на війні: чому український досвід виходить за межі дефенс і змінює модель цифрової держави," *Digital State UA*, 2 gennaio 2026, https://digitalstate.gov.ua/news/tech/shi-na-viyni-chomu-ukrayinskyy-dosvid-vykhodyt-za-mezi-defens-i-zminiuye-model-tsyfrovoyi-derzavy.
[46] GovTech Intelligence Hub, "*Ukraine's Digital Transformation as Europe's Digital Opportunity*," *GovTech Intelligence Hub*, 14 maggio 2025, https://www.govtechintelhub.org/case-study-details/ukraine%27s-digital-transformation-as-europe%27s-digital-opportunity/aJYTG0000000ZXF4A2.

europei (e l'UE)[47] il caso ucraino suggerisce che la competitività nel dominio elettromagnetico non dipende esclusivamente dall'implementazione a livello operativo di piattaforme avanzate ma dalla capacità di costruire ecosistemi di innovazione rapidi, aperti e integrati. In questo senso, Kiev contribuisce attivamente all'apprendimento strategico dell'Alleanza, offrendo un laboratorio operativo per la sperimentazione di dottrine, modelli organizzativi e operativi nel campo elettromagnetico, trasformando la Coalizione per la guerra elettronica da strumento di supporto a piattaforma di collaborazione, con scambio e co-evoluzione reciproci.

Conclusioni

Il conflitto russo-ucraino ha dimostrato in modo esplicito che il dominio elettromagnetico rappresenta oggi una delle arene decisive della competizione strategica contemporanea. Da un lato, le forze russe hanno dimostrato di aver sviluppato un apparato avanzato di guerra elettronica ampio e sofisticato e, dall'altro, il vissuto operativo ucraino ha sottolineato quanto le capacità elettromagnetiche costituiscano un'infrastruttura abilitante a maggiore resistenza nazionale, deterrenza più credibile e crescente autonomia strategica, oltre che fungere da moltiplicatore di forza alternativo a quella militare. Per la NATO, e in particolare per i suoi membri europei, i nuovi scenari operativi hanno evidenziato una certa asimmetria capacitiva segnata dalla marcata dipendenza dagli Stati Uniti in settori e capacità chiave di EW.

Tale vulnerabilità assume crescente spessore strategico se inserita nello scenario di generale ridimensionamento dell'impegno statunitense. In questo scenario, Kiev emerge non come semplice destinatario di assistenza, ma come

[47] Kai Zenner, "Ukraine built a digital state under fire — what's the EU waiting for?," *Euractiv*, 18 settembre 2025, https://www.euractiv.com/opinion/ukraine-built-a-digital-state-under-fire-whats-the-eu-waiting-for/.

ente attivo nel processo di riflessione e apprendimento dell'Alleanza di fronte ai nuovi caratteri della guerra ibrida. Il percorso ucraino di governance tecnologica come *digital state under fire*[48] consente di avanzare una velata critica costruttiva alla lentezza con cui l'Unione Europea ha cercato di tradurre le proprie ambizioni[49] di autonomia e indipendenza strategica in capacità reali in ambito di difesa tecnologica.

Le nuove priorità hanno certamente condotto l'Unione Europea ad un impegno finanziario oltre che politico senza precedenti per rafforzare le basi della difesa europea: ad aprile scorso la Commissione ha proposto modifiche ai programmi di finanziamento UE a sostegno delle tecnologie legate alla difesa, comprese le applicazioni a duplice uso come l'intelligenza artificiale e la sicurezza informatica, oltre ad impegnarsi per accelerare e flessibilizzare gli investimenti nella base industriale e tecnologica di difesa europea (EDTIB)[50]. Tra le tecnologie individuate nel Libro Bianco sulla difesa europea e incluse nella piattaforma per le tecnologie strategiche per l'Europa (STEP)[51], vi sono anche i sistemi di difesa elettronica, considerati pilastro per una difesa europea concreta ma anche identificati tra le aree di vulnerabilità su cui lavorare e investire.

---

[48] Kai Zenner, "Op-ed on 'Ukraine built a digital state under fire – what's the EU waiting for?'," *Digitizing Europe (blog)*, 18 settembre 2025, https://www.kaizenner.eu/post/op-ed-on-ukraine-built-a-digital-state-under-fire-what-s-the-eu-waiting-for/.

[49] Nico Lange e Fabrice Pothier, "To protect itself, Europe needs the systems that make warfare work," *The Economist*, 27 gennaio 2026, https://www.economist.com/by-invitation/2026/01/27/to-protect-itself-europe-needs-the-systems-that-make-warfare-work.

[50] COcyber, "EU budget boost for defence: Commission mobilises €910M and proposes new regulation," *COcyber* (24 ottobre 2025), https://cocyber.eu/index.php/article-news/eu-budget-boost-defence-commission-mobilises-eu910m-and-proposes-new-regulation.

[51] European Commission, *"Strategic Technologies for Europe Platform (STEP) to boost investments in critical technologies,"* Defence Industry and Space, Commissione Europea, pubblicato online, https://defence-industry-space.ec.europa.eu/funding-opportunities/strategic-technologies-europe-platform-step-boost-investments-critical-technologies_en.

Parte della resilienza europea in ambito difesa potrebbe essere ottenuto, come dimostrato per il caso delle capacità elettroniche, da spostamenti nelle strategie di approvvigionamento delle nazioni europee: i paesi europei hanno storicamente acquisito da *prime contractor* della difesa con sede negli Stati Uniti una parte significativa dei loro equipaggiamenti (circa il 64% degli equipaggiamenti esternalizzati proviene dagli Stati Uniti)[52]. Secondo alcune stime, si prevede che il nuovo impegno europeo in materia di difesa e l'impegno a investire nella capacità produttiva nazionale ridurranno gradualmente la quota statunitense negli acquisti di nuovi equipaggiamenti a meno del 30% entro il 2035[53].

Queste dinamiche hanno implicazioni profonde per l'Europa e in particolare per l'Italia, che a livello industriale e tecnologico può giocare un ruolo di primo piano nello sviluppo di capacità avanzate per lo spettro elettromagnetico. Esempio del dinamismo italiano è l'attivismo di aziende nazionali come ELT Group, realtà con oltre 70 anni di esperienza nel settore e nella progettazione di sistemi elettronici applicati alla difesa che sta consolidando la propria posizione di riferimento nel panorama europeo. Attraverso l'espansione a nuovi mercati, l'apertura a nuove opportunità di applicazione delle capacità elettroniche ma soprattutto sancendo alleanze con partner industriali globali[54], il gruppo mira a far convergere gli

[52] Stockholm International Peace Research Institute, "Ukraine the world's biggest arms importer; United States' dominance of global arms exports grows as Russian exports continue to fall," press release, 10 marzo 2025, https://www.sipri.org/media/press-release/2025/ukraine-worlds-biggest-arms-importer-united-states-dominance-global-arms-exports-grows-russian.

[53] Roberto Scaramella, Archag Toulumian, Eric Ciampi, Julien Demotes-Mainard, e Luca Ceragioli, "Key Challenges Facing Europe: Proposed Defense Expansion," Oliver Wyman Insights, agosto 2025, https://www.oliverwyman.com/our-expertise/insights/2025/aug/key-challenges-facing-europe-proposed-defense-expansion.html.

[54] ELT Group, "TENET 2030: Corporate Plan – Innovate, Expand, Conquer," ELT Group (company strategic plan), pubblicato online, https://www.eltgroup.net/company/corporate-plan-tenet-2030/.

sforzi verso la concreta crescita della base industriale del Paese. A luglio 2025 ELT Group e la statunitense L3Harris hanno stretto una partnership per creare un centro di test e calibrazione ISR (Intelligence, Surveillance and Reconnaissance) per programmi commerciali, militari e governativi[55], che per la prima volta sarà disponibile al di fuori degli Stati Uniti e sarà aperto all'uso congiunto con forze alleate e partner strategici.

Tale cooperazione transatlantica, rafforzando l'interoperabilità e l'accesso a competenze di eccellenza, non si traduce tuttavia in una dipendenza strutturale dal partner statunitense. Al contrario, essa si inserisce in una più ampia strategia di diversificazione e proiezione autonoma, volta a rafforzare la capacità sovrana nazionale ed europea nel dominio elettromagnetico. In questa prospettiva si colloca, a titolo esemplificativo, l'accordo siglato da ELT Group con partner industriali dell'Arabia Saudita[56], che testimonia la volontà di ampliare il perimetro delle cooperazioni internazionali al di fuori dell'asse transatlantico, riducendo le vulnerabilità legate alle catene di approvvigionamento e rafforzando la resilienza industriale. Il caso di specie dimostra la crucialità di attori nel settore industriale che siano trainanti nello sviluppo di soluzioni *made in Europe* nel settore della guerra elettronica, contribuendo alla riduzione delle dipendenze esterne e al consolidamento di una reale autonomia tecnologica europea, in linea con le priorità strategiche dell'Unione.

Le evidenze emerse dal conflitto russo-ucraino e dalle vulnerabilità europee analizzate suggeriscono come l'UE debba maturare una piena consapevolezza

[55] "L3Harris ed ELT Group realizzeranno un impianto di collaudo multisensore in Italia," Analisi Difesa, 24 luglio 2025, https://www.analisidifesa.it/2025/07/l3harris-ed-elt-group-realizzeranno-un-impianto-di-collaudo-multisensore-in-italia/.

[56] "ELT Group firma un MoU con Pioneers Technical Systems a Ryad," *Analisi Difesa*, 11 febbraio 2026, https://www.analisidifesa.it/2026/02/elt-group-firma-un-mou-con-pioneers-technical-systems-a-ryad/.

dello spazio elettromagnetico non solo come dominio operativo da proteggere, ma come ambito strategico in cui sviluppare capacità proprie, filiere industriali resilienti e vantaggi tecnologici sostenibili. La risposta europea alla minaccia ibrida passa, dunque, anche dalla capacità di governare l'evoluzione tecnologica e industriale del dominio elettromagnetico, trasformandone la crescente complessità in un fattore di sicurezza, autonomia e competitività strategica.

Parole di guerra e guerra delle parole: il discorso come dominio del conflitto

di Sara Marchetti e Rachele Rigali

Introduzione

Da tempo ormai le Forze Armate hanno integrato nei loro piani operativi i principi della comunicazione e i mezzi di informazione: il controllo delle rappresentazioni e narrazioni della guerra è diventata una variabile strategica, pari all'addestramento del personale, alle risorse economiche o alla forza delle alleanze. L'informazione in tempo di guerra è un'arma a tutti gli effetti, in mano di chi per primo e meglio riesce ad utilizzarla per influenzare le percezioni dell'opinione pubblica.

Il linguaggio non è un mezzo neutrale di descrizione della realtà, bensì un dispositivo cognitivo che definisce le situazioni all'interno di specifici *frame* interpretativi. Le parole non rappresentano solo i fenomeni in maniera oggettiva, ma li classificano e li gerarchizzano, orientando la percezione sociale.

In termini di sicurezza questo meccanismo è fondamentale: a seconda della definizione attribuita a un evento si generano aspettative di risposta diverse. Definire un contesto come "crisi", "competizione", "interferenza" o "guerra" contribuisce a costruirlo nella coscienza comune. Sono le singole parole che si riempiono di significato, ed è significato politico: l'utilizzo di un termine piuttosto che un altro cambia la percezione nella mente di chi legge, di chi ascolta, e può portare a un "successo" o a un "fallimento" mediatico. Il linguaggio così diventa spazio di potere a tutti gli effetti.

Negli ultimi anni, insieme all'inasprimento delle ostilità e al moltiplicarsi degli scenari di guerra nel mondo, la narrazione mediatica sui conflitti è dominata dalla locuzione "guerra ibrida". È una categorizzazione la cui definizione non è condivisa tra attori ed esperti della politica, ma che in genere vuole indicare una strategia di conflitto che combina metodi convenzionali e non convenzionali – come disinformazione, attacchi cyber, pressione economica – volti a instaurare un conflitto sottosoglia rispetto ai conflitti tradizionali, per destabilizzare il nemico senza dichiarare formalmente guerra.

Descritta in questo modo la guerra ibrida non appare nulla di nuovo se confrontata con scenari di conflitto precedenti: già dal secolo scorso le guerre non hanno più bisogno di dichiarazioni per cominciare, gli attori di guerra non sempre sono due stati, l'informazione è utilizzata per manipolare l'opinione pubblica e tra i nemici si verificano solitamente importanti pressioni economiche.

Questo solleva un interrogativo: perché parliamo oggi di "guerra ibrida"? La risposta più immediata è che attraverso le nuove tecnologie gli attori politici possono impiegare strumenti non convenzionali in modo più efficace e pervasivo, creando uno spazio di tensione e conflitto quasi costante: la categorizzazione di "guerra ibrida" non circoscrive un evento o un teatro operativo e non prevede una conclusione definitiva, consolidando la percezione di una minaccia permanente e poliedrica. Tuttavia, questa locuzione non sta semplicemente ad indicare uno scenario di guerra diverso dal passato ma è un termine strategico, usato dai governi spesso per giustificare determinate scelte, per ridefinire la sicurezza nazionale e guidare le percezioni della popolazione.

Dal linguaggio alla percezione della realtà

È servita a tutti la lezione che gli Stati Uniti hanno appreso nella guerra del Vietnam, dove il mancato controllo delle comunicazioni ha giocato un ruolo determinante nella sconfitta americana: nessuna classe politica si può permettere di non curare l'informazione[1] . Ma dalla guerra in Vietnam all'attuale invasione dell'Ucraina molto è cambiato: dai dati relativi al 2025 emerge che il 67.9 % della popolazione totale ha accesso ad Internet e il 63.9 % utilizza account social[2]. Oggi l'informazione diventa ancora più diffusa e capillare, la gestione dei media va ben al di là del controllo delle immagini e dei discorsi ufficiali, si estende a quasi tutti gli aspetti della vita di una figura pubblica o di uno stato.

In questo contesto, affinché sia possibile un controllo accurato dell'informazione che contribuisce alla creazione dell'opinione pubblica, il controllo del linguaggio inteso come sistema formale con la sua sintassi e semantica, assume un ruolo chiave.

Questo concetto era molto chiaro a George Orwell quando in "1984" introdusse la "neolingua" – "newspeak" –: immagina nel futuro una società dominata da un regime totalitario, in cui viene creata una nuova-lingua, per esprimere la concezione del mondo condivisa dal partito dominante, ma soprattutto per rendere impossibile ogni altra forma di pensiero. A differenza di tutte le altre lingue, il vocabolario della neolingua diventa ogni giorno più sottile: minore scelta significa minore possibilità di far spaziare il pensiero. L'assenza di un termine per esprimere una sensazione, un oggetto, un colore, automaticamente rende quegli elementi invisibili alla nostra percezione e al nostro sistema

[1] Taylor, Philip M. *War and the Media: Propaganda and persuasion in the Gulf War*. Manchester University Press (1994). Pag. 40-41

[2] *We Are Social*, "Digital 2025 Global Overview Report". 5 febbraio 2025. https://wearesocial.com/uk/blog/2025/02/digital-2025-the-essential-guide-to-the-global-state-of-digital/.

cognitivo[3]. Orwell, che per immaginare una società del futuro sostanzialmente descrive i totalitarismi della sua epoca, ci insegna che il linguaggio è politico, che il modo in cui descriviamo e pensiamo il mondo non è casuale: le parole che usiamo per descrivere la nostra realtà sono i mezzi attraverso i quali pensiamo alla nostra realtà. Di conseguenza, anche senza arrivare alla censura capillare e sistematica del "grande fratello" (che pure non è distante da alcune realtà contemporanee), il modo in cui una classe politica, un governo, uno stato parla di un determinato fenomeno o evento spesso cerca di crearne una determinata idea o percezione nella popolazione.

L'idea che il linguaggio e il pensiero umano fossero correlati era già stata espressa in termini scientifici all'epoca di Orwell negli studi Benjamin Lee Whorf e Edward Sapir nel 1929, alla base della teoria del relativismo linguistico.[4] La loro tesi è che la nostra percezione del mondo e il nostro modo di pensare siano fortemente influenzati dalla struttura del linguaggio che usiamo. Se inizialmente non venne dato seguito a questa teoria per la mancanza di dati empirici, alcuni studi più recenti hanno effettivamente dimostrato una correlazione tra le strutture linguistiche e il modo di percepire il tempo, i colori, lo spazio, ecc. Per esempio, Boroditsky nel 2001 ha esaminato come il diverso modo di parlare del "tempo" in inglese e in cinese mandarino influenza la percezione del tempo di chi parla queste lingue. Gli inglesi parlano del tempo in modo orizzontale: parlano di persone che sono "ahead of their time" – avanti nel loro tempo – per indicare una persona dalle idee innovative, lungimiranti, e pensano anche che "March comes before April" – marzo viene prima di aprile. Il cinese mandarino invece parla dell'ordine degli eventi in modo verticale: "sopra" sono gli eventi che

[3] Orwell, George. *1984*. Einaudi (2021)

[4] Bruck, Scott E., "Lost In Translation: How Language Affects Perception During Armed Conflict". *Small Wars Journal*, 5 luglio 2019. https://archive.smallwarsjournal.com/jrnl/art/lost-translation-how-language-affects-perception-during-armed-conflict#_edn1

vengono prima, "sotto" sono gli eventi che vengono dopo, e quindi "marzo è sopra aprile".[5] Boroditsky constatò che i cinesi erano più veloci a confermare che agosto viene dopo di giugno se posti davanti a oggetti disposti in modo verticale; viceversa, gli inglesi erano più veloci a rispondere alla stessa domanda se messi davanti a una sequenza di oggetti orizzontale.[6] Questi dati suggeriscono dunque che il linguaggio forma il modo in cui popoli di lingue differenti concettualizzano il tempo.

Studi analoghi sono stati effettuati anche all'interno della stessa lingua: Loftus e Palmer (1974) hanno studiato come cambiamenti nel modo di porre una domanda possono portare a cambiamenti della percezione della realtà e nella memoria di un evento. Le loro analisi hanno riguardato la ricostruzione di un evento complesso, come un incidente automobilistico. I partecipanti a cui venne chiesto quanto veloce andassero le macchine quando si sono "scontrate" o "distrutte", hanno stimato una velocità più elevata dei partecipanti a cui venne chiesto quando andassero veloci le macchine quando si sono "toccate" o "colpite" a vicenda. Questo dimostra come cambiare le parole con cui si parla di un evento cambia la ricostruzione mnemonica che una persona ha dell'evento.[7]

Il linguaggio, dunque, non si limita a descrivere la realtà ma la costruisce, cognitivamente e socialmente. È proprio questa capacità del linguaggio nel modificare le percezioni umane che le classi politiche cercano di usare a proprio vantaggio in tempo di guerra. Oggi il linguaggio assume un ruolo strategico nel

---

[5] Mykhailyuk, O. e H. Pohlod, "The Languages We Speak Affect Our Perceptions of the World". *Journal of Vasyl Stefanyk Precarpathian National University* 2(2-3):36-41. Maggio 2015. https://www.researchgate.net/publication/283783768_The_Languages_We_Speak_Affect_Our_Perceptions_of_the_World

[6] Brousse, Catherine M., "The Effects of Figurative Language on Perceptions of War: A Case of Euphemisms and Dysphemisms". *Order No. 28258033, University of Louisiana at Lafayette*, 2020. https://www.proquest.com/dissertations-theses/effects-figurative-language-on-perceptions-war/docview/2549680749/se-2

[7] Ibidem.

descrivere la realtà durante periodi di guerra e conflitto perché non serve solo come strumento di comunicazione ma come un'arma per modificare le percezioni, mobilitare supporto, de-legittimizzare gli avversari. È quello che nelle scienze sociali viene chiamato "framing": una tecnica di comunicazione secondo cui le persone reagiscono in modo diverso a un'informazione a seconda di come viene presentata, della cornice (frame appunto) nel quale viene posta.[8] In ogni processo di "policy making" il framing è fondamentale. Il modo in cui le persone agiscono davanti a determinate notizie, è stato dimostrato, è influenzato in gran parte dal modo in cui giudicano tali notizie e a chi attribuiscono la responsabilità.[9] In base a questa prospettiva le risposte delle persone davanti a un conflitto sono strutturate da un "framework", una struttura, di significati che definisce la guerra come nobile o ignobile, l'opposizione come esercizio di giudizio politico o violazione della lealtà comunitaria, e così via.

Questo porta cambiamenti non solo su come si "comunica" una guerra ma come la si "definisce".

La dimensione fisica della guerra è sempre accompagnata da una sua dimensione discorsiva. Una guerra, come fatto fisico e materiale, è composta da tre elementi: cause, svolgimento, conseguenze. Le azioni fisiche sul campo di battaglia sono accompagnate costantemente da discorsi e analisi, per la comprensione (e il controllo della narrazione) di cause e conseguenze. Le guerre acquisiscono il significato e lo status di guerra solo insieme alle forme discorsive. Anche i conflitti più cruenti non sono guerre finché non se ne raccontano le storie. Miti, cronache storiche, romanzi, relazioni, monografie, opere di filosofi e

[8] *Frameworks Institute*. "Framing and Policy Making". 3 giugno 2018. https://www.frameworksinstitute.org/articles/framing-and-policy-making/#_edn1

[9] Iyengar, Shanto e Adam Simon. "News Coverage of the Gulf Crisis and Public Opinion". In *Taken by the Storm: The Media, Public Opinion, and U.S. Foreign Policy in the Gulf War*, a cura di W. Lance Bennett e David L. Paletz, 167-185. Chicago: University of Chicago Press, 1994.

storici, relazioni di esperti e analisti, opere sulle arti marziali, sul diritto militare, ecc. – l'elenco delle forme testuali e sociali di comprensione e interpretazione del fenomeno della guerra può essere esteso e ampliato. L'importanza del discorso e del racconto sulla guerra, al di là dello scontro fisico, è presente anche nel diritto internazionale: secondo la Convenzione dell'Aia del 1907 le ostilità non devono iniziare senza un preavviso non equivoco, sotto forma di dichiarazione di guerra motivata o di ultimatum condizionato. Oggi questa disposizione si ritiene superata, tanto che le Convenzioni di Ginevra del 1949 si applicano a qualsiasi conflitto armato si sviluppi sul piano fattuale, ma l'importanza centrale del discorso e della comunicazione della guerra non è venuta meno.[10] Oggi le guerre percepite come più cruenti e preoccupanti dalla popolazione sono le guerre di cui si parla, attraverso le comunicazioni ufficiali ma soprattutto attraverso i social media, strumenti grazie ai quali abbiamo accesso a filmati e dichiarazioni di chi si trova in guerra ma soprattutto di chi si occupa di raccontare la guerra, siano essi giornalisti o lo stato stesso.

Negli ultimi anni non è cambiato solo il racconto di guerra ma anche il parametro con cui la si definisce: oggi le guerre tradizionali sono state sostituite da "guerra ibride", conflitti nella "zona grigia".[11] È certamente cambiato il modo di condurre le guerre: ai mezzi tradizionali si affiancano mezzi non convenzionali, come disinformazione e propaganda, attacchi a infrastrutture e data center, sostegno ad attacchi terroristici o gruppi di opposizione, strumenti diplomatici, ecc. Lo stesso aggettivo "ibrida" indica per sua natura un'unione di più componenti che

[10] Kurbatov, Sergii, e Ihor Shchedrin. "Hybrid War as a Phenomenon of Semantic Postmodern Discourse with Emphasis on the Military Constant as a Factor of National Security." *International Journal of Environmental & Science Education* 17, no. 10 (2022): 833-844. https://www.researchgate.net/publication/367866412_Hybrid_War_as_a_Phenomenon_of_Semantic_Postmodern_Discourse_with_Emphasis_on_the_Military_Constant_as_a_Factor_of_National_Security

[11] Ibidem.

servono allo stesso scopo: una guerra ibrida è una guerra condotta con tutti i mezzi contro un determinato target, concentrando i propri sforzi sulla destabilizzazione di un governo e/o di una società. È una locuzione che ha suscitato il dibattito tra gli studiosi ma che sembra accostarsi alla definizione di guerra come "camaleonte" che "cambia di natura in ogni caso concreto"[12] che Clausewitz presenta già nel XIX sec.

Alla luce dell'importanza che la scelta delle parole assume, come sopra esaminato, è legittimo domandarsi se la locuzione "guerra ibrida" sia semplicemente una nuova definizione di guerra, più aderente alla realtà, o se sia utilizzata per mandare un messaggio, per ottenere una certa percezione nei cittadini, o per giustificare determinate scelte politiche.

Il passaggio dal welfare al warfare nell'Unione Europea

"If Europe wants to avoid war, it must get ready for war" – se l'Europa vuole evitare la guerra, l'Europa deve essere pronta alla guerra –: con questa frase la Presidente della Commissione Europea Ursula Von der Leyen si è espressa poco prima della pubblicazione del "Libro bianco sulla difesa", parlando ai cadetti della Royal Danish Military Academy.[13] È una frase che racchiude l'approccio alla difesa che l'Europa sembra aver intrapreso dall'inizio dell'invasione dell'Ucraina, nel febbraio del 2022.

Negli ultimi anni la spesa per la difesa europea è aumentata drasticamente: in tre anni è passata da 262 a 344 miliardi di euro, con un aumento complessivo di circa il 31%. Gli ultimi dati prevedono che nel 2025 la spesa abbia raggiunto il valore di 381 miliardi.

[12] Clausewitz C. (1837), *Della guerra*, Einaudi, Torino, p. 41.
[13] Speech by President von der Leyen at the Munich Security Conference. *European Commission*, 15 febbraio 2025, https://ec.europa.eu/commission/presscorner/detail/en/speech_25_814.

Un incremento significativo si è registrato anche negli investimenti per la ricerca e lo sviluppo nel settore della difesa: ha raggiunto 13 miliardi di euro nel 2024, con un aumento del 20% rispetto al 2023, e una previsione di 17 miliardi nel 2025.

A partire dall'invasione russa l'Europa ha attuato una serie di misure di supporto per l'Ucraina, come la creazione di fondi, l'invio di missioni di assistenza militare, l'incremento nella produzione di munizioni, che hanno portato molti analisti a sostenere che il vecchio continente abbia adottato "un'economia di guerra".[14] Non c'è una definizione univoca di questa espressione, ma quello che solitamente sta ad indicare è che l'economia di un paese mobilita le proprie risorse e la propria forza lavoro per il supporto alla preparazione militare e della produzione necessaria per sostenere un conflitto, anche attraverso la conversione delle industrie dalla produzione di beni di consumo alla produzione di armi, munizioni, e altro equipaggiamento militare.[15]

Questo processo ha raggiunto il suo apice nel piano ReArm Europe – Readiness 2030, un piano di riarmo ambizioso che prevede nei prossimi quattro anni di raggiungere investimenti nel settore della difesa di 800 miliardi di euro (quanto speso dell'UE per finanziare il Next Generation EU).[16] Questo piano è stato presentato a marzo contestualmente al Libro bianco sulla difesa, documento che punta a ridisegnare la struttura di difesa dell'Unione: prevede nuovi investimenti nell'industria bellica, una semplificazione della legislazione, l'alleggerimento

[14] Di Cicco, Arianna. "La guerra russa in Ucraina e la ridefinizione dell'ordine globale: tra crisi del multilateralismo e nuove alleanze." *DPCE Online* 61, n. 4 (2023): 2601-2624. https://www.dpceonline.it/index.php/dpceonline/article/view/2601/2828.
[15] Eisele, Ines. "What Is a War Economy?" *DW (Deutsche Welle)*, 28 aprile 2025. https://www.dw.com/en/what-is-a-war-economy/a-71996625.
[16] Sotgia, Davide "L'era del riarmo è arrivata". Analisi e considerazioni sul piano "ReArm Europe" della Commissione Europea", *Geopolitica.info*, 17 marzo 2025 https://www.geopolitica.info/europa-rearm-europe/

degli oneri amministrativi. Tutte misure volte ad accelerare l'innovazione e assicurare capacità di risposta di tutti i paesi europei entro il 2030 davanti a situazioni militari estreme.[17]

Non è un documento esente da connotati politici: indica la guerra in Ucraina come cruciale nella determinazione del futuro dell'Europa e la Russia come principale minaccia, seguita da Iran, Corea del Nord e Cina. Ogni misura presa per potenziare la difesa inoltre va concepita all'interno dell'Alleanza atlantica: la cooperazione UE-NATO rimane un "pilastro indispensabile".

Per raggiungere questi obiettivi militari e politici l'Unione ha accompagnato a questi documenti un nuovo strumento finanziario, il SAFE (Security Action for Europe). Si tratta di un piano volto a incoraggiare i Paesi a spendere meglio e in maggiore quantità per raggiungere gli obiettivi fissati collettivamente in materia, anche in ambito NATO. Con questo obiettivo la Commissione ha proposto quattro iniziative per assicurare la prontezza europea: l'iniziativa europea di difesa antidrone, la sorveglianza del fianco orientale, lo scudo aereo europeo e lo scudo spaziale europeo. Inoltre, si prevedono 150 miliardi di euro in prestiti, a cui possono attingere gli Stati membri interessati (sono diciannove i Paesi ad aver fatto richiesta, tra cui l'Italia) attraverso la presentazione di un piano di investimenti nell'industria europea della difesa. Questo strumento è pensato per aiutare l'Europa ad uscire da anni di investimenti insufficienti nella sicurezza militare.[18]

---

[17] *European Commission*, "White Paper for European Defence: Readiness 2030". Bruxelles, 2025. https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en.

[18] *Commissione Europea e Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza*. "Comunicazione congiunta al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni: Una nuova strategia per la difesa europea e la sicurezza economica". Bruxelles, 2025. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52025JC0027.

È con questi progetti, a partire dal SAFE, che l'Unione cerca di prepararsi ad affrontare una "guerra moderna", caratterizzata "dall'evoluzione del panorama delle minacce". Sono progetti pensati per far fronte all'aumento delle provocazioni sconsiderate e degli atti di guerra ibrida contro gli Stati Membri. La guerra ibrida è sempre presente tra le righe di questi programmi, è il contesto all'interno del quale tutte queste azioni di sviluppo della difesa trovano posto.

Il tutto si presenta come un'iniziativa ambiziosa da parte delle istituzioni e dei Paesi europei. La prima questione su cui riflettere circa un progetto di questo tipo – soprattutto nell'Unione, dove fu la stessa decisione popolare a respingere l'idea di una difesa comune ai tempi della CED – è capire come inserirlo all'interno "dell'agenda" europea per l'opinione pubblica. Fondamentale in questo senso è il già menzionato "framing": una situazione diventa un "questione sociale" quando le informazioni in merito sono presentate in modo tale da condurre la società a pensare la situazione come importante e meritevole di attenzione.[19] La scuola di Copenaghen parla di "processo di securitizzazione": secondo Wæver, uno dei principali esponenti, "qualcosa è un problema di sicurezza (solo se e quando) le élite lo dichiarano tale" e la securitizzazione è appunto il modo in cui i politici decidono di sviluppare ed etichettare i problemi di sicurezza nel discorso politico. Gli analisti di questa scuola partono dall'assunto che il termine "sicurezza" nel linguaggio politico indichi esattamente il suo opposto, ovvero l'assenza di sicurezza: dunque indicare una questione in termini di sicurezza significa doverla trattare come suprema priorità e con tutti gli strumenti (anche

[19] Frameworks Institute. "Framing and Policy Making". 3 giugno 2018. https://www.frameworksinstitute.org/articles/framing-and-policy-making/#_edn1

straordinari) necessari.[20] Questo è quello che sta accadendo attualmente nel discorso politico europeo.

È osservabile come in tutti i paesi, contestualmente a questo programma di riarmo, il discorso politico istituzionale si sia concentrato sulle "minacce ibride": la guerra ibrida viene presentata come un contesto quanto più attuale in Europa, da cui il vecchio continente deve imparare a difendersi.

In questi termini si è espresso il Generale Seán Clancy, alto ufficiale irlandese che da giugno 2025 copre la carica di Presidente del Comitato Militare dell'Unione Europea (CEUMC): in più discorsi ha messo in evidenza come la nuova difesa dell'Europa deve guardare alle minacce cyber, davanti alle quali i confini europei non sono più una garanzia. In occasione del Forum "EPC Thought Leadership", il 23 febbraio, ha ribadito che l'Europa si trova a fronteggiare una situazione sempre più complessa davanti alla quale per difendersi serve l'impegno di tutta la società. Le crisi non sono più consequenziali ma sono simultanee: le minacce cyber, ibride, spaziali e la pressione convenzionale si verificano tutte nello stesso momento.[21]

Anche la Presidente della commissione, Ursula Von der Leyen, in un discorso tenuto a dicembre al Parlamento europeo di Strasburgo, ha richiamato la necessità di ridisegnare la sicurezza per difendersi da una "modern hybrid war": l'Europa si trova in una realtà dove è diventato difficile distinguere pace, crisi e conflitto, in cui attacchi a infrastrutture energetiche, campagne di

[20] Boscariol, Marco. "Securitizzazione e Stato Di Eccezione: Sulle Origini Schmittiane Della Scuola Di Copenaghen." *Ragion Pratica*, 2021. https://www.academia.edu/76320317/Securitizzazione_e_stato_di_eccezione_sulle_origini_schmittiane_della_Scuola_di_Copenaghen

[21] Marinov, Svetoslav. "From Ambition to Endurance: EUMC General Sean Clancy on Europe's Defence Shift." *European Policy Centre*, 13 febbraio 2025. https://www.epc.eu/publication/from-ambition-to-endurance-eumc-general-sean-clancy-on-europes-defence-shift/.

disinformazione che vanno a colpire in particolare i processi democratici, sabotaggi hacker a data center e strutture digitali, rendono necessario per il continente riorganizzarsi.[22]

A questi discorsi si sono accompagnate esercitazioni europee e nazionali: tra il 9 e il 12 febbraio 2026 l'agenzia europea Europol a L'Aia ha coinvolto vari Stati membri nell'esercitazione "Allies 2026", volta a testare la cooperazione delle forze europee di fronte a scenari critici, come il traffico di droga internazionale e le minacce ibride. In particolare, le forze sono state poste davanti ad attacchi a infrastrutture, come centrali elettriche, per analizzare le loro capacità di coordinamento e intervento congiunto. La Francia invece l'8 febbraio ha lanciato l'esercitazione "Orion 26", per testare la preparazione delle forze militari davanti alle nuove minacce, come attacchi di droni, disfunzionamenti della rete satellitare e guerra elettronica.[23]

Anche le istituzioni italiane hanno dimostrato inedita attenzione alla guerra ibrida: il ministro della difesa Guido Crosetto ha pubblicato a novembre 2025 un "Non-paper" sul contrasto alla guerra ibrida, che delinea il concetto e i caratteri, della guerra sottosoglia che in questo momento la Russia, la Cina, l'Iran e la Corea del Nord stanno conducendo contro l'Europa. La sua tesi centrale è che "contenere non basta": l'Italia, così come gli altri Paesi Europei devono assumere una posizione attiva, prevenendo gli attacchi ibridi.[24] Propone inoltre, tra le altre

---

[22] *Cybersecurity360*. "UE pronta alla guerra ibrida: di che si tratta, strumenti e scenari". 14 febbraio 2025. https://www.cybersecurity360.it/cybersecurity-nazionale/ue-pronta-alla-guerra-ibrida-di-che-si-tratta-strumenti-e-scenari/.

[23] *Toute l'Europe*. "Orion 26: la France lance son plus grand exercice militaire depuis la fin de la Guerre froide". 20 febbraio 2026. https://www.touteleurope.eu/l-ue-dans-le-monde/orion-26-la-france-lance-son-plus-grand-exercice-militaire-depuis-la-fin-de-la-guerre-froide/.

[24] Calabrese, Anna "Verso un'arma cyber nazionale: la strategia del Min. Crosetto nel contesto europeo". *Geopolitica.info*, 14 novembre 2025 https://www.geopolitica.info/strategia-cyber-crosetto/

cose, l'istituzione di un Centro per il Contrasto alla Guerra Ibrida, che possa aiutare il Paese a difendersi e prevenire le minacce di questo genere.[25]

Dalla formalizzazione strategica alla securitizzazione permanente: il paradigma della guerra ibrida

Con l'inasprirsi della crisi in Crimea, dal 2014, il concetto di "guerra ibrida" si è progressivamente diffuso [26] in maniera sistemica nel discorso politico e istituzionale europeo e atlantico. Tale locuzione è stata infatti incorporata in documenti strategici e dichiarazioni ufficiali di organizzazioni e istituzioni come NATO o Unione Europea, che hanno dato vita a un lessico condiviso, volto ad indicare un nuovo tipo di conflitto contemporaneo, comprendente dimensioni convenzionali e non convenzionali, tecnologiche, industriali, cyber e cognitive.

Una effettiva formalizzazione del concetto si può ritrovare nella Wales Summit Declaration del 2014 [27], un documento adottato dalla NATO concernente la necessità di approfondire nuovi approcci nei riguardi di aggressioni ibride, attraverso la combinazione di strumenti convenzionali e non convenzionali. Con il Joint Framework on Countering Hybrid Threats del 2016[28], anche la Commissione Europea ha delineato una definizione di minacce ibride come "una miscela di attività coercitive e sovversive, metodi convenzionali e non convenzionali (diplomatici, militari, economici, tecnologici) utilizzati da attori statali o non statali al di sotto della soglia di guerra formalmente dichiarata".

[25]Crosetto, Guido. "Non-paper: Il contrasto alla guerra ibrida". *Ministero della Difesa*, 2025. https://www.difesa.it/assets/allegati/83696/non-paper_il_contrasto_alla_guerra_ibrida.pdf.
[26] NATO StratCom COE. "Hybrid Threats – A Strategic Communications Perspective." *StratCom Centre of Excellence*, 2015
[27]NATO. "Wales Summit Declaration." *NATO Official Documents*, 5 settembre 2014.
[28] Commissione Europea. "Joint Framework on Countering Hybrid Threats." *European External Action Service*, 6 aprile 2016.

Come sopracitato, questa locuzione ha ulteriormente rafforzato l'istituzionalizzazione del termine grazie all'adozione sempre maggiore nei discorsi di molti leader e attori politici, che enfatizzano la responsabilità diretta dei governi[29] in proposito della gestione della sicurezza, che appare come un obbligo strategico e non una semplice opzione politica.

La stabilizzazione del frame di "minaccia ibrida permanente" ha destato ambiguità terminologiche, ma la guerra ibrida si inserisce in un quadro concettuale condiviso che permette alle istituzioni di interpretare, anticipare e analizzare eventuali risposte politiche o giustificare investimenti in difesa e cybersicurezza. Questa integrazione nel linguaggio adottato da leader politici europei e mondiali conferma la classificazione del fenomeno come una condizione di minaccia permanente poliedrica, consolidando la guerra ibrida come categoria strategica centrale.

È necessario, tuttavia, evidenziare come il concetto di "guerra ibrida" sia oggetto di svariate critiche accademiche per la sua ambiguità semantica[30] e indeterminatezza definitoria che, nella sua evoluzione temporale, ha portato a inglobare fenomeni fra loro eterogenei sotto un'unica etichetta analitica. Il termine risulta eccessivamente inclusivo e utilizzato nel dibattito strategico per descrivere una vasta gamma di attività.

Come già detto, rientrano sotto questa categoria varie operazioni: impiego combinato di strumenti militari convenzionali e non, attacchi cyber, propaganda, sabotaggi, coercizione economica, operazioni psicologiche e interferenze nei processi democratici. Questa estensione progressiva porta a un

[29] Reuters. "NATO must be ready to respond to hybrid threats, top commander says." *Reuters*, 4 dicembre 2025.
[30] ResearchGate & NSF Journal. *Hybrid War as Semantic Postmodern Discourse* / "Hybrid Warfare: A Dramatic Example of Conceptual Stretching."

concetto-ombrello[31] della definizione di "guerra ibrida", privandola di confini analitici chiari.

In origine la nozione faceva riferimento alla combinazione di forze regolari e irregolari nello stesso teatro operativo, ma dal 2014, con l'avvio del conflitto fra Russia e Ucraina, il significato si è ulteriormente ampliato tramite l'inclusione di operazioni coperte, proxy, campagne di disinformazione, pressioni economiche e migratorie, e azioni "al di sotto della soglia" di guerra dichiarata. Ne risulta la formulazione di una categoria che si adatta a contesti interstatali e asimmetrici, ma sempre più lontana da una definizione concreta.

Questo processo corrisponde alla nozione di *conceptual stretching* proposta da Sartori[32]: quando un concetto è applicato a un universo empirico sempre più vasto, tende a dilatarsi e includere casi differenti, sacrificando precisione analitica. L'etichetta originaria si mantiene, ma si svuota progressivamente del suo contenuto, portando a pensare che "guerra ibrida" significhi "tutto e niente".

Ulteriore criticità emerge confrontandosi con categorie consolidate: guerra politica, guerra irregolare, guerra non convenzionale, guerra sovversiva, guerra dell'informazione descrivono già modalità di conflitto che combinano strumenti militari e non. La guerra politica indica l'uso di mezzi non bellici per perseguire obiettivi nazionali; la guerra irregolare sfrutta il concetto di legittimità e sull'influenza sulle masse; la guerra non convenzionale e quella sovversiva attivano strumenti clandestini o forze irregolari per destabilizzare governi costituiti; la guerra dell'informazione utilizza la stessa informazione come arma

[31] NSF Journal & NATO Veterans – Content Analysis. "Hybrid Warfare: One Term, Many Meanings." *Small Wars Journal*, 2020 & *NSF Journal* Focus Issues, 2022.
[32] NATO. "Countering hybrid threats." *NATO Topic*, aggiornato 29 gennaio 2026.

per plasmare percezioni e comportamenti. La “guerra ibrida” raggruppa tutte queste dimensioni sotto un’unica nomea, combinandole simultaneamente.

Proprio in questa ampiezza si ritrovano sia la sua forza politica che il principale problema analitico: qualificare minacce così differenti come “ibride” porta a una perdita di concretezza nell’analisi e a un ostacolo nella determinazione. Si delinea un parallelismo fra ambiguità operativa e semantica. Attività definite “ibride” collocano tutto al di sotto della soglia del conflitto armato convenzionale, ma la stessa soglia rimane indeterminata. Non esistono criteri universalmente condivisi[33] per stabilire quando campagne di disinformazione o attacchi informatici cessano di essere competizione strategica e diventano guerra effettiva.

Il rischio che ne consegue è l’instaurarsi di una continuità permanente tra pace e guerra. La scarsa trasparenza nella determinazione di inizio e fine del conflitto produce pressione costante su infrastrutture, sistemi informativi e opinione pubblica, contribuendo all’erosione della distinzione tradizionale tra tempo di guerra e tempo di pace.

Questa elasticità concettuale comporta inoltre un’espansione del campo della sicurezza[34]. Poiché la definizione di guerra ibrida offre una copertura ampia di dimensioni militari, economiche, tecnologiche, informative e cognitive, tende a reinterpretare ambiti sempre più ampi della vita sociale in chiave securitaria: industria, energia, comunicazione, infrastrutture digitali, media e università possono essere riclassificati come spazi di conflitto permanente. Prende forma un sistema di economia di guerra, nel quale le priorità produttive, le scelte di

[33] Solmaz, Tarik. Hybrid Warfare: A Dramatic Example of Conceptual Stretching, Volume 23, No. 1, 2022

[34] Language & Society. “Naming and Framing in Political Contexts.” Language and Society Journal, giugno 2025.

investimento, le politiche industriali e la regolazione dei mercati vengono progressivamente orientate alla resilienza, alla protezione delle infrastrutture critiche e alla sicurezza nazionale, trasformando in senso strategico l'intero assetto economico e istituzionale

La "guerra ibrida" non è dunque una mera categoria descrittiva, ma una cornice normativa che orienta priorità politiche e allocazione di risorse. La stessa mancanza di una definizione univoca non costituisce un problema terminologico[35], bensì incide sulla costruzione della minaccia, ampliando il perimetro dell'intervento statale verso una securitizzazione permanente.

Performatività del concetto e trasformazione dell'ordine politico-securitario

Secondo questa prospettiva, la nomea di "guerra ibrida" non costituisce una descrizione superficiale di una realtà preesistente, ma agisce in maniera performativa, influenzando la percezione della realtà e collocandosi in un framing concreto. Il termine "guerra" genera percezione di nemico, attacco e conseguente necessità di difesa, diffondendo emergenza, mobilitazione e sicurezza nazionale. Affiancando la qualifica "ibrida", il conflitto si estende a domini non tradizionalmente militari: cyberspazio, informazione, economia, energia, migrazione, interferenze politiche[36].

Si assiste ad una riorganizzazione cognitiva del fenomeno "minaccia": attacchi armati tradizionali producono una percezione immediata e intensa, azioni definite "ibride" acquisiscono invece una nuova rilevanza strategica che

[35] European Union Institute for Security Studies (EUISS). "Next level partnership – Bolstering EU-NATO cooperation to counter hybrid threats in the Western Balkans." ISS Brief, 2025.
[36] NATO Veterans. "A content analysis on the media coverage of hybrid warfare." NATO Veterans, 2023.

prescinde dal linguaggio tecnico-militare[37]. Dunque, il frame determina il grado di urgenza percepita.

L'uso performativo di questa categoria produce effetti tangibili sul piano politico-istituzionale. Anche se considerato "sotto soglia", questo contesto è definito come guerra, orientando la risposta politica verso reazioni immediate e comprimendo il tempo deliberativo. L'emergenza, da condizione eccezionale, si configura come permanente. Le conseguenze di un conflitto continuo e diffuso si riflettono nelle policy adottate: incremento delle risorse destinate a difesa, intelligence, cybersicurezza e sicurezza informativa, avvertite come requisiti strutturali e non come scelta politica. Lo stato di guerra permanente renderebbe quindi l'investimento militare ordinario, normalizzando l'espansione della spesa per la difesa. In ambito europeo, questa retorica ha contribuito a legittimare programmi di rafforzamento delle capacità militari e industriali, come il piano ReArm Europe, presentato come risposta necessaria, uno strumento di giustificazione politica per il riarmo e per una ridefinizione strutturale delle priorità di spesa pubblica[38].

Poiché la minaccia è percepita al di sotto dell'attacco armato, si legittimano contromisure preventive e ampliamenti dell'intervento statale: sorveglianza estesa, restrizioni informative, controlli economici e interventi anticipatori. Si genera un assottigliamento del confine tra sicurezza nazionale e politica interna: misure normalmente percepite come straordinarie si stabilizzano e l'eccezione diviene struttura. La democraticità viene sostituita dalla tecnica: dalla domanda "quale politica adottare?" si passa a "come neutralizzare la minaccia?". La

[37] Tkachuk, Andriy & Pavlo Tkachuk. "Hybrid War as a Phenomenon of Semantic Postmodern Discourse with Emphasis on the Military Constant as a Factor of National Security." *Postmodern Openings* 2021.
[38]Kovář, Jan. "Hybrid Warfare, Information Operations and the Transformation of Contemporary Conflict." *Kultúrní Studia*, 2/2022.

percezione di minaccia oggettiva e permanente rafforza l'autorità e riduce lo spazio del dissenso, delegittimato come "sottovalutazione" del rischio.

Nella guerra russo-ucraina l'uso semantico di questi termini non rappresenta un semplice strumento descrittivo ma si concretizza in un vero e proprio dispositivo strategico che ha assunto funzione deterrente, mobilitante e legittimante. Dal 2014, con un'accelerazione nel 2022, l'evoluzione lessicale è diventata cruciale per strutturare una narrazione di "guerra delle parole", dove il controllo del linguaggio si accompagna all'uso della forza. Centrale la sostituzione sistematica di termini consolidati, riadattati per orientare l'ideologia comune. Si evince dalla scelta russa iniziale di evitare la parola "guerra" preferendo altresì il termine "operazione militare speciale". Una vera e propria ridefinizione semantica che allude a una legittimità di azione plasmando la portata giuridica e la percezione morale. L'eliminazione del termine "guerra" attenua l'idea di aggressione aggirando categorie giuridiche e morali del diritto internazionale, modificando la realtà oggettiva e diventando uno strumento di "ingegneria percettiva".

Viene praticata una vera e propria costruzione di un nemico comune tramite meccanismi di nominazione e predicazione: si creano categorie identitarie connotate da etichette come, ad esempio, l'uso del termine "nazisti", alle quali vengono associate qualità moralmente assolute, minacce esistenziali, che trasformano l'avversario agli occhi dell'opinione pubblica, in un'entità ontologicamente ostile.

Questa costruzione discorsiva influenza direttamente la legittimazione politica delle scelte strategiche. Grazie a uso di formule allarmistiche, come ad esempio "minaccia ai valori condivisi" o "sicurezza collettiva in pericolo" si sviluppa un senso di urgenza che ha effetti diretti su misure forti come mobilitazioni militari o riorganizzazioni istituzionali che sono dunque "risposte inevitabili". Queste si

pongono in un'ottica difensiva e necessaria mentre l'avversario è dipinto come colui che esercita pressione e manipolazione. Il linguaggio riesce dunque a capovolgere la percezione di aggressività, in un'ottica che precede il controllo territoriale: chi definisce i termini del conflitto ne orienta anche gli esiti politici.

Conclusioni

Nella presente analisi si approfondisce il ruolo della comunicazione e del linguaggio nell'ambito della costruzione strategica dei conflitti contemporanei, con particolare attenzione all'importanza che questi hanno all'interno del concetto di "guerra ibrida". La domanda di ricerca si concentra su come e perché questa locuzione sia diventata centrale nel dibattito sulla sicurezza, evidenziandone la rilevanza strategica nel definire la percezione pubblica e la legittimazione delle scelte politiche.

La locuzione "guerra ibrida" non possiede una definizione univoca né concreta. Ciò complica l'individuazione di strumenti efficaci per contrastarne le minacce. Il termine ha però forte rilevanza strategica: ridefinisce i confini della sicurezza nazionale estendendo il concetto di guerra oltre i teatri convenzionali e penetrando nello spazio della quotidianità. Si consolida così una percezione diffusa e costante di vulnerabilità. Ne deriva una ridefinizione dei tradizionali periodi di guerra e pace, che non si riescono più a distinguere linearmente; le conseguenze si ripercuotono sulla gestione economica, politica e sociale, tendendo a configurarsi sempre di più verso logiche di economia di guerra.

Tale dinamica apre scenari ambivalenti per il futuro. La normalizzazione di una narrativa di "conflitto permanente" rischia di comprimere gli spazi democratici, mantenendo la società in uno stato di allerta costante e legittimando misure eccezionali. Allo stesso tempo essa offre l'opportunità di ripensare le strategie di sicurezza, integrando capacità convenzionali e non convenzionali in maniera più

flessibile e proattiva. Si delinea così un quadro internazionale in cui la sovrapposizione tra dinamiche belliche e condizioni di normalità non appare più contingente, ma tende a configurarsi come una trasformazione strutturale dell'ordine globale.

SEZIONE III: LE RISPOSTE

Europa nella zona grigia: guerra ibrida, fratture interne e il nodo della responsabilità strategica

di Mattia Saitta e Giulio Croce

Introduzione

Negli ultimi anni, e con crescente intensità nel biennio 2024-2026 a causa dell'inasprimento del conflitto russo-ucraino, il confronto tra Federazione Russa e spazio euro-atlantico si è progressivamente spostato in una dimensione operativa che sfugge alle categorie tradizionali di pace e guerra. Attacchi cibernetici, sabotaggi infrastrutturali, operazioni di influenza, interferenze nei processi democratici, pressioni migratorie strumentalizzate e dimostrazioni militari al di sotto della soglia con cui si identificano tradizionalmente atti bellici compongono un mosaico coerente di azioni volte a logorare la coesione europea senza oltrepassare la soglia del conflitto armato aperto.

In questo contesto, la guerra ibrida non rappresenta un insieme episodico di strumenti, ma una strategia sistemica di lungo periodo, finalizzata a ridefinire gli equilibri di potere in Europa attraverso l'erosione graduale della resilienza politica, economica e sociale degli stati membri. L'ambiguità deliberata, la negabilità plausibile e la frammentazione delle operazioni rendono complessa l'attribuzione delle responsabilità e rallentano la risposta collettiva, trasformando la "zona grigia" in un ambiente operativo favorevole agli attori revisionisti.

Parallelamente, la ridefinizione delle priorità strategiche statunitensi – con un'attenzione crescente all'Indo Pacifico, all'Artico e una più marcata richiesta di *burden sharing* agli alleati europei – ha rimarcato la necessità per l'Unione Europea di sviluppare una maggiore capacità di deterrenza e risposta nella zona grigia tra pace e guerra. La questione non è soltanto operativa, ma strutturale: la guerra ibrida mette alla prova la maturità dell'Europa come attore strategico, evidenziando il divario tra ambizione politica e integrazione effettiva di sicurezza tra gli stati membri.

Il presente contributo analizza la guerra ibrida russa come strumento di competizione permanente, esamina le vulnerabilità sistemiche europee che ne amplificano l'efficacia e valuta le capacità dell'Unione di costruire una risposta coerente e credibile. L'obiettivo è comprendere se l'Europa stia evolvendo verso una postura strategica integrata o se continui a reagire in modo frammentato a pressioni che, pur rimanendo sottosoglia, producono effetti cumulativi di natura strategica.

2025: la normalizzazione della guerra ibrida in Europa.

Nonostante nel 2025 il numero di attacchi ibridi sia diminuito in Europa rispetto agli scorsi anni[1], questi si sono ormai imposti come componente strutturale e quotidiana della realtà geopolitica europea. Dei ricercatori dell'Università di Leiden, nei Paesi Bassi, conducono un progetto chiamato "Sorveglianza e Sicurezza" ("Bewaken en Beveiligen" in olandese) che studia le campagne di sabotaggio russe in Europa[2], da cui appare evidente che non assistiamo più a

[1] Seibt, Sebastian. "Russia's hybrid-warfare attacks in Europe dropped this year, but could they pick up in 2026?," *France 24*, 28 dicembre 2025, https://www.france24.com/en/europe/20251228-russia-hybrid-warfare-attacks-europe-dropped-this-year-but-could-they-pick-up-2026.

[2] Schuurman,Bart; van Buuren, Jelle; Hofkamp Roy, van 't Land, Stijn. "Research: Europe increasingly targeted by Russian sabotage", Leiden University, 20 Gennario 2025,

episodi isolati di disturbo, bensì a una sistematizzazione del caos volta a logorare la resilienza delle democrazie liberali tramite una pressione costante e multiforme [Figura 1].

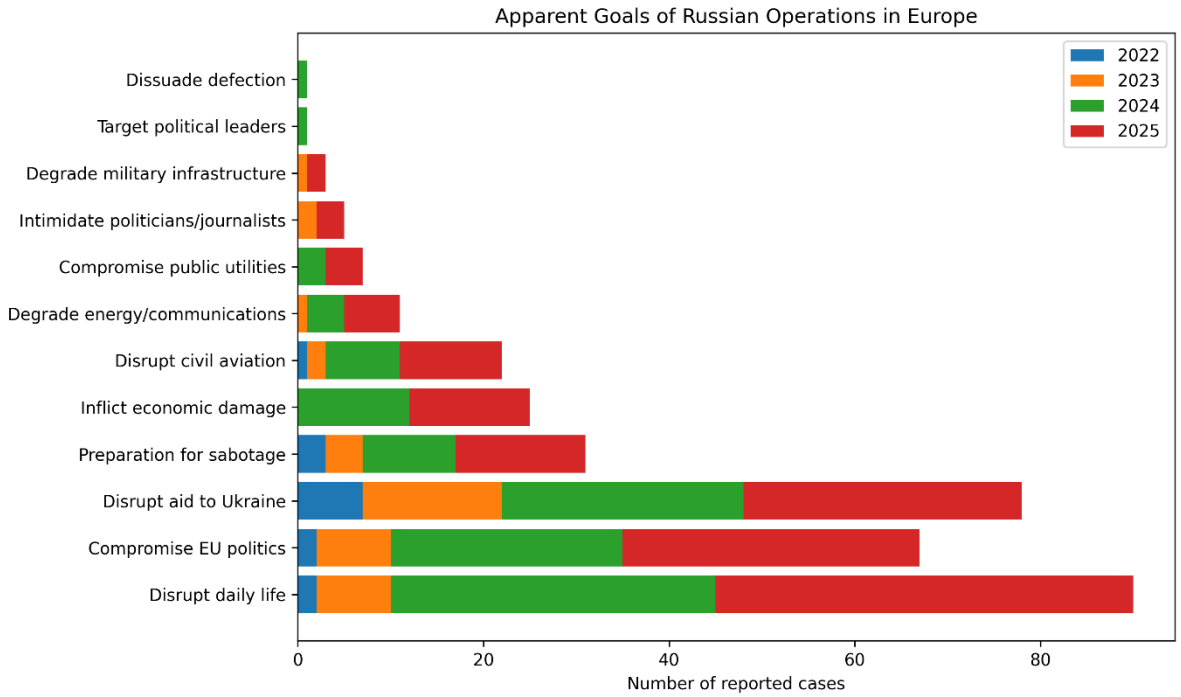


Figura 1. Obiettivo apparente delle operazioni ibride russe in Europa, secondo il progetto dell'Università di Leiden[3]

Lo studio di Schuurman *et al.* rileva un'evoluzione sia nella scelta dei paesi "vittima" (passando dall'Europa Orientale a quella Occidentale) sia nella scelta delle attività. Infatti, queste dapprima erano primariamente incentrate sulla disinformazione e sugli attacchi informatici ma, a causa della crescente evoluzione della guerra ibrida, includono ora anche sabotaggi fisici e omicidi politici[4] [Figura 2].

---

https://www.universiteitleiden.nl/en/news/2025/01/research-europe-increasingly-targeted-by-russian-sabotage

[3] Schuurman, Bart. "Russian Operations Against Europe Dataset, 2022-2025", Harvard Dataverse, V4, 2024. https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/TQ0FMQ

[4] Schuurman, Bart *et. al,* "Research: Europe increasingly targeted by Russian sabotage", *op. cit.*

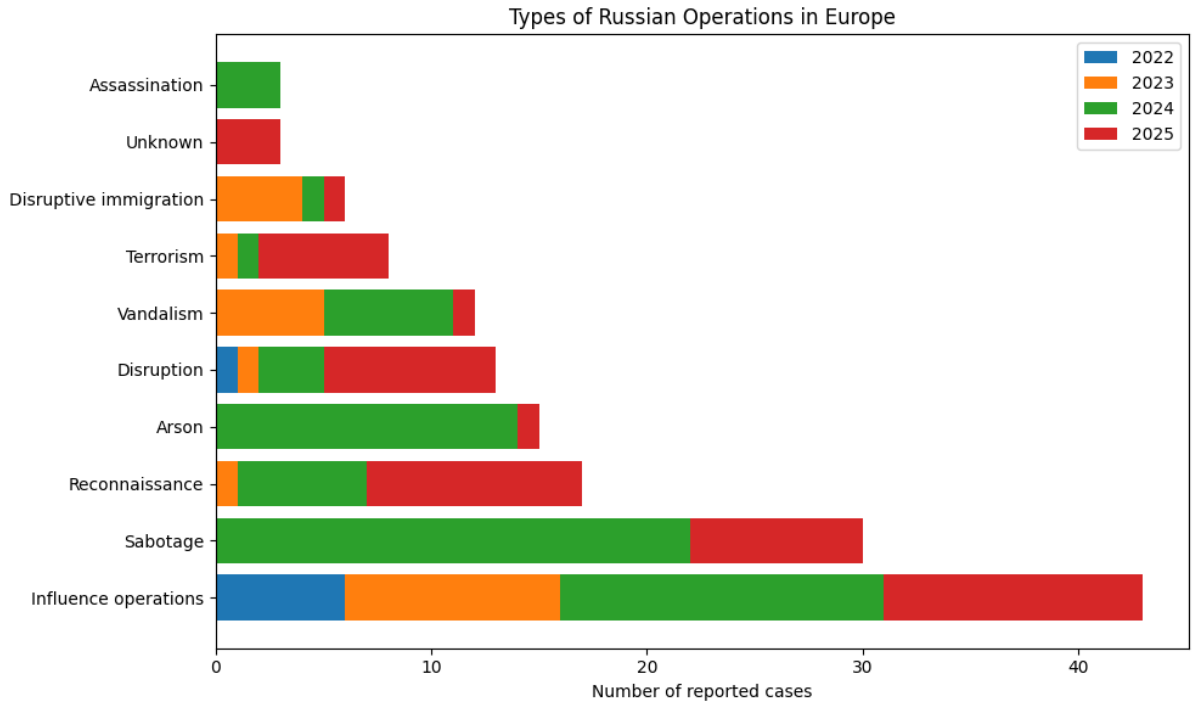


Figura 2. Operazioni ibride russe in Europa, per tipologia, secondo il progetto dell'Università di Leiden[5]

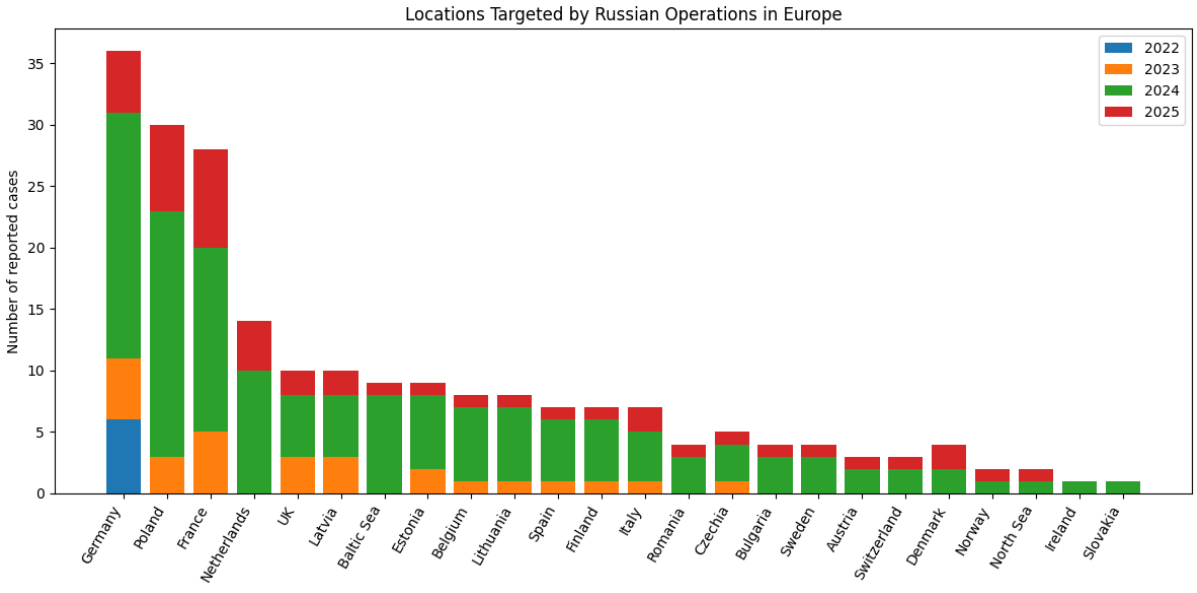


Fig. 3. Principali paesi colpiti dalle operazioni ibride russe, secondo il progetto dell'Università di Leiden.

[5] Schuurman, Bart. "Russian Operations Against Europe Dataset, 2022-2025", *op. cit.*

Il primo semestre del 2025 è stato caratterizzato da danneggiamenti ai cavi in fibra ottica nel Mar Baltico[6] spesso mascherati da incidenti tecnici. Durante l'estate, la rete di telecomunicazioni belga Orange Belgium ha subito un attacco cibernetico su più di 800 mila clienti[7], mentre durante l'autunno si sono verificate diverse incursioni di drone nello spazio aereo di alcuni paesi UE, tra cui Danimarca, Estonia[8], in Polonia[9], insieme alle basi militari di Belgio e Germania[10]. Nello stesso periodo, sono poi stati rilevati due sottomarini russi, uno nel Mediterraneo[11] e un altro a largo delle coste francesi[12], attraverso un'avaria di bordo. L'obiettivo non sembra essere più dunque il semplice spionaggio, ma la volontà di dimostrare la capacità di attaccare infrastrutture vitali.

Le succitate incursioni, pur non sfociando in atti distruttivi diretti, hanno esercitato una forte pressione sui comandi militari ed erano volte a testare i limiti della tecnologia anti-drone NATO per la difesa dello spazio aereo a bassissima

[6] Ball, Tom. "Hunt for Baltic Sea 'saboteurs' as another underwater cable is cut," *The Times*, 6 gennaio 2026, https://www.thetimes.com/world/europe/article/undersea-cables-latvia-lithuania-baltic-sea-russia-r8r7k5cvk?

[7] Orange Belgium, "Orange Belgium informs its customers about a cyberattack," 20 agosto 2025, https://corporate.orange.be/en/node/57971.

[8] Croce, Giulio. "Quali prospettive per il Muro anti-drone europeo e la "Eastern Flank Watch"", *Geopolitica.info,* 8 Ottobre 2025, https://www.geopolitica.info/prospettive-muro-anti-drone-europeo/

[9] Saitta, Mattia. "Droni russi in Polonia: la sfida alla coesione euro-atlantica", *Geopolitica.info,* 29 Settembre 2025, https://www.geopolitica.info/droni-russi-polonia-nato-ue-coesione/

[10] Blackburn, Galvin. "Droni su base militare in Belgio: possibile operazione di spionaggio secondo ministro della Difesa", *Euronews.com,* 3 Novembre 2025, https://it.euronews.com/2025/11/03/droni-su-base-militare-in-belgio-possibile-operazione-di-spionaggio-secondo-ministro-della

[11] De Palo, Francesco. "Sottomarino russo in avaria nel Mediterraneo. Verso un bis della tragedia Kursk?", *Formiche.it,* 28 Settembre 2025, https://formiche.net/2025/09/sottomarino-russo-in-avaria-nel-mediterraneo-verso-un-bis-della-tragedia-kursk/#content

[12] Caruso,Fausto. "Sottomarino russo Novorossiysk in Francia costretto a salire in superficie. Nato: «Grave malfunzionamento». Ma Mosca nega", *Il Messaggero,* 14 Ottobre 2025, https://www.ilmessaggero.it/mondo/malfunzionamento_sottomarino_russo_francia_mosca_nega-9124764.html?refresh_ce

quota, in preparazione a un futuro conflitto[13]. A completare questo quadro di destabilizzazione è stata l'evoluzione delle operazioni informative. Grazie all'integrazione massiccia dell'intelligenza artificiale generativa, le campagne di disinformazione hanno raggiunto una granularità e una velocità di propagazione tali da inquinare il dibattito pubblico in tempo reale, alimentando polarizzazioni sociali e minando la fiducia nelle istituzioni durante i passaggi elettorali più delicati.

Il problema principale degli attacchi ibridi è la loro natura "sotto-soglia" rispetto alla definizione classica di aggressione bellica, che farebbe scattare l'articolo 5 della NATO[14]. La guerra ibrida opera chirurgicamente in quella zona grigia, "in uno stato indefinito tra la pace effettiva e la guerra non dichiarata"[15]. Poiché questi attacchi sono progettati per rimanere al di sotto del livello di attacco tradizionale che farebbe scattare una risposta militare immediata (in particolare la clausola di difesa collettiva dell'Articolo 5 NATO[16] e dell'Articolo 42.7 del Trattato sull'Unione Europea[17]), essi sfruttano la difficoltà di attribuzione certa e la complessità nel qualificare giuridicamente un atto di sabotaggio digitale come costringendo i Paesi occidentali ad un processo di consultazione politica ogni qualvolta si verifichi un evento ostile, esponendo la lentezza e complessità della

---

[13] Salisbury, Daniel. "Drones targeting European nuclear weapons infrastructure", International Institut for Strategic Studies (IISS), 12 dicembre 2025, *https://www.iiss.org/online-analysis/online-analysis/2025/12/drones-targeting-european-nuclear-weapons-infrastructure/*

[14] Bajarūnas, Eitvydas "The Hybrid Threat Imperative: Deterring Russia Before it is Too Late", *Center for European Policy Analysis,* 2 dicembre 2025, https://cepa.org/comprehensive-reports/the-hybrid-threat-imperative-deterring-russia-before-it-is-too-late/

[15] Talia, Antonio. "I fantasmi del Baltico", *Lab24 - Il Sole 24 Ore*, 7 Luglio 2025, https://lab24.ilsole24ore.com/guerra-ibrida-russia-baltico/?refresh_ce=1

[16] NATO, "Collective defence and Article 5", https://www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5

[17] Parlamento Europeo, "Mutual Defence" https://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede200612mutualdefsolidarityclauses_/sede200612mutualdefsolidarityclauses_en.pdf

coesione decisionale della NATO e dell'Unione Europea e la vulnerabilità delle società aperte che caratterizzano le democrazie occidentali[18]. La risposta proporzionata diventa quindi un paradosso: un'azione troppo debole conferma l'impunità dell'aggressore, mentre una reazione eccessiva rischia di innescare un'escalation militare non desiderata[19].

La guerra ibrida si conferma lo strumento più efficace da parte di attori ostili per testare la solidità dei legami intra-europei e transatlantici, facendo anche riflettere sul fatto che di fronte a un'aggressione frammentata e opaca la deterrenza convenzionale è limitata[20].

La guerra ibrida come strategia sistemica russa

La guerra ibrida rappresenta per la Federazione Russa uno strumento strutturale della sua politica di sicurezza, consolidatosi ben prima dell'invasione su larga scala dell'Ucraina del febbraio 2022. Già negli anni precedenti, Mosca aveva progressivamente integrato strumenti militari e non militari in una logica di competizione permanente sotto soglia. L'ibridazione non costituisce dunque un adattamento contingente, bensì un elemento radicato nella cultura strategica russa: un dispositivo volto a esercitare pressioni costanti sul piano politico, psicologico e infrastrutturale, evitando al contempo un'escalation militare diretta. Tale impostazione consente alla Russia di operare in una "zona grigia", sfruttando vulnerabilità sistemiche e fratture sociali senza oltrepassare soglie che potrebbero attivare meccanismi di deterrenza collettiva o giustificare una risposta convenzionale coordinata da parte degli stati europei o della NATO.

[18] Bajarūnas, Eitvydas, *op. cit.*
[19] Williams, Heather; Hartigan,Kelsey; MacKenzie, Lachlan and Younis, Reja. "Deter and Divide: Russia's Nuclear Rhetoric & Escalation Risks in Ukraine," *Center for Strategic and International Studies*, 4 dicembre 2024, https://features.csis.org/deter-and-divide-russia-nuclear-rhetoric
[20] Bajarūnas, Eitvydas, *op. cit.*

Secondo Kashin, la guerra ibrida russa si fonda sulla combinazione di coercizione militare, manipolazione dell'informazione e operazioni di influenza politica, integrate in una logica di lungo periodo volta a destabilizzare il nemico senza ricorrere a conflitti aperti[21]. All'interno di questo quadro, le operazioni ibride russe non mirano primariamente alla destabilizzazione immediata o al collasso degli stati bersaglio, bensì alla produzione di effetti cumulativi sul piano politico, psicologico e infrastrutturale. Sabotaggi mirati, attività di intelligence aggressiva, campagne di disinformazione e interferenze cognitive concorrono a erodere progressivamente la fiducia nelle istituzioni, ad amplificare fratture sociali preesistenti e a testare la resilienza dei sistemi democratici occidentali[22]. La dimensione ibrida assume così una funzione di logoramento controllato, in cui l'ambiguità operativa e la negabilità plausibile rappresentano elementi centrali della strategia.

Le operazioni di intelligence, inoltre, non si limitano alla raccolta informativa, ma comprendono sabotaggi, attività di influenza e interventi mirati a modellare comportamenti e decisioni politiche. Come evidenzia Cristadoro, tali operazioni sono spesso condotte attraverso strutture civili, reti indirette e canali difficilmente tracciabili, rendendo complessa l'attribuzione delle responsabilità e aumentando il valore strategico dell'ambiguità[23]. Un caso emblematico è emerso in Polonia nell'ottobre 2025, quando le autorità di Varsavia hanno

---

[21] Kashin, Vassily. H-Hybrid Warfare, *Russia in Global Affairs*, 26 marzo 2020. https://eng.globalaffairs.ru/articles/h-hybrid-war/

[22] Fridman, Ofer; Kabernik, Vitaly; Pearce, James C. Hybrid conflict and information warfare, *Lynne Rienner*, 2019.

[23] Cristadoro, Nicola. Quando l'orso si traverse da serpente. Le operazioni dell'intelligence russa nella guerra cognitiva contro l'Occidente, *Istituto Gino Germani di Scienze Sociali e Studi Strategici, Research Paper*, Gennaio 2026. https://www.istitutogermani.org/wp-content/uploads/2026/02/N.-Cristadoro-Quando-lorso-si-traveste-da-serpente-2026-Ist.-Germani.pdf

accusato un ex funzionario del registro civile di aver fornito dati autentici utilizzati per costruire identità di copertura destinate ad agenti russi "illegali"[24]. Secondo le ricostruzioni disponibili, tali documenti avrebbero consentito a operatori dell'intelligence russa di operare con identità formalmente legittime sul territorio europeo, facilitando un'infiltrazione di lungo periodo nelle strutture amministrative e nei circuiti economici dell'Unione. Episodi di questo tipo confermano come la dimensione ibrida dell'intelligence russa integri strumenti clandestini e coperture civili in una strategia orientata alla persistenza operativa e alla negabilità plausibile.

Le infrastrutture critiche europee costituiscono uno dei principali terreni di applicazione della guerra ibrida russa. Attacchi e tentativi di sabotaggio contro reti energetiche, infrastrutture logistiche e cavi sottomarini hanno evidenziato come Mosca punti a generare effetti cumulativi sul piano operativo ed economico, costringendo i governi a rafforzare i dispositivi di protezione, rivedere i protocolli di resilienza e sostenere costi crescenti per la messa in sicurezza delle reti[25]. Tali costi non si limitano ai danni diretti, ma includono investimenti strutturali in sorveglianza, cybersecurity e protezione fisica delle infrastrutture strategiche. Parallelamente, l'analisi *dell'International Institute for Strategic Studies* mostra come la scala delle operazioni russe contro infrastrutture europee si sia intensificata tra il 2024 e il 2025, con particolare esposizione di Germania, Polonia e paesi baltici, oltre alle aree del Mar Baltico e del Mare del

[24] Marzano, Jacopo. Dati reali, identità false. Varsavia accusa un ex impiegato di aver fornito coperture per agenti russi. *Formiche.net.* 11 ottobre 2025, https://formiche.net/2025/10/spionaggio-intelligence-polonia-russia-kgb/#content

[25] Franceschini, Caterina. Gli attacchi russi alle infrastrutture energetiche critiche europee: le sfide per il vecchio continente. *IARI*. 29 dicembre 2025. https://iari.site/2025/12/29/gli-attacchi-russi-alle-infrastrutture-energetiche-critiche-europee-le-sfide-per-il-vecchio-continente/

Nord per quanto riguarda cavi e collegamenti energetici sottomarini[26]. Le operazioni registrate non appaiono come episodi isolati, ma come parte di una strategia coerente di pressione sistemica, volta a ridurre la capacità complessiva di risposta degli stati europei e a generare incertezza strategica di lungo periodo.

Un livello parallelo della strategia russa riguarda la guerra narrativa e cognitiva, concepita per influenzare l'opinione pubblica e decisioni politiche attraverso la diffusione selettiva di informazioni, fake news e narrazioni polarizzanti volte a erodere fiducia e coesione sociale. Tali operazioni non si esauriscono in iniziative episodiche, ma puntano a produrre effetti cumulativi di lungo periodo, favorendo dinamiche di destabilizzazione graduale[27].

La vulnerabilità di questo dominio è confermata da studi internazionali sulla fiducia nei media e sulla percezione della disinformazione. Il Reuters Institute Digital News Report del 2025 evidenzia come in numerosi paesi europei la fiducia delle notizie resti strutturalmente fragile – attorno al 40% in media – e come una quota significativa di cittadini dichiari difficoltà nel distinguere tra informazione verificata e contenuti manipolati[28]. In un contesto caratterizzato da polarizzazione e bassa fiducia, campagne di influenza statali trovano un ambiente favorevole all'amplificazione di narrazioni divisive – dinamica che la Russia ha integrato stabilmente nella propria competizione strategica con

[26] Edwards, Charlie. The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure, *The International Institute for Strategic Studies (IISS)*, 19 agosto 2025. https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/.

[27] Ministero degli Affari Esteri e della Cooperazione Internazionale. Narrative warfare e guerra ibrida nel disordine globale. Quale impatto nelle aree di interesse strategico per l'Italia, 2026. https://www.esteri.it/wp-content/uploads/2026/01/FPC-ECFR_Narrative-warfare-e-guerra-ibrida-nel-disordine-globale_FINALE.pdf

[28] Reuters Institute for te Study of Journalism. Digital News Report 2025, Reuters Institute. 2025. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2025-06/Digital_News-Report_2025.pdf

l'Occidente. In questo quadro si inserisce anche la politica dei "compatrioti" e la tutela dei cittadini russi all'estero, che possono offrire una cornice politico-giuridica funzionale a legittimare attività di influenza e intelligence[29].

La disinformazione si configura così come uno strumento strutturale della competizione strategica contemporanea, capace di incidere sulla percezione della realtà e sulla tenuta delle società democratiche. Come sottolinea Gerrits, la sua efficacia aumenta quando è integrata in una strategia statale coerente, capace di sfruttare l'ambiguità informativa e la difficoltà di attribuzione per condizionare processi politici e decisionali senza ricorrere alla forza militare diretta[30]. In questo senso, la guerra ibrida russa utilizza l'informazione come moltiplicatore di potenza, trasformando il dominio cognitivo in uno spazio di competizione permanente.

Chiarire il significato di "guerra ibrida" diventa quindi essenziale per comprendere la portata di queste pratiche. Il non-paper del Ministero della Difesa Italiano definisce la guerra ibrida come l'impiego coordinato e simultaneo di strumenti militari e non militari – politici, economici, informativi, cibernetici e psicologici – finalizzati a sfruttare le vulnerabilità dell'avversario mantenendosi al di sotto della soglia del conflitto armato convenzionale[31]. Tale approccio si fonda sulla progressiva erosione delle capacità decisionale e della resilienza dello stato bersaglio, più che sulla conquista territoriale o sullo scontro

---

[29] Nascetti, Giulia Ginevra. La dottrina Karaganov e la policy dei "compatrioti": la protezione dei russi nell'estero vicino, *Centro Studi Geopolitica.info*, 23 ottobre 2020. https://www.geopolitica.info/la-dottrina-karaganov-e-la-policy-dei-compatrioti-la-protezione-dei-russi-nellestero-vicino/

[30] Gerrits, André W.M. Disinformation in International Relations: how importanti s it? *Security and Human Rights*. 12 dicembre 2018. https://brill.com/view/journals/shrs/29/1-4/article-p3_3.xml?language=en

[31] Ministero della Difesa. Il contrasto alla guerra ibrida: una strategia attiva, *Non-paper del Ministero della Difesa Guido Crosetto*, novembre 2025. https://www.difesa.it/assets/allegati/83696/non-paper_il_contrasto_alla_guerra_ibrida.pdf.

militare diretto. Secondo questa prospettiva, la guerra ibrida non può essere interpretata come una somma di azioni episodiche, bensì come una modalità strutturata di competizione strategica, inserita nella pianificazione militare e politico-strategica degli stati che la adottano. L'ibridazione degli strumenti consente di modulare l'intensità della pressione esercitata, adattandola al contesto e alle reazioni dell'avversario, preservando al contempo un elevato grado di ambiguità operativa[32]. La guerra ibrida diventa così un mezzo per condizionare il comportamento degli avversari senza oltrepassare soglie che attiverebbero meccanismi di deterrenza collettiva.

È all'interno di questo quadro teorico che si colloca il dibattito sulla cosiddetta "dottrina Gerasimov"[33]. Come ricostruito da Morini, i rapporti tra Russia e Occidente sono stati segnati da accuse reciproche di interferenze politiche, operazioni di intelligence e dal sostegno statunitense alle rivoluzioni colorate, fenomeni che il Capo di Stato russo Valerij Gerasimov ha interpretato come forme di aggressione non convenzionali alla sovranità russa. Secondo questa lettura, attacchi cibernetici, operazioni psicologiche e campagne di disinformazione costituiscono gli elementi centrali di una nuova guerra non lineare, nella quale diventa sempre più difficile distinguere tra pace e conflitto, tra attori statali e non statali e tra azioni offensive e difensive, con il rischio di una condizione di "Total Chaos Warfare"[34]. Tuttavia, è fondamentale sottolineare come l'analisi di Gerasimov non sia orientata alla formalizzazione di una dottrina

[32] Allegri, Riccardo. Hybrid and Information Warfare: Moscow's strategy and the Russian asymmetric challenge to the world. *Centro Alti Studi Difesa*, 2021-2024. https://eldcasd.difesa.it/pluginfile.php/22712/mod_page/content/206/Riccardo%20Allegri.pdf

[33] Valerij Gerasimov, Capo di Stato Maggiore delle Forze Armate russe dal 2012, è stato spesso associato al concetto di guerra non lineare e alla rilevanza delle operazioni cibernetiche e psicologiche nella strategia russa.

[34] Morini, Mara. La Russia di Putin, *Il Mulino*, 2020, pp. 1949-150.

offensiva russa codificata, bensì alla descrizione delle minacce percepite da Mosca. In questo senso, le sue riflessioni si inseriscono in una narrazione prevalentemente difensiva, volta a denunciare l'uso occidentale di strumenti politici, informativi ed economici per influenzare assetti interni e dinamiche sociali ritenute vulnerabili. Come chiarisce Bartles, la cosiddetta "dottrina Gerasimov" rappresenta più una categoria interpretativa elaborata in ambito occidentale che un corpus dottrinale ufficialmente adottato dalla Federazione Russa[35]. Lo stesso Galeotti, che contribuì alla diffusione dell'espressione, ha successivamente riconosciuto come tale dottrina sia una semplificazione analitica utile a descrivere l'approccio russo alla competizione ibrida, ma non un documento strategico ufficiale[36].

Oggi si discute della fase post-Gerasimov, caratterizzata dalla sistematizzazione operativa di azioni a bassa intensità concepite per logorare progressivamente l'avversario. Questa strategia dei "mille tagli", frammentata ma cumulativa, erode la resilienza politica, economica e sociale dei paesi occidentali senza superare la soglia[37]. In tale contesto, la dimensione cognitiva è centrale: l'obiettivo è colpire l'anima della società nemica, sfruttando polarizzazioni interne e sfiducia istituzionale per amplificare divisioni e ridurre la capacità decisionale degli stati bersaglio[38]. Complessivamente, il dibattito sulla "dottrina Gerasimov" e sulla sua evoluzione post-Gerasimov mostra come la guerra ibrida

[35] Bartles, Charles. Getting Gerasimov Right, *Military Review 1*, 2016. pp. pp.30-38
[36] Galeotti, Mark. I'm Sorry for Creating the 'Gerasimov Doctrine', *Foreign Policy*, 2018. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/
[37] Marzano, Jacopo. Guerra ibrida russa, i mille tagli ibridi del Cremlino contro l'Occidente, *Formiche.net*, 22 dicembre 2025. https://formiche.net/2025/12/guerra-ibrida-russa-i-mille-tagli-ibridi-del-cremlino-contro-loccidente/#content
[38] Marzano, Jacopo. Colpire l'anima della società nemica per erodere l'Occidente. Ecco la dottrina russa. *Formiche.net,* 4 dicembre 2025. https://formiche.net/2025/12/colpire-lanima-della-societa-nemica-per-erodere-loccidente-ecco-la-dottrina-russa/#content.

russa non sia un singolo paradigma dottrinale, ma un'espressione di una cultura strategica orientata alla competizione sotto soglia e alla gestione dell'ambiguità, in cui gradualità, difficoltà di attribuzione e integrazione di strumenti militari e non militari costituiscono elementi strutturali dell'azione strategica russa.

Il fattore statunitense e il trasferimento degli oneri di sicurezza

La *National Security Strategy* (NSS) statunitense del 2025 rappresenta un passaggio di rilevanza strutturale nella ridefinizione delle priorità strategiche di Washington. Il documento sancisce un riposizionamento sistematico dell'attenzione strategica americana verso l'Indo-Pacifico e l'Artico, ridimensionando il peso del teatro europeo nella pianificazione globale degli Stati Uniti[39]. Pur riaffermando formalmente l'impegno nei confronti dell'Alleanza Atlantica, la NSS introduce una logica sempre più esplicita di delega funzionale e responsabilizzazione degli alleati europei, chiamati ad assumere un ruolo primario nella gestione della deterrenza regionale e della sicurezza collettiva[40].

Questa impostazione strategica si inserisce in un contesto politico caratterizzato da dichiarazioni dell'amministrazione Trump che sono state interpretate da diversi osservatori come segnali di una possibile ridefinizione del livello e delle modalità dell'impegno statunitense nel teatro europeo. In diverse occasioni pubbliche e interviste, il Presidente ha descritto i paesi dell'Unione Europea come politicamente fragili, incapaci di sostenere autonomamente il peso della propria sicurezza e strutturalmente dipendenti dalla protezione americana,

[39] National Security Strategy USA 2025 https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

[40] Evangelisti, Alberto. "Europa sotto pressione: come la National Security Strategy 2025 ridefinisce l'alleanza atlantica.", *Centro Studi Geopolitica.info*, 12 gennaio 2026. https://www.geopolitica.info/europa-national-security-strategy-alleanza-transatlantica/

mettendo apertamente in discussione il valore strategico dell'Europa per gli interessi nazionali statunitensi[41]. Secondo Ben Hodges, ex comandante delle forze statunitensi in Europa, questa narrazione riflette un orientamento sempre più diffuso a Washington che tende a considerare il continente europeo come marginale rispetto alle priorità strategiche americane[42]. Tali dichiarazioni si inseriscono in un quadro più ampio di ridefinizione del rapporto transatlantico, in cui l'impegno statunitense verso l'Europa è stato frequentemente ricondotto a una logica di *burden-sharing* e di valutazione costi-benefici in termini di ritorno politico e strategico per Washington[43].

Nel loro insieme, questi segnali contribuiscono a delineare un crescente *credibility gap*: la deterrenza collettiva resta formalmente garantita, ma la certezza di un intervento statunitense tempestivo e risolutivo in risposta a crisi ibride o ad azioni ostili condotte al di sotto della soglia del conflitto armato appare progressivamente meno scontata[44]. Sul piano operativo e istituzionale, il trasferimento degli oneri di sicurezza si manifesta con particolare chiarezza nell'orientamento statunitense verso una progressiva europeizzazione della deterrenza NATO[45]. Washington, infatti, sembra aver definito una scadenza indicativa al 2027 per una transizione verso una difesa dell'Alleanza a guida in

---

[41] Adnkronos, "Trump torna alla carica: "Paesi Ue decadenti e leader deboli, non sanno cosa fare". Bruxelles replica: "Orgogliosi di loro", 9 dicembre 2025. https://www.adnkronos.com/Archivio/internazionale/esteri/trump-insiste-paesi-ue-decadenti-e-leader-deboli-la-reazione-di-bruxelles_7xaEN049AuT2YHiXTobMA8.

[42] Euronews, "*Washington vede l'Europa come irrilevante, intervista* a Ben Hodges", 1° dicembre 2025. https://it.euronews.com/my-europe/2025/12/01/washington-vede-leuropa-come-irrilevante-dice-a-euronews-lex-comandante-generale-degli-sta

[43] Wright, Thomas. The Trump doctrine and the emerging international system. Brookings Institution. 2017.

[44] Mazarr, Michael J. Dr. *Mastering the Gray Zone: understanding a changing era of conflict*. U.S. Army War College Press, 2015. https://press.armywarcollege.edu/monographs/428/

[45] Centro Studi Geopolitica.info, La NATO verso l'AIA. Geopolitical Brief/Serie Speciale n.1, 24 giugno 2025. https://www.geopolitica.info/wp-content/uploads/2025/06/n.-1.pdf

misura crescente dagli alleati europei, riducendo il proprio coinvolgimento diretto nella gestione ordinaria della deterrenza sul fianco orientale[46].

Numerosi studi convergono nel sottolineare come l'Europa debba prepararsi a operare in un contesto caratterizzato da una presenza americana più selettiva, condizionata e strettamente funzionale agli interessi strategici statunitensi. Secondo il Center for Strategic and International Studies (CSIS), l'Unione Europea è chiamata a sviluppare capacità autonome di deterrenza, resilienza e risposta, imparando a "difendersi con meno America"[47]. In termini analoghi, l'*Istituto per gli Studi di Politica Internazionale* (ISPI) descrive l'attuale fase come una transizione critica, nella quale il venir meno delle garanzie operative statunitensi impone agli europei di colmare rapidamente vulnerabilità strutturali e deficit di coordinamento, pena una crescente esposizione alle pressioni strategiche russe[48]. In questo quadro, il disimpegno americano non si limita a ridurre l'ombrello di sicurezza esterno, ma agisce come un fattore di moltiplicatore delle fragilità europee, portando in superficie dipendenze operative e asimmetrie capacitive che per lungo tempo erano state compensate dalla presenza statunitense, sia sul piano militare sia su quello organizzativo e decisionale[49].

---

[46] Reuters, "US sets 2027 deadline for Europe-led NATO defense, officials say", 6 dicembre 2025 https://www.reuters.com/business/aerospace-defense/us-sets-2027-deadline-europe-led-nato-defense-officials-say-2025-12-05/.

[47] Bergmann, Max and Svendsen, Otto. *How Europe can defend itself with less America. Center for Strategic and International Studies (CSIS)*, 2025. https://www.csis.org/analysis/how-europe-can-defend-itself-less-america

[48] De Luca, Alessia. Washington volta pagina: l'Europa ora è sola, *Istituto per gli Studi di Politica Internazionale (ISPI)*, 2025. https://www.ispionline.it/it/pubblicazione/washington-volta-pagina-leuropa-ora-e-sola-225264

[49] Calabrese, Anna. "Disimpegno americano e sicurezza europea: una lettura tra dipendenze operative e prospettive per l'UE*". Centro Studi Geopolitica.info*, 9 gennaio 2026. https://www.geopolitica.info/disimpegno-americano-sicurezza-europea/

A fronte di questa evoluzione, la trasformazione del ruolo statunitense nella sicurezza europea assume una dimensione che va oltre la semplice riallocazione di risorse o la ridefinizione delle priorità geografiche. Si profila piuttosto un mutamento qualitativo dell'equilibrio transatlantico, nel quale la garanzia americana permane sul piano formale ma si accompagna a una crescente aspettativa di autonomia operativa da parte degli alleati. In tale contesto, la tenuta della deterrenza sul fianco orientale e la gestione delle minacce sotto soglia dipendono sempre più dalla capacità degli stati europei di coordinare strumenti militari, resilienza infrastrutturale e processi decisionali in modo integrato[50]. In questa prospettiva, la transizione delineata dalla NSS 2025 si inserisce in un dibattito già avviato a livello europeo sulla *strategic autonomy* e sul rafforzamento del pilastro europeo della NATO, come formalizzato nello Strategic Compass dell'Unione Europea[51]. Tale evoluzione sollecita una riflessione sul ruolo dell'Unione quale attore di sicurezza regionale, sia in termini di strumenti militari sia di governance strategica.

Le risposte europee tra strumenti e fratture interne

Sotto questa pressione, l'Unione Europa ha avviato una serie di iniziative volte a rafforzare la propria capacità di risposta. Il dibattito sull'autonomia strategica, il potenziamento della cooperazione in materia di difesa e il lancio di strumenti come RearmEU[52] rappresentano tentativi concreti di adattamento a un contesto in cui la leadership americana non è più onnipresente. Non a caso, fonti europee sottolineano la necessità di accelerare il percorso verso una maggiore autonomia

[50] Howorth Jolyon, Strategic autonomy in European defense: Progress or pipe dream? *European Politics and Society, 19*(5), pp. 523–537, 2018.
[51] Council of European Union. *A strategic compass for security and defence.* 2022. *https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en*
[52] Saitta, Mattia. RearmEU e il mito degli 800 miliardi: numeri, strumenti e realtà dell'iniziativa europea per la difesa, *Centro Studi Geopolitica.info*, 26 giugno 2025. https://www.geopolitica.info/rearm-europe/

strategica proprio in risposta al progressivo ridimensionamento dell'impegno statunitense[53]. Tuttavia, tali iniziative continuano a scontrarsi con persistenti fratture politiche e organizzative tra gli Stati Membri, che ne limitano la traduzione in una postura realmente coerente ed efficace. Questa frammentazione emerge con particolare evidenza nel dominio informativo, cruciale nel contrasto alla guerra ibrida. Nonostante il rafforzamento militare, l'UE continua a dipendere da ventisette sistemi di intelligence nazionali con priorità e capacità eterogenee, senza una reale integrazione analitica. In questo senso, il vero "anello mancante" dell'integrazione europea[54] è di natura informativa e cognitiva: un limite cruciale nella competizione ibrida, dove superiorità analitica e rapidità decisionale sono determinanti. Ne deriva un disallineamento tra ambizione strategica e capacità cognitiva che indebolisce la risposta europea sottosoglia.

L'architettura di sicurezza predisposta dall'UE per fronteggiare le minacce ibride ha subito un'accelerazione significativa nell'ultimo triennio, evolvendo da una fase di semplice osservazione a una di codifica normativa e operativa più strutturata. Il fulcro di questa strategia risiede nel recente consolidamento del cosiddetto "Hybrid Toolbox", un quadro d'azione contenente oltre 200 misure civili e militari identificate che possono essere mobilitate quando uno Stato membro si trova ad affrontare una campagna ibrida[55]. Inoltre, l'UE aveva già

[53] ANSA, Fonti Ue, 'dobbiamo accelerare sulla nostra autonomia strategica', 22 gennaio 2026. https://www.ansa.it/sito/notizie/mondo/2026/01/22/fonti-ue-dobbiamo-accelerare-sulla-nostra-autonomia-strategica_443676ce-28ca-42bd-a527-57e6434d25d2.html.

[54] Saitta, Mattia. L'anello mancante della difesa europea: verso un servizio segreto comune? *Centro Studi Geopolitica.info* 24 novembre 2025. https://www.geopolitica.info/anello-mancante-difesa-europea/

[55] Lasoen, Kenneth "Realising the EU Hybrid Toolbox: opportunities and pitfalls", *Clingendael,* Dicembre 2022, https://www.clingendael.org/sites/default/files/2022-12/Policy_brief_EU_Hybrid_Toolbox.pdf

creato la piattaforma EUvsDisinfo, volta a sfatare le fake news[56], a cui è stata integrata una strategia più ampia di contrasto alla manipolazione dell'informazione e all'interferenza esterna (FIMI)[57], segnando il passaggio da una semplice attività di *debunking* a una vera e propria analisi proattiva dei vettori di influenza ostile, supportata dai Centri di Analisi e Condivisione delle Informazioni (ISACs).

Parallelamente alla dimensione cognitiva, la protezione fisica ha assunto una urgenza senza precedenti, manifestandosi in iniziative di difesa dei confini e delle infrastrutture critiche che cercano di colmare il divario tra sicurezza interna e difesa esterna. Il rafforzamento della postura sul fianco orientale non è più affidato solo alla presenza militare convenzionale, ma si sta delineando attraverso progetti tecnologici d'avanguardia come il "Muro Anti-Drone" Europeo e l'Eastern Flank Watch[58]. La prima iniziativa, promossa con vigore da Polonia, Finlandia e Repubbliche Baltiche, mira a creare una barriera digitale e cinetica integrata, capace di neutralizzare l'uso strumentale dei droni per attività di sorveglianza o per la gestione artificiale dei flussi migratori. L'Eastern Flank Watch invece è un sistema di monitoraggio costante che tenta di armonizzare la sorveglianza di frontiera con la protezione delle reti energetiche e digitali.

---

[56]EUvsDisinfo, "Mission", https://euvsdisinfo.eu/about/?_gl=1*hkmdnc*_up*MQ..*_ga*MTYzNzQwMTkwNS4xNzcwODI1MjM4*_ga_9SH0NZ5558*czE3NzA4MjUyMzckbzEkZzAkdDE3NzA4MjUyMzckajYwJGwwJGgw

[57] European External Action Service, "Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)", 27 Gennaio 2026, https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en#104639.

[58] Croce, Giulio. "Quali prospettive per il Muro anti-drone europeo e la "Eastern Flank Watch", *op. cit.*

Entrambe sono state identificate, nella Roadmap per la Prontezza 2030, come progetti di punta per la resilienza difensiva europea[59].

La vulnerabilità dei fondali marini, evidenziata drammaticamente dai sabotaggi ai gasdotti nel Baltico, ha spinto l'Unione a cercare forme di cooperazione che superino i perimetri istituzionali classici. Il pattugliamento congiunto tra Regno Unito e Norvegia nel Mare del Nord[60], pur coinvolgendo attori non appartenenti all'UE, è oggi considerato una componente vitale della sicurezza collettiva europea, fungendo da catalizzatore per la nuova Task Force NATO-UE sulla resilienza delle infrastrutture critiche. Questo coordinamento riflette l'attuazione della Strategia di Sicurezza Marittima dell'UE aggiornata del 2023[61], che riconosce esplicitamente la protezione dei cavi sottomarini e delle pipeline come un interesse vitale che richiede una sorveglianza costante e una capacità di risposta rapida.

Queste misure si aggiungono alle sanzioni, che dal 2019 fanno parte della risposta europea agli attacchi cibernetici[62] e alla propaganda filorussa. Le sanzioni includono il congelamento dei beni e il divieto di viaggio per le persone, e il divieto di fornire fondi o risorse economiche per le entità[63].

---

[59] Croce, Giulio. “La Roadmap per la prontezza difensiva europea: obiettivo 2030”, 17 Ottobre 2025, *Geopolitica.info,* https://www.geopolitica.info/roadmap-prontezza-difensiva-europea/

[60] Croce, Giulio. 22:30’, Intervista di Gianpaolo Musumeci, *Nessun Luogo è Lontano,* Radio 24, 4 Dicembre 2025, https://www.radio24.ilsole24ore.com/programmi/luogo-lontano/puntata/trasmissione-4-dicembre-2025-160500-2344327946455809.

[61] Consiglio dell’Unione Europea, “Sicurezza marittima: il Consiglio approva la strategia riveduta e il piano d'azione dell'UE, 24 Ottobre 2023 ”https://www.consilium.europa.eu/it/press/press-releases/2023/10/24/maritime-security-council-approves-revised-eu-strategy-and-action-plan/

[62] Consiglio dell’Unione Europea, “Timeline - Sanctions against cyber-attacks”. https://www.consilium.europa.eu/it/policies/sanctions-against-cyber-attacks/timeline-sanctions-cyber-attacks/

[63] Consiglio dell'Unione Europea, “Minacce ibride russe: il Consiglio impone sanzioni nei confronti di dodici persone e due entità per manipolazione delle informazioni e attacchi informatici”, 15 dicembre 2025, https://www.consilium.europa.eu/it/press/press-

Conclusioni

Nonostante la proliferazione di iniziative europee volte a rafforzare la resilienza e la capacità di risposta alle minacce ibride, l'efficacia complessiva dell'azione dell'Unione continua a scontrarsi con limiti strutturali profondamente radicati nelle diverse culture strategiche degli Stati membri. Emerge, in particolare, una persistente asimmetria nella percezione della minaccia: mentre i paesi della frontiera orientale interpretano le operazioni ibride russe come una sfida esistenziale immediata, altre capitali – e in particolare i paesi dell'Europa meridionale – tendono a ricondurle a problematiche di natura prevalentemente securitaria, economica o commerciale. Questa divergenza contribuisce a rallentare l'adozione di misure coercitive più incisive e a indebolire la coerenza dell'azione europea.

Tale frattura non è soltanto politica, ma anche organizzativa e procedurale. La conseguente frammentazione dei processi decisionali favorisce un approccio prevalentemente reattivo, incentrato sulla gestione dell'emergenza piuttosto che sulla costruzione di una deterrenza credibile nello spazio sottosoglia. La difficoltà nel raggiungere un'attribuzione politica univoca e tempestiva delle azioni ostili impedisce all'Unione Europea di trasformare la propria architettura di risposta in uno strumento realmente dissuasivo, lasciando ampie zone d'ombra operative in cui gli attori avversari possono continuare ad agire con costi politici e strategici contenuti.

Questo limite assume una rilevanza ancora maggiore alla luce del progressivo trasferimento degli oneri di sicurezza dagli Stati Uniti agli alleati europei. In un contesto in cui l'ombrello strategico americano appare sempre più selettivo e condizionato, l'incapacità europea di operare come soggetto unitario nella zona

releases/2025/12/15/russian-hybrid-threats-council-sanctions-twelve-individuals-and-two-entities-over-information-manipulation-and-cyber-attacks/.

grigia rischia di tradursi in una vulnerabilità strutturale. La guerra ibrida, proprio perché concepita per sfruttare ambiguità, divisioni e lentezze decisionali, diventa così uno strumento particolarmente efficace nel testare la solidità del progetto europeo nel suo complesso.

In ultima analisi, la sfida che si pone a Bruxelles non riguarda più la disponibilità di strumenti tecnici o di quadri normativi, ormai ampiamente sviluppati, bensì la capacità di sintetizzare interessi, percezioni e priorità nazionali in una visione strategica condivisa, capace di tradursi in volontà politica e azione coerente. La risposta europea alla guerra ibrida russa rappresenta quindi un banco di prova cruciale: non solo per la sicurezza del continente, ma per la credibilità stessa dell'Unione Europea come attore strategico in un contesto di competizione permanente sotto soglia.

Tra vulnerabilità e contromisure: una fotografia della minaccia ibrida in Italia

di Davide Sotgia

Introduzione

In questo periodo di grandi cambiamenti nello scenario internazionale, la tematica della minaccia ibrida ha attirato l'attenzione e le preoccupazioni di molti tra decisori, analisti e cittadini. Oggi parlare di minaccia ibrida è fondamentale dato che essa rappresenta un fenomeno che mina la sicurezza e la prosperità degli Stati dal loro interno, tramite operazioni economiche, informatiche, informative e di manipolazione mediatica che agiscono direttamente sul tessuto economico e sociale, aggirando gli apparati di difesa convenzionali. Di conseguenza, ci si chiede come definirla, come si manifesti e cosa fare per arginarla. Il presente lavoro si inserisce in questo spazio, adottando la prospettiva dell'Italia e analizzando il modo in cui questa subisce e risponde al fenomeno, mirando al contempo a sistematizzare i rischi che il nostro Paese corre e le misure che ha adottato per affrontarli.

L'analisi è divisa in tre sezioni: la prima è dedicata al chiarimento dei concetti di minaccia ibrida, guerra ibrida e zona grigia con le loro caratteristiche e manifestazioni. La seconda sezione riguarda l'individuazione e l'analisi di alcuni dei profili di vulnerabilità presenti in Italia con relativi esempi concreti, da quelli più conosciuti a quelli meno manifesti. La terza parte esamina le iniziative, misure e strumenti adottati dall'Italia nel corso degli anni per recepire, comprendere e reagire al fenomeno, al fine di assicurare la maggiore resilienza possibile del tessuto sociale ed economico nazionale.

Comprendere la minaccia ibrida

Per trattare la questione della "minaccia ibrida" nel contesto italiano, occorre preliminarmente valutare il grado di consapevolezza, informazione e interesse manifestato dal Paese attraverso le sue diverse articolazioni istituzionali, sociali e politiche. In Occidente, la discussione sul tema risale almeno al 2006, come tentativo di spiegare i successi tangibili di Hezbollah contro le Forze Armate israeliane durante la seconda guerra del Libano[1]. L'obiettivo era quello di inquadrare l'azione di un gruppo non statale in grado di procurarsi e adoperare strumenti fino a quel momento solo di monopolio statale.

Un mutamento significativo si è verificato nel 2014 con l'occupazione della Crimea. In questo caso un attore statale, la Russia, ha agito con mezzi non convenzionali, riuscendo a gestire la narrativa interna e internazionale ed evitare ripercussioni militari ed economiche significative. A seguito di questo evento la ricerca sul tema si è concentrata prevalentemente sull'azione degli Stati, sui possibili effetti e sulle contromisure da adottare[2]. La guerra in Ucraina del 2022 ha rappresentato un ulteriore punto di svolta. Gli Stati occidentali sono divenuti bersaglio di pratiche variegate e flessibili volte a paralizzarli o a rendere insostenibile il loro supporto all'Ucraina. Queste azioni hanno reso evidenti le fragilità strutturali occidentali e hanno provocato un'accelerazione della diffusione di consapevolezza presso Governo e cittadinanza circa l'impatto e la portata reale del fenomeno e sulla necessità di adottare misure adeguate ad affrontarlo.

[1] Gunneriusson, H. (2021). "Hybrid warfare: Development, historical context, challenges and interpretations" *Icono 14, 19*(1), 15-37. https://icono14.net/ojs/index.php/icono14/article/view/1608/1809

[2] ibidem

Per quanto riguarda l'odierno panorama italiano, è possibile affermare che il mondo delle istituzioni, delle autorità e dell'accademia è a conoscenza del fenomeno e parla apertamente della sua esistenza, delle sue possibili conseguenze e della necessità di mobilitarsi per affrontarlo. A dimostrazione di ciò si può fare riferimento alle relazioni annuali non classificate sulla politica dell'informazione per la sicurezza, che dalla sua edizione del 2023 tratta esplicitamente la minaccia ibrida[3], al "non-paper [o documento non ufficiale] sul contrasto alla guerra ibrida" del Ministero della Difesa[4], riconducibile a un tentativo di sistematizzazione della minaccia e promozione del dibattito, fino alle dichiarazioni del COPASIR[5] e del Consiglio supremo di difesa[6], che riconoscono il fenomeno e mettono in guardia dagli strumenti di pressione e destabilizzazione e dalla loro sintesi in una sfida unitaria.

Invece, nel caso della gran parte della cittadinanza la conoscenza e consapevolezza del fenomeno della minaccia ibrida risulta, nonostante la forte e recente popolarità della tematica, parziale e frammentata. Tendenzialmente, gli Italiani sono a conoscenza, spesso grazie all'azione dei media, dell'esistenza di fenomeni come la disinformazione, la manipolazione mediatica, i cyberattacchi, ecc., ma non sono portati, a causa della mancanza di uno sforzo di sistematizzazione e di divulgazione della tematica della minaccia ibrida, ad

[3] Sistema di Informazione per la Sicurezza della Repubblica. "Relazione annuale dell'intelligence al Parlamento sulla politica dell'informazione per la sicurezza relativa all'anno 2023", 4 marzo 2024. https://www.sicurezzanazionale.gov.it/cosa-facciamo/relazione-annuale

[4] Ministero della Difesa italiano. "Il contrasto alla guerra ibrida: una strategia attiva", novembre 2025. https://www.difesa.it/assets/allegati/83696/non-paper_il_contrasto_alla_guerra_ibrida.pdf

[5] Marzano, Jacopo. "Dieci anni di allarmi dagli 007 italiani (e dal Parlamento): ecco i dossier che raccontano la guerra ibrida" *Il Riformista*, 22 novembre 2025 https://www.ilriformista.it/dieci-anni-di-allarmi-dagli-007-italiani-e-dal-parlamento-ecco-i-dossier-che-raccontano-la-guerra-ibrida-490200

[6] Ministero della Difesa italiano. "Supreme Defence Council", 17 novembre 2025 https://www.difesa.it/eng/primo-piano/supreme-defence-council/83732.html

associare i vari singoli eventi a uno sforzo strutturato e coordinato da parte di un altro attore, al fine di raggiungere i suoi obiettivi a danno del Paese bersaglio della campagna[7]. Questa mancanza di consapevolezza, particolarmente preoccupante in quanto la cittadinanza è uno dei bersagli privilegiati, è rafforzata da un generale disinteresse verso le tematiche legate alla sicurezza e alla difesa[8], dal tecnicismo e opacità dei termini comunemente utilizzati e dal fatto che la minaccia ibrida si presenta come un fenomeno variegato e in continua evoluzione[9]. In tal senso, è possibile trovare un riscontro nei dati riportati dall'Eurobarometro nel settembre 2025. Alla domanda "Quali delle seguenti opzioni è per te la principale sfida che l'Europa sta affrontando?" (Q3), gli italiani hanno indicato in modo minore, in assoluto e rispetto alla media UE, i temi di difesa e sicurezza e si collocano tra gli ultimi per quanto riguarda la preoccupazione rispetto a disinformazione e manipolazione mediatica. Alla domanda "Quale tra queste è per te la minaccia più seria alla democrazia in Europa?" (Q12), gli italiani hanno mostrato una maggiore sensibilità alla disinformazione in generale (con un buon incremento rispetto al 2024), ma sono decisamente sotto alla media per quanto riguarda la disinformazione proveniente da un attore esterno non democratico. Rientrano nella media europea per quanto riguarda le interferenze politiche ed economiche sotto copertura[10].

---

[7] Bompani, Antonio. "La guerra ibrida in casa. La minaccia della disinformazione è entrata nel dibattito pubblico, finalmente" *Linkiesta*, 24 novembre 2025 https://www.linkiesta.it/2025/11/disinformazione-guerra-ibrida-risposta-politica-fake-news-democrazia.

[8] Mauri, Paolo. "L'Italia non è pronta alla guerra? Paolo Mauri: "no, e non è solo una questione di armi" *InsideOver*, 18 settembre 2025 https://it.insideover.com/difesa/litalia-non-e-pronta-alla-guerra-paolo-mauri-no-e-non-e-solo-una-questione-di-armi.html

[9] Consiglio dell'Unione Europea. "Minacce Ibride", novembre 2025 https://www.consilium.europa.eu/it/policies/hybrid-threats

[10] Commissione Europea. "Flash Eurobarometer 569. EU challenges and priorities", settembre 2025 https://europa.eu/eurobarometer/surveys/detail/3380

Nel dibattito pubblico italiano, i concetti di “minaccia ibrida”, di “zona grigia” e di “guerra ibrida” risultano ancora particolarmente opachi e vengono spesso utilizzati in modo interscambiabile. In realtà i vari termini fanno riferimento a concetti differenti, anche se collegati. Il risultato è quello di generare una confusione concettuale che rende ancora più complicato comprendere e affrontare il fenomeno. Di conseguenza, al fine di permettere una migliore comprensione, risulta necessario provare, nonostante la mancanza di una definizione universalmente accettata, a chiarire i vari concetti e fissare le loro caratteristiche generali.

Il concetto di “minaccia ibrida” non fa riferimento a un’azione o a un soggetto in particolare, ma sta a indicare la potenzialità di un attore di combinare e integrare strumenti appartenenti a vari settori e domini, al fine di raggiungere un determinato scopo. Trattare in questo modo il concetto permette anche di sottolineare che ogni attore dell’odierno scenario internazionale, dagli Stati avversari a quelli alleati, fino ai gruppi non statali più organizzati, può rappresentare una minaccia[11].

Nel momento in cui l’attore portatore di una potenzialità decide di tradurre le sue capacità in azioni, si possono aprire due strade: la prima prevede il superamento della soglia della violenza, una “somma” di intensità, visibilità e attribuibilità dell’azione[12], per condurre una vera e propria “guerra ibrida”. Secondo Frank G. Hoffman, si tratta di un modo di combattere un conflitto armato che applica simultaneamente e in modo integrato forze, risorse e tattiche regolari e irregolari

[11] Nel corso del testo si utilizzerà spesso il termine “attori” e mai quelli di “Stati autoritari”, “Stati non democratici” e simili. Ciò è motivato dal fatto che ogni Paese, indipendentemente dal suo regime politico, è potenzialmente soggetto o potenzialmente portatore di una potenzialità ibrida. È quindi possibile sostenere che la concezione per cui solo gli Stati autoritari siano portatori o utilizzatori di potenzialità ibrida sia errata.
[12] Mazarr, Michael J. “Mastering the Gray Zone: Understanding a Changing Era of Conflict”. Washington, DC: Center for Strategic and Budgetary Assessments (CSBA), 2015.

all'interno dello stesso campo di battaglia e a tutti i livelli del conflitto (strategico, operativo e tattico) per raggiungere un determinato obiettivo[13]. Un esempio è costituito dalla fase iniziale della guerra in Ucraina nel 2022 con l'impiego da parte russa di un dispositivo di separatisti delle regioni orientali del Paese, di gruppi di paramilitari, di manipolazione informativa, sabotaggi di infrastrutture e attacchi cyber, che ha agito in modo integrato e coordinato con le forze regolari per ottenere un moltiplicatore di forza.

La seconda strada è quella in cui le potenzialità ibride dell'attore sono impiegate al di sotto della soglia della violenza, operando nella c.d. "zona grigia", ma sempre nel tentativo di raggiungere un determinato obiettivo prestabilito. La zona grigia è quindi il luogo dove l'azione avviene e in cui il bersaglio subisce un'invasione del suo spazio interno attraverso l'impiego in più domini di vari strumenti, spesso collegati tra loro e con effetti a cascata, in grado di lavorare all'interno del "grigio", grazie alla loro capacità di sfumare le soglie di intensità, visibilità e, soprattutto, attribuibilità[14]. Un'ulteriore particolarità riguarda la flessibilità e il potenziale di escalation delle attività condotte nella zona grigia. Queste possono essere impiegate in riferimento a un tentativo d'influenza, come base per la preparazione di una successiva operazione militare, ibrida o convenzionale, oppure possono cessare per ritornare a uno stadio di "semplice" minaccia potenziale[15].

È utile sottolineare che i vari attori portatori di una minaccia ibrida sono in grado di operare su più direttrici con vari strumenti e attività. Le strategie adottate non

[13] Hoffman, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007.

[14] Joint Research Centre & Commissione europea & Hybrid CoE. "The Landscape of Hybrid Threats: a conceptual model public version", 2021 https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

[15] Ibidem

sono lineari, statiche o uniformi, ma dipendono dalle capacità e risorse di chi agisce, dal suo obiettivo e dalle caratteristiche e vulnerabilità specifiche del bersaglio[16]. Un caso molto famoso e studiato, utilizzabile come esempio, è quello della Federazione russa e del suo modo di perseguire i suoi obiettivi restando al di sotto della soglia della violenza. All'interno del pensiero russo è radicato il concetto di "reflexive control", ovvero la pratica di indirizzare il bersaglio a prendere determinate decisioni prestabilite tramite una profonda opera di manipolazione e pressione, condotta attraverso la combinazione e il coordinamento di vari strumenti, in costante adattamento, con intensità costante e sotto la soglia dell'individuabilità, al fine di raggiungere obiettivo predeterminato[17].

Come già sottolineato, obiettivi diversi e bersagli diversi richiedono l'impiego mirato e su misura di mezzi appartengono a uno spettro molto ampio di attività e in grado di provocare un danno al bersaglio. Non risulta possibile individuare a priori il più dannoso o pericoloso strumento o settore della potenziale minaccia. Alcune attività in certi settori creano danni e pressioni immediate, visibili e in alcuni casi ingenti, ma risolvibili in un tempo più o meno breve. Altre ne creano di strutturali, con la potenzialità di trasformare la società bersaglio e di alterare il suo processo decisionale. È sempre possibile una combinazione tra vari strumenti e settori per ottenere entrambi gli effetti, ma in generale la scelta del mezzo dipenderà dall'obiettivo dell'attore e dal contesto in cui agisce[18].

Le superfici di vulnerabilità

In Italia, il dibattito pubblico si è concentrato particolarmente sulle potenziali minacce derivanti da attacchi informatici, dalle campagne di disinformazione e

[16] Ibidem
[17] Ibidem
[18] Ibidem

manipolazione mediatica e dai sabotaggi alle infrastrutture critiche[19]. In modo minore, e spesso solo in contesti istituzionali o accademici, si trattano i temi di investimenti esteri diretti, spionaggio industriale e accademico, migrazioni di massa impiegate come strumento di destabilizzazione e sovranità tecnologica ed energetica.

La differenza di visibilità e di presenza nel dibattito pubblico non è casuale, ma dipende dal fatto che alcuni di questi elementi risultano naturalmente più intuitivi, mediaticamente vendibili, in grado di produrre effetti immediatamente tangibili, come ad esempio un attacco informatico che blocca i sistemi di un aeroporto. Altri sono invece più complessi, difficili da individuare, comprendere e spiegare in quanto parte di un processo graduale di infiltrazione e destabilizzazione che può durare anni e restare dormiente fino al momento più opportuno. In questa categoria possono rientrare casi come gli investimenti esteri diretti, l'infiltrazione accademica e la sicurezza delle infrastrutture.

In Italia, le minacce di natura informatica hanno rappresentato la maggior parte dei casi con danni immediati. Secondo l'ACN, nel primo semestre del 2025 sono stati gestiti in Italia 1549 eventi cyber (+53% sul 2024) e 346 incidenti rilevanti[20]

[19] Le infrastrutture critiche sono sistemi e servizi fisici o digitali il cui funzionamento è vitale per la società e l'economia di un Pease. Sono critiche in quanto un loro malfunzionamento prolungato o la loro distruzione avrebbe un impatto enorme su economia, salute pubblica o sicurezza nazionale. Diddi, T. & Franchina, L. & Longo, A. "Come proteggere le infrastrutture critiche nazionali: best practice, norme e tecnologie" *NextWork*, 23 ottobre 2025 https://www.agendadigitale.eu/sicurezza/come-proteggere-le-infrastrutture-critiche-nazionali-best-practice-norme-e-tecnologie.

[20] Un evento informatico è un qualsiasi evento osservabile che può generare un sospetto. Un incidente informatico è un evento o una serie di eventi che compromette realmente la sicurezza e coinvolge riservatezza, integrità o disponibilità del dato. Agenzia per la Cybersicurezza Nazionale. "2024 year in review", 2025. https://www.acn.gov.it/portale/documents/20119/868186/ACN_2024_year_in_review.pdf/c7a1252f-5186-6cee-ea71-ddf24c6ffe8a?t=1750867894723

(+98% sul 2024)[21]. Il rapporto CLUSIT fornisce informazioni di tendenza sui dati degli incidenti informatici del primo semestre 2025 e rivela che circa il 10% degli attacchi informatici globali è rivolto verso l'Italia, nonostante rappresenti solo l'1% della popolazione e il 2% del PIL mondiale, e che il numero di incidenti segnalati è aumentato di molto[22]. Il rapporto indica la Pubblica Amministrazione, il settore manifatturiero e quello dei trasporti e della logistica come i settori più frequentemente colpiti da attacchi informatici[23]. Sempre secondo il rapporto CLUSIT per il primo semestre 2025, più del 54% degli attacchi informatici registrati in Italia rientra nella categoria dell'"hacktivism", con attacchi frequenti a siti governativi e di Forze Armate e di sicurezza (38% del totale), al settore dei trasporti e stoccaggio (sostanzialmente la logistica, con il 17% del totale) e verso il settore manifatturiero (13% del totale). Gli scopi potrebbero essere quelli di bloccare o rallentare temporaneamente i servizi e gli approvvigionamenti, aumentare la propria visibilità, diffondere messaggi politici, creare sfiducia, "punire" lo Stato per certe scelte e minare la credibilità internazionale del Paese[24]. Alcuni esempi sono gli attacchi condotti e/o rivendicati da collettivi come "KillNet"[25], molto attivo nel 2022, e dal gruppo

[21] Agenzia per la Cybersicurezza Nazionale. "Cyberattacchi in Italia: +53% gli eventi nel primo semestre 2025, raddoppiano gli incidenti con impatto, ma cresce la capacità di rilevamento e risposta", 4 agosto 2025 https://www.acn.gov.it/portale/en/w/cyberattacchi-in-italia-53-gli-eventi-nel-primo-semestre-2025-raddoppiano-gli-incidenti-con-impatto-ma-cresce-la-capacita-di-rilevamento-e-risposta.

[22] Associazione Italiana per la Sicurezza Informatica (CLUSIT). "Rapporto Clusit 2025 – Edizione di metà anno", ottobre 2025. https://clusit.it/rapporto-clusit. La motivazione dell'aumento potrebbe anche trovarsi nell'introduzione delle nuove norme, come la legge 90/2024 o la direttiva NIS2, che impongono la denuncia alla Pubblica Amministrazione e agli operatori di servizi essenziali e di infrastrutture critiche o per via della difficoltà delle nostre piccole e medie imprese di adeguare i loro sistemi ai più recenti standard di sicurezza informatica.

[23] ibidem

[24] ibidem

[25] Canè, Stephanie. "Portali italiani sotto attacco: il caso Killnet" *NTT DATA*,1 giugno 2022. https://it.nttdata.com/insights/blog/cyber-attacchi-hacker-italia

"NoName057"[26], presumibilmente[27] legati al Governo russo, contro istituzioni governative, enti pubblici, infrastrutture grandi aziende, ecc. in coincidenza con dichiarazioni, votazioni parlamentari e misure di supporto prese dal Governo italiano a favore dell'Ucraina. Attacchi informatici sono frequenti anche in occasione di eventi internazionali con grande visibilità come i recenti G7 di Borgo Egnazia o all'apertura delle Olimpiadi di Milano-Cortina. A questo genere di azioni spesso non segue un danno significativo ma esse puntano a uno scopo dimostrativo e propagandistico e mirano a ottenere visibilità, dimostrare capacità d'azione, creare un senso di vulnerabilità e mandare messaggi politici. Oltre alle azioni "dimostrative", questi gruppi sono in grado di condurre operazioni molto più complesse e dannose, note come "Advanced Persistent Threat", contro settori critici. Particolare è il caso del gruppo noto come "Conti Ransomware Group" che ha colpito aziende di media taglia del settore aerospaziale in Piemonte e Lombardia per sottrarre tecnologie militari classificate, interrompere le operazioni e chiedere riscatti[28]. L'evidente frequenza del fenomeno degli attacchi informatici ha generato un grande dibattito e varie proposte. Oltre alla promozione dell'azione "civile" dell'Agenzia Nazionale per la Cybersicurezza, è in corso lo sviluppo di un corpo cyber presso le Forze Armate e l'aggiornamento dell'appartato normativo. L'obiettivo è quello di consentire alle Forze Armate italiane di agire efficacemente nello spazio cyber, anche in tempo di pace e al di fuori di teatri di

[26] EuroPol. "Global operation targets NoName057(16) pro-Russian cybercrime network", 16 luglio 2025 https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

[27] È importante sottolineare che, nonostante i forti sospetti legati al lavoro di alcuni di questi gruppi, non è possibile dimostrare in modo comprovato e definitivo la loro appartenenza o dipendenza agli apparti di un Governo straniero, rendendo il loro impiego particolarmente vantaggioso ed efficace.

[28] IncidentBuddy. "Italy Defense Sector: Critical Cyber Threat Landscape", 22 gennaio 2026 https://incidentbuddy.ai/threat-profiles/it/defense

guerra. È importante sottolineare che è prevista anche la possibilità di avvalersi del supporto di soggetti esterni specializzati nel settore per incrementare le capacità di difesa e di azione[29].

La concretizzazione delle potenzialità della minaccia ibrida di uno Stato estero diventa particolarmente preoccupante quando le sue risorse e capacità nei vari domini e settori sono impiegate al fine di condurre operazioni su larga scala, in grado di creare danni strutturali al Paese bersaglio, sfruttando le sue caratteristiche e particolarità. Le pratiche, utilizzate anche modo coordinato, vanno dalla manipolazione delle opinioni della popolazione alla delegittimazione delle sue strutture di governo e alla coercizione economica, fino ai furti di tecnologie e infiltrazioni nell'accademia. Questo tipo di strategia generalmente richiede una programmazione e una messa in pratica di lungo periodo e sfrutta al massimo la possibilità di sfruttare la bassa visibilità e la negabilità plausibile per provocare danni potenzialmente critici[30].

Negli ultimi anni, l'Italia è stata coinvolta in quelle che il Servizio Europeo per l'Azione Esterna chiama "foreign Information Manipolation and Interference" (FIMI) e che descrive come un'attività manipolativa, condotta in modo intenzionale e coordinato, che mira a influenzare negativamente i valori, procedure e processi politici, sfruttando divisioni e polarizzazione già esistenti e minando l'abilità del bersaglio di perseguire i suoi obiettivi e interessi[31].

---

[29] Calabrese, A. "Verso un'arma cyber nazionale: la strategia del Min. Crosetto nel contesto europeo" *Geopolitica.info*, 14 novembre 2025 https://www.geopolitica.info/strategia-cyber-crosetto/.

[30] Joint Research Centre & Commissione europea & Hybrid CoE. "The Landscape of Hybrid Threats: a conceptual model public version", 2021https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

[31] European Union External Action. "Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)", 27 gennaio 2026.

Tipicamente, questa pratica sfrutta reti coordinate di account sui vari social network e piattaforme per aumentare la visibilità di specifici contenuti, promuovere certe narrative e simulare movimenti spontanei di attivisti locali. Altra pratica molto diffusa è quella della creazione di siti web "giornalistici" e di cloni di testate affermate per riportare notizie false o riproporre in lingua locale i contenuti provenienti da fonti controllate da uno Stato[32]. EuVsDisinfo ha documentato alcune delle operazioni FIMI in cui l'Italia è rimasta coinvolta insieme ad altri importanti Paesi europei, come l'operazione Doppelgänger, l'Overload e l'Undercut. La prima di esse è stata rilevata per la prima volta nel 2022[33] e prevede la clonazione di diverse testate giornalistiche europee e di agenzie di stampa, tra cui l'ANSA, La Stampa e Repubblica, per la pubblicazione di articoli, sondaggi e video falsi in prossimità di elezioni nazionali o europee, momento in cui la popolazione è più sensibile e recettiva[34]. L'operazione Overload ha riguardato un tentativo del 2023 di sovraccaricare i fact-checkers indipendenti, tramite l'invio di migliaia di mail e segnalazioni coordinate al fine di intralciare l'elaborazione di richieste di verifica reali e quindi favorire la diffusione di certe narrative[35]. L'operazione Undercut riguarda invece la creazione e la distribuzione di contenuti IA e deepfake in varie lingue per minare la fiducia nei media tradizionali, provocare divisioni interne e creare

———

https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

[32] European Union External Action. "3rd EEAS Report on Foreign Information Manipulation and Interference Threats", 19 marzo 2025 https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

[33] EU Disinfo Lab. "Doppelganger – Media clones serving Russian propaganda", 27 settembre 2022 https://www.disinfo.eu/doppelganger.

[34] EUvsDisinfo. "Doppelganger colpisce ancora: Rivelazione delle attività FIMI per le elezioni del Parlamento europeo", 19 giugno 2024 https://euvsdisinfo.eu/it/doppelganger-colpisce-ancora-rivelazione-delle-attivita-fimi-per-le-elezioni-del-parlamento-europeo

[35] EUvsDisinfo. "Glossario: chi è chi nel mondo FIMI", 22 aprile 2025 https://euvsdisinfo.eu/it/glossario-chi-e-chi-nel-mondo-fimi

sfiducia verso le istituzioni[36]. Tutte queste operazioni hanno in comune l'obiettivo di promuovere narrazioni pro-Russia in Italia, vista come particolarmente permeabile per via dei suoi legami storici con la Russia e quindi come porta d'accesso per il più generale ecosistema europeo, ridurre la fiducia verso l'Unione Europea e ridurre il supporto verso NATO e Kiev[37] [38].

Altri possibili danni strutturali possono derivare da azioni ostili che coinvolgono i settori di economia, infrastrutture strategiche e accademia, con possibili conseguenze in termini di riduzione della competitività delle aziende del Paese, di creazione di dipendenze in settori strategici e di manipolazione del settore economico e finanziario[39]. Il rischio di questo genere di azioni è stato riconosciuto nella Relazione Annuale sulla Politica dell'Informazione per la Sicurezza 2025 con la necessità di "tutelare il know-how tecnico e scientifico nazionale, potenzialmente minacciato sia da attori economici esteri spinti da finalità non commerciali, sia da azioni di spionaggio ed esfiltrazione. Tale minaccia si articola su più piani: l'ambito accademico e universitario, i centri

[36] Eu Disinfo Lab. "Building a common operational picture of fimi. Using IMS to strengthen attribution and disruption", 15 gennaio 2026 https://euvsdisinfo.eu/uploads/2026/01/20260115_building-a-common-operational-picture-of-FIMI_01.pdf

[37] Di Vincenti, Joseph. "The Russian Hybrid Threat in Italy: Political Influence, Propaganda and Disinformation" *Vilnus University Press,* vol.1 2025 https://www.journals.vu.lt/open-series/en/article/view/43827

[38] Interessante sottolineare che tutte queste azioni avvengono in rete e che quindi hanno anche un effetto sui sistemi di IA generativa, come Gemini e ChatGPT, e sui risultati che questi forniscono ai loro utenti. Tokariuk, Olga. "Pravda network. I siti della propaganda russa sono fatti apposta per finire nei motori dell'IA" *Linkiesta,* 12 aprile 2025 https://www.linkiesta.it/2025/04/siti-propaganda-russa-pravda/.

[39] Joint Research Centre & Commissione europea & Hybrid CoE. "The Landscape of Hybrid Threats: a conceptual model public version", 2021https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

industriali di ricerca e sviluppo, gli attori della catena del valore nazionale"[40]. Particolarmente sensibile è il tema degli investimenti esteri diretti[41]. Come ogni settore della potenziale minaccia, questa tipologia di azione non è di per sé dannosa, anzi si tratta di un dominio che rappresenta in alcuni casi un moltiplicatore di forza e innovazione. Tuttavia, esso potrebbe essere impiegato da parte di uno Stato estero al fine di assumere il controllo di aziende e asset critici di un Paese bersaglio, assorbire le tecnologie più sensibili e creare dipendenze economiche. Sostanzialmente, il rischio è quello di subire l'infiltrazione di una potenza estera nel proprio tessuto economico e industriale, nelle linee di approvvigionamento e nei settori critici come infrastrutture, gestione dei dati finanza, telecomunicazione, logistica, dotandosi così della capacità di esercitare una forte influenza e pressione politica o, addirittura, di sottrarre dati, informazione e tecnologie per arricchire la propria economia, impoverendo inevitabilmente quella del bersaglio[42]. In Italia, si verificano continuamente tentativi di investimenti esteri diretti in settori strategici. I più sospetti o critici vengono bloccati o limitati tramite l'impiego del c.d. "Golden Power". Casi famosi sono quelli legato alla Pirelli, alla LPE e alla questione Safran-Microtecnica[43]. In tutti questi casi c'è stato il tentativo di assumere il

[40] Sistema di Informazione per la Sicurezza della Repubblica. "Relazione annuale dell'intelligence al Parlamento sulla politica dell'informazione per la sicurezza relativa all'anno 2024", 4 marzo 2025. https://www.sicurezzanazionale.gov.it/cosa-facciamo/relazione-annuale

[41] Si tratta di sostanzialmente di acquisti di società esistenti o di sue quote, di fusioni o di apertura di filiere di aziende straniere sul territorio nazionale.

[42] National Crisis Center (Belgio). "Foreign direct investments", 2026 https://crisiscenter.be/en/risks-belgium/security-risks/foreign-direct-investments#impact-and-probability.

[43] Il caso Pirelli ha riguardato la presenza, con quota di maggioranza relativa al 37%, della cinese Sinochem. Nel 2023 il Governo è intervenuto a tutela delle tecnologie, in particolare di sensori in grado di rilevare posizione e stato delle infrastrutture, e della gestione societaria, limitando le possibilità di Sinochem di stabilire governance e nomine e ponendo limiti sull'accesso alle informazioni più critiche. L'ingerenza è stata gravosa e ha di fatto escluso il socio cinese. Picotti, Luca. "Pirelli: dal takeover cinese del 2015 al golden power del 2023" *Osservatorio Golden Power,* 2023

controllo di una società proprietaria di tecnologie avanzate e *dual use*[44]. La relazione annuale del Dipartimento delle Informazioni per la Sicurezza 2026, relativo all'anno 2025, riporta che "l'esercizio della sovranità di un Paese si manifesta sempre più nella sua autonomia strategica, ovverosia la capacità di gestire dati, infrastrutture critiche, algoritmi e filiere tecnologiche. Dipendenze non governate possono trasformarsi in punti di pressione strutturali, riducendo la libertà d'azione di un Paese"[45].

Altrettanto importante e sensibile è il fronte della ricerca. Varie agenzie e organizzazioni, dal Dipartimento delle Informazioni per la Sicurezza[46]

---

https://www.osservatoriogoldenpower.eu/pirelli-dal-takeover-cinese-del-2015-al-golden-power-del-2023.
Il caso LPE, azienda produttrice di componenti per semiconduttori, ha riguardato il veto del Governo alla cessione al 70% ai cinesi della Shenzen investment holding. De Bortoli, Ferruccio. "Golden power, la Lpe e la difesa del made in Italy (non solo dai cinesi)" *Corriere della Sera,* 20 aprile 2021
https://www.corriere.it/economia/aziende/21_aprile_20/golden-power-caso-lpe-serve-piano-europeo-difendere-made-italy-anche-cinesi-38d47eea-a1a5-11eb-b3ed-ee5b64f415b7.shtml.
Il caso Safran-Microtecnica ha riguardato l'opposizione, poi superata, del Governo all'acquisizione da parte della francese Safran dell'italiana Microtecnica, parte del gruppo americano RTX. Il veto ha riguardato la necessità di tutelare la filiera italiana e il coinvolgimento dell'azienda nei programmi Eurofighter e Tornado. Il sollevamento è avvenuto solo a seguito di garanzie di su occupazione, mantenimento dei siti e investimenti in Italia. Arnese, M. & Rossi, C. "Perché Meloni ha ritirato il veto su Microtecnica alla francese Safran" *START magazine,* 14 giugno 2024
https://www.startmag.it/economia/governo-italiano-microtecnica-safran-francia

[44] Silvestri, Violetta. "Cos'è il Golden power e come funziona? Quando è stato usato in Italia" *Money.it,* 2 dicembre 2024
https://www.money.it/cos-e-il-golden-power-e-come-funziona-quando-e-stato-usato-in-italia#I-casi-di-Golden-power-piu-famosi-in-Italia

[45] Sistema di Informazione per la Sicurezza della Repubblica. "Relazione annuale dell'intelligence al Parlamento sulla politica dell'informazione per la sicurezza relativa all'anno 2025", 4 marzo 2026. https://www.sicurezzanazionale.gov.it/cosa-facciamo/relazione-annuale

[46] Sistema di Informazione per la Sicurezza della Repubblica. "Relazione annuale dell'intelligence al Parlamento sulla politica dell'informazione per la sicurezza relativa all'anno 2025", 4 marzo 2026.

all'Agenzia per la Cybersicurezza[47], fino alla Commissione europea[48], evidenziano che l'accademia produce innovazione e tecnologie critiche, e spesso *dual use*, in settori chiave per la competitività e competizione del futuro come l'IA, i semiconduttori, l'aerospazio. Risulta quindi necessario tutelare la ricerca da furti di brevetti, collaborazioni opache con università estere e scambi di ricercatori[49].

Le risposte dello Stato

Per poter esaminare il ventaglio di misure adottate e adottabili dall'Italia, è necessario considerare che la risposta all'azione ibrida è, in primo luogo, competenza e responsabilità primaria del singolo Stato bersaglio, tramite l'impiego del suo diritto nazionale[50]. Tuttavia, trovare soluzioni appropriate alle potenzialità e alle manifestazioni della possibilità della minaccia ibrida risulta essere particolarmente complicato, specie per uno Stato democratico che deve bilanciare le misure adottate con i diritti e le libertà della cittadinanza. Date le caratteristiche di multi-settorialità, opacità, non attribuibilità e velocità di adattamento e innovazione, non si è in grado di conoscere con certezza l'attore che agisce, il suo obiettivo finale, la portata della sua conoscenza del bersaglio e il suo livello di infiltrazione e preparazione. Le difficoltà aumentano data l'impossibilità di controllare in maniera costante e approfondita ogni singolo settore della vita associata e le loro interazioni. Di conseguenza, diviene

---

[47] Agenzia per la Cybersicurezza Nazionale. "Linee guida per il rafforzamento della resilienza e referente per la cybersicurezza", novembre 2024 https://www.acn.gov.it/portale/en/linee-guida-rafforzamento-resilienza

[48] https://european-research-area.ec.europa.eu/documents/tackling-ri-foreign-interference-staff-working-document-2022

[49] Ministero Università e Ricerca. "Modello Nazionale e Linee Guida", agosto 2025 https://www.sicurezzaricerca.mur.gov.it/modello-nazionale-e-linee-guida/modello-nazionale

[50] Sanz-Caballero, Susana. "The concepts and laws applicable to hybrid threats, with a special focus on Europe" *Nature*, 29 giugno 2023 https://www.nature.com/articles/s41599-023-01864-y?utm

necessario lavorare sulla base di sospetti più o meno solidi, dell'esperienza maturata in ambito domestico e internazionale e tramite l'individuazione preventiva delle vulnerabilità specifiche. In sostanza, è necessario identificare le aree di interesse e le funzioni critiche, fortemente legate a sicurezza nazionale e capacità decisionale e d'azione, e renderle il più resistenti e resilienti possibile[51]. Inoltre, è importante sottolineare che, nel caso dell'Italia e di molti altri Paesi Occidentali, il livello di apertura e di interconnessione del tessuto economico e sociale è tale che le manifestazioni della potenzialità ibrida sul proprio territorio o su quello di un altro Stato potrebbero essere in grado di provocare pericolosi effetti a cascata transnazionali, aggiungendo un nuovo livello di pericolosità. Questa caratteristica ha spinto l'Italia a collaborare con altri Paesi, a livello bilaterale ed europeo, per condividere informazioni e sviluppare strategie e misure comuni. Alcuni esempi sono la partecipazione all'"Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats", pensato per incrementare la consapevolezza e resilienza degli Stati membri dell'Unione Europea rispetto alle campagne di influenza e manipolazione mediatica[52], e a centri di eccellenza per la promozione di analisi, modelli e cooperazione tra Paesi, come l'Hybrid CoE[53].

---

[51] Joint Research Centre & Commissione europea & Hybrid CoE. "The Landscape of Hybrid Threats: a conceptual model public version", 2021https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

[52] Consiglio dell'Unione Europea. "Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats", 4 aprile 2024 https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/horizontal-working-party-on-enhancing-resilience-and-countering-hybrid-threats/

[53] Hybrid Coe. "Hybrid CoE" https://www.hybridcoe.fi/

Al fine di tutelarsi dalla potenzialità[54] ibrida, l'Italia sta portando avanti un tentativo di mobilitazione coordinata e multilivello delle varie parti della società, dalle autorità all'industria fino alla società civile, per rendere il Paese il più preparato e resiliente possibile. L'impegno riguarda molteplici settori economici e sociali e si compone spesso di un intervento "dall'alto" dello Stato a tutela dei settori strategici e di uno sforzo di sensibilizzazione e responsabilizzazione delle aziende private e/o partecipate e della popolazione, specie nel campo informatico e dell'informazione. L'obiettivo finale è quello di massimizzare la protezione e la consapevolezza anche nei punti in cui lo Stato non vuole o non è in grado di arrivare e, viceversa, nelle aree non accessibili per i privati. Elemento cardine per la sicurezza dello Stato è rappresentato dal lavoro del Sistema di Informazione per la sicurezza della Repubblica. Dal rapporto annuale elaborato dal Dipartimento delle Informazioni per la Sicurezza relativo all'anno 2025, l'organo di coordinamento del Sistema, emerge un ruolo importantissimo legato all'individuazione, l'analisi, valutazione del rischio e supporto decisionale in relazione alle varie componenti della potenzialità ibrida[55]. All'interno della prefazione del rapporto è riportato esplicitamente che "il documento non descrive le singole tecnologie o i singoli eventi, ma offre un quadro di riferimento unitario per comprendere l'evoluzione delle minacce, individuare le vulnerabilità dei sistemi e rafforzare la capacità di prevenzione e di governo dei rischi, nella consapevolezza che la sicurezza oggi non può essere affidata alla sola reazione, ma richiede visione strategica, responsabilità e capacità di

[54] È importante sottolineare che la difesa e la resilienza devo essere pensate in modo proattivo e non reattivo. Di conseguenza, è necessario prepararsi sin dal momento in cui si tratta solo di potenzialità.

[55] Sistema di Informazione per la Sicurezza della Repubblica. "Relazione annuale dell'intelligence al Parlamento sulla politica dell'informazione per la sicurezza relativa all'anno 2025", 4 marzo 2026. https://www.sicurezzanazionale.gov.it/cosa-facciamo/relazione-annuale

anticipazione”[56]. Il funzionamento del Dipartimento è stato recentemente riformato[57], con l’abrogazione del Dpcm del 2022 che scorporava la cybersicurezza e istituiva un’agenzia dedicata[58] (l’Agenzia per la Cybersicurezza nazionale). La riforma punta a chiarificare l’assetto istituzionale e a consolidare il ruolo del DIS come centro di sintesi e analisi delle informazioni. Il nuovo assetto dovrebbe permettere ai servizi di informazione di essere in grado di adattarsi più rapidamente all’evoluzione delle nuove e vecchie minacce[59]. Elemento vitale per il funzionamento dello Stato è l’integrità del sistema infrastrutturale del Paese. L’Italia si impegna attivamente per la protezione fisica e digitale delle infrastrutture critiche grazie all’adozione delle normative europee, che impongono standard minimi di protezione per gli operatori dei servizi essenziali[60], all’azione delle Forze Armate e di polizia e dell’Agenzia per la Cybersicurezza Nazionale. Un esempio concreto dell’azione diretta dello Stato può essere l’accordo del 2022 tra Marina Militare e Sparkle, società del gruppo TIM che si occupa di telecomunicazioni sottomarine, per la protezione delle

[56] ibidem
[57] Gazzetta Ufficiale della Repubblica Italiana. “Comunicato relativo all'adozione del decreto del Presidente del Consiglio dei ministri 8 gennaio 2026, n. 1.” https://www.gazzettaufficiale.it/eli/id/2026/01/15/26A00150/SG
[58] Bentivoglio, Mario. “Sicurezza nazionale. Via libera del governo alla riorganizzazione del Dis” *Formiche,* 16 gennaio 2026 https://formiche.net/2026/01/sicurezza-nazionale-via-libera-del-governo-alla-riorganizzazione-del-dis/#content
[59] Carlin, Mattia. “Intelligence e sicurezza nazionale, l’Italia rafforza il DIS e il Sistema di informazione per la sicurezza”, *The Italian Globe,* 17 gennaio 2026 https://www.italianglobe.it/2026/01/17/intelligence-e-sicurezza-nazionale-litalia-rafforza-il-dis-e-il-sistema-di-informazione-per-la-sicurezza
[60] In particolare, si tratta della direttiva CER per il tema della resilienza fisica delle infrastrutture critiche e della direttiva NIS2 per quanto riguarda gli obblighi di sicurezza informatica. Diddi, T. & Franchina, L. & Longo, A. “Come proteggere le infrastrutture critiche nazionali: best practice, norme e tecnologie” *NextWork*, 23 ottobre 2025 https://www.agendadigitale.eu/sicurezza/come-proteggere-le-infrastrutture-critiche-nazionali-best-practice-norme-e-tecnologie.

infrastrutture subacquee vitali per lo sviluppo socioeconomico del Paese[61]. La collaborazione è stata approfondita nel 2025, con la definizione delle procedure di scambio informativo tra la Centrale Operativa della Marina Militare presso il Comando in Capo della Squadra Navale e il Global Operation Center di Sparkle a Catania. Lo scambio riguarderà i movimenti anomali di navi in prossimità delle infrastrutture sottomarine[62].

La protezione delle componenti digitali delle infrastrutture critiche nazionali, la prevenzione delle minacce e il coordinamento di vari enti sono poi a carico dell'Agenzia per la Cybersicurezza Nazionale. L'Agenzia si occupa in prima persona di guidare e monitorare l'implementazione della strategia di cybersicurezza nazionale, di assicurare il recepimento, l'applicazione e la vigilanza della direttiva europea NIS2, di monitorare e gestire gli attacchi informatici tramite la sua unità operativa, il Computer Security Incident Response Team, e di coordinare le varie autorità coinvolte nella protezione informatica del Paese con forum interministeriali come il Comitato Interministeriale per la Cybersicurezza e il Nucleo per la cybersicurezza, tra le altre. Ultimo compito è quello della promozione di standard e di linee guida per la sicurezza, della certificazione de beni e servizi digitali utilizzati da pubblico e privato e della formazione di professionisti del settore[63].
Per proteggere il tessuto economico e sociale del Paese da investimenti esteri

[61] Gruppo TIM. "Firmato il protocollo d'intesa tra Marina Militare e Sparkle per la protezione dei cavi di telecomunicazione sottomarini", 12 luglio 2022 https://www.gruppotim.it/it/archivio-stampa/sparkle/2022/CS-Firmato-il-protocollo-d-intesa-tra-Marina-Militare-e-Sparkle-per-la-protezione-dei-cavi-di-telecomunicazione-sottomarini.html
[62] Marina Militare. "Scambio informativo tra la Marina Militare e la società Sparkle", a ottobre 2025 https://www.marina.difesa.it/media-cultura/Notiziario-online/Pagine/20251001_ATA-e-SOP-per-lo-scambio-informativo.aspx.
[63] Agenzia per la Cybersicurezza Nazionale. "2024 year in review", 2025 https://www.acn.gov.it/portale/documents/20119/868186/ACN_2024_year_in_review.pdf/c7a1252f-5186-6cee-ea71-ddf24c6ffe8a?t=1750867894723

diretti potenzialmente dannosi, è stato inoltre introdotto nel 2012 lo strumento del c.d. Golden Power al fine di dare al Governo la possibilità di controllare gli investimenti esteri in settori strategici. La normativa, riformata e "allargata" più volte nel corso del tempo[64], si applica sia per operazioni di acquisto di quote rilevanti di aziende nazionali considerate strategiche che per operazioni interne alla società, spesso successive all'acquisto, consentendo anche di monitorare la vita dell'impresa in modo continuato e a posteriori. Con questo strumento il Governo può opporsi alle operazioni o imporre obblighi e/o condizioni specifiche a tutte le società appartenenti a determinate categorie o settori[65].
Al fine di tutelare la ricerca da possibili ingerenze straniere, nell'ambito della competizione globale e delle tensioni internazionali e in sintonia con le istituzioni europee[66], il Ministero dell'Università e della ricerca ha fornito a università ed enti di ricerca *best practices* e linee guida per auto-valutare in modo volontario la sicurezza della ricerca. L'Italia tiene conto della libertà accademica, composta da autonomia e responsabilità accademica, ma ritiene indispensabile che le istituzioni si attivino per proteggere la loro ricerca ed evitare furti o utilizzi per fini impropri o indesiderabili, con relative possibili conseguenze negati su ampia scala, in termini di fiducia nella ricerca, danno reputazionale e perdita di dati e prodotti di elevato valore e interesse scientifico[67].

---

[64] Dipartimento per gli Affari Europei. "Golden Power". https://www.affarieuropei.gov.it/it/comunicazione/europarole/golden-power. Con "allargata" si intende che sono aumentati i suoi ambiti di applicazione.
[65] Picotti, Luca. "Il Golden Power non è solo uno strumento di foreign direct investment screening" *Osservatorio Golden Power,* https://www.osservatoriogoldenpower.eu/il-golden-power-non-e-solo-uno-strumento-di-foreign-direct-investment-screening
[66] Consiglio dell'Unione Europea. "Sicurezza economica europea", 11 dicembre 2025 https://www.consilium.europa.eu/it/policies/european-economic-security/
[67] Ministero Università e Ricerca. "Modello Nazionale e Linee Guida", agosto 2025 https://www.sicurezzaricerca.mur.gov.it/modello-nazionale-e-linee-guida/modello-nazionale/

Per quanto riguarda le possibili misure per il contrasto alla disinformazione e alle operazioni di FIMI, è possibile notare che in Italia, così come per molti Paesi europei[68], non esiste una normativa o strategia specifica. Ciò è dovuto in parte alle difficoltà di legiferare su una tematica così complessa e al timore di possibili ricadute negative impreviste. In Italia, il fenomeno è sostanzialmente regolato dalle leggi generali sui crimini d'odio, sulla diffamazione e dalle normative europee sulla responsabilità delle piattaforme online e sui suoi codici di condotta[69]. Una proposta significativa per rafforzare le capacità italiane di contrastare la disinformazione e la manipolazione mediatica è quella del Senatore Enrico Borghi, membro del Copasir, per l'istituzione di un'agenzia specifica per la disinformazione e la sicurezza cognitiva con la funzione di analisi del flusso informativo su media tradizionali e social media per registrare eventuali ingerenze e manipolazioni[70].

Oltre alla creazione e sviluppo di strumenti normativi e di agenzie, risulta necessario investire anche nell'educazione tradizionale e digitale della popolazione, preferibilmente a partire dall'infanzia, al fine di adottare un pensiero critico e sviluppare la capacità di distinguere le informazioni vere da quelle false e di tutelarsi al meglio in rete. In questo senso, è attivo in Italia un

[68] Secondo il report SAUFEX del 12 novembre 2024, solo due Stati membri dell'UE, l'Olanda e la Lettonia, dispongono di una strategia dedicata esclusivamente al contrasto della disinformazione e della FIMI. Molti altri Stati europei riconoscono la disinformazione e la FIMI come una minaccia al funzionamento delle società democratiche e discutono del fenomeno in molteplici documenti, ma lo trattano solo come un elemento di una più generale minaccia ibrida o del mondo della cybersicurezza. Il risultato è la frequente mancanza di chiarezza concettuale e quindi di difficoltà d'azione. Robert Kupiecki et al., "D1.2 – Current State of Detection and Response to FIMI (1st Draft)" *SAUFEX Project*, 12 novembre 2024. https://docs.saufex.eu/STATE-OF-FIMI-draft.pdf.

[69] Eu Disinfo Lab. "The disinformation landscape in Italy", 15 dicembre 2025 https://www.disinfo.eu/publications/disinformation-landscape-in-italy

70 D'Amato, Alessandro. "Adisc: l'agenzia proposta da Italia Viva per dare la caccia ai putiniani in tv e sui social media" Open, 30 marzo 2024 https://www.open.online/2024/03/30/adisc-agenzia-disinformazione-italia-viva-putiniani

progetto pilota della TheGuardian Foundation, il NewsWise, per portare avanti programmi nelle scuole primarie, indirizzati ai bambini e ai loro docenti, pensati per combattere la disinformazione e sviluppare la capacità di valutare in modo critici il mondo dei media e dell'informazione[71]. Altra iniziativa significativa è quella dell'iniziativa governativa di "Repubblica Digitale". L'iniziativa, attiva dal 2019, agisce come ente di coordinamento e collaborazione di vari attori, dall'università ai privati, fino alla Pubblica Amministrazione, e punta a promuovere lo sviluppo delle competenze digitali nell'ottica di rendere la cittadinanza più capace di utilizzare gli odierni strumenti digitali e più consapevoli dei possibili rischi[72].

Programmi di educazione sono necessari anche nel mondo del lavoro per quanto riguarda la sicurezza informatica e fisica di aziende e infrastrutture. Oltre alla promozione della ridondanza dei sistemi e di piani di emergenza, occorre affrontare le vulnerabilità derivanti dall'azione dell'operatore umano. I dipendenti, di qualsiasi livello e posizione, devono essere necessariamente informati e sensibilizzati sulle tematiche relative alla sicurezza, per evitare che un errore umano, dovuto alla sottovalutazione delle minacce o alla mancata applicazione delle procedure, vanifichi le difese digitali o fisiche previste[73]. In particolare, sono attive iniziative finanziate da Stato e Unione Europea per la formazione dei dipendenti della Pubblica Amministrazione[74] e programmi di

71 Bompani, Antonio. "La guerra ibrida in casa. La minaccia della disinformazione è entrata nel dibattito pubblico, finalmente" Linkiesta, 24 novembre 2025 https://www.linkiesta.it/2025/11/disinformazione-guerra-ibrida-risposta-politica-fake-news-democrazia

72 Repubblica Digitale, "Missione e adesione", https://repubblicadigitale.gov.it/portale/it/missione-e-adesione

73 Sellari, Paolo, a cura di. "Saggi di geopolitica e sicurezza delle infrastrutture". Roma: Edizioni Nuova Cultura, 2024.

74 Cyber 4.0. "MIMIT and Cyber 4.0: The Cybersecurity Awareness Program for PAs, a piece of the National Cybersecurity Strategy ", 15 aprile 2024 https://www.cyber40.it/en/mimit-and-

scuole specializzate per aziende e lavoratori. Lo scopo è quello di promuovere la consapevolezza rispetto alle possibili minacce digitali e di diffondere pratiche utili a prevenire e affrontare incidenti informatici[75].

Conclusioni

Nel tentativo di sistematizzare il fenomeno della minaccia ibrida in Italia, è stato possibile osservare che il nostro Paese è esposto, potenzialmente e/o effettivamente, a un ampio spettro di minacce che agiscono sfruttando le sue particolarità e le caratteristiche dell'assetto istituzionale democratico. Data la capacità degli attori portatori di minaccia di colpire più settori in modo simultaneo e coordinato, risulta necessario adottare una protezione a tutto tondo (c.d. *whole of society*), in grado di tutelare contemporaneamente il maggior numero possibile di settori potenzialmente vulnerabili. In questo senso, l'Italia si sta impegnando nella costruzione di un sistema di risposta efficace tramite l'adesione a framework di cooperazione e organismi internazionali, l'adozione di norme stringenti e precise nei settori di economia e infrastrutture, l'istituzione di agenzie ad hoc e progetti mirati a incrementare la consapevolezza della cittadinanza. In particolare, è da riconoscere lo sviluppo degli strumenti dedicati al contrasto del fenomeno degli attacchi informatici, l'impegno a livello internazionale finalizzato al rafforzamento dell'azione comune e l'allargamento dei settori sottoposti a golden power, al fine di tutelare i settori, le aziende e le conoscenze più critiche.

Tuttavia, sono presenti ancora alcune carenze che devono essere affrontate. In primo luogo, sarà necessario adottare ulteriori misure per rendere la

cyber-4-0-the-cybersecurity-awareness-program-for-pas-a-piece-of-the-national-cybersecurity-strategy

[75] European Energy Information Sharing and Analysis Centre. "CYBER SECURITY INCIDENT RESPONSE" 2020 https://www.ee-isac.eu/media/2023/05/EE-ISAC-Incident-Response-White-Paper.pdf

cittadinanza, cuore del sistema Paese e suo punto debole, maggiormente consapevole rispetto alle manipolazioni mediatiche, agli attacchi informatici e alle precauzioni da adottare in materia di investimenti esteri diretti. Una maggiore consapevolezza e responsabilizzazione della cittadinanza è necessaria al fine di incrementare la resilienza dei singoli settori coinvolti e del Paese nel suo complesso.

Ulteriori sforzi saranno necessari per superare la settorialità della risposta e raggiungere un vero approccio sistemico integrato. La necessità di dotarsi di strutture integrate e flessibili deriva dal fatto che l'efficacia delle varie misure dipenderà dalla capacità di coordinare e integrare gli strumenti di risposta, di incentivare la collaborazione tra pubblico e privato e di adattarsi rapidamente all'evoluzione delle minacce. In tal senso, è rilevante la proposta del Ministro della Difesa Guido Crosetto per l'istituzione di una struttura ad hoc, il "Centro Nazionale di Coordinamento per la Minaccia Ibrida", con l'obiettivo di garantire il coordinamento tra agenzie, istituzioni, settore privato e Forze Armate e di promuovere la condivisione di informazioni e *best practices*.

In definitiva, è ragionevole attendersi un progressivo perfezionamento e integrazione della strategia italiana e un incremento della resilienza della società nel suo complesso. Ciò sarà possibile grazie all'approfondimento della conoscenza sulla materia e delle sue manifestazioni, alla diffusione della consapevolezza nella popolazione, alla raccolta di dati e di esperienze sia nazionali che estere, all'adozione di nuovi strumenti e al perfezionamento di quelli esistenti.

L'Alleanza Atlantica alla prova delle minacce ibride: evoluzione e stato dell'arte dell'approccio NATO al contrasto alla guerra ibrida

di Fabio Maina

Introduzione

Durante l'anno appena trascorso, il termine "guerra ibrida" ha assunto un ruolo di primo piano sia nel dibattito pubblico che tra la comunità di analisti ed esperti del settore. Gli sconfinamenti da parte di droni russi in diversi paesi europei, tra cui la Polonia[1], i sabotaggi dei cavi in fibra ottica nel Mar Baltico[2] e l'aumento dei cyberattacchi contro i membri della NATO[3] sono alcuni degli esempi più lampanti delle minacce ibride che l'Alleanza si trova oggi ad affrontare.

Va però riconosciuto che la guerra ibrida condotta (soprattutto) dalla Russia non è una novità: i membri NATO fanno i conti con questa minaccia almeno dal 2014, anno dell'annessione della Crimea alla Federazione Russa. Ciononostante, il 2022, anno dell'invasione russa dell'Ucraina, ha segnato uno spartiacque anche nelle modalità di conduzione delle azioni ibride da parte di Mosca, sempre più frequenti e talvolta anche violente.

Questo capitolo ricostruisce l'evoluzione delle minacce ibride nei confronti dell'Alleanza Atlantica, individuandone i principali attori responsabili, per poi

---

[1] Avesani, L. "Droni russi sconfinano il territorio polacco: sfida alla NATO?" *Geopolitica.info*, 10 settembre 2025. https://www.geopolitica.info/droni-russi-polonia/

[2] Leicester, J., e E. Burrows. "At least 11 Baltic cables have been damaged in 15 months, prompting NATO to up its guard." *Associated Press*, 28 gennaio 2025, https://tinyurl.com/55a4d52f

[3] Milmo, D. "Russian cyber-attacks against Nato states up by 25% in a year, analysis finds." *The Guardian*, 16 ottobre 2025, https://www.theguardian.com/world/2025/oct/16/russian-cyber-attacks-against-nato-states-up-by-25-in-a-year-analysis-finds.

esaminare le contromisure adottate dalla NATO, nonché le prospettive future dell'approccio dell'Alleanza a tali minacce.

La crescente minaccia ibrida

Il termine stesso "guerra ibrida" rimane oggetto di ampie discussioni (e critiche)[4]. Il concetto "nasce" nei primi anni Duemila e fa riferimento all'integrazione di attori e tattiche convenzionali e irregolari nel campo di battaglia, superando la rigida distinzione tra le due modalità di conduzione della guerra[5]. Proprio in sede NATO avverrà la reinterpretazione della nozione di guerra ibrida che ad oggi permea il dibattito pubblico.

L'idea che l'Alleanza potesse trovarsi a fronteggiare minacce di natura ibrida risale al 2009, anno di pubblicazione di un rapporto volto a immaginare le principali sfide alla sicurezza euro-atlantica nel "mondo del 2030"[6]. Tra le potenziali fonti di minacce individuate da questo rapporto figurano in particolare attori non-statali quali individui straordinariamente influenti, gruppi estremisti e crimine organizzato, seguiti dai cosiddetti "stati canaglia", dalle potenze aggressive e dagli eventi naturali. In un contesto internazionale caratterizzato da asimmetrie di potere, interconnessione crescente e proliferazione di attori non convenzionali, si prevedeva che eventuali avversari futuri avrebbero evitato azioni aperte, cinetiche e dirette contro l'Alleanza, preferendo atti di sabotaggio,

[4] Si veda, ad esempio, Libiseller, Chiara. "'Hybrid Warfare' as an Academic Fashion." *Journal of Strategic Studies* 46, no. 4 (2023): 858–80. https://doi.org/10.1080/01402390.2023.2177987.
[5] Nemeth, William J. *Future War and Chechnya: A Case for Hybrid Warfare*. Monterey, CA: Naval Postgraduate School 2002.
[6] NATO Allied Command Transformation. *Multiple Futures Project, 2009. Navigating Towards 2030*. https://www.defencetalk.com/wp-content/uploads/2009/05/20090503_mfp_finalrep.pdf. Si veda anche Aaronson, Michael, Sverre Diessen, Yves De Kermabon, Mary Beth Long, e Michael Miklaucic. "NATO Countering the Hybrid Threat." PRISM 2, no. 4 (2011): 111–24. http://www.jstor.org/stable/26469152.

sovversione, terrorismo e "guerra cognitiva"[7]. Questa previsione si concretizzerà nel 2014, a seguito dell'annessione della Crimea e dell'incursione nel Donbass ad opera della Federazione Russa. In tale occasione, Mosca ha infatti impiegato in maniera integrata una serie di strumenti riconducibili alla logica della "guerra ibrida", dall'invio di truppe prive di insegne (i cosiddetti "omini verdi") a campagne di disinformazione e cyberattacchi contro le infrastrutture governative ucraine.

Di conseguenza, il vertice NATO tenutosi in Galles nel 2014 dedica un intero paragrafo alle minacce ibride, caratterizzate dall'utilizzo coordinato di strumenti militari, paramilitari e civili in maniera più o meno aperta[8]. Da allora, il concetto di guerra ibrida ha acquisito una popolarità crescente, discostandosi ulteriormente dalla definizione "tattica" originaria, ponendo maggiormente l'accento sugli strumenti non strettamente militari e sulla dimensione cognitiva. Sebbene non vi sia una definizione unanimemente accettata di guerra ibrida, essa è contraddistinta da tre elementi chiave. In primis, le azioni ibride si inseriscono in una zona "grigia" tra la pace e il conflitto aperto: esse rappresentano azioni ostili rivolte ad un avversario, che rimangono sotto la soglia del conflitto armato. Inoltre, spesso queste azioni sono realizzate "per procura", ossia da terze parti (o *proxy*) per conto dell'avversario, invece che direttamente da quest'ultimo. Il livello "sotto soglia" dell'azione, il fatto che si tratta spesso di azioni covert o condotte da *proxy* consentono al responsabile principale di mantenere un margine di ambiguità e di ridurre il rischio di attribuzione diretta

[7] NATO Allied Command Transformation. *Multiple Futures Project, 2009. Navigating Towards 2030*. https://www.defencetalk.com/wp-content/uploads/2009/05/20090503_mfp_finalrep.pdf.
[8] "Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales," NATO, 5 settembre 2014, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2014/09/05/wales-summit-declaration.

e conseguenti rappresaglie. Secondo, le azioni ibride mirano principalmente a destabilizzare la società del paese bersaglio, alimentando le divisioni interne e riducendo indirettamente la capacità di risposta. Terzo, in tale contesto assumono una sempre maggiore importanza le operazioni di "guerra cognitiva", come le *information operations* e la propaganda, rendendo la dimensione psicologica un terreno di scontro sempre più rilevante.

I principali avversari dell'Alleanza nel campo della guerra ibrida sono soprattutto due. Il più importante è la Russia, che da anni conduce azioni ibride contro i membri NATO e ha intensificato le proprie operazioni a seguito dell'invasione dell'Ucraina del 2022. Prima dell'invasione, le azioni ibride russe erano costituite principalmente da campagne di disinformazione e supporto, anche finanziario, ad attori locali (politici, personalità pubbliche, pagine sui social media) vicini alle posizioni di Mosca. Secondo alcuni analisti la Russia avrebbe, ad esempio, contribuito alla vittoria dei sostenitori della Brexit nel referendum del 2016, trasmettendo narrative e disinformazione anti-UE attraverso i propri media statali e i social media[9]. L'intelligence statunitense ha inoltre indicato la Federazione Russa come responsabile di interferenze elettorali nel contesto delle elezioni statunitensi del 2016, tramite cyberattacchi all'infrastruttura elettorale e *information operations* soprattutto attraverso i social media[10].

L'intensificazione della guerra ibrida di Mosca nei confronti dell'Alleanza a partire dal 2022 è dovuta al supporto che i paesi NATO forniscono al governo di Kyiv. Un rapporto redatto dalla Commissione sulla Sicurezza e sulla

[9] Ruy, D. "Did Russia Influence Brexit?" *Center for Strategic & International Studies*, 21 luglio 2020, https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit.
[10] *U.S. Senate Select Committee on Intelligence*. "Senate Intel Releases New Report on Intel Community Assessment of Russian Interference." 21 aprile 2020. https://www.intelligence.senate.gov/2020/04/21/press-senate-intel-releases-new-report-intel-community-assessment-russian-interference/.

Cooperazione in Europa (nota anche come "U.S. Helsinki Commission") individua quasi 150 azioni ibride attribuite o imputabili alla Russia dall'inizio dell'invasione fino al 2024[11]. Le più comuni rimangono le campagne di disinformazione e i tentativi di ingerenze elettorali. Nella primavera 2024, ad esempio, un'indagine internazionale condotta dai servizi segreti di Belgio e Repubblica Ceca ha rivelato l'utilizzo, da parte di individui affiliati a Mosca, della piattaforma web "Voice of Europe" allo scopo di diffondere propaganda e disinformazione tra l'opinione pubblica europea[12]. Altri esempi di disinformazione citati dal rapporto sono alcune notizie e pagine internet false diffuse in Francia e in Polonia le quali alludevano al reclutamento di cittadini negli eserciti nazionali, presumibilmente allo scopo di intervenire militarmente al fianco dell'Ucraina. Lo scopo di queste operazioni è erodere il consenso tra gli alleati NATO, sfruttando l'apertura delle società occidentali: attraverso le operazioni di influenza e disinformazione, Mosca mira a indurre l'opinione pubblica a supportare soggetti politici domestici con agende favorevoli agli obiettivi della politica estera russa.

Negli ultimi quattro anni sono aumentati considerevolmente altri tipi di azioni ibride, in particolare atti di sabotaggio, sia cyber che fisico, diretti contro infrastrutture critiche (ad esempio reti ferroviarie, strutture sanitarie, aeroporti, cavi subacquei). Gli attacchi hanno colpito sia obiettivi civili che obiettivi militari, anche attraverso atti violenti. Il 14 agosto 2024, le autorità tedesche hanno segnalato un possibile sabotaggio al sistema di fornitura idrica della base NATO di Geilenkirchen, un hub logistico importante per l'addestramento dei soldati

[11] McGrath, S. "Spotlight on the Shadow War: Inside Russia's attacks on NATO Territory." U.S. Helsinki Commission Staff, 12 dicembre 2024. https://www.csce.gov/publications/spotlight-on-the-shadow-war-inside-russias-attacks-on-nato-territory/.
[12] Vincour, N., P. Haeck e E. Wax. "Russian influence scandal rocks EU." *POLITICO*, 29 marzo 2024. https://www.politico.eu/article/voice-of-europe-russia-influence-scandal-election/.

ucraini in territorio alleato[13]. Sono stati registrati anche numerosi casi di incendi dolosi attribuiti a Mosca: sono stati attribuiti alla Russia, ad esempio, il rogo di centro commerciale di Varsavia[14], di un negozio IKEA in Lituania, di un magazzino a Londra utilizzato per inviare materiale in Ucraina (tra cui terminali Starlink)[15] e di un'acciaieria a Berlino appartenente al produttore di materiale bellico Diehl[16]. Una delle azioni più eclatanti è stata il tentato assassinio del CEO di Rheinmetall Armin Papperger[17]. Queste operazioni sono volte a dissuadere governi, ma anche entità e individui dal fornire supporto all'Ucraina, rappresentando al contempo uno strumento di pressione sulle società dei paesi NATO che si affianca alle operazioni di informazione e influenza, drenando inoltre risorse e attenzione dalle istituzioni dei paesi bersaglio[18].

Il 2025 ha visto un'ulteriore escalation delle operazioni ibride russe, dai cyberattacchi[19] e le interferenze elettorali[20] alle incursioni di droni nel territorio

---

[13] Soave, I. "Germania, due casi di sospetto sabotaggio: coinvolte una base Nato e una base militare." *Corriere della Sera*, 14 agosto 2024. https://tinyurl.com/4t2ayuea.
[14] Walker, S. "Poland to close Russian consulate in Kraków over Warsaw fire." *The Guardian*, 12 maggio 2025, https://tinyurl.com/2wxf4kxk.
[15] Sandford, D., e A. Rhodenpaul. "Men jailed over arson attack for Russia on Ukrainian business in London." *BBC*, 24 ottobre 2025, https://www.bbc.com/news/articles/c04g5x1wq5vo.
[16] Nöstlinger, N., e J. Klöckner. "Russia started Berlin factory fire as part of hybrid war on Europe, report says." *POLITICO*, 24 giugno 2024, https://www.politico.eu/article/russia-berlin-fire-diehl-behind-arson-attack-on-factory/.
[17] Körömi, C. "NATO: There was officially a Russian plot to kill European weapons chief." *POLITICO*, 28 gennaio 2025, https://www.politico.eu/article/nato-official-confirms-russian-plot-kill-european-weapons-chief-armin-papperger/.
[18] Jones, S. G. "Russia's Shadow War Against the West." *Center for Strategic & International Studies*, 18 marzo 2025, https://www.csis.org/analysis/russias-shadow-war-against-west#h2-russian-strategy.
[19] Milmo, D. "Russian cyber-attacks against Nato states up by 25% in a year, analysis finds." *The Guardian*, 16 ottobre 2025, https://www.theguardian.com/world/2025/oct/16/russian-cyber-attacks-against-nato-states-up-by-25-in-a-year-analysis-finds.
[20] J. Urbancik. "Russia's hybrid war is weakening Europe's cohesion, expert says." *Euronews*, 29 gennaio 2026, https://www.euronews.com/2026/01/29/russias-hybrid-war-is-weakening-europes-cohesion-expert-says.

degli alleati[21]. Per il 2026, si prevede che una combinazione di difficoltà sul campo, esaurimento delle riserve di armamenti e nuovi round di negoziati spingerà Mosca a fare un affidamento sempre maggiore sulle azioni ibride per minare il supporto alleato al governo di Kyiv, sfruttando le persistenti vulnerabilità dei paesi NATO, tra cui le tensioni domestiche[22].

Sebbene il principale avversario nel campo della guerra ibrida sia la Russia, l'Alleanza individua altri attori impegnati in azioni ibride. La Cina, ad esempio, rappresenta una minaccia ibrida crescente sia per via del supporto fornito alla Russia (anche nell'esecuzione stessa di attacchi ibridi)[23], sia in quanto essa conduce le proprie attività di guerra ibrida contro gli Stati Uniti e altri alleati NATO. Le azioni ibride di Pechino consistono principalmente in cyberattacchi, campagne di disinformazione e nell'utilizzo della dipendenza degli altri paesi nei confronti della Cina per terre rare ed altri materiali critici come strumento di coercizione. Tra gli attori coinvolti in azioni ibride contro i paesi NATO figurano anche l'Iran e la Corea del Nord, attivi principalmente nel dominio cyber[24].

La NATO alla prova delle minacce ibride: strumenti e vulnerabilità

Già a partire dai primi anni Duemila, la NATO ha iniziato ad attrezzarsi per fare fronte alle minacce cyber. Il Cooperative Cyber Defence Centre of Excellence (CCD CoE) fu infatti proposto dall'Estonia nel 2004, e assunse ulteriore rilevanza a seguito del cyberattacco subito dal Paese nel 2007. A seguito della

---

[21] Avesani, L. "Droni russi sconfinano il territorio polacco: sfida alla NATO?" *Geopolitica.info*, 10 settembre 2025. https://www.geopolitica.info/droni-russi-polonia/.
[22] Beznosiuk, M., e W. Dixon. "How Russia's Hybrid Warfare Will Escalate in 2026 and What Europe Must Do?" *GLOBSEC*, 13 gennaio 2026, https://www.globsec.org/what-we-do/commentaries/how-russias-hybrid-warfare-will-escalate-2026-and-what-europe-must-do.
[23] Si veda, ad esempio Smith, K. "Chinese Cyber Espionage Surges 150%, House Committee Warns." *ExecutiveGov,* 4 novembre 2025, https://www.executivegov.com/articles/house-cyber-snapshot-china-critical-sectors.
[24] *ANSA*. "Fonti Nato, contro di noi attacchi ibridi e cyber costanti." 3 dicembre 2024, https://tinyurl.com/265cvxun.

materializzazione della minaccia ibrida, il CCD CoE ha assunto un ruolo progressivamente crescente nella formazione e nell'addestramento sia del personale NATO che quello dei Paesi alleati nell'ambito della *cyber defense*[25].

A seguito del vertice NATO in Galles, l'Alleanza ha provveduto a un rafforzamento e a una crescente articolazione degli strumenti dedicati al contrasto delle minacce ibride[26]. Lo Strategic Communications Centre of Excellence, situato in Lettonia e operativo dal 2014, contribuisce principalmente al contrasto alle campagne di influenza e disinformazione[27]. Sempre nel 2014, la NATO ha condotto la prima esercitazione contenente elementi di guerra ibrida, mentre nel 2015 fu rilasciata la prima strategia di contrasto alle minacce ibride[28]. L'Alleanza ha così iniziato la costruzione di un ecosistema di centri, dottrine ed esercitazioni volto a rafforzare la propria capacità di risposta alle azioni ostili sottosoglia.

Con il comunicato prodotto dal vertice tenutosi a Varsavia nel 2016, gli alleati dichiararono esplicitamente che avrebbero considerato la difesa contro le minacce ibride come una componente della difesa collettiva, e che, sebbene la responsabilità di rispondere a un attacco ibrido spetti in primo luogo allo stato bersaglio, non sarebbe stata esclusa a priori la possibilità, da parte del Consiglio

[25] "About Us," NATO Cooperative Cyber Defence Centre of Excellence, ultimo accesso 14 febbraio 2026, https://www.ccdcoe.org/about-us/.
[26] "Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales," NATO, 5 settembre 2014, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2014/09/05/wales-summit-declaration.
[27] "Program of Work," NATO Strategic Communications Centre of Excellence, ultimo accesso 14 febbraio 2026, https://stratcomcoe.org/projects/program-of-work.
[28] Colom Piella, G. "NATO's Strategies For Responding To Hybrid Conflicts." *Barcelona Centre for International Affairs*, settembre 2022, https://www.cidob.org/en/publications/natos-strategies-responding-hybrid-conflicts.

Atlantico, di invocare l'Articolo 5[29]. Negli anni successivi, l'Alleanza ha introdotto ulteriori strumenti operativi volti a potenziare la capacità di risposta alle azioni ibride. Nel 2018, ad esempio, è stato istituito il NATO Counter-Hybrid Support Team, schierato per la prima volta nel 2019 in Montenegro e successivamente, nel 2021, in Lituania[30].

Nel contrasto alla guerra ibrida, l'Alleanza si avvale anche di collaborazioni sia con l'Unione Europea (UE) che con altri Paesi partner oggetto di attacchi ibridi. Dalla cooperazione UE-NATO nasce infatti, nel 2017, lo European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), un hub intergovernativo che riunisce UE, NATO e 35 Stati partecipanti membri delle due organizzazioni[31]. L'Hybrid CoE fornisce principalmente analisi, formazione, addestramento ed esercitazioni in tutti i domini rilevanti della guerra ibrida[32].

Il NATO Strategic Concept del 2022, a pochi mesi dall'inizio dell'invasione russa dell'Ucraina, riconosce che "le operazioni ibride contro i Paesi alleati potrebbero raggiungere il livello di attacco armato e indurre il Consiglio del Nord Atlantico ad invocare l'Articolo 5"[33]. Come dimostrato dall'escalation sia in termini di quantità che di qualità delle azioni ibride negli ultimi anni, però, i ripetuti

---

[29] "Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016," NATO, 9 luglio 2016, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique.
[30] *The Baltic Times*. "NATO Counter Hybrid Support Team arrives in Lithuania." 7 settembre 2021, https://www.baltictimes.com/nato_counter_hybrid_support_team_arrives_in_lithuania/.
[31] Gli stati partecipanti all'Hybrid CoE erano 36 fino al 10 febbraio 2026, data in cui gli Stati Uniti hanno annunciato il proprio ritiro. Si veda "The United States withdraws from Hybrid CoE," European Centre of Excellence for Countering Hybrid Threats, 10 febbraio 2026, https://www.hybridcoe.fi/news/the-united-states-withdraws-from-hybrid-coe/.
[32] "Hybrid threats," European Centre of Excellence for Countering Hybrid Threats, ultimo accesso 14 febbraio 2026, https://www.hybridcoe.fi/hybrid-threats/.
[33] "NATO 2022 Strategic Concept", NATO, ultimo aggiornamento 3 marzo 2023, https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept.

avvertimenti dell'Alleanza non hanno sortito l'effetto di deterrenza auspicato[34]. La NATO, infatti, sconta una serie di debolezze nella competizione sotto soglia per quanto concerne la deterrenza tramite punizione (*deterrence-by-punishment*). In particolare, gli alleati hanno percezioni della minaccia russa molto variabili tra di loro[35]. Ciò rende difficile organizzare una risposta coordinata alle azioni ibride, le quali, oltretutto, sono spesso difficili da attribuire con certezza ad un determinato attore. Inoltre, dato che le decisioni del Consiglio Atlantico sono prese con il consenso unanime dei membri, un'attivazione dell'Articolo 5 a seguito di una minaccia ibrida appare ad oggi improbabile. Inoltre, in quanto alleanza difensiva, la NATO tende ad adottare una postura reattiva dinanzi alle azioni ibride avversarie, con l'intento di evitare escalation. La mancanza di risposte decise alle azioni ibride russe sembra però essere interpretata dalla controparte come debolezza, aprendo la strada a nuovi attacchi ibridi. Pertanto, negli ultimi anni, diverse voci hanno invocato il bisogno di adottare una postura più "offensiva" nel campo della guerra ibrida[36].

Altrettanto importante è la resilienza delle istituzioni e delle società degli alleati, che costituisce la base della deterrenza tramite negazione (*deterrence-by-denial*) nella competizione sottosoglia. Il principio di resilienza e di preparazione civile (*civil preparedness*) trova il suo fondamento nell'impegno degli alleati, sancito dall'Articolo 3 del Trattato dell'Atlantico del Nord, a mantenere ed accrescere "la

[34] Jones, Seth G. "Russia's Shadow War Against the West." *Center for Strategic & International Studies*, 18 marzo 2025, https://www.csis.org/analysis/russias-shadow-war-against-west#h2-russian-strategy.
[35] Davidson, Jason W. NATO after Russia's Invasion of Ukraine: Threat Perceptions and Their Consequences. Washington, D.C., DC: Georgetown University Press, 2026.
[36] Deni, John R. "What NATO can do now to apply lessons from Russia's war in Ukraine." *Atlantic Council*, 20 marzo 2023, https://www.atlanticcouncil.org/blogs/new-atlanticist/what-nato-can-do-now-to-apply-lessons-from-russias-war-in-ukraine.

loro capacità individuale e collettiva di resistere ad un attacco armato"[37]. L'impegno a rafforzare la resilienza nazionale e collettiva è stato reiterato e rafforzato a più riprese, e dal 2022 il NATO Resilience Committee definisce le linee guida in materia di resilienza e preparazione civile[38]. È supportato da sei *planning groups*, ognuno dei quali ha la propria area di *expertise* (settore delle comunicazioni, protezione civile, pianificazione energetica, settore alimentare e idrico, settore sanitario e trasporto). Nonostante i progressi compiuti dal 2014, le società dei paesi NATO sono ancora molto permeabili alle minacce ibride. Un commento dell'istituto RUSI redatto da Joe Morley-Davies e pubblicato nell'agosto del 2025 denota una carenza di preparazione da parte dei membri NATO[39], soprattutto per quanto riguarda la resilienza delle società occidentali. Un esempio virtuoso è quello del libretto "*In Case of Crisis or War*" distribuito dal governo svedese alla propria cittadinanza e contenente istruzioni da seguire in varie situazioni di crisi, da eventi meteorologici estremi a bombardamenti aerei, nonché consigli sulla sicurezza digitale personale e l'identificazione di fake news[40]. Il modello svedese di "difesa totale"[41] è un esempio di approccio *whole-of-society* alla preparazione alle azioni ibride, con la popolazione civile che diventa un attore attivo in situazioni di crisi e parte integrante della difesa della nazione.

---

[37] Trattato Nord Atlantico, 4 aprile 1949, https://tinyurl.com/y2ksvcbr. Si veda anche "Resilience, civil preparedness and Article 3," NATO, ultimo aggiornamento 13 novembre 2024, https://tinyurl.com/3er8teht.

[38] "Resilience Committee," NATO, ultimo aggiornamento 7 ottobre 2022, https://www.nato.int/en/about-us/organization/nato-structure/resilience-committee.

[39] Morley-Davies, J. "Deterring Kremlin Grey Zone Aggression Against NATO." *Royal United Services Institute for Defence and Security Studies (RUSI)*, 29 agosto 2025, https://www.rusi.org/explore-our-research/publications/commentary/deterring-kremlin-grey-zone-aggression-against-nato.

[40] *Small Wars Journal*, "The Swedish handbook: "In Case of Crisis or War" (Official Resistance & Resilience Brochure for Citizens)," 26 marzo 2025. https://tinyurl.com/3em3zt82.

[41] "Total defence – you are part of Sweden's overall emergency preparedness," Swedish Civil Defence and Resilience Agency, ultimo aggiornamento 14 novembre 2025, https://www.mcf.se/en/advice-for-individuals/swedish-defence/total-defence--you-are-part-of-swedens-overall-emergency-preparedness/.

Altri esempi virtuosi di approcci *whole-of-society* sono gli altri paesi scandinavi[42] e la Lettonia[43] (dove la percezione della minaccia russa è alta), mentre l'idea di preparazione civile rimane secondaria in paesi meno esposti[44].

Un altro aspetto centrale è la resilienza delle infrastrutture critiche. Questa necessità accomuna NATO e UE, ragion per cui, nella primavera del 2023, le due organizzazioni hanno istituito una Task Force incaricata di fornire una valutazione comprensiva sul tema. Il report finale fornisce alcune raccomandazioni ad entrambe le organizzazioni, tra cui valutazioni congiunte delle minacce, esercitazioni coordinate, protezione cyber e marittima, riduzione delle dipendenze strategiche (ad esempio rotte di trasporto, *supply chains*) e maggiore cooperazione civile-militare e pubblico-privato[45]. Quest'ultima assume particolare importanza dal momento che, rispetto al periodo della Guerra Fredda, oggi buona parte delle infrastrutture critiche è gestita dal settore privato[46]. A due anni di distanza dal rilascio del report della Task Force NATO-UE, nuove valutazioni della resilienza europea segnalano gap persistenti in materia di preparazione a shock ibridi, specie per quanto riguarda la mobilità militare, la sicurezza delle reti 5G e la protezione dei cavi sottomarini[47].

---

[42] Zgórzak, M. "Security is not only military—it is societal. Something worth learning from the Scandinavians." *Defence24*, https://defence24.com/defence-policy/security-is-not-only-military-it-is-societal-something-worth-learning-from-the-scandinavians.
[43] Hardt, H., e Māris C. "Crisis management and resilience: Lessons from Latvia for NATO allies." *Atlantic Council*, 21 agosto 2025, https://www.atlanticcouncil.org/blogs/new-atlanticist/crisis-management-and-resilience-lessons-from-latvia-for-nato-allies.
[44] Martisiute, M. "Civil preparedness is a right." *European Policy Centre*, 14 gennaio 2025, https://www.epc.eu/publication/Civil-preparedness-is-a-right-60949c/.
[45] "EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure," Commissione Europea, 29 giugno 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564.
[46] Si veda "Resilience, civil preparedness and Article 3." NATO, ultimo aggiornamento 13 novembre 2024, https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3.
[47] Horan, H., P.-J. Vandoren, D. Fiott, e J. Feldhusen. "Assessing Europe's Resilience and Preparedness in an Era of Strategic Risks." *The Hague Centre for Strategic Studies*, 2 dicembre

Il 2026 e gli anni a venire pongono dinanzi agli alleati alcuni importanti ostacoli al raggiungimento di un livello ideale di resilienza e deterrenza. In primo luogo, il desiderio statunitense di ribilanciare la relazione transatlantica si interseca con un apparente disinteresse verso il contrasto alle minacce ibride, esemplificato dalla recente uscita statunitense dall'Hybrid CoE[48], inserito tra le 66 organizzazioni internazionali ritenute contrarie agli interessi degli Stati Uniti[49]. Ciò implicherà la perdita di un canale importante di coordinamento, e rappresenta un ulteriore segnale di una profonda divergenza tra il maggiore azionista dell'Alleanza ed il resto degli alleati, che ha raggiunto il suo apice con le minacce di annessione della Groenlandia agli Stati Uniti[50]. A ciò si uniscono le tensioni tra gli alleati europei e all'interno di alcuni paesi come la Repubblica Ceca[51] che rendono l'Alleanza ancora più permeabile a operazioni ibride[52].

Conclusione

La cosiddetta "guerra ibrida" è ormai un elemento strutturale del confronto tra potenze; in quanto principale alleanza del sistema internazionale, impegnata in una rivalità sotto la soglia del conflitto armato diretto con la Federazione Russa,

---

2025, disponibile su: https://hcss.nl/news/new-report-assessing-europes-resilience-and-preparedness-in-an-era-of-strategic-risks/.

[48] "The United States withdraws from Hybrid CoE." European Centre of Excellence for Countering Hybrid Threats, 10 febbraio 2026, https://www.hybridcoe.fi/news/the-united-states-withdraws-from-hybrid-coe/.

[49] "Withdrawing the United States from International Organizations, Conventions, and Treaties that Are Contrary to the Interests of the United States." The White House, 7 gennaio 2026, https://tinyurl.com/3nchh3sk.

[50] Saitta, M. "Groenlandia: quando la sicurezza americana diventa una minaccia per la NATO." *Geopolitica.info*, 19 gennaio 2026, https://www.geopolitica.info/groenlandia-sicurezza-americana-minaccia-nato/

[51] Avesani, L. "Lo scontro istituzionale indebolisce e polarizza la Repubblica Ceca." *Geopolitica.info*, 4 febbraio 2026, https://www.geopolitica.info/scontro-istituzionale-indebolisce-polarizza-repubblica-ceca/.

[52] Beznosiuk, M., e W. Dixon. "How Russia's Hybrid Warfare Will Escalate in 2026 and What Europe Must Do?" *GLOBSEC*, 13 gennaio 2026, https://www.globsec.org/what-we-do/commentaries/how-russias-hybrid-warfare-will-escalate-2026-and-what-europe-must-do.

e consapevole del ruolo che la Cina gioca sia nel supporto alla Russia sia tramite la propria guerra ibrida, la NATO è e rimarrà un bersaglio di sabotaggi, atti violenti, cyberattacchi, campagne di disinformazione e azioni cinetiche sottosoglia.

La NATO, che già nel 2009 ipotizzava un futuro caratterizzato dalle minacce ibride, ha introdotto a partire dal 2014 una serie di strumenti volti a rafforzare la capacità degli alleati di resistere ad azioni ibride di varia natura, dalla disinformazione al sabotaggio delle infrastrutture critiche. Inoltre, gli alleati hanno dichiarato più volte di considerare un attacco ibrido una condizione sufficiente per invocare l'Articolo 5, ossia la clausola di difesa collettiva. Ciononostante, permangono alcune debolezze nell'approccio NATO alle minacce ibride. Nonostante i progressi fatti, le società e le infrastrutture critiche dei Paesi alleati rimangono permeabili alle azioni ibride. Inoltre, a causa delle diverse percezioni della minaccia russa tra i vari alleati e la postura esclusivamente difensiva dell'Alleanza nella risposta alle minacce ibride, la deterrenza tramite punizione manca di credibilità e incentiva gli avversari a proseguire la propria guerra ibrida.

Infine, l'Alleanza dovrà aspettarsi una crescente pressione negli anni a venire sul fronte ibrido: da un lato, si prevede che Mosca intensificherà le proprie operazioni ibride a fronte delle difficoltà sul campo in Ucraina e di un'apparente ripresa dei negoziati, mentre la Cina continuerà il suo supporto tacito alla Russia, traendone anche qualche spunto, e proseguirà le proprie azioni ibride, facendo specialmente leva sulla dipendenza dei Paesi occidentali da Pechino in alcuni settori strategici, come batterie e minerali critici. Contemporaneamente, si assiste a crescenti tensioni all'interno dell'Alleanza stessa, con gli Stati Uniti a guida dell'amministrazione Trump apparentemente disinteressati alle iniziative

di contrasto alle minacce ibride - come testimonia l'uscita statunitense dall'Hybrid CoE - e in disaccordo con gli alleati sulla percezione di Mosca come minaccia, insieme ad altri alleati "scettici" quali l'Ungheria e la Slovacchia.

Metodologie didattiche e *best practices* per una formazione orientata al contrasto delle minacce ibride

di Antonino Cambria

Introduzione

In ambito internazionale, dottrinale ed accademico è ampiamente riconosciuto che la guerra ibrida rappresenta una delle principali sfide strategiche contemporanee, caratterizzata dalla combinazione di tattiche convenzionali e non convenzionali, dall'ambiguità operativa e da ambienti multidimensionali complessi e incerti. Essa si sviluppa spesso attraverso confronti indiretti e *proxy wars*, sfruttando le vulnerabilità dell'avversario e rendendo difficile l'attribuzione delle responsabilità.[1]

In questo ambiente strategico, le sfide legate all'educazione dei futuri leader stanno cambiando rapidamente, in un processo che deve tenere il passo con l'evoluzione di molteplici fattori. I concetti di *Fourth Generation Warfare* e di *Soldati 4.0* contribuiscono a ridefinire il modo di concepire il futuro della guerra e il ruolo dei combattenti.[2]

Per rispondere efficacemente alla minaccia ibrida, gli Stati, e in particolare le istituzioni di istruzione superiore nel settore della sicurezza e difesa, devono adattare nuovi modelli educativi. Appare sempre più necessario adottare nuovi paradigmi formativi che integrino guerra convenzionale e non convenzionale,

[1] Cambria, A., et al. 2023a. "Educational Innovation in Hybrid Warfare." In *Proceedings of the 16th International Conference of Education, Research and Innovation (iCERI2023)*, 9433–9440. Seville: IATED. https://doi.org/10.21125/iceri.2023.2432

[2] Lewis, T. M. S. 2009. "*Educating for Land Power"*. Strategy Research Project. Carlisle Barracks, PA: U.S. Army War College, Department of Military Strategy, Planning, and Operatio

promuovano pensiero critico, capacità decisionali etiche, discernimento informativo e flessibilità cognitiva.[3]

La guerra ibrida, intesa come la combinazione di tattiche convenzionali e non convenzionali, pone sfide significative nel moderno panorama geopolitico. La natura in rapido cambiamento della guerra ibrida richiede un approccio educativo dinamico e globale. In risposta a questa minaccia in evoluzione, le istituzioni di istruzione superiore dovrebbero adattare i propri curricula per dotare gli studenti delle conoscenze e delle competenze necessarie ad affrontare efficacemente la complessità della guerra ibrida.

Educazione e addestramento assumono un ruolo centrale e complementare: la prima per accrescere la consapevolezza strategica, il secondo per garantire la prontezza operativa. Secondo la letteratura corrente approcci innovativi, come il *blended learning*, l'apprendimento collaborativo, le simulazioni e i programmi intensivi internazionali, favoriscono interoperabilità, cooperazione civile-militare e sviluppo di competenze trasversali.[4] In un contesto globale in rapido mutamento, la priorità non è solo insegnare "cosa pensare", ma soprattutto "come pensare", in modo tale da avere la potenzialità di formare leader adattivi, critici e capaci di operare efficacemente in ambienti multi-dominio e ibridi[5].

Sono necessari nuovi paradigmi per progettare programmi di studio che coprano i principi della guerra convenzionale e, allo stesso tempo, abbraccino gli aspetti non convenzionali della guerra ibrida. Inoltre, gli approcci didattici alla guerra

[3] Cambria, A., et al. 2023a. *op. cit*., pp. 9433-9440.
[4] Barana, A., et al. 2024. "Detecting Blended Learning, Collaborative Learning and Internationalization in Military Education: A Systematic Literature Review." In *Proceedings of the 18th International Conference on e-Learning and Digital Learning 2024 and Sustainability, Technology and Education 2024*, 137–144. Budapest.
[5] Barana, A., et al. 2025. "Investigating the Development of Intercultural Competences through Blended Intensive Programmes." In *Proceedings of the International Conferences on Mobile Learning 2025 and Educational Technologies 2025*, 177–184. Madeira Island, Portugal.

ibrida dovrebbero incoraggiare il pensiero critico, il processo decisionale etico e la capacità di distinguere tra informazioni affidabili e disinformazione. Per facilitare l'implementazione di pratiche didattiche innovative nell'educazione alla Sicurezza e alla Difesa, i docenti sono invitati ad adottare nuove metodologie di insegnamento e a sfruttare efficacemente la tecnologia.

La prima sezione dell'articolo identifica le definizioni utili alla comprensione delle motivazioni intrinseche e cause dei fenomeni ricercati. Una volta definiti i concetti, la seconda sezione spiega come il collante dell'educazione e formazione nel campo difesa e sicurezza sia importante in un contesto di guerre ibride e di presenza nel multi-dominio. La sezione successiva descrive l'ambiente dove sono stati raccolti i dati partendo dalla formulazione di una domanda utile a dirigere la raccolta dei dati verso un risultato concreto. Nella quarta sezione i dati raccolti sono stati sintetizzati in una serie di *best practices*. Questi elementi di natura tattica sono stati utilizzati per trarre delle conclusioni ad un livello più strategico e di *policy advising*.

Definizioni

Nel contesto internazionale attuale emergono due caratteristiche principali: discontinuità e complessità. Le operazioni militari moderne o le azioni di vari attori risultano spesso ambigue, difficili da riconoscere e caratterizzate da elementi nuovi in ambienti multidimensionali (terra, aria, mare, cyber, cognitivo, spazio etc). Si introduce un acronimo che può essere usato come epiteto e che permette di definire ciascuna dimensione con tratti di volatilità, incertezza, complessità e ambiguità: VUCA.

Questi elementi costituiscono il fondamento di un mondo globale e competitivo in cui la guerra rappresenta una sfida ai tradizionali modelli di concezione, gestione e mitigazione delle minacce. La complessità è ulteriormente accresciuta

dal confronto indiretto tra attori, che ricorrono a proxy war per colpire altri Stati perseguendo i propri interessi. Le guerre per procura costituiscono oggi una forma ricorrente di confronto tra Stati e gruppi non statali. Pertanto si creano delle necessità nei vari sistemi, domini, ambienti e terreni, a cui poi vengono poste delle domande per definire e comprendere le forme degli approcci delle operazioni militari.

In risposta alla necessità di descrivere un approccio alle operazioni militari che vada oltre i tradizionali domini di terra, mare e cielo, includendo anche i nuovi domini del cyber e dello spazio, dalla collettività della difesa e sicurezza è stato introdotto il termine multi-dominio. La base di partenza per comprendere e definire questo termine è proprio la definizione di dominio. Nel campo della difesa e sicurezza si può intendere il dominio come un insieme di capacità e attività che vengono applicate al campo di battaglia, in un ambiente di riferimento (marittimo, terrestre, aereo, cibernetico e spaziale).[6]

Con l'interconnessione dei tradizionali domini e l'aggiunta di ulteriori si generano molti più effetti cinetici e non, che si ripercuotono sulle dimensioni militari principali. Ciò espande il campo di battaglia e permette di fronteggiare strategie di potenziali rivali che, utilizzando tutti gli strumenti del potere, cercano di impedire alla controparte di rispondere e di perseguire i propri interessi strategici senza ostacoli. La sincronizzazione degli effetti è un elemento cardine delle operazioni in contesti multi-dominio e di guerra ibrida.

Un ulteriore elemento cardine delle operazioni che vengono svolte nel multi-dominio riguarda il raggiungimento di un alto livello di integrazione e di interoperabilità tra sistemi, processi ed attori coinvolti nei diversi domini, sia a

[6] Ministero della Difesa – Stato Maggiore della Difesa. 2022. *Approccio della Difesa alle Operazioni Multidominio*. Edizione 2022. Roma. pp. 1-8.

livello nazionale, sia a livello internazionale/sovranazionale. Da non dimenticare è il nuovo ruolo della dimensione umana nel suo rapporto con le tecnologie emergenti, ovvero l'intelligenza artificiale.[7]

In particolare, l'uso di campagne di disinformazione ha sottolineato l'importanza dell'ambiente elettromagnetico e della dimensione cognitiva nel conflitto, facendo emergere il crescente peso dell'ambiente informativo. Il concetto di multi-dominio si sta evolvendo verso un approccio che punta a sviluppare la capacità di generare effetti in tutte le dimensioni possibili del confronto: fisica, cognitiva e virtuale, dove comunque l'idea centrale è quella di affrontare le aggressioni dei rivali, che assumono un carattere ibrido.

Nel quadro di un contesto internazionale VUCA delle operazioni multi-dominio, le minacce ibride rappresentano la concreta manifestazione operativa di azioni cinetiche e non inerenti a un conflitto che si sviluppa in modo coordinato e sinergico attraverso più domini. Esse possono essere definite come l'insieme di azioni coordinate e integrate, condotte da attori statuali e non statuali che agiscono come agenti o proxy (al di sotto della soglia del conflitto armato) spesso caratterizzate da difficoltà di attribuzione, mirate a danneggiare, destabilizzare o indebolire gli interessi nazionali di uno Stato.[8] Tali azioni, sfruttando vulnerabilità strutturali, dipendenze strategiche e fragilità sociali, coinvolgono simultaneamente i vari sistemi diplomatico, informativo, militare, economico-finanziario, cibernetico e dell'intelligence.[9] Possono manifestarsi su vari livelli

[7] Ibidem, p. 38.
[8] Sistema di informazione per la sicurezza della Repubblica. 2025. "Glossario Intelligence." Consultato il 24 dicembre 2025. https://www.sicurezzanazionale.gov.it/comunicazione/glossario/450
[9] Ministro della Difesa Crosetto, G. 2025. Il contrasto alla guerra ibrida: Una strategia attiva. Non-paper. Roma: Stato Maggiore della Difesa, pp.1-5.

strategico-operativo-tattico e con una caratteristica di onnicomprensività elevata.

In continuità con il concetto di multi-dominio, la minaccia ibrida mira a erodere la resilienza democratica, minare la fiducia dei cittadini nelle istituzioni e influenzare i processi decisionali e l'opinione pubblica attraverso campagne di disinformazione, guerra cognitiva, interferenze nei processi democratici e uso sistemico della corruzione. L'evoluzione dello spazio cibernetico e dell'ecosistema mediatico amplifica l'efficacia di tali azioni, rendendole pervasive, continue e difficilmente contrastabili con strumenti tradizionali. La guerra ibrida, infatti, tende a manifestarsi in forma persistente, colpendo infrastrutture critiche, centri decisionali e servizi essenziali. Così facendo, questa espone gli Stati al rischio di effetti strategici cumulativi.[10] La guerra ibrida rende opache le dinamiche del conflitto, poiché offre una gamma sempre più ampia di strumenti per indebolire l'avversario e minare la sicurezza su più fronti simultaneamente.

Il collante tra multi-dominio e guerra ibrida risiede dunque nella crescente integrazione funzionale dei domini e degli strumenti impiegati, che rende il capitale umano un fattore decisivo. La sua centralità rimane sul fatto che ogni dominio ha comunque una visione antropocentrica. Il fattore del capitale umano deve quindi essere continuamente formato. Diventa strategico il rinnovamento dei processi di formazione e sviluppo del personale, orientandoli sia al rafforzamento di competenze tecnico-specialistiche sia alla crescita di leader capaci di operare in ambienti complessi, interconnessi e in rapido mutamento, sfruttando pienamente le opportunità offerte dal paradigma multi-dominio. [11]

[10] Ibidem, p.62.
[11] MINISTERO DELLA DIFESA - Stato Maggiore della Difesa, op. cit., p.5.

Military education e situazione italiana

In questa visione di formazione in linee generali, è possibile distinguere due filoni per sviluppare la professionalità di personale militare, a cui si deve accompagnare indissolubilmente e necessariamente quella di personale civile. La prima partirebbe dalla visione tradizionalmente classica e modernista sull'educazione, che promuove un ambiente di apprendimento che abbraccia l'uniformità e potenzia gli esercizi già pianificati basati su scenari come metodi per condurre operazioni militari. Tuttavia, una prospettiva alternativa che abbraccia la differenza piuttosto che l'uniformità come mezzo per sviluppare le unità militari e i loro soldati, può aiutare a trovare nuovi modi efficienti di apprendere e insegnare nel campo dell'educazione militare.[12]

Questo comporta che devono essere tenuti in considerazione molti fattori e soprattutto molte variabili. In relazione a questa seconda teoria, si può riscontrare nel panorama europeo e degli stati membri che numerose istituzioni europee di educazione e formazione di base per gli ufficiali sono impegnate a migliorare gli scambi tra di loro con personale civile.

Pertanto, in questo ambiente di cooperazione che si traduce in una diffusione di coscienza collettiva nel campo della Sicurezza e della Difesa, l'educazione e la formazione mirano a preparare il personale militare (ufficiali) e i civili altamente specializzati a cooperare in ambienti nazionali e internazionali con colleghi di altre nazioni. Pertanto, sono necessari sforzi per armonizzare i sistemi per renderli "compatibili" per gli scambi e per facilitare la mobilità.[13]

---

[12] Sookermany, A. M. 2017. "Military Education Reconsidered: A Postmodern Update." *Journal of Philosophy of Education* 51 (1): 310–330. https://doi.org/10.1111/1467-9752.12224

[13] Paile-Calvo, S. 2016. *From European Mobility to Military Interoperability: Exchanging Young Officers, Knowledge and Know-How*. Brussels: European Security and Defence College. Vedi anche Barana, A., et al. 2024. *op. cit.,* 137–144.

In considerazione della revisione della letteratura esistente, un primo tentativo di definizione di cosa sia la “Military Education” può partire da una fusione di concetti esposti da alcuni studiosi militari. L'educazione di base degli ufficiali militari, infatti, è generalmente composta da due aspetti: “educazione accademica”, che sarà anche riferita come “educazione”, e “formazione professionale”. L'aspetto accademico deriva dalla definizione di un percorso appunto accademico. Si tratta di un fenomeno complesso costituito da formazione ed educazione, dove la formazione può essere riferita all'apprendimento pratico legato alle competenze professionali del ‘gestire la violenza’, mentre l'educazione può essere riferita all'apprendimento accademico o intellettuale legato alla capacità di decidere come e quando le competenze professionali acquisite possano essere applicate nell'ambiente operativo in cambiamento.[14]

Il generale Dempsey identifica lo sviluppo del pensiero critico come l'ingrediente chiave per il futuro dell'educazione militare (ME). Questa deve instillare la capacità cognitiva di comprendere, ricevere e esprimere chiaramente l'intento, di prendere l'iniziativa decisiva all'interno dell'intento, accettare rischi prudenti e costruire fiducia all'interno della forza.[15] In accordo con il generale, l'educazione militare in un ambiente professionale è dedicata a sviluppare le “abitudini mentali essenziali per la nostra professione basate principalmente sul pensiero critico”.[16]

---

[14] Melnikovas, A. 2019. “Officer Education Policy Development in the Context of the Changing European Security and Defence Identity.” *Šiuolaikinės visuomenės ugdymo veiksniai* 4 (1): 79–94. https://doi.org/10.47459/svuv.2019.4.5

[15] Murray, N. 2016. “The Role of Professional Military Education in Mission Command.” *Joint Force Quarterly* 72: 13–15.

[16] Paile-Calvo, S. 2016. *op. cit.*, Vedi anche Barana, A., et al., 2024a. *op. cit*., pp. 137-144.

Alla luce dell'analisi di queste definizioni e del fissaggio di questi punti di riferimento dell'ambiente in cui viene sviluppata questa ricerca è possibile dire che tra i risultati degli approcci educativi innovativi emerge la necessità di una maggiore cooperazione e interoperabilità tra le forze armate ad un livello nazionale e guardando in un'ottica più vasta e allargata anche tra quelle degli Stati membri. Da uno studio condotto in questi anni, è possibile affermare che processi di internazionalizzazione (I), *blended learning* (BL) e *collaborative learning* (CL) possono essere considerati strumenti potenzialmente efficaci per sviluppare tale interoperabilità. Questo deriva dal fatto che la globalizzazione rende le minacce ibride più evidenti nei sistemi di relazioni internazionali, e richiede team interconnessi capaci di operare efficacemente in contesti in continuo mutamento.[17]

Un possibile approccio consiste nella creazione di gruppi universitari in cui civili e militari collaborino, condividano un linguaggio comune e operino in ambienti multiculturali, eterogenei e internazionali. I nuovi corsi devono consentire ai giovani ufficiali di familiarizzare con ambienti conflittuali dinamici. Le caratteristiche della guerra ibrida impongono standard innovativi per i sistemi di istruzione e addestramento militare, basati su flessibilità, pensiero innovativo e capacità cognitive avanzate.[18]

L'educazione è considerata il principale fattore per sviluppare consapevolezza, mentre l'addestramento è essenziale per la prontezza operativa. Entrambi mirano a preparare personale militare e civile ad ambienti dinamici, multi-dominio e multilivello, anche attraverso l'uso di tecnologie e ambienti di apprendimento basati su simulazioni. In tali contesti, è fondamentale sviluppare

[17] Cambria, A., et al. 2023a. *op. cit.,* pp.9433-9440.
[18] Otaiku, A. 2018. "A Framework for Hybrid Warfare: Threats, Challenges and Solutions." *Journal of Defense Management* 8 (3): 1–13. https://doi.org/10.4178/2167-0374.1000178.

capacità di *problem solving*, pensiero critico e creativo, anche sotto pressione, riprendendo così quello che è stato evidenziato nella definizione di *Military Education* qualche paragrafo precedente.

Riprendendo il lavoro di Hedlund e le due tendenze espresse nella sezione di *military education*, esistono diversi approcci in Europa: nel suo lavoro lo studioso ha sistematizzato quanto avviene presso la Royal Naval Academy; ciò che accade a livello di Belgio e Paesi Bassi; nel terzo modello di sistema misto che si riscontra nei sistemi svedese e ceco; in un quarto modello si trova in Finlandia ed Estonia e infine un quinto modello nell'esercito e nell'aeronautica inglese.[19]

Tra i nuovi e innovativi approcci educativi, uno dei risultati più evidenti è la necessità di una migliore cooperazione e interoperabilità tra le forze armate degli Stati membri. Un importante tentativo di migliorare l'interoperabilità tra le forze armate dei Paesi dell'Unione Europea (UE) è stato avviato a partire dal 2008, offrendo numerose opportunità di scambio di competenze tra gli Stati membri dell'UE: Il programma Erasmus *Military for Young Officers* (EMilYO). Questo programma si pone come incubatore di grandi potenzialità che devono essere sapute sfruttare. Con il passare del tempo e l'approfondimento della ricerca su questa tematica, è stato riscontrato che i processi di internazionalizzazione, associati al *blended learning* e al *collaborative learning*, sono particolarmente efficaci per sviluppare tale interoperabilità.[20]

Il ruolo dell'istruzione è considerato il fattore principale per accrescere la consapevolezza, mentre l'addestramento è ritenuto il fattore chiave per la

[19] Hedlund, E. 2018. "A Generic Pedagogic Model for Academically Based Professional Officer Education." *Armed Forces & Society* 45 (2): 333–348. https://doi.org/10.1177/0095327X17749488

[20] Cambria, A., et al. 2023b. "Blended Intensive Programs for Fostering Collaboration and Knowledge Exchange in Security and Defence Education." In *Proceedings of the 16th International Conference of Education, Research and Innovation (iCERI2023)*, 9441–9448. Seville: IATED. https://doi.org/10.21125/iceri.2023.2433

prontezza operativa. I processi educativi e addestrativi mirano a creare azioni specifiche per sviluppare e progettare organizzazioni formative in grado di preparare futuri "guerrieri ibridi", pienamente immersi in ambienti dinamici, multi-dominio e multilivello.[21]

Nei contesti formativi, un percorso di apprendimento e crescita individuale si trasforma in un addestramento collettivo, favorendo la collaborazione, la cooperazione e lo sviluppo di competenze di apprendimento collaborativo (*collaborative learning*) all'interno di un gruppo, attraverso l'uso di strumenti di problem solving e pensiero critico. In questa prospettiva, l'obiettivo è far comprendere allo studente che è più importante "come pensare" piuttosto che "cosa pensare".[22]

Con questa categorizzazione dei modelli educativi militari, è possibile comprendere il panorama educativo europeo e verso quale direzione si stia orientando.

Il nostro modello italiano è in continua evoluzione, è ricco di esempi che rendono alcune esperienze rilevanti. In Italia, questi esempi si manifestano con l'esperienza maturata da centri di formazione come la Scuola ufficiali dell'esercito di Torino che collabora con l'Università di Torino per la formazione dei giovani Ufficiali e dei civili frequentanti il corso in Scienze Strategiche alla SUISS.[23]

---

[21] Anton, M. 2016. "Hybrid Pedagogies for Hybrid War." *Scientific Research and Education in the Air Force* 18 (2). https://doi.org/10.19062/2247-3173.2016.18.2.3

[22] Vassileva, B., and M. Zwilling. 2018. "Hybrid Warfare Simulation-Based Learning: Challenges and Opportunities." *Information & Security: An International Journal* 39 (3). https://doi.org/10.11610/isij.3919. Vedi anche Barana, A., et al. 2025. *op. cit.,* p.177-184.

[23] Spinello, E., et al. 2021. "Alcune strategie Moodle-based per facilitare le attività formative in ambito sicurezza e difesa in uno scenario hybrid." In *MoodleMoot Italia – Atti E-learning in ambito difesa*. https://hdl.handle.net/2318/1927880. Vedi anche Barana, A., et al. 2024a. *op.cit.*, pp. 137-144.

Successivamente, il Centro Alti Studi Difesa (CASD) che è diventata Scuola Superiore Universitaria (SSU) presenta alcune esperienze rilevanti. Questo istituto di formazione ha un importante ruolo nel contesto del *digital learning*, fornisce vari corsi tra quali, l'ISSMI con presenza di personale civile per Master di I e II livello, con attenzione all'aspetto della leadership, il corso di consigliere giuridico e implementa inoltre attraverso l'IRAD corsi di dottorato congiunti civile-militare, a cui si aggiunge il lavoro del Centro Formazione Logistica Interforze (CEFLI). Tutti questi percorsi spingono verso un'acquisizione non solo di conoscenze teoriche ma anche trasversali ed essenziali alla difesa per il contrasto alle minacce ibride.

Continuando su questa linea, la Marina permette ogni anno ad una vasta schiera di studenti civili (di varie discipline, partendo dal dipartimento di scienze politiche a quello di lingue, passando da ingegneria) di mettere piede sul campo insieme ai militari nell'esercitazione Mare Aperto, Joint Star, Medstrike, e altri.

Oltre alle attività di simulazione e cyber-training, l'Aeronautica partecipa a esercitazioni come Falcon Strike 2025, che combinano asset aerei, terrestri e navali con partner NATO, ponendo particolare enfasi sull'impiego di sensori avanzati; integrazione delle capacità di comando e controllo; decision-making in tempo reale in scenari complessi e incerti.

Questa formazione "reale" nelle varie forze armate e nei vari istituti di ricerca e analisi della difesa, in un contesto multinazionale è fondamentale per prepararsi ad affrontare minacce ibride operative e cognitive. Questa postura verso l'innovazione significa imparare dal passato, comprendere gli eventuali errori e modificare le tattiche, considerando la costante evoluzione degli attori avversari.[24]

[24] Lewis, T.M.S. (2009). *op. cit*., p.5.

Terreno di analisi

Se ci si sposta dall'alto livello delle definizioni alle esigenze concrete del "come fare", emerge una domanda semplice ma decisiva: come formare oggi persone civili e militari capaci di lavorare insieme in uno scenario complesso, fatto di domini diversi e minacce ibride? Un osservatorio particolarmente interessante per rispondere a questa domanda è quello dei Blended Intensive Programmes (BIP). Si tratta di programmi europei che combinano una fase online con una fase in presenza e che coinvolgono almeno tre istituzioni di Paesi diversi. Gli studenti lavorano fianco a fianco per periodi relativamente brevi ma intensi che vanno da cinque a trenta giorni, vivendo esperienze di mobilità concentrate, scambi interculturali e un forte ampliamento delle competenze personali e professionali.

Proprio per queste caratteristiche, i BIP si prestano a diventare un laboratorio di analisi, perché contengono gruppi eterogenei, misti di genere e di origine, con differenti background. In relazione agli ultimi risultati raggiunti ed espressi, i BIPs dell'Università di Torino – SUISS e della Scuola Ufficiali di Torino, adottano un modello formativo innovativo basato su apprendimento collaborativo, blended learning e internazionalizzazione, valorizzando la diversità culturale e disciplinare come risorsa educativa. Attraverso gruppi eterogenei, metodologie attive e immersive, uso di ambienti digitali e cooperazione tra studenti civili e giovani ufficiali, i BIPs favoriscono lo sviluppo di competenze trasversali fondamentali per i settori della sicurezza e della difesa, quali comunicazione, leadership, pensiero critico e problem solving. I moduli tematici affrontano ambiti chiave come *problem solving* avanzato, *hybrid threats*, dinamiche di genere, biosicurezza, diritto dei conflitti armati e politiche europee di difesa,

rispondendo alle esigenze degli attuali scenari internazionali e contribuendo alla formazione di professionisti capaci di operare efficacemente in contesti multiculturali e multi-dominio.[25]

Best practices

Durante le attività di ricerca, dai risultati ottenuti è emerso che nel processo di design di curriculum e attività formative-educative nel campo della difesa e sicurezza si manifesta l'opportunità di concentrarsi sull'organizzazione di attività di *collaborative learning* che coinvolgono contemporaneamente studenti civili e militari. Ogni attore dell'ambiente è considerato una risorsa e un'opportunità. Il processo di apprendimento, partendo dall'individualità, si sviluppa attraverso dinamiche di reciprocità, circondate dalla possibilità di uno scambio reciproco di conoscenze, abilità e competenze.

Le attività di *collaborative learning* producono un duplice effetto:

- lo sviluppo delle capacità di lavoro di squadra;
- lo sviluppo delle capacità di cooperazione per future interazioni tra militari e civili.

Sia il lavoro di squadra sia la cooperazione costituiscono la base per l'acquisizione e il consolidamento di capacità di leadership, problem solving e pensiero critico. Tutte queste competenze trasversali sono molto utili per la carriera di un ufficiale o di un civile che desideri operare nel campo della sicurezza e della difesa. Nel lungo periodo, una formazione di base orientata alla cooperazione civile-militare, con la creazione di veri e propri laboratori di *collaborative learning*, potrebbe costituire un potenziale investimento adeguato

[25] Barana, A., et al. 2024b. "Unpacking the Three Spheres of Interest in a Blended Intensive Programme: Collaborative Learning, Blended Learning and Internationalization." In *Proceedings of the 21st International Conference on Cognition and Exploratory Learning in the Digital Age (CELDA 2024)*, 43–50. Zagreb.

alle istituzioni internazionali nella lotta congiunta contro le minacce ibride. I processi concreti e puramente operativi per poter sviluppare tali competenze sono illustrati attraverso una serie di esempi di attività di *collaborative learning* in tabella 1.[26]

[26] Barana, A., Cambria, A., Fissore, C., Floris, F., Fradiante, V., Marchisio Conte, M., Roman, F., Sacchet, M., Salusso, D., and Spinello, E. 2025. "Best Practices." In *Handbook on Teaching Methodology for the Education, Training and Simulation of Hybrid Warfare: An Appendix to the Hybrid Warfare Reference Curriculum*, 43–74. Budapest: Ludovika University. https://doi.org/10.36250/01238_03

	Risultati riscontrati dall'implementazione di determinate attività didattiche implementate				
Attività di gruppo	sviluppare la capacità di comunicare in modo efficace all'interno del gruppo	costruire il pensiero critico	potenziare l'intelligenza emotiva ed empatica	favorire la mediazione e la risoluzione dei conflitti	rafforzare le capacità decisionali
Giochi di squadra	introdurre elementi di *gamification* e situazioni sfidanti	stimolare la motivazione intrinseca e il rispetto delle regole	promuovere il raggiungimento di obiettivi comuni	consolidare legami di fiducia tra i partecipanti	
Simulazioni e giochi di ruolo	simulare situazioni operative realistiche assegnando compiti differenziati	interpretare ruoli specifici in contesti complessi ed emotivamente coinvolgenti	integrare strumenti informatici e piattaforme virtuali per il decision-making in tempo reale		
Analisi di casi di studio	collegare teoria e pratica.	confrontare prospettive differenti grazie a background eterogenei.	sviluppare capacità di analisi e sintesi	identificare elementi critici e punti focali dei casi analizzati	
Dibattiti	esprimere, argomentare e difendere idee in modo strutturato	sviluppare competenze comunicative avanzate	promuovere l'interazione civile-militare	rafforzare il pensiero critico	migliorare la relazione docente-studente
Attività di valutazione tra pari (*peer evaluation*)	fornire feedback costruttivo sul lavoro altrui	rafforzare la fiducia nell'applicazione di criteri condivisi	stimolare l'autovalutazione e la riflessione critica	ridurre l'enfasi sulla valutazione numerica, ma aumentarla su quella concettuale	

Tabella 1. Descrizione dei risultati riscontrati dall'implementazione di determinate attività didattiche.

Le pratiche menzionate, nel momento dell'implementazione e delle attività di osservazione partecipante, hanno mostrato un potenziale impatto positivo sul livello di engagement e di interesse degli studenti, favorendo un innalzamento delle competenze trasversali e delle conoscenze.[27]

[27] *Ibidem,* pp.44. vedi anche Cambria, A., et al. 2023b. *op. cit*. pp. 9441-9448.

Il lavoro di gruppo consente di sviluppare *soft skills* nel campo della comunicazione, poiché gli studenti sono chiamati a gestire dinamiche e attività di mediazione e risoluzione dei conflitti che emergono inevitabilmente nei contesti collaborativi. Inoltre, nei momenti di controversia si necessita di dialogo e capacità decisionali. Il lavoro di gruppo permette di sviluppare la costruzione del pensiero critico osservando un fenomeno da diversi punti di vista per comprenderne le cause e parti dell'intelligenza emotiva ed empatica.

I giochi di squadra, introducendo metodi di gamification, permettono di creare contesti sfidanti che favoriscono la motivazione intrinseca e il rispetto delle regole, strumento fondamentale per sviluppare senso del dovere e responsabilità, soprattutto nella formazione in ambito sicurezza e difesa. Lavorare in squadra implica il raggiungimento di obiettivi comuni, creando forti legami tra i partecipanti.

La simulazione di situazioni reali assegna compiti diversi a studenti civili e militari per comprendere meglio le dinamiche studiate a livello teorico offrendo così la possibilità di sperimentare quanto appreso. Il *role-playing* consiste nell'interpretare ruoli specifici in contesti realistici ed emotivamente coinvolgenti. Questa attività stimola l'apprendimento attraverso imitazione, azione, osservazione dei comportamenti altrui e feedback ricevuti. Con l'ausilio e inclusione di strumenti informatici o piattaforme virtuali che consentono decisioni in tempo reale e interazioni tra i partecipanti.

Le analisi dei casi studio, nell'educazione alla sicurezza e difesa, sono uno strumento privilegiato per collegare teoria e pratica. Il caso di studio può essere analizzato individualmente o in gruppo da studenti civili e militari con background diversi, per confrontare prospettive differenti. Questa attività sviluppa capacità di analisi e di sintesi per identificare i punti focali del caso.

L'aggiunta dei dibattiti, prima e dopo lo studio di un argomento, aiutano ad organizzare discussioni che permettano a studenti civili e militari di esprimere, argomentare e difendere le proprie idee. Questi dibattiti, sviluppano capacità comunicative, promuovono l'interazione civile-militare e rafforza il pensiero critico. I dibattiti contribuiscono al miglioramento dell'interazione tra docente e studenti, in un ciclo continuo di apprendimento maestro-discente.

Un ulteriore elemento emerso dall'analisi è rappresentato dalla *peer evaluation* tra civili e militari aggiunge valore, poiché implica fornire feedback sul lavoro altrui. Tale pratica, rafforza la fiducia nell'applicazione di criteri condivisi ed è prevalentemente formativa, riducendo l'enfasi sui voti. Elemento necessario è la supervisione del docente, al fine di garantire un feedback individuale o collettivo per stimolare, chiarire, correggere e valorizzare.

Conclusioni

Lo scenario contemporaneo pone sfide rilevanti per le Forze Armate e per l'intero Paese, imponendo lo sviluppo di capacità multi-dominio avanzate: nei settori cyber, dell'intelligenza artificiale, della protezione delle supply chain e della difesa dalle minacce cognitive. Risulta imprescindibile un approccio, fondato su un efficace coordinamento interistituzionale e tra gli attori coinvolti nella sicurezza nazionale. In tale contesto, si evidenzia la necessità di valutare approcci alternativi e superare una postura meramente contenitiva a favore di una difesa proattiva e tempestiva, coerente con la natura continua e adattiva della minaccia ibrida.

Il primo obiettivo sarà quello di formare ed educare la leadership militare, attuale e futura, con una *forma mentis* idonea alla comprensione e alla gestione di tutti i domini. Una leardership con un approccio aperto e creativo per ottenere il

risultato richiesto ad un costo accettabile, gestendo una situazione intrisa di interazioni e dinamiche che originano problemi di nuova natura.[28]

Cruciale è lo sviluppo di nuovi modelli di preparazione delle forze, sviluppando un linguaggio comune tra Istituzioni e Cittadino con un approccio di *soft power* volto a rafforzare il senso di appartenenza e l'identità nazionale. Questo processo di crescita culturale deve poi essere approfondito nella formazione della leadership strategica per adeguare il processo decisionale (*decision making*) al nuovo contesto multidimensionale.[29]

Per facilitare l'adozione di pratiche didattiche innovative nell'educazione alla sicurezza e alla difesa, i docenti sono chiamati ad adottare nuove metodologie e a sfruttare efficacemente le tecnologie. Gli approcci educativi non devono limitarsi all'addestramento convenzionale, ma includere quello non convenzionale, affinché i partecipanti possano abituarsi a riconoscere, identificare e contrastare le minacce ibride.

Risulta necessario sviluppare approcci realistici, interdisciplinari, collettivi, non convenzionali, insieme a pensiero critico, creativo e capacità di *problem solving*.[30]

Oggi, tra i vari strumenti utilizzati per l'innovazione didattica, si segnala che UE e NATO stanno adattando la propria struttura e le proprie capacità agli scenari ibridi, sottoponendole a esercitazioni regolari e irregolari. La base di partenza è esporre il personale professionista della Difesa e Sicurezza a diverse scuole di pensiero.[31] L'obiettivo generale di tali esercitazioni è educare i partecipanti e migliorare i meccanismi di risposta a diversi incidenti o crisi legati alle minacce

[28] MINISTERO DELLA DIFESA - Stato Maggiore della Difesa, *op.cit.,* p.*8.*
[29] Ibidem.
[30] Cirdei, I. A. 2023. "Training of the Forces for Carrying Out Military Actions in Operational Environments Characterized by the Existence of Hybrid Threats." *Land Forces Academy Review* 28 (1): 11–19. https://doi.org/10.2478/raft-2023-0002
[31] Lewis, T.M.S., (2009). *op. cit*., p.5.

ibride. Ad un livello strategico, le esercitazioni rafforzano inoltre le relazioni tra le organizzazioni e gli individui coinvolti e possono talvolta essere utilizzate come strumento per confrontare punti di vista e prospettive differenti negli ambienti educativi.[32] A livello tattico, le metodologie didattiche e le *best pracitces* individuate permettono di ottenere un risultato positivo che può essere speso a livello strategico.

Per sviluppare competenze trasversali e cooperative, è necessario disporre di laboratori pratici e sicuri in cui sperimentare buone pratiche.[33] Uno degli elementi fondamentali è lo spirito di adattamento. In situazioni asimmetriche e in ambienti ostili, lo studente deve essere addestrato alla certezza ed educato all'incertezza.[34]

Rispondendo alla domanda posta come centro di gravità per la conduzione della raccolta dati, si può concludere che, in un contesto di difesa e sicurezza, si possono identificare i BIPs, ricchi di attività di CL, BL, e I, come metodologie didattiche innovative utili a formare personale civile e militare in previsione di un contrasto alle minacce ibride.

[32] Hagelstam, A. 2018. "Cooperating to Counter Hybrid Threats." *NATO Review*. NATO.
[33] Cambria, A., Marchisio, M., & Spinello, E. 2023c. "Higher Education Training Activities in International Environments for Developing Skills of Civil-Military Cooperation." In *Proceedings of CELDA 2023 – Cognition and Exploratory Learning in the Digital Age*, 402–406.
[34] NATO SHAPE. 2023. Civil Military Cooperation as a Way to Counter Hybrid Activity. NATO.

Biografie degli autori

LORENZO AVESANI è Junior fellow del Programma Europa presso il Centro Studi Geopolitica.info. Laureato magistrale in Scienze Internazionali e Diplomatiche presso l'Università di Bologna, i suoi interessi vertono sulle dinamiche geopolitiche e di sicurezza dell'Europa centrorientale con enfasi sui Paesi del "Gruppo di Visegrád".

ANNA CALABRESE è Senior Fellow del Centro Studi Geopolitica.info all'interno del Programma Europa, Vice-Coordinatrice del medesimo programma e responsabile editoriale del CSG. Attualmente si occupa di relazioni esterne presso il Centro Studi Americani di Roma. Laureata Magistrale in Scienze Strategiche presso la Scuola di Applicazione dell'Esercito di Torino, i suoi interessi di ricerca vertono su difesa e sicurezza europea e transatlantica, con interesse particolare alla minaccia ibrida e agli aspetti normativi e giuridici delle nuove tecnologie in ambito militare.

ANTONINO CAMBRIA ha conseguito la laurea specialistica in scienze strategiche presso l'Università di Torino. Sta concludendo il dottorato di ricerca al CASD-Unito in scienze strategiche. Il suo campo di ricerca è la formazione e lo sviluppo di competenze interculturali nel contesto della difesa e sicurezza.

ANNALAURA DI MICHELE è laureanda magistrale in Sicurezza Globale presso l'Università La Sapienza di Roma. Ha svolto un tirocinio presso il CASD- Centro Alti Studi Difesa. Si sta specializzando in studi strategici con particolare riguardo nei temi relativi alla guerra ibrida, attenzionando la dimensione marittima e l'analisi dei settori di guerra. É attualmente presidente e fondatrice del progetto "Athena Centro Studi ".

FABIO MAINA è attualmente dottorando in Sicurezza, Rischio e Vulnerabilità presso l'Università di Genova. Ha conseguito la laurea magistrale con lode in Scienze Internazionali presso l'Università di Torino. È inoltre parte del progetto Dossier Difesa come Digital Content Creator, fa parte del Comitato Scientifico del Centro Einstein di Studi Internazionali (CESI). I suoi principali temi di ricerca sono le alleanze militari, la Foreign Policy Analysis, e le relazioni euro-atlantiche.

SARA MARCHETTI è Junior Fellow del Centro Studi Geopolitica.info, dove si occupa di disinformazione e guerra ibrida. È laureata in Scienze Politiche e Relazioni Internazionali presso l'università la Sapienza di Roma, con una tesi sui media americani nella guerra del Golfo, ed attualmente studentessa magistrale in Relazioni Internazionali presso il medesimo ateneo. I suoi interessi di ricerca riguardano la comunicazione e la disinformazione politica, in particolare nell'ambito delle guerre ibride, e il diritto dell'Unione Europea.

JACOPO MARZANO è analista per l'area Medioriente e Nordafrica per "Geopolitica.info" e analista di geopolitica e difesa per "Formiche". Si occupa di minacce ibride, guerre economiche, cognitive e geopolitica delle migrazioni, prediligendo la ricerca e l'analisi sul campo. Ha conseguito la laurea triennale in Scienze Politiche per la Sicurezza Internazionale e quindi la laurea magistrale con lode e menzione d'onore in Investigazione, Criminalità e Sicurezza Internazionale sempre presso l'Università degli Studi Internazionali di Roma (UNINT).

LILIANA NITTI è dottoressa di ricerca in Scienze Politiche e analista Cyber Threat Intelligence presso Yarix. È senior fellow del centro studi Geopolitica.info e junior fellow del Centro Studi Americani. Ha svolto collaborazioni didattiche presso l'Università RomaTre, il Centro Alti Studi per la Difesa e UNINT. In precedenza, ha lavorato presso il NATO Defense College dove ha collaborato

all'organizzazione del 25° Corso Strategico sulla Difesa e la Sicurezza Internazionale in Medio Oriente e la 10^ Senior Executive Regional Conference.

ALESSANDRO PAOLINELLI è collaboratore del Centro Studi Geopolitica.info e studente del corso di laurea magistrale in Relazioni Internazionali ed Istituzioni Sovranazionali presso Sapienza Università di Roma. Il suo principale interesse di studio è l'Underwater Domain e spionaggio scientifico e tecnologico. Ex membro del consiglio direttivo organizzatore di eventi TEDx presso Sapienza, è attualmente addetto alle relazioni esterne per il Centro Studi Americani.

SVEVA CRISTINA PONTIROLI è Junior Fellow presso il Centro Studi Geopolitica.info, dove si occupa di Cina e Taiwan per il desk Indo-Pacifico. I suoi principali interessi di ricerca includono la politica estera cinese, Cross-Strait relations e le dinamiche tra Cina e Stati Uniti. Sta svolgendo una laurea magistrale in Relazioni Internazionali presso la Sapienza Università di Roma. Attualmente collabora con il Taiwan Studies Center della Sapienza ed è coinvolta nell'organizzazione della Conferenza Annuale 2026 della European Association for Taiwan Studies (EATS). È Alumna dello Youth Council dell'Ambasciata degli Stati Uniti a Roma e Junior Fellow presso il Centro Studi Americani.

RACHELE RIGALI è Junior Fellow presso il Centro Studi Geopolitica.info, dove si concentra prevalentemente sulle dinamiche Europa-America Latina, minacce ibride, cybersecurity e disinformazione. Laureanda in Scienze Politiche e Relazioni Internazionali presso la Sapienza Università di Roma, è interessata ai temi della diplomazia e della difesa, con un focus sulle strategie di sicurezza internazionale e sull'analisi delle minacce transnazionali e dei rischi geopolitici.

LORENZO ROSSI è Junior Fellow del Centro Studi Geopolitica.info per il Programma Stati Uniti e Nord America. È studente magistrale in Relazioni Internazionali presso l'Università "La Sapienza" di Roma, laureato con lode in

Scienze Politiche e Relazioni Internazionali. Ha contribuito ad articoli e report sui temi di sicurezza economica, politica industriale e relazioni transatlantiche.

MATTIA SAITTA è collaboratore del Centro Studi Geopolitica.info nell'ambito del programma Europa. Ha conseguito una laurea triennale in Scienze Internazionali e Diplomatiche presso l'Università degli Studi di Genova e prosegue il suo percorso accademico nel medesimo ateneo, dove è iscritto al corso magistrale Security and International Relations. I suoi contributi si concentrano sull'analisi del rapporto tra NATO e Russia, con particolare attenzione alla guerra in Ucraina, alla difesa europea e alle dinamiche di sicurezza internazionale.

DAVIDE SOTGIA è Junior Fellow del Centro Studi Geopolitica.info nell'ambito del Programma Europa. Laureato in Scienze Politiche e Relazioni Internazionali, presso l'università la Sapienza di Roma, con una tesi sulle Medie Potenze. Attualmente studente magistrale in Sicurezza Internazionale presso il medesimo Ateneo. I suoi interessi di ricerca riguardano le questioni europee, in particolare quelle legate alle politiche di difesa e sicurezza.

TOMMASO TARTAGLIONE è Junior Fellow presso il Centro Studi Geopolitica.info, dove si occupa di Corea del Nord all'interno del programma Cina e Indo-Pacifico. I suoi interessi di ricerca riguardano la politica estera, interna e militare della Corea del Nord, la società nordcoreana, le relazioni intercoreane e le dinamiche di sicurezza nella regione. Ha conseguito la laurea magistrale in Scienze politiche e di governo presso l'Università degli Studi di Milano. È analista geopolitico e collaboratore editoriale della rivista Domino, per la quale si occupa dell'analisi di eventi contemporanei e internazionali relativi a Europa, Asia, Americhe e Medio Oriente. Scrive per diverse testate, tra cui Il Caffè Geopolitico, Orizzonti Internazionali, Formiche e Kosmos.

LORENZO ZACCHI è ricercatore del Centro Studi Geopolitica.info dal 2016, per il quale si occupa di Medio Oriente, concentrandosi sull'impatto regionale delle politiche della Repubblica islamica dell'Iran. E' dal 2018 consulente legislativo presso il Senato della Repubblica, occupandosi di tematiche relative a politiche di difesa, politica internazionale e affari europei.

Geopolitica.info

CENTRO STUDI

Il Centro Studi

Il Centro Studi Il Centro Studi Geopolitica.info nasce nel 2004 con l'obiettivo di offrire un contributo al dibattito sulla politica estera, la geopolitica e le relazioni internazionali dalla prospettiva dell'Italia. Le attività del Centro Studi si articolano in tre filoni principali: la pubblicazione della Rivista online Geopolitica.info e la ricerca in materia di politica internazionale e geopolitica; la formazione attraverso i corsi in presenza e i corsi online sulla piattaforma www.onlineducation.it; l'organizzazione di momenti di dibattito pubblico sui temi dell'agenda politica italiana relativi alle relazioni internazionali. Tutte le attività sono consultabili sul sito web www.geopolitica.info.

I Report del Centro Studi

I report del Centro Studi Geopolitica.info sono collezioni di saggi, realizzati dai ricercatori afferenti alle varie aree del Centro, dedicati ai grandi temi dell'attualità della politica internazionale. Pubblicati a cadenza trimestrale, i report si contraddistinguono per il rigore metodologico e la profondità analitica. Combinando insieme accessibilità e solidità scientifica, essi offrono analisi rigorose e tempestive sui principali dossier della scena globale.

Centro Studi Geopolitica.info

www.geopolitica.info | centrostudi@geopolitica.info