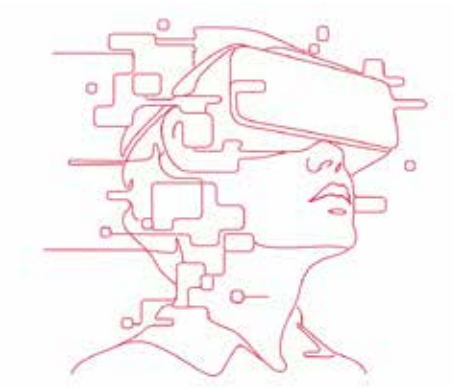
MASSIMILIANO D'ELIA



È guerra ibrida

Una democrazia resiliente non è quella che non subisce attacchi ma è quella che riesce a riconoscere l'attacco, attribuirlo con sufficiente rapidità, comunicare informazioni attendibili e impedire che la paura produca decisioni irrazionali



Il 4 agosto 2026, il ritrovamento di un drone carico di esplosivo all'aeroporto di Lipsia/Halle, apparentemente destinato a colpire un aereo cargo ucraino, ha riportato al centro dell'attenzione la crescente minaccia della guerra ibrida russa in Europa. Il 1° settembre il governo tedesco ha attribuito alla Russia la responsabilità del tentato attacco, sulla base delle indagini di polizia, delle informazioni raccolte dai servizi di sicurezza e delle modalità operative individuate. Berlino ha inserito, l'episodio in un quadro più ampio di sabotaggi, cyberattacchi, interferenze elettromagnetiche e operazioni clandestine.

È proprio nella combinazione di queste azioni che si trova uno dei punti di forza della guerra ibrida: colpire senza esporsi, agire attraverso soggetti intermedi e rendere più complessa l'attribuzione dell'operazione. La cosiddetta "plausible deniability" che consente, infatti, all'autore di un'operazione ostile di rendere difficile l'attribuzione, mantenendo l'azione in quella zona di ambiguità strategica che viene definita "zona grigia", cioè al di sotto della soglia che prevede la "risposta armata".

Dietro questo modello di guerra "invisibile", opera un ecosistema composto da strutture dell'intelligence militare e civile, apparati di influenza e propaganda, gruppi cyber, contractor e intermediari esteri. All'interno del GRU, l'intelligence militare russa, esiste l'Unità 29155, che opera a stretto contatto con diversi gruppi hacker, uno fra tutti il Cadet Blizzard che risulta, tra l'altro, tra quelli sanzionati dall'Unione Europea per il coinvolgimento in attività cyber contro organizzazioni governative ucraine, e per aver preso di mira Stati membri dell'UE e Alleati NATO. L'UE ha, inoltre, sanzionato anche il "142nd

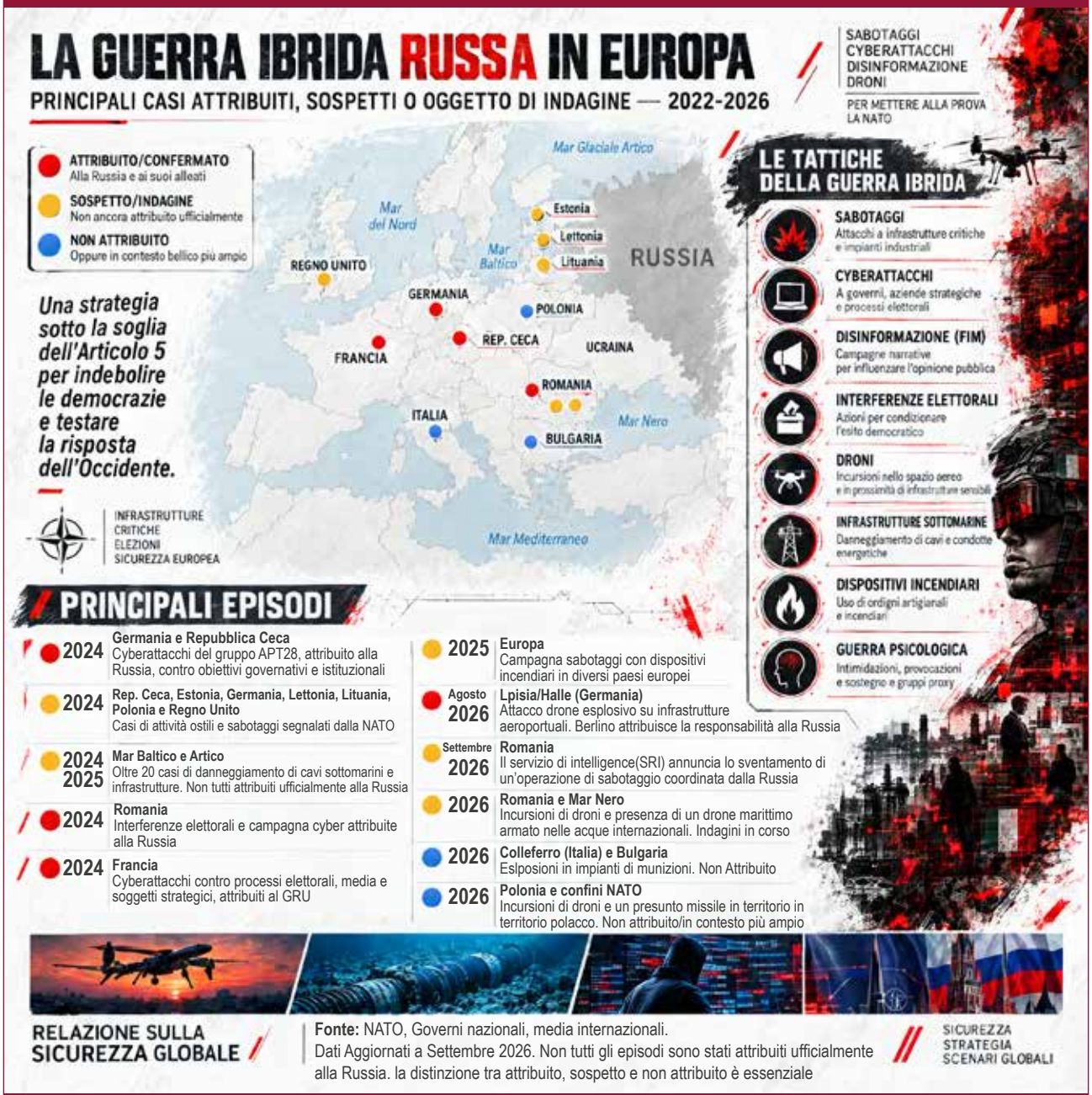
Separate Electronic Warfare Battalion", con sede nella regione di Kaliningrad, collegandolo ad attività di guerra elettronica (disturbing e spoofing dei seganli GPS), che hanno interessato soprattutto l'area degli Stati baltici.
Il 31 agosto 2025, l'aereo che trasportava la presidente della Commissione europea Ursula von der Leyen, in avvicinamento a Plovdiv, in Bulgaria, registrò un'interferenza del segnale GPS. L'episodio venne ricondotto dalle autorità bulgare a un possibile disturbo di origine russa, mentre la Commissione Europea ha poi confermato l'interferenza.

«La minaccia ibrida è una guerra continua che ci colpisce, giorno e notte, ogni giorno. Prende di mira le nostre infrastrutture critiche, i servizi essenziali, le industrie strategiche, le reti di comunicazione, le istituzioni democratiche, minando la fiducia dei cittadini e la stabilità stessa del Paese. Non siamo di fronte a un rischio potenziale, ma a un'aggressione costante che non conosce tregua e non conosce confini».

Camera dei deputati, 12 novembre 2025
Intervento del Ministro della Difesa Guido Crosetto

Secondo un'inchiesta di Reuters del 10 settembre 2026, Regno Unito, Norvegia e Stati Uniti hanno individuato nel Nord Atlantico un'attività del GUGI (Main Directorate of Deep-Sea Research), l'unità russa specializzata nelle operazioni subacquee, durante la quale sarebbero state testate nuove capacità per danneggiare o mettere fuori uso cavi sottomarini. Secondo la ricostruzione di Reuters, l'attività è stata intercettata e nessun cavo è stato danneggiato.
Una delle recenti evoluzioni più preoccupanti della metodologia russa, per compiere operazioni clandestine in Europa, riguarda il reclutamento attraverso social network, piattaforme di gioco e servizi di messaggistica, con la promessa di pagamento in denaro, in contanti o tramite criptovalute. Si tratta di comuni cittadini che possono essere coinvolti in attività apparentemente semplici, come la produzione di fotografie, video o la raccolta di informazioni, senza necessariamente conoscere il committente finale. Il servizio di sicurezza danese PET, nel settembre 2026, ha rilevato attività concrete di pianificazione e preparazione di sabotaggi russi in Danimarca, rivolte soprattutto ad aziende della difesa e ad imprese collegate al sostegno militare all'Ucraina. Il PET ha, inoltre, documentato tentativi di reclutamento attraverso social network, piattaforme di gaming e Telegram.
Tra i casi più documentati c'è quello statunitense di "Tenet Media", attraverso il quale, secondo il Dipartimento di Giustizia americano, due dipendenti di RT, l'emittente statale russa, hanno trasferito quasi 10 milioni di dollari attraverso società-schermo, per finanziare la produzione di migliaia di contenuti fake destinati al pubblico statunitense.
Altre campagne di disinformazione, come Doppelgänger e Storm-1516, attive dalla metà del 2022, mostrano l'evoluzione nel tempo delle tecniche russe di manipolazione dell'informazione. La prima campagna ha utilizzato soprattutto la clonazione di siti e testate occidentali per diffondere contenuti falsi o manipolati; la seconda, ha sviluppato una rete di siti, account e contenuti costruiti ad arte per alimentare e amplificare false narrazioni, anche attraverso video e materiali apparentemente giornalistici.
Il 21 aprile 2026, Bruxelles ha inserito nella lista delle entità sottoposte a sanzioni anche la piattaforma filorussa "Euromore" e la "Foundation for the Support and Protection of the Rights of Compatriots Living Abroad", Pravfond, accusate di svolgere un ruolo attivo nelle attività russe di

Non occorre far credere a tutti una stessa versione dei fatti, spesso è sufficiente produrre un numero sufficiente di versioni alternative per rendere difficile stabilire quale sia quella vera



Cosa può fare uno Stato per la sua resilienza democratica

Rafforzare i sistemi di early warning, proteggere infrastrutture e processi elettorali, contrastare disinformazione e interferenze straniere, garantire la continuità delle funzioni essenziali dello Stato. Decisivi sono il coordinamento tra Istituzioni, Difesa, Intelligence, industria e società civile, la formazione dei cittadini e una comunicazione pubblica tempestiva e credibile

manipolazione delle informazioni, propaganda e influenza.
Nell'agosto del 2026, OpenAI ha individuato e bloccato un gruppo di account ChatGPT, riconducibili alla Russia, utilizzati per promuovere l'International Burke Institute, una sedicente organizzazione con sede in Israele. Secondo OpenAI, gli operatori utilizzavano ChatGPT per generare contenuti destinati a social network e piattaforme online, cercando contemporaneamente di nascondere la propria origine.
Di fronte a una minaccia, quella della guerra ibrida, meno evidente e immediatamente letale rispetto a un conflitto tradizionale, NATO, Unione Europea e singoli Paesi hanno adottato misure diverse di prevenzione e resilienza. Le risposte sono state organizzate, in alcuni casi in modo centralizzato, in altri, come in Italia, attraverso un modello interministeriale e interagenzia che coinvolge più strutture e competenze.
Sul piano strategico, nel novembre 2025 il Ministro della Difesa Guido Crosetto ha presentato

Il Copasir ha acceso l'allerta sulle possibili interferenze straniere nel prossimo ciclo elettorale

Ansa , 09 settembre 2026

al Consiglio Supremo di Difesa il non-paper "Il contrasto alla guerra ibrida: una strategia attiva". A questo si aggiunge la "Strategia digitale della Difesa 2026-2030", orientata a rafforzare la capacità di operare in un ambiente digitale complesso e a sviluppare un approccio integrato con le altre amministrazioni dello Stato. La Strategia, emanata nel 2026, individua tra i propri pilastri la valorizzazione del dato, la connettività e la sicurezza nel dominio cibernetico.
La Difesa italiana, nel disegno di legge di riforma della Difesa, presentato al Consiglio dei Ministri il 7 agosto, prevede un "Centro interforze di addestramento per il combattimento e il contrasto alla minaccia ibrida". Tale Centro, posto alle dirette dipendenze del Capo di Stato Maggiore della Difesa, si pone l'obiettivo di sviluppare capacità comuni tra le Forze Armate per affrontare scenari nei quali cyberattacchi, guerra elettronica, campagne di disinformazione e operazioni militari tradizionali agiscono in maniera integrata.
L'Unione Europea, attraverso l'EU Hybrid



Crosetto sul deep fake:
«.....prima di credere a quello che vediamo sui social, chiediamoci sempre chi lo ha creato. Anche l'informazione va difesa.
Perché il falso non è mai sembrato così vero».

Così, in un video pubblicato sui canali social del Ministero della Difesa, appositamente rigenerato con l'intelligenza artificiale, in cui si vede la figura del Ministro che in un passaggio dice:

«Ciò che vediamo può sembrare assolutamente reale. Per questo, prima di credere a quello che vediamo sui social dobbiamo chiederci sempre chi lo ha creato. Per le informazioni ufficiali, affidiamoci ai canali ufficiali».

Link video fake Ministro della Difesa Guido Crosetto

I PRINCIPALI GRUPPI CYBER ATTRIBUITI ALLA RUSSIA
E I LORO LEGAMI CON L'APPARATO DI SICUREZZA RUSSO

CYBER
SPAZIO
INFORMAZIONE
POTERE

STRUMENTI DIGITALI
PER OBIETTIVI GEOPOLITICI



GRU
INTELLIGENCE MILITARE

Unità responsabile delle operazioni cyber offensive, del sabotaggio e delle attività di intelligence militare.

APT28
Alias: Fancy Bear, Forest Blizzard, Sofacy, Sednit, Strontium

Attività principale: spionaggio, operazioni di influenza

Principali bersagli: governi, NATO, processi elettorali, settore difesa

Attività globali

Sandworm
Alias: Voodoo Bear, Seashell Blizzard, APT44, Iridium

Attività principale: sabotaggio, attacchi distruttivi

Principali bersagli: infrastrutture critiche (energia, trasporti, telecomunicazioni), forze armate

Attività globali (in particolare Ucraina e Paesi NATO)

SVR
INTELLIGENCE ESTERA

Raccoglie informazioni all'estero e conduce operazioni di spionaggio globale.

APT29
Alias: Cozy Bear, Midnight Blizzard, Nobelium, Yttrium, UNC2452

Attività principale: spionaggio, furto di dati, accesso a lungo termine

Principali bersagli: governi, think tank, organizzazioni internazionali, settore tecnologico e sanitario

Attività globali

FSB
SICUREZZA INTERNA

Responsabile di controspionaggio, controllo interno e operazioni cyber.

Gamaredon
Alias: Actinium, Aqua Blizzard, Primitive Bear, UAC-0010

Attività principale: spionaggio, phishing, raccolta di informazioni

Principali bersagli: enti governativi, militari (soprattutto Ucraina)

Attività regionale (focalizzata su Ucraina)

Turla
Alias: Snake, Uroburos, Venomous Bear, Secret Blizzard, Krypton

Attività principale: spionaggio, ricognizione, accesso a lungo termine

Principali bersagli: governi, ambasciate, settore difesa, ricerca

Attività globale

Energetic Bear
Alias: Dragonfly, Berserk Bear, Crouching Yeti, Ghost Blizzard

Attività principale: spionaggio e preparazione di operazioni contro infrastrutture critiche

Principali bersagli: energia, manifattura, aviazione, difesa, settori industriali

Attività globale

Altri gruppi
ATTRIBUTI ALLA RUSSIA

Gruppi con forti attribuzioni russe, attivi in operazioni cyber e di influenza.

Callisto
Alias: Seaborgium, Star Blizzard, ColdRiver, BlueCharlie, TA446

Attività principale: spionaggio, phishing, operazioni di influenza

Principali bersagli: governi, settore difesa, organizzazioni internazionali

Attività globale

Cadet Blizzard
Alias: DEV-0568

Attività principale: operazioni distruttive

Principali bersagli: infrastrutture critiche

Attività regionale (Ucraina ed Europa)

Indrik Spider
Alias: Manatee Tempest, DEV-0243

Attività principale: operazioni cyber

Principali bersagli: governi, difesa

Attività globale

Storm-1516
Alias: CopyCop, New Flood

Attività principale: operazioni di influenza

Principali bersagli: opinione pubblica, processi elettorali

Attività globale

Storm-1679
Alias: Ruza Flood

Attività principale: operazioni di influenza

Principali bersagli: Paesi occidentali

Attività globale

PRINCIPALI TIPI DI ATTIVITÀ

- Spionaggio e furto di dati
- Sabotaggio e attacchi distruttivi
- Attacchi a infrastrutture critiche
- Operazioni di influenza (FIM)
- Phishing e accesso iniziale
- Ricognizione e preparazione operativa

PRINCIPALI SETTORI BERSAGLIO

- Governi e istituzioni
- Difesa e militare
- Energia
- Trasporti
- Telecomunicazioni
- Industria manifatturiera
- Settore tecnologico
- Sanità e ricerca

PRINCIPALI AREE GEOGRAFICHE DI ATTIVITÀ



- Russia (base operativa)
- Paesi principalmente colpiti
- Altre aree di attività



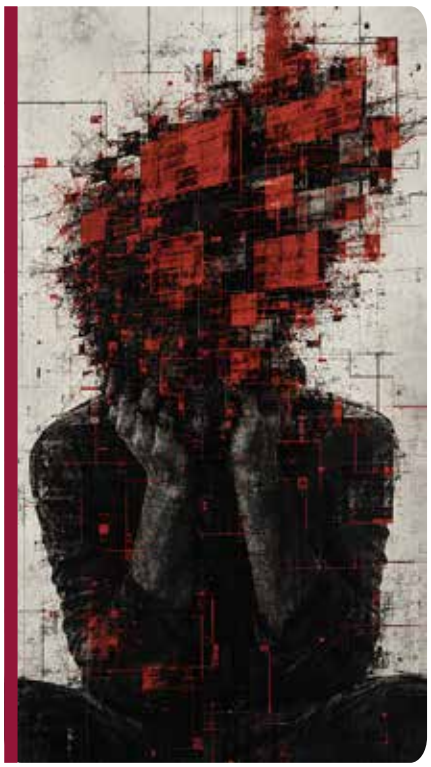


LA GUERRA IBRIDA RUSSA

SICUREZZA
STRATEGIA
SCENARI GLOBALI

AI Generate

Toolbox, coordina misure preventive, di resilienza, cooperazione, sostegno e sanzione. Al suo interno operano il FIMI Toolbox, contro la manipolazione delle informazioni e le ingerenze straniere, il Cyber Diplomacy Toolbox, per la risposta alle minacce e agli attacchi informatici, e gli Hybrid Rapid Response Teams, capaci di fornire rapidamente assistenza agli Stati colpiti.
A livello NATO, si parla di "Cognitive Warfare" e della possibilità di considerare il dominio umano/cognitivo nell'evoluzione futura del concetto multidominio, ma non esiste ancora attualmente il riconoscimento di un reale "sesto dominio operativo" dell'Alleanza. La stessa documentazione descrive il Cognitive Warfare come un ambito in fase di studio e sviluppo concettuale.
Nel Vertice di Vilnius del luglio 2023, l'Alleanza ha precisato che le operazioni ibride contro un Paese membro possono raggiungere il livello di un attacco armato e, in determinate circostanze, condurre all'invocazione dell'Articolo 5 (un attacco armato contro un Paese membro della NATO è considerato un attacco contro tutti gli Alleati). Per quanto riguarda, invece, il dominio cyber, la NATO aveva già stabilito nella "Comprehensive Cyber Defence Policy del 2021", che anche l'effetto cumulativo di attività informatiche malevole significative può, in determinate circostanze, essere considerato alla stregua di un attacco armato.
Il nodo più delicato riguarda però il passaggio dalla difesa all'iniziativa perchè oggi, il contrasto alla guerra ibrida è ancora concentrato soprattutto sulla prevenzione, sulla protezione delle infrastrutture e sulla resilienza.
La sfida per i Paesi occidentali è quindi sviluppare anche la capacità di individuare, attribuire e contrastare le operazioni ostili, prima che producano i loro effetti, arrivando, quando necessario e nel rispetto del diritto internazionale, a colpire le capacità con cui l'avversario conduce la propria guerra ibrida.



«Sulla guerra ibrida noi, nei paesi occidentali, non stiamo facendo molto, la subiamo e basta, perché la guerra ibrida è una guerra strana in cui o reagisci e in qualche modo la porti dall'altra parte, cosa che non abbiamo mai voluto fare, oppure la subisci e cerchi di difenderti, noi lo facciamo di fronte a centinaia di attacchi quotidiani, ad esempio cyber, o lo facciamo nel tentativo di fermare una disinformazione che è sempre più forte e costante.»

Guido Crosetto - Ministro della Difesa
Sky Tg24 , 21 settembre 2026

Fonti
- UK Government, Profile: GRU cyber and hybrid threat operations, 2025. UK Government – Profile: GRU cyber and hybrid threat operations
- FBI – CISA – NSA, Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure, 5 settembre 2024. CISA – Joint Cybersecurity Advisory
- U.S. Department of Justice, Five Russian GRU Officers and One Civilian Charged with Conspiring to Hack Ukrainian Government, 5 settembre 2024. U.S. Department of Justice
- European Union – EUR-Lex, Council Implementing Regulation (EU) 2025/2568, 12 dicembre 2025. EUR-Lex – EU sanctions concerning Unit 29155/Cadet Blizzard
- European Union – EUR-Lex, Council Decision (CFSP) 2024/2643, testo consolidato al 13 luglio 2026. EUR-Lex – EU restrictive measures