New Direction
the Foundation for European Conservatism

Costantino Pistilli

SENZA DICHIARAZIONE

Minacce ibride nell'area euroatlantica

New Direction

the Foundation for European Conservatism

New Direction – Foundation for European Conservatism is the official foundation of the European Conservatives and Reformists family at the European level. Founded in 2009 under the patronage of Margaret Thatcher, New Direction is the intellectual home of Europe's growing conservative movement, giving a voice to national movements that promote the rule of law, traditional values, free markets, and respect for the principle of protecting national sovereignty.

Through research, reports, lectures, conferences, and working groups, New Direction helps to inform the work of conservative lawmakers at the European, National, and regional level. At the same time, New Directions Summer University and series of Academies helps to bring conservative principles to a new and younger generation. By equipping politicians and activists with the tools they need, New Direction stands ready to help take the movement forwards.

newdirection.online @ndconservatism

New Direction is registered in Belgium as a not-for-profit organisation and is partly funded by the European Parliament.
The European Parliament and New Direction assume no responsibility for the opinions expressed in this publication. Sole liability rests with the author.

SOMMARIO

1

INTRODUZIONE

La condanna nel luglio 2025 di tre uomini per l'incendio doloso di un magazzino londinese usato da aziende ucraine rappresenta solo la punta dell'iceberg di una più ampia strategia di destabilizzazione che ha investito l'Europa tra il 2024 e i primi mesi del 2025. Un tribunale britannico ha riconosciuto colpevoli i tre imputati per l'attacco incendiario, avvenuto nel marzo 2024, contro il magazzino utilizzato da due imprese di un imprenditore ucraino. L'incendio provocò danni per circa 1,2 milioni di euro e distrusse materiale destinato all'Ucraina, inclusi generatori e terminali del servizio satellitare Starlink. Dieci giorni dopo, quando un magazzino appartenente alla stessa azienda venne incendiato nella capitale spagnola Madrid, gli investigatori capirono che si trattava di un incendio molto più grave di un semplice incendio doloso.

Già nel luglio 2024 erano stati intercettati due pacchi incendiari destinati al trasporto aereo internazionale, uno in un centro logistico DHL a Birmingham e l'altro a Lipsia. Secondo fonti di sicurezza, l'ordigno trovato in Germania era destinato a un volo transatlantico diretto verso Stati Uniti o Canada e, se fosse esploso in volo, avrebbe potuto provocare un grave disastro aereo.

Questi episodi rientrano in un *pattern* di sabotaggi fisici, che comprendono danni a cavi sottomarini, reti ferroviarie, stabilimenti strategici e depositi di munizioni in vari Paesi dell'Area euroatlantica. Le indagini segnalano frequenti atti dolosi. Contemporaneamente, il fronte digitale è stato colpito da attacchi DDoS (*Distributed Denial of Service*) e intrusioni, che hanno coinvolto portali pubblici, infrastrutture critiche e servizi essenziali.

Tentativi di *phishing* hanno preso di mira i ministeri della Difesa e dell'Interno di vari Paesi, mentre interferenze GPS[1] nei cieli baltici e scandinavi hanno causato ritardi e dirottamenti di voli civili. Sul piano della manipolazione informativa, l'attacco informatico alla *Polska Agencja Prasowa* ha portato alla diffusione di una *fake news* sulla mobilitazione di 200.000 riservisti polacchi, rapidamente smentita dal Governo; l'episodio ha evidenziato l'impatto destabilizzante della disinformazione, amplificata da reti di siti web clone che replicavano testate giornalistiche legittime per diffondere contenuti ostili.

Mentre in Francia, azioni simili hanno visto il posizionamento di bare funebri finte vicino alla Torre Eiffel, con scritte contro la partecipazione della Francia in Ucraina, parte di una campagna di disinformazione volta a minare il sostegno pubblico e influenzare le elezioni europee. Questi contenuti venivano diffusi da account automatizzati e *bot* in decine di lingue, spesso accompagnati da *deepfake* e manipolazioni audiovisive, mostrando come la disinformazione possa diventare uno strumento diretto di guerra ibrida.

Sabotaggi materiali, cyberattacchi e campagne di disinformazione – pur nella loro eterogeneità di forma e scala – convergono verso una medesima logica operativa: quella della guerra ibrida. Un conflitto che agisce nella "zona grigia", uno spazio ambiguo e fluido ma concretamente pericoloso, sospeso tra l'azione pacifica e l'ostilità dichiarata, dove la destabilizzazione diventa arma strategica.

Se in Europa si fa riferimento alla "guerra ibrida" o "minaccia ibrida", negli Stati Uniti è prevalente il termine "influenza straniera maligna"; mentre nell'Indo-Pacifico si parla di "tattiche della zona grigia". Indipendentemente dalla terminologia adottata, gli strumenti utilizzati rientrano spesso nel modello DIMEFIL (*Diplomatic*, *Information*, *Military, Economic*, *Financial*, *Intelligence*, *Law Enforcement*)[2]. Le pratiche più frequenti includono interferenze nei processi elettorali, coercizione economica, manipolazione dell'informazione, gestione politica dei flussi migratori, sabotaggi alle infrastrutture critiche e attacchi informatici. Tali attività, difficili da attribuire con certezza a un determinato aggressore, sono generalmente concepite per mantenersi al di sotto la soglia (*sub-threshold*) del conflitto armato. Come evidenziato anche dalle audizioni parlamentari italiane[3], il fine ultimo è quello di ridurre la resilienza interna delle democrazie, sfruttando eventuali vulnerabilità istituzionali, economiche, sociali e cognitive.

Il punto di forza di queste tattiche è la loro natura asimmetrica e multidimensionale. Sono difficili da prevedere, complicate da contrastare e spesso onerose da neutralizzare. La "zona grigia" non è una formula astratta, ma uno spazio operativo concreto, dove la conflittualità è costante e strisciante. In

1 Il 31 agosto 2025 l'aereo che trasportava il Presidente della Commissione europea Ursula von der Leyen ha subito interferenze a Plovdiv, in Bulgaria, costringendolo a sorvolare l'aeroporto per un'ora e atterrare senza GPS. Il jamming blocca i segnali e lo spoofing inganna la posizione, aumentando i rischi. Problemi simili erano capitati a luglio 2025 a Carsten Breuer, e la Lituania ha denunciato un picco di interferenze attribuito alla Russia.

2 Hybrid Threats and Modern Political Warfare: The Architecture of Cross-Domain Conflict (*The Jamestown Foundation*, 2025. Beniamino Irdi)

3 Minacce ibride: come difendere la democrazia nel XXI secolo

questa ottica, qualsiasi realtà della vita quotidiana diventa potenzialmente un campo di battaglia: l'economia, la tecnologia, i media, la dimensione legale, quella cognitiva e quella sociale. Navi commerciali usate per danneggiare cavi sottomarini; forniture energetiche trasformate in strumenti di pressione geopolitica; flussi migratori resi arma (*weaponized migration*); campagne di disinformazione volte a minare la fiducia interna. Qualsiasi elemento civile può essere trasformato in strumento offensivo.

Solamente nell'anno 2024, nell'Unione Europea sono stati segnalati circa 10.000 attacchi informatici. Di questi, il 41,1% ha riguardato campagne DDoS, il 25,7% è stato attribuito a malware e il 19% ha coinvolto violazioni di dati personali. I settori maggiormente colpiti includono la pubblica amministrazione (19%), i trasporti (11%) e l'ambito bancario e finanziario (9%).

Questi dati sono contenuti nel rapporto annuale dell'ENISA[4] che costituisce un pilastro fondamentale per la resilienza informatica all'interno dell'Unione.

Negli ultimi anni, la Federazione Russa, la Repubblica Popolare Cinese -e con differenti intensità e ingerenza anche la Repubblica Islamica dell'Iran e la Repubblica Popolare Democratica di Corea- hanno aumentato le loro operazioni ibride contro i Paesi dell'area euro-atlantica, impiegando approcci multidimensionali. Un'alleanza cristallizzata in particolar modo dalla cooperazione strategico-militare implementata durante il conflitto in Ucraina iniziato nel 2022 con l'invasione perpetrata dalla Federazione Russa. Il loro obiettivo è chiaro: sfruttare le fragilità intrinseche delle società aperte. Vale a dire, attaccare attraverso ciò che rende le rende tali: libertà e tolleranza. Senza una dichiarazione di guerra.

4 L'agenzia europea responsabile della supervisione dello stato della sicurezza informatica nell'UE

2

MINACCE IBRIDE, ZONA GRIGIA, INFLUENZA MALIGNA STRANIERA

Il termine "guerra ibrida" non designa una nozione astratta, bensì rappresenta un concetto di rilevanza ormai consolidata all'interno del dibattito politico, strategico e accademico. Tuttavia, questa minaccia viene talvolta sottovalutata, non riconosciuta, oppure, nei casi più critici, persino confutata. Nel tempo l'evoluzione dei conflitti armati ha evidenziato come la guerra abbia superato il tradizionale confronto diretto o l'impiego esclusivo dei sistemi d'arma convenzionali. Oggi il conflitto ingloba strumenti sia convenzionali che non convenzionali, coinvolgendo elementi militari e civili, armi classiche e tecnologie avanzate. Fenomeni quali propaganda, disinformazione, attacchi di natura economica, pressioni politiche e operazioni informatiche si manifestano congiuntamente all'interno del medesimo spazio operativo. Di conseguenza, un'analisi approfondita di queste dinamiche richiede l'integrazione di prospettive storiche, dottrinali, politiche e culturali, andando oltre la sola dimensione militare.

Mao Zedong, padre della rivoluzione cinese e della dottrina della guerra popolare che doveva coinvolgere l'intera società, già nel 1937 con *On Guerrilla Warfare* spiegava come forze più deboli potessero mettere in difficoltà eserciti molto più potenti sfruttando tattiche irregolari, il sostegno popolare e la mobilità sul terreno. Decenni dopo, gli storici militari Allan R. Millett, Williamson Murray e Kenneth H. Watman, nel volume *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (2012), hanno mostrato che la commistione tra guerra regolare e irregolare è un filo rosso che attraversa i secoli: dalle legioni romane alle campagne moderne. Oggi, però, quel modello si trasforma, spinto da nuovi equilibri geopolitici e dalle nuove tecnologie.

È in questo contesto che nasce il concetto di "minaccia ibrida". Nelle guerre vengono utilizzati strumenti meno visibili ma altrettanto incisivi: propaganda, pressione economica, operazioni clandestine, fino ad arrivare ai cyber-attacchi e alle campagne di disinformazione digitale. Andrew Mumford[5], studioso britannico di conflitti contemporanei, nel 2013 descrive la guerra ibrida come un *continuum* che va dallo scontro convenzionale fino a forme di lotta non dichiarata. Si tratta di quelle che in ambito militare vengono chiamate *grey-zone operations*: azioni condotte nella "zona grigia", calibrate per restare al di sotto della soglia di un conflitto aperto ma con l'obiettivo preciso di destabilizzare l'avversario.

L'obiettivo principale consiste nell'indebolire internamente le democrazie, minando la fiducia dei cittadini nelle istituzioni e manipolando le informazioni, sfruttando aree di ambiguità in cui la verità viene reinterpretata o trasformata in post-verità. L'avvento del cyberspazio e, più recentemente, il consolidamento delle nuove tecniche di *machine learning* ed *e-learning* (come l'Intelligenza Artificiale generativa) hanno consentito alle minacce ibride di evolversi notevolmente. Tali minacce non sono più fenomeni isolati, ma costituiscono una strategia permanente, diffusa e difficilmente rilevabile, in grado di agire senza essere identificata. Lo scopo non è quello di occupare territori, bensì di paralizzare i processi decisionali; non si tratta di invadere fisicamente, ma di destabilizzare. Si configura così una forma di conflitto silenzioso, privo di confini temporali o geografici, che incide progressivamente sulla legittimità politica e sulla fiducia sociale nelle proprie istituzioni.

5 Ambiguity in hybrid warfare (2020)

3

NORTH ATLANTIC TREATY ORGANIZATION

Per il *North Atlantic Treaty Organization* (NATO) le minacce ibride non sono un concetto astratto, ma una realtà quotidiana che segna il confine più incerto tra sicurezza e instabilità. L'Alleanza atlantica definisce "ibrido" tutto ciò che combina strumenti militari e non militari, azioni visibili e occulte, con lo scopo di rendere labile la distinzione tra pace e conflitto. Non è un caso che già dal vertice di Varsavia del 2016 sia stato riconosciuto ufficialmente che anche un attacco ibrido, se sufficientemente grave, può giustificare l'attivazione dell'Articolo 5 del Trattato di Washington – la clausola di difesa collettiva che obbliga tutti i membri a considerare un'aggressione a uno di loro come un'aggressione all'intera Alleanza. È un passaggio storico: significa ammettere che la guerra oggi non si combatte solo con carri armati e aerei, ma anche con *malware*, sabotaggi energetici e campagne di disinformazione.

Per affrontare questa nuova dimensione, nel 2017 la NATO ha creato una Divisione per le minacce ibride, con capacità autonome di intelligence e risposta rapida. L'anno successivo sono nati i *Counter Hybrid Support Teams*, squadre di esperti che gli Stati membri possono richiedere per rafforzare la resilienza nazionale. Questi gruppi sono già stati schierati in Paesi esposti a pressioni esterne, come il Montenegro, la Lituania e la Norvegia, dove hanno contribuito a proteggere infrastrutture critiche e a gestire operazioni di destabilizzazione.

Negli ultimi anni l'impegno si è esteso a domini ancora più delicati. Nel 2024 la NATO ha inaugurato nel Mare del Nord un Centro per la protezione delle infrastrutture sottomarine, dotato di sistemi avanzati di sorveglianza su cavi energetici e reti digitali: una risposta diretta agli episodi di sabotaggio che hanno mostrato quanto siano vulnerabili le dorsali energetiche e le connessioni globali. Parallelamente, nell'ambito della Task Force X, è stata sviluppata una rete di droni navali e sottomarini capaci di pattugliare autonomamente aree strategiche, moltiplicando le possibilità di deterrenza.

La formazione gioca un ruolo centrale. La NATO collabora stabilmente con l'Hybrid CoE (*Hybrid Centre of Excellence*) di Helsinki, un centro internazionale dedicato alla ricerca e alla simulazione di scenari ibridi. Non si tratta solo di addestramento tecnico, ma di un laboratorio che unisce civili e militari, studiosi e operatori sul campo. Anche il NATO *Defence College* di Roma ha contribuito con studi strategici sul tema, sottolineando come le minacce ibride non vadano viste come eventi isolati, ma come una pressione costante.

Inoltre, nel 2024 la maxi-esercitazione *Steadfast Defender* ha integrato scenari cyber, simulazioni di sabotaggio alle reti energetiche e persino moduli di guerra cognitiva, mettendo alla prova la capacità degli alleati di rispondere in modo coordinato. Al vertice de L'Aia del 2025 i membri dell'Alleanza Atlantica hanno compiuto un ulteriore passo, impegnandosi a destinare il 5% del PIL alla sicurezza nazionale, con almeno il 30% riservato a resilienza e difesa contro minacce ibride e informatiche.

Il messaggio è chiaro: la NATO sa che la guerra moderna non è fatta solo di truppe e missili, ma di attacchi invisibili che colpiscono opinioni pubbliche, reti energetiche e sistemi digitali. È un campo in cui la tecnologia corre velocissima, e in cui i nuovi approdi tecnologici come l'IA generativa -capace di creare testi, immagini, video e contenuti inediti- aprono possibilità inedite per la manipolazione e la propaganda. In questo senso, la sfida non è soltanto militare, ma anche sociale e culturale: si combatte tanto nello spazio cibernetico quanto nella mente dei cittadini.

4

L'UNIONE EUROPEA E IL CONTRASTO ALLE MINACCE IBRIDE

L'Unione Europea ha dovuto imparare presto che gli attacchi ibridi non sono solo scenari militari, ma realtà capaci di colpire cittadini, istituzioni e imprese. Un esempio concreto è arrivato nell'estate del 2025, quando un'operazione internazionale coordinata da Europol ed Eurojust ha smantellato la rete del gruppo pro-russo *NoName057*. Attivo dal 2022, questo collettivo *haker* era responsabile di centinaia di attacchi informatici contro governi, media e aziende europee e nordamericane. Non si trattava di un'organizzazione tradizionale, bensì di una comunità digitale che operava tramite un software distribuito su Telegram, chiamato *DDoSia*, usato da migliaia di volontari.

L'operazione, denominata *Eastwood*, ha visto la collaborazione di undici Paesi, tra cui Francia, Germania, Italia, Polonia, Spagna, Svezia e Stati Uniti. Sono stati effettuati arresti, perquisizioni e soprattutto la disattivazione di oltre cento server. In Germania, le autorità hanno emesso sei mandati d'arresto internazionali, mentre la Spagna ne ha ottenuto uno aggiuntivo. Parallelamente, più di mille utenti attivi sulla piattaforma sono stati avvertiti delle implicazioni legali delle loro azioni. Questo passaggio, spesso trascurato, è significativo: dimostra che oggi i confini tra "hacker attivista" (*haktivista*) e criminale non sono più netti, e che anche chi partecipa in modo apparentemente ludico può essere chiamato a rispondere davanti alla legge.

La forza di *NoName057(16)* stava proprio nella *gamificazione*: i volontari non erano motivati soltanto da ideologia, ma da dinamiche tipiche dei videogiochi, come classifiche pubbliche, *badge* e premi in criptovalute. Gli obiettivi degli attacchi, aggiornati quotidianamente, puntavano a creare risonanza mediatica più che veri danni operativi. Bastava colpire un sito governativo nel giorno di un *summit* internazionale o durante una visita del presidente ucraino Volodymyr Zelensky per ottenere titoli sui giornali e amplificare la percezione di vulnerabilità.

A questi attacchi cibernetici si sommano campagne di disinformazione strategica, che hanno come obiettivo diretto i leader politici europei. Nel 2025, ad esempio, sono emersi episodi di propaganda russa su larga scala rivolti a screditare figure quali i presidenti Emmanuel Macron e Giorgia Meloni. Emblematico un video[6] diffuso sui canali russi suggeriva un uso improprio di narcotici da parte dei due leader europei, amplificando speculazioni. In Italia, la propaganda ha manipolato le immagini della premier Meloni durante un vertice NATO, insinuando feste e comportamenti inappropriati con il presidente ucraino, per minarne la credibilità e creare divisioni nell'opinione pubblica. Questi episodi mostrano chiaramente come la disinformazione possa essere orchestrata con precisione, sfruttando piattaforme digitali e social media per raggiungere un pubblico vasto e generare dubbi sulla stabilità democratica.

Di fronte a tali fenomeni l'UE ha cercato di definire un quadro chiaro. Nello *Strategic Compass*[7] del 2022 le minacce ibride sono descritte come azioni coordinate che usano strumenti diplomatici, militari, economici e tecnologici per sfruttare vulnerabilità degli Stati membri senza dichiarare guerra. Colpire nelle aperture delle nostre democrazie, sfruttando zone grigie legali e tecnologiche. Per affrontare le minacce ibride Bruxelles ha elaborato un toolkit integrato che include misure di prevenzione, protezione e risposta. Le azioni adottate riguardano la difesa informatica, la resilienza energetica, il monitoraggio della manipolazione informativa e il coordinamento delle sanzioni. Dal 2023 è operativo l'Osservatorio europeo sulle minacce ibride, che raccoglie dati su disinformazione, incidenti informatici e sabotaggi, lavorando in collaborazione con l'*Hybrid CoE* di Helsinki. Nel 2024 sono state attivate le *Hybrid Rapid Response Teams*, composte da specialisti in cyber-sicurezza, comunicazione strategica e logistica, che possono essere impiegati su richiesta in diversi Paesi, tra cui Moldavia, Balcani occidentali e Lettonia.

Il coordinamento delle attività dell'Unione Europea volte al contrasto della disinformazione è affidato al Servizio Europeo per l'Azione Esterna (SEAE). Parallelamente, l'UE ha favorito la costituzione dell'Osservatorio Europeo dei Media Digitali (EDMO) con l'obiettivo di potenziare le competenze e rafforzare la capacità di verifica delle informazioni. EDMO, realtà indipendente che riunisce *fact-checker*, accademici ed esperti di alfabetizzazione mediatica, si occupa dell'analisi dei fenomeni di disinformazione, della promozione di servizi

6 "Meloni si droga", l'allusione a un festino con Zelensky con cocaina e alcool dopo l'intervista al vertice Nato – il VIDEO di Russia Today

7 La Bussola strategica per la sicurezza e la difesa è un documento di roadmap redatto dal Servizio europeo per l'azione esterna nel 2022 per rafforzare la politica di sicurezza e di difesa dell'UE entro il 2030

di *fact-checking* e del supporto alle autorità pubbliche. L'osservatorio si articola in un *hub* centrale situato a Firenze, connesso ad altri 14 *hub* nazionali o regionali distribuiti nei Paesi membri dell'Unione Europea. Questa rete favorisce la cooperazione transfrontaliera, lo svolgimento di indagini congiunte su campagne di disinformazione a livello comunitario e la redazione di *briefing* mensili sulle tendenze emerse.

Mentre sul piano normativo, nel 2024 è entrata in vigore la direttiva NIS2 (*Network and Information Security Directive*) che introduce requisiti più stringenti per i settori energia, sanità, trasporti, finanza e digitale. L'ENISA (*European Network and Information Security Agency*) ha ricevuto ulteriori competenze per l'ispezione e la valutazione del rischio. Nel luglio 2025 il Consiglio dell'UE ha invece ampliato la lista FIMI (*Foreign Information Manipulation and Interference toolbox*), applicando congelamenti di beni e restrizioni sui visti a individui e organizzazioni coinvolti in manipolazione informativa, attacchi informatici o sabotaggi. Misure che hanno prodotto effetti positivi nel contrastare le minacce ibride.

Come la campagna *Doppelgänger*[8], segnalata dall'EU Disinfo Lab nel settembre 2022. Si tratta di un'operazione russa di FIMI mirata a manipolare l'opinione pubblica, indebolire il sostegno all'Ucraina e creare divisioni tra Paesi europei. Per farlo, diffonde disinformazione tramite cloni di siti governativi e media legittimi, amplificata su social come X e Facebook, sfruttando tecniche di *typosquatting* [9]che la rendono credibile.

Esempi di contenuti falsificati su domini clonati

Fonte: EUvsDisinfo 2024

I contenuti sono poi calibrati in base ai singoli Paesi: in Francia puntano su migrazione e guerra in Ucraina, in Germania su energia e clima, in Polonia su rifugiati e conflitto. L'infrastruttura alla base della campagna comprende domini che imitano testate giornalistiche note come *Die Welt*, *Le Point*, *La Stampa*, *La Repubblica* e *Polskie Radio*, registrati tra gennaio e maggio 2024, poco prima delle elezioni europee di giugno dello stesso anno.

8 Il termine tedesco *Doppelgänger* si riferisce a un sosia, un "doppio" di una persona vivente, che può essere inteso come una copia fisica o spirituale. Le principali tecniche includono la creazione di domini con errori di battitura comuni (es. "google.con"), l'uso di errori di spelling (es. "gogle.com"), la riformulazione del nome (es. "google.com" invece di "googles.com"), o l'utilizzo di Top-Level Domain (TLD) diversi (es. "google.org" invece di "google.com").

9 Chiamati anche URL hijacking, tali attacchi si basano sulla registrazione di nomi di dominio simili a quelli legittimi per sfruttare gli errori di battitura degli utenti, indirizzandoli verso siti fraudolenti

5

REGNO UNITO: MINACCE IBRIDE E INTERFERENZE STATALI

Il Regno Unito è da tempo bersaglio di operazioni ibride condotte da attori statali ostili che vanno ben oltre il tradizionale spionaggio, includendo sabotaggi, rapimenti, tentativi di omicidio, cyber-attacchi e interferenze politiche. Nel suo rapporto sulla Russia, pubblicato nel luglio 2020, la Commissione per l'intelligence e la sicurezza del Parlamento britannico ha definito l'influenza russa nel Regno Unito "la nuova normalità"[10]. Nel 2024, ad esempio, tre cittadini bulgari sono stati condannati per spionaggio a favore della Russia: facevano parte del gruppo *Honeytrap*, che ricorreva a seduzione, intercettazioni telefoniche e attacchi informatici per colpire diplomatici e attivisti. L'ostilità russa ha precedenti noti: l'avvelenamento di Alexander Litvinenko nel 2006 e il caso Skripal nel 2018 con l'agente nervino *Novichok* hanno segnato escalation di violenza sul suolo britannico. Con l'invasione russa dell'Ucraina, Mosca ha intensificato una strategia mista che punta a infiltrarsi nelle reti economiche, politiche e culturali del Regno Unito, destabilizzare valori occidentali e diffondere narrazioni filorusse.

Londra ha attirato oligarchi russi fin dagli anni Novanta, favorendo investimenti in media, club calcistici e persino nel sistema politico[11]. Sul piano informatico, il servizio di intelligence militare russo ha orchestrato campagne di *phishing* contro il Foreign and Commonwealth Office – FCO (Ministero degli Esteri e del Commonwealth britannico) e il DSTL (*Defence Science and Technology Laboratory*, laboratorio scientifico-tecnologico della difesa), tentando di infiltrarsi nelle *Critical National Infrastructures* (infrastrutture critiche nazionali), spesso in collaborazione con reti criminali.

Particolarmente delicata è poi la questione dei cavi sottomarini che rappresentano per il Regno Unito un'infrastruttura strategica vitale, dato che trasportano quasi il 99 % del traffico dati intercontinentale e sostengono settori cruciali come finanza, difesa e comunicazioni civili. Questa centralità li rende un obiettivo privilegiato nella *grey-zone warfare*. Negli ultimi anni Londra è stata ripetutamente indicata come un *hub* critico dell'Atlantico e quindi altamente vulnerabile a sabotaggi sottomarini o a operazioni di sorveglianza clandestina. Un rapporto del *China Strategic Risks Institute* ha registrato tra il 2021 e il 2025 ben dodici episodi sospetti di manipolazione o avvicinamento anomalo ai cavi, attribuiti a navi legate a Russia o Cina. Tale vulnerabilità è stata riconosciuta anche dal Governo britannico, che ha avviato una revisione legislativa e strategica per colmare i vuoti nella protezione. Parallelamente Londra ha rafforzato le proprie capacità operative.

The UK has around 60 undersea cables that come ashore at various points along its coastline.

Fonte: BBC 2025

10 *Countering Russian influence in the UK* (2025)

11 Secondo l'*Intelligence and Security Committee Russia report* (2020) ci sono prove sostanziali che l'interferenza russa nell'economia e nella politica britannica è comune; inoltre, sono state scoperte prove che dettagliano l'interferenza nel referendum sull'indipendenza scozzese del 2014, volto a promuovere l'indipendenza scozzese nel tentativo di dividere e conquistare il Regno Unito.

Il rischio non è teorico. Nel gennaio 2025 la nave russa Yantar[12] è stata avvistata in prossimità delle acque britanniche: ufficialmente un vascello da ricerca oceanografica, in realtà dotato di sistemi per mappare e potenzialmente manipolare i cavi e per monitorare i sottomarini nucleari della *Royal Navy*. L'episodio ha spinto Londra a una risposta di forza, con l'emersione deliberata di un sottomarino britannico nelle vicinanze della nave russa: un segnale politico destinato a scoraggiare ulteriori incursioni. Secondo fonti militari, la Yantar ospita dispositivi subacquei in grado non solo di raccogliere intelligence, ma anche di condurre operazioni di sabotaggio mirato.

Tali episodi dimostrano come la protezione dei cavi sottomarini sia oggi al centro della sicurezza nazionale britannica.

Di fronte a tali minacce, la NATO ha avviato l'operazione *Baltic Sentry* con fregate, droni e pattugliamenti nei mari baltici, mentre il Regno Unito ha rafforzato la sorveglianza navale con la RFA Proteus (*Royal Fleet Auxiliary Proteus*, nave da supporto ausiliaria) e sistemi autonomi sottomarini, e ha avviato con Paesi Bassi e Norvegia l'operazione *NorthSeal* per proteggere le infrastrutture del Mare del Nord. La protezione dei cavi è ormai riconosciuta come parte integrante della sicurezza nazionale e della strategia occidentale contro la guerra ibrida russa, insieme a sanzioni mirate, al controllo della flotta ombra e alle iniziative multilaterali UE–UK, come il vertice di Londra del maggio 2025, che ha rilanciato la cooperazione sulla sicurezza dopo la Brexit.

12 UK Shadows Russian Ship Yantar in Demonstration of Surveillance Role in Deterring CUI threats (2025)

6

MASKIROVKA

Maskirovka è un principio centrale della dottrina militare e di intelligence russa (prima sovietica), traducibile come "mascheramento" o "inganno". Indica un insieme di pratiche pensate per nascondere capacità, intenzioni e piani al nemico, facendo leva sul segreto e sulla manipolazione. Le tecniche non sono rigide: richiedono inventiva, risorse e una costante capacità di adattamento, perché devono funzionare su piani tattici, operativi e strategici diversi. Parte integrante della *maskirovka* sono le cosiddette "misure attive", descritte da Vasiliy Mitrokhin nel Lessico del KGB del 2002. Si tratta di operazioni condotte da agenti per influenzare, persuadere, intimidire o attrarre individui e gruppi, con l'obiettivo di facilitare la politica sovietica. In questo senso, la *maskirovka* non si limita al camuffamento militare: ingloba manipolazione psicologica e politica, trasformandosi in uno strumento coordinato di guerra e intelligence.

Dall'invasione dell'Ucraina nel 2022 Europa e Regno Unito sono immersi in una guerra "ombra" orchestrata da Mosca. L'attacco combina cyberoperazioni, sabotaggi, disinformazione e manipolazioni economiche e migratorie, con l'obiettivo di indebolire la coesione democratica, ridurre il sostegno a Kiev e fratturare le istituzioni occidentali. La disinformazione, *dezinformatsiya*, è diventata un pilastro permanente della strategia russa. Non si tratta tanto di convincere quanto di confondere: Mosca moltiplica versioni contrastanti, genera sfiducia e paralizza il dibattito pubblico. È una continuità delle "misure attive" sovietiche — falsificazione, disinformazione, operazioni politiche — aggiornate con *social network*, *deepfake* e Intelligenza Artificiale generativa. Al centro dell'apparato ci sono servizi segreti, media statali come RT e Sputnik, organizzazioni di facciata, *troll farm* e reti di influencer che diffondono contenuti manipolati in maniera sistematica.

Misure attive sovietiche: Falsificazione, Disinformazione, Operazioni Politiche (1981).

Approved For Release 2007/03/21 : CIA-RDP84B00274

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

FROM: PCS/PGLO

EXTENSION: [redacted] NO: 25X1 25X1

DATE: 8 February 1982

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. C/PCS/PGLO		A		Attached is a paper entitled "Soviet 'Active Measures': Forgery, Disinformation, Political Operations," which is an unclassified State Department summary of a classified paper produced by IAD [redacted]. The State Department released the paper at a press conference in October 1981. 25X1
2.				
3. C/EPDS				
4.				
5. SA/ODDO				As requested by the DCI (see attached reference) the attached copy of "Soviet 'Active Measures" is for transmittal to Representative William Dickinson (R. Al.), the ranking minority member of the House Armed Services Committee. The two other papers requested by the DCI are DDI papers.
6.				
7. [redacted] Legislative Liaison				25X1
8.				
9.				

Documento della CIA declassificato

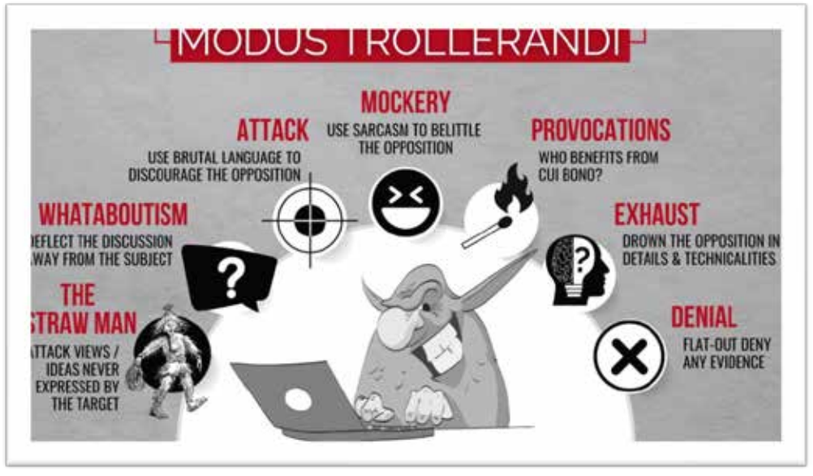
Il Regno Unito è bersaglio di cyberattacchi russi dal 2016. Nel 2025 il MI5 ha denunciato "sforzi prolungati" su infrastrutture energetiche, sanitarie, agricole e di telecomunicazioni. Reti pro-Russia, tra cui gli hacktivisti NoName057, hanno colpito siti governativi e summit NATO con attacchi DDoS. Europol conferma centinaia di azioni di sabotaggio e incendi dolosi attribuiti a network legati a Mosca e alla compagnia militare privata Wagner. Mentre nel 2024-2025, l'UE ha registrato oltre 500 operazioni di manipolazione digitale su 38.000 canali. In Germania, il gruppo Storm-1516 ha diffuso *fake news* su migrazioni e scandali inventati, favorendo indirettamente movimenti populisti filorussi. Quest'anno Londra ha imposto nuove sanzioni a 18 ufficiali e tre unità della GRU responsabili dell'attacco al teatro di Mariupol nel marzo 2022, che provocò

circa 600 morti, tra cui numerosi bambini. Tra le unità sanzionate figurano l'Unità 26165, nota per cyberattacchi dal 2013, e l'Unità 74455, coinvolta in offensive contro il Ministero degli Esteri britannico. Le misure colpiscono anche organizzazioni di facciata come *l'African Initiative*, utilizzate per propaganda antivaccini e campagne disinformative in Africa.

Le democrazie liberali si fondano sul libero scambio di idee, principio che la dottrina russa sfrutta come vulnerabilità. Difatti *fact-checking* e smentite non bastano contro un apparato adattivo e in continua evoluzione. La strategia di Mosca combina manipolazione dei contenuti e tecniche di diffusione avanzate, intrecciando dominio informativo, operazioni cibernetiche e azioni fisiche. Tra le tattiche più sofisticate vi sono gli "alibi informativi"[13]: falsi diffusi in anticipo per deviare la responsabilità di crimini o operazioni militari. Emblematico il caso del teatro di Mariupol, presentato come provocazione ucraina prima che venisse bombardato. Al tempo stesso la storia viene riscritta e piegata a fini politici. L'equiparazione dell'Ucraina al nazismo, con un aumento del 300% dell'uso del termine "nazista" nei media russi alla vigilia dell'invasione, ne è un esempio.

Il "*whataboutism*" resta una tecnica chiave: rispondere a critiche con contro-accuse scollegate, creando false simmetrie morali. Per esempio, parlando dell'invasione russa in Ucraina, la risposta tipica potrebbe essere "ma cosa dite di Gaza?". Un altro esempio da manuale: dopo il disastro di Chernobyl, l'agenzia di stampa statale sovietica TASS pubblicò resoconti sugli incidenti negli impianti nucleari degli Stati Uniti, come le centrali nucleari di Three Mile Island e Jinnah. I propagandisti sovietici affermarono che il gruppo antinucleare americano aveva registrato 2300 incidenti e altri malfunzionamenti nel 1979.

How Democracy is SWAMPED: Seven Cheap Tricks.



Fonte: EUvsDisinfo (2024)

Le narrative circolano secondo un doppio flusso: da dichiarazioni ufficiali poi amplificate da media, *bot* e *influencer*, oppure da fonti marginali rilanciate dai media statali per accreditarle come opinioni diffuse. Il Comportamento Inautentico Coordinato[14] sfrutta reti di account automatici e umani per simulare consenso, pilotare hashtag e colpire critici. La clonazione di siti di testate giornalistiche autorevoli permette di diffondere articoli falsi, credibili per via del formato. Le campagne sono poi propagate su più piattaforme – X, Facebook, Instagram, YouTube, TikTok e Telegram – anche tramite inserzioni a pagamento. L'intelligenza artificiale generativa ha moltiplicato la produzione di articoli, *post* e *deepfake* multilingua, impersonando figure pubbliche o fabbricando prove. Parallelamente, la disinformazione identitaria colpisce target specifici, ottenendo fiducia e inserendo contenuti divisivi. Tecniche SEO avanzate garantiscono visibilità nei primi risultati dei motori di ricerca.

Queste operazioni non avvengono isolate: spesso accompagnano o anticipano attacchi informatici a infrastrutture critiche, enti governativi e aziende strategiche, o azioni fisiche condotte da proxy per ridurre la tracciabilità. L'episodio delle finte bare collocate vicino alla Torre Eiffel, amplificato online, mostra l'integrazione tra sabotaggio e propaganda. Yevgeny Prigozhin, oligarca vicino a Putin, fondatore della *Internet Research Agency* e capo della Compagnia militare privata Wagner, ha avuto un ruolo cruciale. La sua morte non ha però smantellato la macchina: la struttura rimane centralizzata, con società di facciata, ONG e reti semi-indipendenti capaci di amplificare divisioni interne. L'uso dell'IA generativa accelera la produzione di contenuti falsi, rendendo più complessa la verifica.

L'apparato integra attori statali e non statali per massimizzare impatto e opacità. L'intelligence militare, in particolare la Direzione generale per le informazioni militari con gruppi come APT28 (*Fancy Bear*) e Storm-1516, conduce attacchi informatici, *deepfake* e interferenze elettorali. Media statali e proxy – tra cui *Internet Research Agency* e *Social Design Agency* – amplificano i messaggi. ONG di facciata conferiscono legittimità, mentre blogger, *hacktivisti* e cittadini comuni diffondono contenuti in modo apparentemente organico. Il SEAE ha rilevato 505 episodi di manipolazione informativa e ingerenza straniera in 90 Paesi, coinvolgendo 38.000 canali. La campagna *Doppelgänger* ha mobilitato centinaia di migliaia di account falsi su X, generando milioni di post e raggiungendo 38 milioni di utenti in Germania tra agosto 2023 e marzo 2024. Secondo EUvsDisinfo, tra il 2015 e il 2022 si registrano oltre 14.000 casi di disinformazione pro-Cremlino.

Eppure, agosto 2025 segna la diffusione di una notizia che evidenzia un cambiamento nelle operazioni russe in Europa, confermando l'adattamento costante della loro strategia. La Russia ha ridotto le attività di sabotaggio dopo una serie di fallimenti, arresti e crescenti pressioni occidentali, hanno affermato funzionari statunitensi ed europei. Mosca avrebbe rafforzato il controllo sulle operazioni, tagliando fuori contractor ritenuti inaffidabili e aumentando la supervisione sugli intermediari locali impiegati per attacchi, incendi dolosi e sabotaggi. In seguito all'espulsione di massa di diplomatici e agenti dell'intelligence russa, il Cremlino ha tentato di proseguire le operazioni ibride pagando direttamente agenti locali. Tuttavia, numerosi fallimenti hanno costretto Mosca a riconsiderare il proprio approccio. Secondo *l'International Institute for Strategic Studies* (IISS), da gennaio a maggio 2025 in Europa si sono verificati 11 incidenti con presunto supporto russo, tra cui tentativi di danneggiare cavi in fibra ottica e attacchi alle infrastrutture di telecomunicazione in Svezia. Per confronto, nel 2024 gli episodi erano stati più di 30, stabilendo un record.

Sono diverse le cause del calo delle attività: il rafforzamento dei controlli sui contractor imprevedibili, la riorganizzazione di risorse della Direzione principale dell'intelligence verso la guerra in Ucraina, la paura degli arresti e delle punizioni da parte dei potenziali sabotatori, e l'obbligo imposto da Mosca di filmare e riferire ogni attacco. Inoltre, non è da escludere che il Cremlino stia deliberatamente cercando di minimizzare le tensioni per non complicare i rapporti con Donald Trump all'inizio del suo secondo mandato, periodo in cui il presidente statunitense avrebbe cercato di mediare un accordo di pace sull'Ucraina.

Nonostante il calo del numero di attacchi Mosca non ha abbandonato la strategia ibrida. Al contrario, amplia gli strumenti di *cyber-intelligence* per controllare non solo la propria opinione pubblica, ma anche quella delle democrazie occidentali. A febbraio 2025 *Forbes Russia* ha rivelato che il Centro principale per le radiofrequenze avvierà corsi di formazione OSINT (*Open Source Intelligence*) per i propri dipendenti. L'obiettivo è creare un'unità di analisti capaci di sfruttare fonti aperte e tecniche avanzate di monitoraggio informatico. Nello stesso mese, anche *Roskomnadzor*, l'agenzia che supervisiona l'informazione, ha bandito un concorso per formare personale in OSINT. I programmi includono ricerca tramite e-mail, numeri di telefono, nickname, foto e geolocalizzazione, oltre ad analisi di *social*, banche dati, siti *web* e *deep Internet*. Inoltre, ai funzionari sarà insegnato a costruire un "ritratto comportamentale" degli individui – valori, convinzioni, modelli di pensiero – per valutarne rischi e affidabilità. Il pacchetto formativo comprende anche lo studio di strategie e tattiche di guerra dell'informazione. Mosca ha dunque implementato un sistema progettato per trasformare dati, segnali e informazioni in strumenti capaci di modellare opinioni, anticipare reazioni e influenzare decisioni politiche a livello nazionale e internazionale.

13 La "Guerra Ibrida" della Russia (2025)

14 Disinformazione per destabilizzare gli equilibri geopolitici: gli scenari di rischio (2024)

7

STRUMENTALIZZAZIONE DEI FLUSSI MIGRATORI

Tra le operazioni di natura ibrida assume rilevanza l'utilizzo strumentale e *weaponizzato* dell'immigrazione[15]. Secondo Agenzia europea della Guardia di Frontiera e Costiera[16] nel 2025 sono stati registrati 75.900 attraversamenti irregolari nell'UE, circa 420 al giorno. Mosca utilizza i flussi come leva politica: dal 2023 Finlandia e Polonia denunciano pressioni orchestrate tramite la Bielorussia, mentre migranti africani transitano dalla Russia verso l'UE, coordinati con Minsk.

Il 10 luglio 2025 il Servizio di Intelligence ceco ha documentato che il Servizio di Sicurezza Federale russo (FSB) recluta migranti provenienti da Paesi terzi tramite canali come Telegram per condurre attività criminali nell'UE. L'obiettivo è destabilizzare, minare la fiducia nelle istituzioni pubbliche, ridurre il sostegno all'Ucraina e aumentare la percezione di insicurezza nei confronti dei rifugiati. Le operazioni si svolgono al di fuori dei tradizionali circuiti diplomatici: il FSB punta su reclute vulnerabili, prive di legami ufficiali, invece di agenti sotto copertura.

Analogamente, nel maggio 2024 l'intelligence polacca ha arrestato persone sospettate di spionaggio per conto della Russia, tra cui rifugiati giunti in Polonia dopo l'inizio dell'invasione dell'Ucraina nel 2022. Le autorità polacche hanno documentato attività di sorveglianza: installazione di telecamere nascoste lungo linee ferroviarie, raccolta di dati logistici su mezzi e convogli diretti in Ucraina, documentazione fotografica dei punti di transito strategici. Il reclutamento avveniva anche nei centri di accoglienza e ai valichi di frontiera, dove agenti sotto copertura si fingono funzionari locali per ottenere informazioni personali, legami con l'intelligence ucraina e dati sensibili sul supporto logistico militare. Particolare attenzione è rivolta ai giovani, considerati più manipolabili, per operazioni mirate contro infrastrutture civili e umanitarie ucraine.

L'immigrazione irregolare è diventata uno strumento di pressione strategica nel contesto della guerra ibrida, con potenziali effetti destabilizzanti anche sul Regno Unito. Secondo dati di Frontex, l'agenzia europea per la gestione della cooperazione operativa alle frontiere esterne, nel 2025 sono stati registrati circa 75.900 attraversamenti irregolari verso l'UE, con il Regno Unito come destinazione indiretta di parte dei flussi provenienti da Francia e Belgio. Questi movimenti possono essere amplificati tramite reti criminali transnazionali o campagne di disinformazione *online* che mirano a instillare sfiducia tra la popolazione e delegittimare le politiche migratorie governative. Nel contesto della guerra ibrida, l'immigrazione non è solo un fenomeno sociale, ma un vettore utilizzato per sondare vulnerabilità, testare la resilienza delle autorità britanniche e generare pressione diplomatica senza ricorrere a conflitti militari diretti.

Questi individui vengono utilizzati come materiale sacrificabile, senza protezione legale, supporto diplomatico o riconoscimento. La strategia russa è flessibile e non si limita ai canali clandestini: coinvolge ONG, *think tank*, cellule dormienti e agenti "una tantum", reclutati per singole azioni. I risultati numerici possono essere limitati, ma l'effetto cumulativo può compromettere la tenuta interna dei Paesi europei.

Un caso emblematico è quello della Bielorussia nel 2021[17]. Il regime di Alexander Lukashenko ha utilizzato l'immigrazione irregolare come strumento di pressione geopolitica, facilitando il rilascio di visti turistici a cittadini di Iraq e Siria tramite tour operator compiacenti. I pacchetti, pubblicizzati sui social come "vacanze a Minsk", prevedevano voli da Istanbul, Damasco e Dubai. Arrivati in Bielorussia, i migranti venivano ospitati in hotel statali e trasferiti al confine con Polonia e Lituania, anche tramite taxi o autobus.

Solamente nell'estate 2021, secondo le autorità polacche, ci furono circa 30.000 tentativi di attraversamento. La foresta di Białowieża divenne teatro tragico: centinaia di persone, spesso con indumenti inadatti al clima (t-shirt, pantaloncini, indossati in uno dei luoghi più freddi in Europa) furono respinte dai militari polacchi e rimandate indietro dalle autorità bielorusse, tra manganelli e cani, con decine di morti per il freddo. «Non li fermerò – dichiarò Lukashenko alla BBC – perché non vengono nel mio Paese, ma nel vostro».

15

16 Nota anche come Frontex (denominazione informale nata dalla contrazione di *Frontières extérieures*)

17 *Il grande ricatto* (Costantino Pistilli, 2023)

8

IL SILENZIO STRATEGICO DELLA CINA

La Repubblica Popolare Cinese adotta una strategia internazionale di pressione e influenza che punta alla penetrazione silenziosa dei sistemi politici, economici e tecnologici di altri Paesi, senza ricorrere apertamente alla forza militare convenzionale. Un proverbio cinese esprime bene questa filosofia: "*Xiao li cang dao*", letteralmente, "nascondere un coltello in un sorriso". Le operazioni cinesi combinano più livelli d'azione: penetrazione cognitiva, ossia la capacità di influenzare percezioni e narrazioni; supremazia tecnologica, con l'uso avanzato della tecnologia per consolidare vantaggi competitivi; e guerre di influenza (*influence warfare*), mirate a controllare la narrativa internazionale e a orientare l'opinione pubblica in maniera favorevole agli interessi di Pechino.

In Europa l'attività di spionaggio e le campagne di guerra ibrida cinese hanno raggiunto dimensioni significative, spesso in convergenza con le operazioni russe, generando una minaccia complessa per la sicurezza occidentale. La guerra ibrida combina mezzi militari e non militari: cyber-attacchi, disinformazione, sabotaggio, spionaggio industriale e finanziario, pressione economica e politica. L'obiettivo principale è minare la governance democratica e la resilienza delle istituzioni occidentali, sfruttando vulnerabilità tecnologiche e normative.

I gruppi sponsorizzati dallo Stato cinese, storicamente concentrati in Asia orientale, hanno esteso le loro attività all'Europa, replicando modelli simili a quelli utilizzati da operatori russi nel cyber-spionaggio. Le intrusioni informatiche mirano a sottrarre dati sensibili di governi, aziende tecnologiche e infrastrutture critiche, mentre le campagne di disinformazione cercano di orientare l'opinione pubblica e i decisori politici. La normativa cinese sulla sicurezza nazionale e sulla cybersicurezza obbliga cittadini e aziende a fornire supporto e assistenza alle autorità per fini di sicurezza nazionale, anche se non sempre chiaramente definiti, aumentando il rischio di coinvolgimento in operazioni di spionaggio.

In Spagna, ad esempio, il Ministero dell'Interno ha affidato a Huawei[18] un contratto da 12,3 milioni di euro per la gestione delle intercettazioni giudiziarie, suscitando critiche da Stati Uniti e Unione Europea per i rischi di accesso remoto ai dati sensibili. Allo stesso modo, Hangzhou Hikvision Digital Technology Co., nota globalmente come Hikvision e leader nella videosorveglianza, rappresenta un potenziale rischio di sicurezza. In passato sono state documentate numerose backdoor nei dispositivi Hikvision, ovvero porte nascoste nel software che consentono accessi remoti non autorizzati. Anche la Cyberspace Administration of China, l'ente nazionale cinese di regolamentazione e censura di Internet, ha espresso preoccupazioni per la sicurezza, ad esempio in relazione all'acquisizione del chip AI H20 di Nvidia.

Negli ultimi anni, la Cina ha ampliato il proprio raggio d'azione attraverso leve economiche e criminali che si collocano al confine tra illeciti e guerra ibrida. La strumentalizzazione migratoria resta meno sistematica rispetto a Russia o Bielorussia: migliaia di cittadini cinesi hanno percorso rotte balcaniche per cercare asilo in Europa, affrontando viaggi estremamente rischiosi, ma senza una strategia coordinata di *weaponization of migration*.

Più incisiva appare l'attività di riciclaggio e transito finanziario. Operazioni coordinate dall'EPPO (*European Public Prosecutor's Office* – Ufficio del Procuratore Europeo) hanno smantellato reti di *shadow banking*, ossia istituti finanziari non ufficiali, coinvolti in frodi IVA per centinaia di milioni di euro attraverso società fittizie in Italia (Prato, Milano, Bologna, Ancona, Vicenza e Brescia). Tra le modalità più diffuse spicca lo schema *Fei ch'ien* (*flying money*), un sistema di trasferimenti informali che bypassa banche e norme antiriciclaggio (AML/CFT – *Anti-Money Laundering/Combating the Financing of Terrorism*), usato per trasferire miliardi in contanti verso la Cina tramite intermediari italiani. Tra il 2019 e il 2021, fino a 4 milioni di euro a settimana sono stati esportati dall'Italia, in particolare tramite aeroporti come Fiumicino. Maxioperazioni di polizia hanno bloccato 2 miliardi di euro di frodi fiscali, sequestrando beni per oltre 300 milioni di euro e coinvolgendo decine di soggetti cinesi e italiani.

La criminalità transnazionale mostra connessioni sempre più strette con le mafie italiane. Rapporti della Direzione Investigativa Antimafia indicano una collaborazione crescente tra Triadi cinesi e *'ndrangheta*[19], soprattutto nei settori dei trasporti, traffico di esseri umani, sfruttamento del lavoro e riciclaggio, anche attraverso infrastrutture pubbliche, come progetti legati al *Next Generation EU*. A Roma, un omicidio in stile mafioso di un esattore cinese ha evidenziato rivalità tra gang cinesi di Prato estese alla capitale, con collegamenti diretti al sistema *Fei ch'ien* e alla logistica clandestina europea.

18 In data 29 agosto c.a. il Governo spagnolo rende noto che il Ministero per la Trasformazione Digitale annulla il finanziamento da 10 milioni di euro a Telefónica per il potenziamento della rete pubblica in fibra ottica Red.es, dotata di componenti del produttore cinese.

19 Origini e sviluppo della mafia cinese in Italia: la triade ieri e oggi, Salvatore Calleri, presidente della Fondazione Caponnetto e consulente della Commissione Antimafia

Oltre alle leve economiche e criminali, la Cina integra azioni di guerra ibrida dirette, che comprendono cyber-attacchi sofisticati a governi e infrastrutture critiche, campagne di disinformazione online, sabotaggi economici tramite società *proxy*, furti di proprietà intellettuale e pressioni politiche camuffate da iniziative commerciali o culturali. L'obiettivo di queste operazioni è proiettare potenza e influenza in Europa senza conflitti convenzionali, sfruttando la vulnerabilità dei sistemi democratici, la digitalizzazione e le opportunità offerte dai flussi finanziari globali.

In sintesi, la strategia cinese si distingue per la combinazione di mezzi tecnologici, economici, criminali e informativi, realizzando un approccio coordinato e multidimensionale di guerra ibrida, con impatti concreti sulla sicurezza europea e globale di una nazione che tra il 1995 e il 2020 ha aumentato la sua quota globale in 10 settori strategici dal 3% al 25%, mentre i Paesi OCSE sono passati dall'85% al 58%. Pechino domina sette dei dieci settori, producendo in alcuni casi più di tutti gli altri Paesi messi insieme, dimostrando una capacità di pianificazione industriale molto più efficace rispetto a nazioni occidentali[20].

20 Rapporto *Hamilton Index* del ITIF (*Information Technology and Innovation Foundation*) che misura la competitività dei Paesi nelle industrie avanzate. *Threats and Modern Political Warfare: The Architecture of Cross-Domain Conflict*, B. Irdi, op.cit, Nota 1

9

CONTROLLO NARRATIVO

TikTok, il cui nome richiama il suono di un orologio che scandisce il tempo, simboleggia la rapidità e la brevità dei contenuti che la piattaforma propone. L'idea alla base è quella di un flusso continuo di video corti, pensati per catturare rapidamente l'attenzione degli utenti, in linea con i cambiamenti nelle abitudini di consumo digitale.

Negli ultimi anni, TikTok è emerso non solo come piattaforma di intrattenimento, ma anche come vettore significativo di informazione, soprattutto tra i giovani adulti. Nel 2024 il 17% degli adulti statunitensi ha dichiarato di ricevere regolarmente notizie tramite TikTok, rispetto al solo 3% nel 2020. La diffusione è ancora più marcata nella fascia di età tra i 18 e i 29 anni, dove quasi il 39% degli utenti utilizza la piattaforma come fonte primaria di informazione. Tra gli utenti complessivi di TikTok il 52% riferisce di ricevere notizie regolarmente attraverso la piattaforma, un dato in forte crescita rispetto al 22% registrato nel 2020, mentre l'attenzione media sugli schermi è scesa da 2,5 minuti nel 2004 a soli 47 secondi oggi. Studi inglesi del 2022 evidenziano che circa il 49% del pubblico ritiene di avere capacità di concentrazione inferiori rispetto al passato, mentre molti credono erroneamente che la soglia media di attenzione sia di appena 8 secondi. La combinazione tra breve durata dei contenuti e capacità di attenzione ridotta crea un ambiente in cui l'informazione viene consumata rapidamente, spesso senza verifica approfondita.

TikTok è dominato da contenuti brevi, virali e spesso creati da influencer piuttosto che da giornalisti professionisti. Negli Stati Uniti, solo lo 0,4% degli account seguiti dagli utenti appartiene a giornalisti o testate, mentre l'84% dei post di notizia visti è composto da contenuti comici o di opinione. In altre parole, la maggior parte delle informazioni che raggiungono gli utenti proviene da account non istituzionali, con un forte impatto sulla percezione del mondo. Il legame tra TikTok, riduzione dell'attenzione e potere narrativo è chiaro. Con la soglia di attenzione media così bassa, i contenuti devono essere rapidi, visivamente accattivanti e spesso emotivamente polarizzanti.

L'algoritmo della piattaforma filtra ciò che viene mostrato agli utenti, determinando indirettamente quali contenuti raggiungono un pubblico più ampio. Chi controlla il *feed* e le modalità di raccomandazione ha quindi una capacità significativa di plasmare la percezione, influenzando opinioni e potenzialmente scelte politiche individuali.

La piattaforma cinese è diventata un vettore centrale di informazione soprattutto per i giovan/adolescenti. La prevalenza di contenuti virali, la marginalità delle fonti giornalistiche tradizionali e la struttura algoritmica della piattaforma creano un ecosistema in cui il controllo del flusso informativo si traduce in potere narrativo digitale, capace di modellare percezioni e orientare opinioni politiche in modo significativo. Un fenomeno che, nel contesto geopolitico contemporaneo, non può essere ignorato.

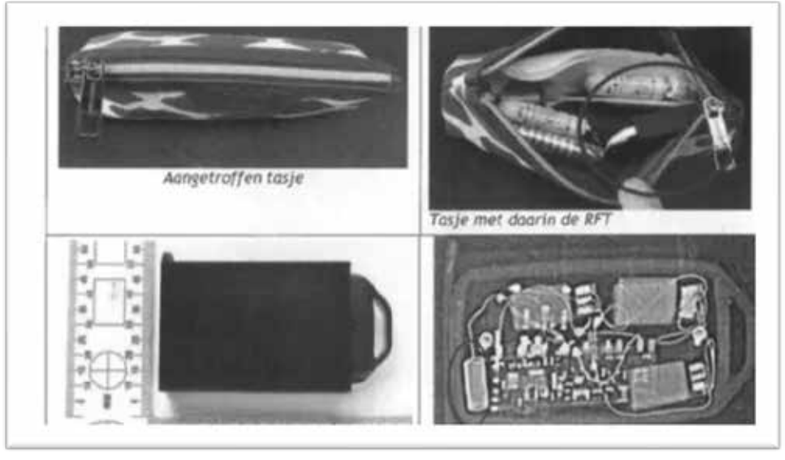
10

L'INFLUENZA IRANIANA MALIGNA

Seppur con minore intensità rispetto a Cina e Russia, l'Iran continua a svolgere in Europa attività di influenza maligna, che spaziano da operazioni di spionaggio e intimidazione a complotti terroristici e campagne cibernetiche. Il *think tank* statunitense *Washington Institute for Near East Policy* ha sviluppato una mappa interattiva[21] che raccoglie oltre 400 casi di operazioni esterne iraniane dal 1979 a oggi, tra cui omicidi, tentati omicidi, sequestri, campagne di pressione e attività di intelligence. Filtrando per Europa e dissidenti iraniani tra il 2023 e il 2025, la mappa documenta 44 attacchi diretti, confermando come Teheran persegua i propri obiettivi strategici attraverso una rete di proxy, gruppi criminali e operazioni clandestine coordinate. In questo contesto emergono azioni contro giornalisti dissidenti, oppositori della Repubblica Islamica e comunità ebraiche, con una combinazione di attività fisiche e cibernetiche che accrescono la pressione sulle istituzioni europee.

Il caso più emblematico resta quello di Assadollah Asadi, ex terzo segretario dell'ambasciata iraniana a Vienna, arrestato nel 2018 in Germania mentre trasportava esplosivi destinati a un attentato contro un raduno del Consiglio Nazionale della Resistenza Iraniana a Parigi. Nel 2021 un tribunale belga lo ha condannato a 20 anni di carcere per tentato omicidio e terrorismo, riconoscendo il legame diretto con il Ministero dell'Intelligence e della Sicurezza iraniano (MOIS). Asadi è il primo diplomatico iraniano condannato in Europa per attività terroristiche, dimostrando l'uso di figure diplomatiche come agenti operativi. Nel maggio 2023 è stato rilasciato a seguito di uno scambio di prigionieri mediato dall'Oman, in cambio del lavoratore umanitario belga Olivier Vandecasteele, sollevando timori di impunità per il terrorismo di Stato.

Esplosivo nascosto in beauty-case per compiere l'attentato



Tra il 2023 e il 2025, le operazioni iraniane in Europa hanno incluso almeno 15 complotti nel Regno Unito, tutti collegati all'Unità 840 della Forza Quds, il reparto delle Guardie della Rivoluzione Islamica (IRGC, *Islamic Revolutionary Guard Corps*) responsabile delle operazioni esterne. Tra questi, il tentato attentato all'ambasciata israeliana a Londra nel maggio 2025, sventato grazie alla cooperazione tra intelligence britannica e servizi alleati. In Svezia, opera la cosiddetta "Foxtrot Network", una rete criminale legata alla Forza Quds, specializzata in attacchi contro dissidenti iraniani, istituzioni israeliane e sinagoghe, che spesso arruola minorenni per ridurre il rischio di condanne. In Germania gruppi criminali come quelli collegati agli *Hells Angels* sono stati coinvolti in attacchi a sinagoghe a Bochum ed Essen e in complotti sventati a Berlino nel 2025, rivelando l'ampiezza del ricorso iraniano a reti *proxy*.

21 Mapping Iranian External Operations Worldwide (2024)

In Italia una rete di influenza con base a Roma e legata all'ambasciata iraniana ha monitorato e intimidito dissidenti e giornalisti, sfruttando anche la cooperazione culturale e accademica finanziata da fondi statali di Teheran. In Francia, sono stati registrati tentativi di colpire oppositori della Repubblica Islamica e comunità ebraiche, inclusi piani di attacco a sinagoghe a Parigi e Berlino tra il 2024 e il 2025.

Parallelamente, l'Unione Europea ha sanzionato la Zindashti Network, collegata al MOIS e all'IRGC, accusata di omicidi di dissidenti in Europa e Nord America; il leader Naji Sharifi-Zindashti è inoltre coinvolto nel narcotraffico internazionale. Secondo Freedom House, l'Iran figura tra i primi dieci Stati responsabili di repressione transnazionale, con almeno 47 episodi documentati tra il 2014 e il 2023 contro dissidenti in esilio, incluso il Regno Unito.

Oltre alle azioni fisiche, Teheran ha intensificato gli attacchi informatici in Europa. Secondo Unit 42 di *Palo Alto Networks*, tra il 2022 e il 2025 si sono registrati oltre 140 attacchi *ransomware* sponsorizzati dallo Stato iraniano, che hanno colpito principalmente i settori sanitario, bancario e dei trasporti, causando perdite superiori a 1,2 miliardi di euro. Questi attacchi, combinati con la repressione fisica e l'uso di reti criminali, delineano un approccio integrato di guerra per procura che si estende al dominio digitale, creando pressione simultanea su dissidenti, istituzioni e infrastrutture critiche.

Le operazioni iraniane evidenziano una crescente sofisticazione: l'impiego di diplomatici come agenti sotto copertura, il ricorso a reti criminali locali, gli attacchi hacker e le attività di sorveglianza avanzata permettono a Teheran di perseguire obiettivi geopolitici e di sicurezza interna anche al di fuori dei propri confini. Questa strategia integrata rappresenta una sfida cruciale per la sicurezza europea, imponendo una risposta coordinata tra Stati, intelligence e forze dell'ordine per contrastare minacce fisiche e cibernetiche e proteggere dissidenti, comunità vulnerabili e infrastrutture critiche.

11

LA STRATEGIA CIBERNETICA DELLA COREA DEL NORD

A differenza di potenze come Russia, Cina e Iran, che impiegano una vasta gamma di strumenti nella loro guerra ibrida, la Corea del Nord ha sviluppato una strategia cibernetica altamente specializzata e mirata. Mentre le altre nazioni combinano attacchi informatici con operazioni militari, disinformazione e altre forme di pressione, Pyongyang si concentra principalmente su attacchi cibernetici per finanziare il proprio programma nucleare e aggirare le sanzioni internazionali.

Il gruppo Lazarus, noto anche come APT38, è un'unità di *hacker* altamente sofisticata associata al governo nordcoreano. Questo gruppo è stato responsabile di alcuni dei più significativi furti di criptovalute nella storia recente. Nel febbraio 2025, Lazarus ha rubato circa 1,5 miliardi di dollari in criptovalute dall'*exchange* Bybit, un attacco che l'FBI statunitense ha denominato *TraderTraitor*. Questo furto ha superato in valore tutti gli altri attacchi informatici attribuiti alla Corea del Nord tra il 2017 e il 2023. Inoltre, nel 2024, Lazarus è stato responsabile di furti per oltre 650 milioni di dollari in criptovalute, tra cui attacchi a WazirX e DMM Bitcoin.

Le operazioni del gruppo Lazarus sono caratterizzate da un alto livello di sofisticazione tecnica. Utilizzano tecniche come il *phishing* mirato, l'infiltrazione di fornitori di servizi *cloud* e la compromissione di piattaforme di gioco online per accedere a fondi in criptovalute. Ad esempio, nel 2022, hanno rubato 620 milioni di dollari dalla Ronin Network, una piattaforma utilizzata per il gioco Axie Infinity. Questi fondi vengono poi riciclati attraverso mixer di criptovalute come Blender.io, per mascherare la loro origine e facilitare il trasferimento a entità statali nordcoreane.

Gli attacchi informatici della Corea del Nord hanno implicazioni significative per la sicurezza internazionale. I fondi ottenuti tramite queste operazioni vengono spesso utilizzati per finanziare il programma nucleare del paese, aggirando le sanzioni imposte dalle Nazioni Unite. In risposta, diversi paesi hanno imposto sanzioni al gruppo Lazarus e ad altre entità collegate al regime nordcoreano. Tuttavia, la natura anonima delle criptovalute e la complessità delle operazioni rende difficile tracciare e fermare efficacemente queste attività.

Pyongyang ha sviluppato una strategia cibernetica focalizzandosi principalmente su attacchi informatici per finanziare il proprio programma nucleare e aggirare le sanzioni internazionali. Questo approccio differisce sostanzialmente dalle strategie di guerra ibrida adottate da altre potenze, che impiegano una combinazione di strumenti militari, informatici e diplomatici.

12

CONCLUSIONI

I conflitti ibridi sfuggono a definizioni rigide ma restano un utile strumento interpretativo per leggere i conflitti contemporanei. Non un modello dottrinale, piuttosto un quadro analitico che aiuta a collegare tattiche frammentate, riconoscerle e contenerle. Il punto di partenza è trattare tali minacce come parte di una strategia complessiva, capace di limitarne la dispersione e di trasformarle in sfide tracciabili e affrontabili. Non esistono scorciatoie, ma un insieme coordinato di misure può rafforzare in modo decisivo la resilienza delle democrazie. Significa, soprattutto, riconoscere lo spazio informativo come dominio della difesa nazionale.

Nella società contemporanea un ostacolo a implementare resilienza contro le influenze straniere maligne è rappresentato in parte da un *modus vivendi* scandito dal *I am seen, therefore I am*: la visibilità diventa sorveglianza, e la sorveglianza è volontaria, in una realtà dove l'informazione è la linfa del sistema democratico. Come ricordava il filosofo francese Etienne de la Boétie, la servitù nasce dall'abitudine.

La sorveglianza non ha più muri né inferriate: attraverso l'uso delle nuove tecnologie è indossata ciascuno di noi. La repressione perfetta è favorita dalla soddisfazione perfetta dei desideri altrui. Nella *grey zone* agiscono Stati, *proxy*, organizzazioni criminali e terroristiche, mossi da obiettivi strategici di lungo periodo che sfruttano le libertà dei Paesi fondati sulla sacralità dello Stato di diritto, della libertà e della tolleranza. Non cercano vittorie rapide, ma l'erosione della coesione interna, la paralisi decisionale, la sfiducia tra cittadini e istituzioni. L'influenza straniera maligna non rappresenta una minaccia ipotetica. È un processo in corso, silenzioso e persistente. Non si vince con il mero *hard power* ma con resilienza, conoscenza e integrazione di difesa e cultura, intelligence e tecnologia, pubblico e privato. Non basta riarmare i confini: il nemico non è solamente fuori, si muove dentro le nostre crepe.

RIFERIMENTI

- **Hybrid Threats and Modern Political Warfare: The Architecture of Cross-Domain Conflict**, *The Jamestown Foundation* (2025. B. Irdi)
- **Russia and the West Are Entering the 'Grey Zone' of Warfare – and the Oceans Are a Key Battleground**, *The Conversation* (2024)
- **Testing the Waters: Securing the UK's Undersea Cables Against Grey-Zone Threats**, *China Strategic Risks Institute* (2025)
- **Misure attive sovietiche: Falsificazione, Disinformazione, Operazioni Politiche**, *Istituto Bruno Germani* (1981)

newdirection.online @ndconservatism

New Direction is registered in Belgium as a not-for-profit organisation and is partly funded by the European Parliament.
The European Parliament and New Direction assume no responsibility for the opinions expressed in this publication. Sole liability rests with the author.