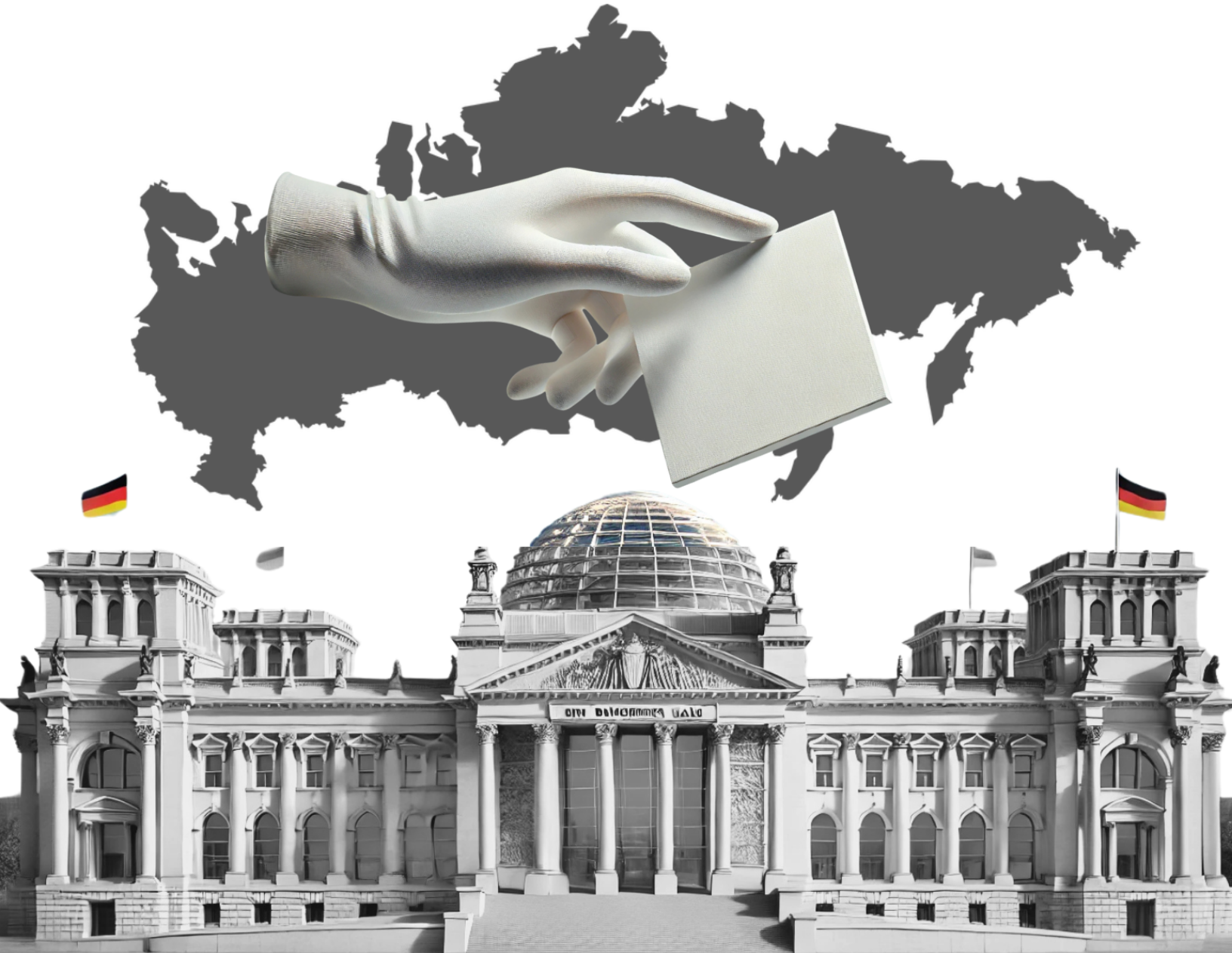
NSSI
Network Studenti
di Sicurezza Italiani

Comprendere le Operazioni di Guerra Ibrida Russe in Europa: Un DoppelGänger che Minaccia le Elezioni Federali Tedesche del 2025

Cosimo Ceccarelli



Introduzione

Nell'ultimo decennio il concetto di guerra ibrida è emerso come una caratteristica chiave dei conflitti moderni, fondendo mezzi militari e non militari in un'unica strategia. Combinando la guerra cibernetica, le operazioni psicologiche, le campagne di disinformazione, la coercizione economica, la corruzione e operazioni sotto copertura, l'ibridazione della guerra mira a destabilizzare gli avversari senza provocare o farsi coinvolgere in un confronto militare diretto. Nonostante la guerra ibrida sia diventata un termine di moda dopo l'annessione della Crimea da parte della Federazione Russa nel 2014, essa affonda le sue radici molto più in profondità nella teoria e nella storia militare, riflettendo nella sua essenza la continua evoluzione della guerra teorizzata da Carl von Clausewitz.

La Federazione Russa si è rivelata maestra nel condurre la guerra ibrida, impiegandola sistematicamente per destabilizzare le democrazie occidentali. Negli ultimi dieci anni, puntando sulla '*weaponization of information*', la Russia ha lanciato campagne di disinformazione su larga scala, mirando alla mente dell'opinione pubblica con l'obiettivo di guadagnare consenso verso i partiti politici simpatizzanti di Mosca durante i periodi elettorali. Le prossime elezioni federali tedesche del 2025 rappresentano l'ennesimo campo di battaglia, in quanto la Russia cercherà di sfruttare la polarizzazione politica per indebolire il sostegno della Germania all'Ucraina attraverso il partito di estrema destra e populista *Alternative für Deutschland* (AfD). Prima di analizzare l'influenza russa sulle elezioni federali tedesche, quest'analisi riflette sull'essenza della guerra ibrida, esamina la dottrina e le tattiche principali impiegata dal Cremlino e fornisce una panoramica delle recenti operazioni ibride russe contro Stati europei.

Guerra Ibrida: Definizione e Comprensione del Fenomeno

Definire la guerra ibrida ha spesso rappresentato una sfida non solo dal punto di vista accademico, poiché la definizione stessa può determinare la sua comprensione da parte dei decisori politici e militari. In sostanza la guerra ibrida implica il ricorso da parte di un attore a misure convenzionali (operazioni cinetiche condotte dalle forze armate regolari di uno stato) e non convenzionali contro un

determinato obiettivo. Tali mezzi non convenzionali possono implicare l'uso di gruppi armati non statali come *proxies* (milizie, gruppi terroristici, singoli individui), operazioni cibernetiche, operazioni psicologiche (PSYOPS), guerra dell'informazione (in termini di disinformazione e di disinformazione), pressione economica e operazioni 'coperte'. Naturalmente questo elenco non può essere considerato esaustivo. Citando il *Military Balance*, la guerra ibrida è definita come "l'uso di strumenti militari e non militari in una campagna integrata, progettata per raggiungere la sorpresa, prendere l'iniziativa e ottenere vantaggi psicologici e fisici utilizzando mezzi diplomatici; sofisticate e rapide operazioni informative, elettroniche e informatiche; azioni militari e di intelligence segrete e occasionalmente palesi; e pressione economica" (IISS, 2015).

Nonostante la guerra ibrida sia diventata un termine popolare dopo l'invasione russa della Crimea nel 2014, essa non è un prodotto delle strategie militari del XXI secolo. Già nel XIX secolo, il teorico militare prussiano Carl von Clausewitz definiva la guerra come un 'camaleonte', cioè imprevedibile e in continua evoluzione in base alle caratteristiche delle entità coinvolte e del tempo. Questo aspetto camaleontico della guerra sottolinea la capacità degli attori di utilizzare mezzi diversi, determinati dalle loro capacità tecnologiche ed economiche in uno specifico momento. In questo contesto il concetto di 'asimmetria' si rivela di aiuto, in quanto "la guerra ibrida è per sua natura asimmetrica" (Wither, 2016). L'asimmetria evidenzia le differenze nei mezzi, nei valori, nei metodi, nei comportamenti e nelle strutture organizzative impiegate per potenziare i propri punti di forza o sfruttare le debolezze del nemico per ottenere risultati che superano di gran lunga il valore materiale delle risorse utilizzate. Tuttavia, l'asimmetria è sempre stata una componente della guerra. Pertanto, pur essendo utile per descrivere efficacemente alcuni aspetti della realtà contemporanea, non ne esaurisce la peculiarità né ne evidenzia il cambiamento. Ad esempio, i Greci e i Romani tra il V e il I secolo a.C. ricorsero alla propaganda e alla disinformazione su larga scala come strategie ingannevoli per influenzare il morale degli eserciti e della popolazione nemica. Durante la Guerra dei Trent'anni (1618-1648), cattolici e protestanti ricorsero alla religione in campagne di propaganda su larga scala, mentre durante la Guerra rivoluzionaria americana (1775-1783) le tattiche di sabotaggio e di *hit-and-run* impiegate dai rivoluzionari predominarono sulla strategia di guerra tradizionale britannica. Lo stesso vale per la campagna

napoleonica in Spagna tra il 1808 e il 1814. L'Operazione Fortitude, lanciata nel 1944 dagli Alleati, rappresenta un chiaro esempio di operazione psicologica basata sull'inganno, in quanto mirava a fuorviare i tedeschi sul luogo dello sbarco del D-Day. Altri esempi di PSYOPS si trovano durante la guerra del Vietnam (1955-1975) e il sostegno degli Stati Uniti al movimento anticomunista dei Contras in Nicaragua tra il 1979 e il 1990, con la pubblicazione di un manuale su come sostenere le suddette milizie attraverso l'inganno, l'intimidazione, la propaganda e la violenza (cfr. CIA Manual for Psychological Operations in Guerrilla Warfare, 1983).

Le Operazioni di Guerra Ibrida Russe: Dottrina e Tattiche

Come anticipato, il termine 'guerra ibrida' è salito alla ribalta nel 2014 con l'annessione russa della Crimea e la guerra nel Donbas. Oltre alle tattiche convenzionali, la Russia ha fatto ricorso a cyberattacchi contro le infrastrutture critiche nazionali ucraine (NCIs) e a vaste campagne di disinformazione basate sul sottolineare la russofobia sia da parte dei cittadini comuni ucraini che dello Stato, la distruzione e la promozione di valori non tradizionali nelle 'regioni russe' e le restrizioni ai diritti della Chiesa ortodossa russa (Iashchenko, 2023). Inoltre, invece di schierare direttamente truppe regolari, il Cremlino ha utilizzato *proxies*, come la compagnia militare privata (PMC) Wagner Group, per effettuare operazioni militari '*boots on the ground*', e persino soldati senza patch identificative (divenuti poi famosi come gli 'omini verdi') come forma di '*deniable intervention*'. La guerra dell'informazione ha caratterizzato e tuttora rileva notevolmente nella guerra russa all'Ucraina lanciata nel febbraio 2022. La Russia ha spesso dipinto il governo ucraino come ispirato dal nazismo e dal satanismo, attivamente coinvolto nella perpetrazione di un genocidio contro la popolazione russofona. Quest'ultimo aspetto è stato ampiamente utilizzato per screditare le operazioni ucraine nel Donbas. La propaganda russa prende ampiamente di mira la NATO, sostenendo che l'organizzazione controlli direttamente il governo di Kiev e che possieda infrastrutture militari in Ucraina. La disinformazione viene persino utilizzata dal Cremlino per coprire la commissione di atrocità di massa in Ucraina, e internamente per reprimere l'opposizione alla guerra.

La '*weaponization of information*' è da intendersi come il fulcro della cosiddetta 'Dottrina Gerasimov', delineata nel febbraio 2013 dal generale Valery Gerasimov, capo di Stato Maggiore russo. In sostanza, Gerasimov afferma che "le stesse 'regole della guerra' sono cambiate. Il ruolo dei mezzi non militari per raggiungere obiettivi politici e strategici è cresciuto e, in molti casi, hanno superato in efficacia il potere delle armi. [...] Tutto questo è integrato da mezzi militari non visibili" (McKew, 2017). Ancora una volta, i mezzi non militari sono da considerarsi *proxies*, la guerra cibernetica, le PSYOPS, le campagne di disinformazione e di depistaggio, la pressione economica, ecc. Il centro di gravità diventa la stabilità sociale, politica e finanziaria interna di un Paese. Pertanto, la guerra ibrida russa mira a provocare e consolidare uno stato di caos permanente all'interno di un Paese avversario. Tra le tattiche di guerra ibrida elencate, la guerra d'informazione sembra essere il fulcro della dottrina russa. Essa mira principalmente a sfumare il confine tra verità e inganno, promuovendo la narrativa di una realtà alternativa. Essa capitalizza le vulnerabilità della società all'interno delle nazioni avversarie, con l'obiettivo di destabilizzare le istituzioni statali e minare la fiducia dell'opinione pubblica nella legittimità del governo (Wither, 2016). La mente è quindi il centro del campo di battaglia, colpita psicologicamente per ridurre al minimo la comprensione della realtà effettiva e virare l'opinione pubblica verso gli obiettivi politici del Cremlino. In questo contesto l'uso convenzionale della forza è ridotto al minimo, evitando così di scatenare una risposta militare simmetrica da parte del nemico. La manipolazione della mente del nemico nella dottrina russa risale all'epoca sovietica, al concetto di '*maskirovka*', inganno. L'*information warfare* è quindi una forma di controllo riflessivo, un'informazione accuratamente elaborata per influenzare le decisioni dell'avversario, indirizzandolo verso scelte in linea con gli obiettivi fissati dalla fonte stessa dell'informazione. In sostanza il tutto è strutturato per influenzare il processo decisionale dell'avversario in modo da sostenere implicitamente gli obiettivi russi. Intesa in questi termini, la manipolazione elettorale è sicuramente uno dei principali scopi che la guerra ibrida russa può perseguire.

Esempi di Operazioni Ibride Russe contro Stati Europei

Nell'ultimo decennio la Russia ha spesso fatto ricorso ad operazioni ibride per influenzare processi elettorali su scala globale. Di seguito viene fornita una panoramica di alcune operazioni guerra ibrida russa contro Stati europei, ovviamente non esaustiva ed escludendo riflessioni sulle interferenze nelle elezioni negli Stati Uniti (cfr. Select Committee on Intelligence United States Senate, 2019) e in vari Stati dell'Africa (cfr. Africa Center for Strategic Studies, 2023). Analizzando la campagna russa per influenzare la politica europea, denominata '*DoppelGänger*' (US Cyber Command, 2024), si possono individuare tre principali strumenti o tattiche di guerra ibrida.

In primo luogo, gli attacchi cyber. Gruppi di hacker russi sono stati ripetutamente autori di attacchi DDoS (*Distributed Denial-of-Service*), sabotando infrastrutture critiche, e siti web elettorali per minare la fiducia dei cittadini nel processo democratico. Gli attacchi DDoS hanno preso di mira anche partiti politici e istituzioni governative. Nei mesi di aprile e maggio 2015, il gruppo di hacker russi APT28 ha attaccato il Parlamento federale tedesco (*Deutscher Bundestag*), compromettendo l'operatività del suo sistema informatico per diversi giorni. Inoltre, sono stati lanciati attacchi di *phishing* contro la posta elettronica di centinaia di membri del parlamento, nel tentativo di provocare una fuga di dati su larga scala.

In secondo luogo, il sostegno finanziario occulto ai partiti politici. Dal 2014 si sospetta infatti che la Russia finanzi partiti di estrema destra e populisti all'interno dell'Unione europea (UE) per promuovere politiche filorusse, creare divisioni all'interno dell'UE stessa e favorire le voci contro il sostegno all'Ucraina. Nella primavera del 2024 le autorità moldave hanno intercettato ingenti fondi (circa 100 milioni di euro) connesse a tentativi russi di interferire nelle elezioni presidenziali e nel referendum sull'adesione all'UE previsti per l'ottobre 2024, con l'obiettivo di deviare il Paese dalla sua traiettoria pro-europea. Una consistente percentuale dei finanziamenti sarebbe stata indirizzata a Ilan Shor, uomo d'affari moldavo in esilio a Mosca. Secondo le accuse, Shor e il Cremlino avrebbero messo in piedi un "complesso schema di acquisto di voti in stile mafioso, corrompendo 130.000 moldavi affinché votassero contro il referendum e a favore di candidati allineati alla Russia" (Sauer, 2024).

In terzo luogo, la disinformazione. La guerra dell'informazione può essere condotta attraverso la manipolazione dei social media come nel caso dell'Internet Research

Agency (IRA) e di Voice of Europe, entrambe sostenute dalla Russia e che hanno utilizzato Facebook, X, TikTok e Telegram per diffondere disinformazione e amplificare narrative polarizzanti durante i momenti elettorali. Mosca ha poi creato una vera e propria industria delle fake news: Russia Today (RT) e Sputnik News sono chiari esempi di media sponsorizzati dallo Stato che diffondono narrazioni false o distorte favorevoli al Cremlino, rivolgendosi al pubblico europeo. La guerra dell'informazione russa ha impiegato anche *deepfakes* e 'media sintetici', sfruttando contenuti generati dall'intelligenza artificiale per minare la fiducia nelle istituzioni. Le campagne sui social media che promuovono la disinformazione sono state intensivamente condotte durante il referendum sulla Brexit nel 2016 e le elezioni presidenziali del 2017 in Francia. In modo più evidente, il 6 dicembre 2024 la Corte Costituzionale della Romania ha annullato il primo turno delle elezioni presidenziali in seguito alle accuse di interferenze russe che avrebbero minato la correttezza del processo elettorale. Le elezioni tenutesi a fine novembre 2024 hanno registrato un consistente aumento dei consensi per il candidato ultranazionalista Calin Georgescu e per il suo programma filo-russo, anti-Ucraina, UE e NATO. Importante notare che nel novembre 2024 sono apparsi, apparentemente dal nulla, 25.000 post su TikTok a favore di Georgescu, supportato ulteriormente da migliaia di post su Facebook e Telegram che diffondevano una disinformazione orchestrata basata sulla seguente agenda: "un'economia rumena autosufficiente, nazionalizzare le aziende straniere, interrompere gli aiuti all'Ucraina, sbarazzarsi dello scudo missilistico statunitense schierato in Romania ed esprimere simpatia per il presidente russo Vladimir Putin" (Popescu, 2024).

Guerra Ibrida Russa contro la Germania: Un Rischio per le Elezioni del 2025?

A causa della sua importanza politica, forza economica e del suo ruolo di primo piano all'interno delle istituzioni dell'UE, la Germania è già stata un obiettivo della guerra ibrida russa negli ultimi anni. Oltre al '*Bundestag Hack*' del 2015, nel 2020 e nel 2021 i partiti politici tedeschi moderati, l'Unione Cristiano-Democratica (CDU), il Partito socialista (SPD) e il Partito dei Verdi, sono stati vittime di una campagna di cyberattacchi che ha sottratto dati sensibili e negato l'accesso ai loro siti web. Anche il sito web del think tank German Council on Foreign Relations fu

pesantemente violato. Nel 2023 i cyberattacchi hanno causato gravi disagi al sistema ferroviario tedesco e alle infrastrutture critiche nazionali, come gli impianti di stoccaggio del gas e le reti elettriche. Tuttavia, le operazioni ibride russe di maggior impatto consistono nel sostegno occulto del Cremlino all'AfD, partito di estrema destra. Quest'ultimo sostiene apertamente le politiche russe e riceve fondi da Mosca, come evidenziato da una recente indagine dell'Organized Crime and Corruption Reporting Project (OCCRP, 2023). Oltre al sostegno finanziario, le operazioni ibride russe sfruttano l'AfD come amplificatore per la guerra d'informazione. In termini di politica estera, l'AfD ha ampiamente promosso narrative anti-Ucraina in linea con quelle del Cremlino, come ad esempio considerare legittimo il referendum russo del 2014 sulla Crimea e la guerra nel Donbas come una questione interna ucraina. Dopo l'invasione russa dell'Ucraina nel 2022, l'AfD si è costantemente opposto alle sanzioni internazionali contro la Russia, alla fornitura di armamenti a Kiev da parte della Germania e alla possibilità di adesione dell'Ucraina all'UE (Hasselbach, 2024; Weisskircher, 2025). Per quanto riguarda la diffusione della disinformazione, l'AfD ha fatto eco ai media di propaganda russi affermando più volte che i rifugiati ucraini fossero 'privilegiati' rispetto ai tedeschi e che le sanzioni contro la Russia danneggiassero i cittadini tedeschi più che la Russia. È interessante notare che, da un punto di vista di politico interna tedesca, la Russia ha fatto grande affidamento sulle narrative anti-migranti per aumentare il sostegno popolare all'AfD. Nel 2016, i media russi hanno fabbricato una notizia ad hoc, riportando che una ragazza russo-tedesca di 13 anni di nome Lisa fosse stata rapita e violentata dai migranti a Berlino. La fake news è stata poi sfruttata dall'AdF, fomentando proteste anti-migranti in tutta la Germania. Anche il Ministero degli Esteri russo, compreso Sergei Lavrov, ha amplificato la notizia falsa, strumentalizzandola per criticare la gestione della crisi dei rifugiati da parte della Germania (NATO, 2016).

Data l'importanza delle prossime elezioni federali previste per il 23 febbraio 2025, la Germania sembra essere al momento il centro della campagna di influenza russa '*DoppelGänger*'. Si prevede infatti che la Russia intensifichi le sue operazioni di influenza online nel tentativo di indebolire il sostegno pubblico al governo guidato dalla SPD e all'Ucraina. Questa strategia sarà probabilmente incentrata sulla manipolazione delle piattaforme social per diffondere narrazioni minanti la coalizione al governo e a sostegno dell'AfD. Il 20 gennaio 2025 il think tank tedesco

CeMAS ha infatti annunciato di aver tracciato centinaia di post in lingua tedesca sui principali social "che incolpavano il partito dei Verdi per i problemi economici della Germania, [che criticavano] il cancelliere Olaf Scholz per il suo sostegno all'Ucraina, [e] che consideravano i conservatori inaffidabili, e allo stesso tempo a favore dell'AfD" (Reuters, 2025). Oltre a sostenere l'AfD, la Russia sta probabilmente cercando di erodere la fiducia dell'opinione pubblica nel processo elettorale e nella legittimità del voto, puntando a lanciare attacchi informatici contro siti web legati alle elezioni durante i periodi di voto per causare interruzioni del sistema.

Rimane tuttavia improbabile che le operazioni ibride russe permettano all'AfD di vincere le elezioni. In base ai sondaggi attuali la coalizione centrista formata dalla CDU e dall'Unione Cristiano-Sociale (CSU) è in testa con il 32%, l'AfD ha ottenuto il 21% (anche considerando l'aperto sostegno di Elon Musk al partito di estrema destra), mentre la SPD e i Verdi seguono rispettivamente con il 16% e il 12%. È quindi plausibile che la CDU/CSU formi una coalizione con la SPD e i Verdi, escludendo così l'AfD dal governo. Vale la pena menzionare il rischio di disordini sociali che potrebbero derivare da una sconfitta elettorale dell'AfD, soprattutto considerando lo scenario di un risultato del partito di estrema destra peggiore rispetto alle previsioni dei sondaggi. In tal caso la propaganda sostenuta dai russi e l'AfD probabilmente sarà centrata sul minare la legittimità del voto e a indire proteste in tutta la Germania, soprattutto nelle città della Germania orientale dove l'AfD gode di maggiore consenso. A loro volta, tali disordini potrebbero provocare una reazione da parte degli attivisti di sinistra, spingendo le contro-proteste a degenerare in scontri violenti.

Conclusione

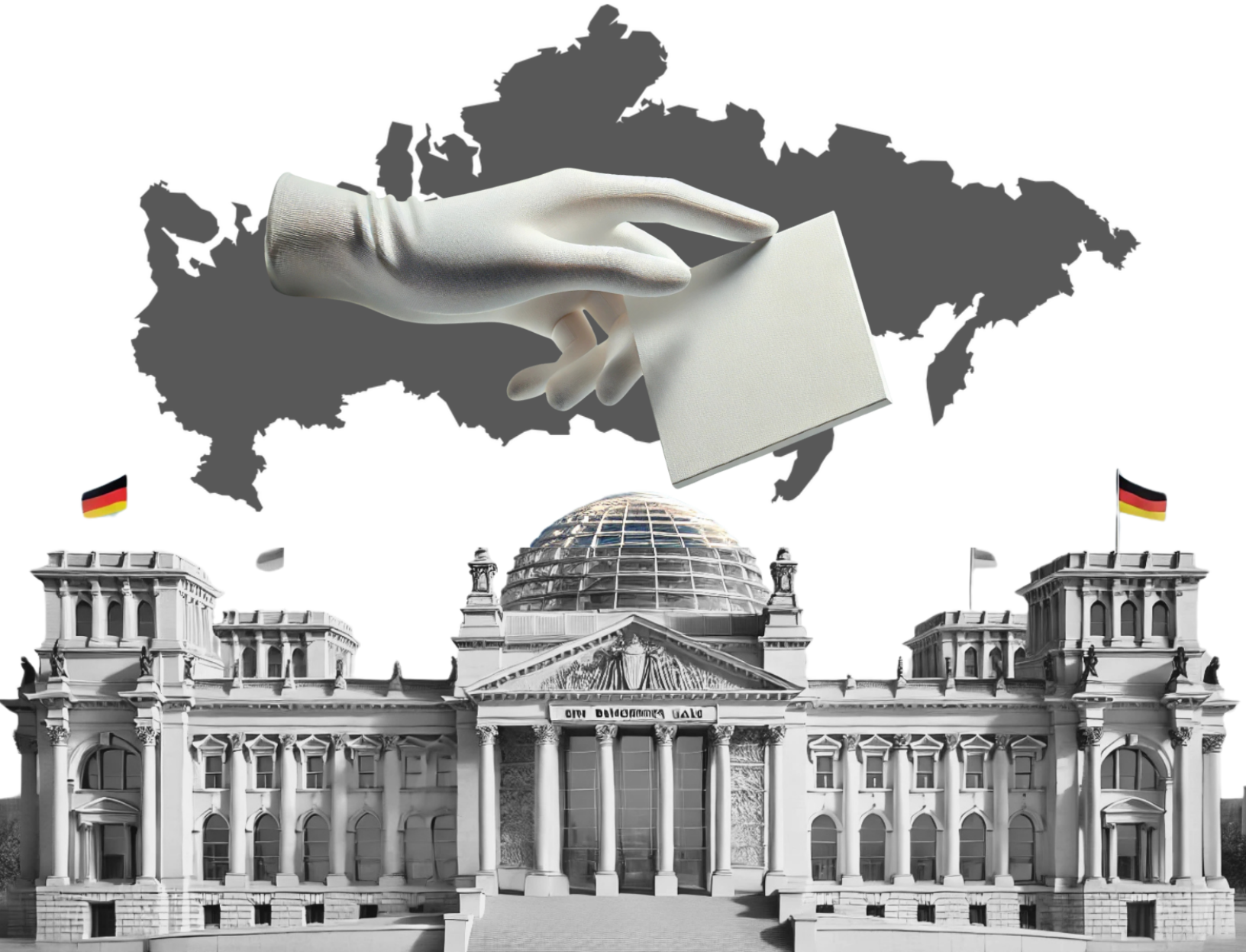
La guerra ibrida rappresenta l'essenza camaleontica della guerra. Quest'analisi ne ha analizzato innanzitutto la definizione e gli elementi fondamentali. Facendo grande affidamento sull'inganno, la comprensione del significato di guerra ibrida è essenziale per aumentare la consapevolezza del fenomeno e cogliere le sue tattiche ingannevoli. Nell'ultimo decennio, la Russia ha imparato a padroneggiare le operazioni informatiche e la guerra dell'informazione nel costante tentativo di minare la democrazia e i processi elettorali. Il Cremlino ha trasferito il campo di

battaglia al pubblico, puntando a influenzare i cuori e le menti del dominio sociale dei suoi avversari. Le operazioni ibride contro le democrazie europee sono diventate una regolarità nella politica estera russa, a volte con successo, altre volte senza successo. Il mescolarsi di guerra e pace apre una zona grigia che pone sfide significative alla sicurezza nazionale e alla tenuta democratica. Le elezioni federali tedesche del 2025 sono il prossimo banco di prova per valutare la comprensione della minaccia ibrida russa da parte delle democrazie occidentali. Anche se un risultato d'impatto sulla performance elettorale dell'AfD appare improbabile, le campagne di disinformazione restano suscettibili di provocare un'ulteriore polarizzazione politica e normalizzare il discorso estremista in Germania, un Paese in cui l'estrema destra ha raggiunto il 20% dei consensi nei sondaggi per la prima volta dalla caduta del regime nazista nel 1945.

NSSI
Network Studenti
di Sicurezza Italiani

Understanding Russian Hybrid Operations in Europe: A DoppelGänger Threatening the 2025 German Federal Elections

Cosimo Ceccarelli



Introduction

Over the last decade, the concept of hybrid warfare has emerged as a key feature of modern conflicts, merging military and non-military means into a single strategy. Combining cyber warfare, psychological operations, disinformation campaigns, economic coercion, corruption, and cover operations, the hybridization of war aims to destabilize adversaries without engaging and triggering a direct military confrontation. Notwithstanding hybrid warfare became a fashionable term following the Russian Federation's annexation of Crimea in 2014, it is rooted far deeper into military theory and story, in its essence reflecting the continuous evolution of warfare as theorized by Carl von Clausewitz.

The Russian Federation has proven to be a master in conducting hybrid warfare, systematically employing it to destabilize Western democracies. In the past decade, focusing on the weaponization of information, Russia has launched large-scale disinformation campaigns, targeting the mind of public opinion, aiming at gaining consensus towards Russian-oriented political parties during electoral periods. The upcoming 2025 German federal elections represent the umpteenth battlefield, as Russia seeks to exploit political polarization to weaken Germany's support for Ukraine through the far-right and populist party Alternative für Deutschland (AfD). Before delving into the analysis of Russian influence over the German federal elections, this analysis reflects on the essence of hybrid warfare, scrutinizes the doctrine and main tactics employed by the Kremlin, and provides an overview of recent Russian hybrid operations targeting European states.

Hybrid Warfare: Defining and Understanding the Phenomenon

Defining hybrid warfare has often been a challenge, not only from an academic perspective, as the definition may determine its understanding by political and military decision-makers. In essence, hybrid warfare implies the resort by an actor of conventional (kinetic operations carried out by the regular armed forces) and non-conventional measures against a determined target. Such non-conventional measures may imply the usage of non-state armed groups as proxies (militias, terrorist groups, individuals), cyber operations, psychological operations (PSYOPS),

information warfare (in terms of disinformation and misinformation), economic pressure, and covert operations. Of course, this list cannot be considered as exhaustive. Quoting the Military Balance, hybrid warfare is defined as "the use of military and nonmilitary tools in an integrated campaign, designed to achieve surprise, seize the initiative and gain psychological as well as physical advantages utilizing diplomatic means; sophisticated and rapid information, electronic and cyber operations; covert and occasionally overt military and intelligence action; and economic pressure" (IISS, 2015).

Despite hybrid warfare becoming a popular term after the Russian invasion of Crimea in 2014, it is not a product of 21st-century strategies for conducting war. As early as the 19th century, Prussian military theorist Carl von Clausewitz defined war as a "chameleon," meaning it is unpredictable and continually evolves based on the characteristics of the entities involved. This chameleonic aspect of warfare emphasizes the ability of actors to use different means, certainly influenced by their technological and economic capabilities at a certain time. In this context, the concept of asymmetry proves useful, as "hybrid warfare is by its very nature asymmetrical" (Wither, 2016). Asymmetry highlights the differences in the means, values, methods, behaviors, and organizational structures employed to enhance one's strengths or exploit the weaknesses of the enemy to achieve results that far exceed the material value of the resources used. However, asymmetry has always been a component of warfare. Hence, while useful in effectively describing some aspects of contemporary reality, it does not exhaust its distinctiveness or highlight its change. For example, the Greeks and Romans between the 5th and 1st century BCE resorted to large propaganda and disinformation as deceptive strategies to influence the morale of their enemies' armies and population. During the Thirty Years War (1618-1648), Catholics and Protestants resorted to religion in large-scale propaganda campaigns, whereas during the American Revolutionary War (1775-1783) sabotage and hit-and-run tactics employed by revolutionaries predominated over the British traditional warfare. The same applies to the Napoleonic campaign in Spain between 1808 and 1814. Operation Fortitude, launched in 1944 by the Allies, clearly represents a deceptive operation, as it aimed at misleading the Germans about the D-Day landing location. Further examples of PSYOPS are to be found during the Vietnam War (1955-1975), and the US support to the anti-communist 'Contras'

movement in Nicaragua between 1979 and 1990, even releasing a handbook on how to support the said militias through deceit, intimidation, propaganda, and violence (see CIA Manual for Psychological Operations in Guerrilla Warfare, 1983).

Russian Hybrid Operations: Doctrine and Tactics

As said, the term 'hybrid warfare' made its way to the forefront in 2014 with the Russian annexation of Crimea and the war in Donbas. Alongside conventional tactics, Russia resorted to cyberattacks against Ukrainian national critical infrastructures (NCIs) and large disinformation campaigns stressing Russophobia on the part of both ordinary Ukrainians and the state, the destruction and promotion of non-traditional values in 'Russian regions', and restrictions on the rights of the Russian Orthodox Church (Iashchenko, 2023). Furthermore, instead of directly deploying regular troops, the Kremlin used proxy forces, such as the private military company (PMC) Wagner Group, to carry out military operations 'boots on the ground', and even unmarked soldiers (known as 'little green man') as a form of deniable intervention. Information warfare has characterized and still matters in the Russian war on Ukraine launched in February 2022. Russia has often depicted the Ukrainian government as inspired by Nazism and Satanism and as actively involved in perpetrating genocide against Russian speakers. Of note, this latter has largely been used to discredit Ukrainian operations in Donbas. Russian propaganda widely targets NATO, claiming that the organization directly controls the Ukrainian government and possesses military infrastructure in Ukraine. Disinformation is even used to cover the commission of mass atrocity crimes, and internally by the Kremlin to repress the opposition against the war.

The weaponization of information is to be understood as the core of the so-called 'Gerasimov Doctrine', outlined in February 2013 by General Valery Gerasimov, Russia's chief of the General Staff. Briefly, Gerasimov stated that "the very 'rules of war' have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. […] All this is supplemented by military means of a concealed character" (McKew, 2017). Once again, nonmilitary means are to be considered armed proxies, cyber warfare, PSYOPS, disinformation and

misinformation campaigns, economic pressure, etc. The center of gravity becomes a country's internal social, political, and financial stability. Hence, Russian hybrid warfare aims at achieving a status of permanent chaos within a targeted country. Among the listed hybrid warfare tactics, information warfare appears to be the core of the Russian doctrine. Indeed, it mainly strives to obscure the boundary between truth and deception, fostering an alternate reality. It capitalizes on societal vulnerabilities within target nations, aiming to destabilize state institutions and undermine the public's trust in government legitimacy (Wither, 2016). The mind is, therefore, the center of the battlefield, psychologically struck to reduce a clear understanding of reality and shift the public opinion towards the Kremlin's political objectives. In this context, the conventional usage of force is reduced to the minimum, avoiding triggering a symmetric military response by the enemy. The manipulation of the enemy's mind is something that dates back to the Soviet era, to the military deception concept of '*maskirovka*'. Information warfare is then a form of reflexive control, that is, carefully crafted information designed to influence an opponent's decisions, steering them toward choices that align with the objectives set by the source of the information. In essence, the process is designed to influence an opponent's decision-making to ultimately support Russian objectives. Understood in these terms, electoral manipulation appears to be one of the main achievements Russian hybrid warfare can pursue.

Examples of Russian Hybrid Operations Targeting European States

Over the last decade, Russia has often engaged in hybrid operations to influence electoral processes worldwide. For the sake of conciseness, an overview of Russian hybrid warfare targeting European states is provided below, excluding reflections on the interferences in elections in the United States (see Select Committee on Intelligence United States Senate, 2019) and Africa (see Africa Center for Strategic Studies, 2023). Three main hybrid warfare instruments can be tracked in analyzing the Russian campaign to influence European politics, named "DoppelGänger" (US Cyber Command, 2024).

First, cyberattacks. Russian hacking groups have been involved in Distributed Denial-of-Service (DDoS) attacks, sabotaging critical infrastructure, such as

election websites, to undermine confidence in democratic processes. DDoS attacks also targeted political parties and government institutions. In April and May 2015, the Russian hacking group APT28 targeted the German Federal Parliament (Deutscher Bundestag), compromising the parliament's information system and affecting its operability for several days. Furthermore, phishing attacks targeted hundreds of members of the parliament email, attempting to achieve a large-scale data leak.

Second, covert financial support to political parties. Since 2014, Russia has been suspected of providing financial backing to far-right and populist parties within the European Union (EU) to promote pro-Russian policies, create divisions within the EU, and foster positions against Ukraine. In Spring 2024, Moldovan authorities intercepted significant funds (around €100m) linked to Russian attempts to meddle in Moldova's presidential election and EU membership referendum scheduled for October 2024, aiming to sway the country away from its pro-European trajectory. A consistent percentage of that amount was believed to be directed to Ilan Shor, a Moldovan businessman based in Moscow. Allegations claim that Shor and the Kremlin have set up a "complex 'mafia-style' voter-buying scheme and bribing 130,000 Moldovans to vote against the referendum and in favor of Russia-friendly candidates" (Sauer, 2024).

Third, disinformation. Information warfare can be pursued through social media manipulation, as in the case of the Russian-backed Internet Research Agency (IRA) and the Voice of Europe, weaponizing Facebook, X, TikTok, and Telegram to spread disinformation and amplify polarizing narratives during election cycles. Furthermore, Russia has created a fake news industry: Russia Today (RT) and Sputnik News are prominent examples of state-sponsored media outlets disseminating false or distorted narratives favorable to the Kremlin, targeting European audiences. Russian information warfare also employed deepfakes and synthetic media, exploiting AI-generated content to undermine trust in institutions. Social media campaigns promoting disinformation have been largely pursued during the Brexit Referendum in 2016 and the 2017 presidential elections in France. More prominently, on 6th December 2024, Romania's Constitutional Court nullified the first round of the presidential elections, following allegations of Russian interference undermining the fairness of the electoral process. The elections, held in late

November 2024, registered a consistent rise in support for ultra-nationalist candidate Calin Georgescu and its pro-Russian, anti-Ukraine, EU, and NATO agenda. Of note, in November 2024 25,000 pro-Georgescu TikTok posts appeared seemingly out of nowhere, complemented by thousands of posts on Facebook and Telegram, spreading an orchestrated disinformation prioritizing achieving a "self-sufficient Romanian economy, nationalize foreign companies, stop aid to Ukraine, get rid of the US missile defense shield hosted in Romania, and expressed sympathy for Russian president Vladimir Putin" (Popescu, 2024)

Russian Hybrid Warfare against Germany: Are the 2025 Elections at Risk?

As anticipated, due to its political significance, economic strength, and prominent role within the EU institutions, Germany has already been a target of Russian hybrid warfare over the last decade. Apart from the 2015 'Bundestag Hack', in 2020 and 2021 moderated German political parties, namely the Christian Democratic Union (CDU), the Socialist Party (SPD), and the Green Party were victims of a cyberattack campaign, stealing sensitive data and denying access to their websites. Even the think tank German Council on Foreign Relations's website was hacked. In 2023, cyberattacks caused large disruption of Germany's railway system and NCIs, such as gas storage facilities and power grids. However, the most impactful Russian hybrid operations are to be located in the Kremlin's covert support to the far-right AfD. This latter openly supports Russian policies and receives funds from Moscow, as highlighted by an investigation by the Organized Crime and Corruption Reporting Project (OCCRP, 2023). Apart from financial support, Russian hybrid operations exploit AfD as an amplifier for information warfare. In terms of foreign policy, the AfD has largely promoted anti-Ukraine narratives in line with the Kremlin's, such as considering the 2014 Russian Crimea Referendum to be legitimate and the war in Donbas as a Ukrainian internal matter. After the Russian invasion of Ukraine in 2022, the AfD has continuously opposed international sanctions against Russia, Germany's supply of armaments to Kyiv, and the possibility of Ukrainian membership in the EU (Hasselbach, 2024; Weisskircher, 2025). In terms of spreading disinformation, the AfD echoed Russian propaganda media by stating that Ukrainian refugees were 'privileged' over native Germans and

that sanctions against Russia were harming German citizens more than Russia. Interestingly, from an internal political perspective, Russia has heavily relied on anti-migrant narratives to increase popular support for the AfD. In 2016, Russian media 'fabricated' ad hoc news, reporting a 13-year-old Russian-German girl named Lisa being kidnapped and raped by migrants in Berlin. The fake news has been exploited by the AdF, fueling anti-migrant protests across Germany. Notably, even The Russian Foreign Ministry, including Sergei Lavrov, amplified the false narrative, using it to criticize Germany's handling of the refugee crisis (NATO, 2016).

Given the salience of the upcoming federal elections scheduled for 23rd February 2025, Germany appears to be at the center of the Russian 'DoppelGänger' influence campaign. Russia is expected to escalate its online influence operations in an effort to weaken public backing for both the SPD-led government and Ukraine. This strategy would likely center on manipulating social media platforms to spread narratives that undermine the ruling coalition while bolstering the AfD. Indeed, on 20 January 2025, the German think tank CeMAS announced it had tracked down hundreds of German-language posts on the main social media platforms, "[blaming] the Green Party for Germany's economic woes, [lambasting] Chancellor Olaf Scholz for his support of Ukraine, [and casting] the conservatives as untrustworthy but [speaking] in favor of the AfD" (Reuters, 2025). In addition to bolstering support for the AfD, Russia is likely seeking to erode public trust in the electoral process and the legitimacy of the vote by launching cyberattacks on election-related websites during voting periods to cause disruptions.

However, it remains unlikely that Russian influence operations will let the AfD win the elections. Based on current polls, the centrist coalition formed by the CDU and the Christian Social Union (CSU) leads with 32%, the AfD scored 21% (even considering Elon Musk's open support to the far-right party), whilst the SPD and the Greens follow respectively with a 16% and a 12%. It is then plausible that the CDU/CSU will form a coalition with the SPD and the Greens, thereby excluding the AfD from the government. It is worth remarking on the risk of social unrest that may stem from an electoral loss by the AfD, especially considering the scenario of the far-right party scoring worse than the polls' forecasts. In such a case, Russian-backed propaganda and the AfD will probably turn to undermining the legitimacy of the

vote and calling for protests across Germany, especially in East German cities where the AfD enjoys more consensus. In turn, such unrest is likely to cause a reaction by left-wing activists, prompting counter-protests to potentially escalate into violent confrontations.

Conclusion

In conclusion, hybrid warfare represents the chameleonic essence of war. This analysis has first analyzed its definition and core elements. Heavily relying on deviousness, understanding what hybrid warfare means is essential to raise awareness of the phenomena and catch its deceptive tactics. Russia has mastered cyber operations and information warfare over the last decade in a constant attempt to undermine democracy and electoral processes. The Kremlin has transferred the battlefield to public audiences, aiming at influencing the hearths and the minds of the social domain of its adversaries. Hybrid operations against European democracies have become a regularity in Russian foreign policy, at times successful, at others unsuccessful. The blurring of war and peace opens a grey zone, posing significant challenges to national security and democratic resilience. The 2025 German federal elections are the next bench test to assess the understanding by Western democracies of the Russian hybrid threat. Even if an impactful outcome on the AfD electoral performance appears to be unlikely, disinformation campaigns remain amenable to cause further political polarization and normalize extremist discourse in Germany, a country where the far-right reached a 20% consensus in the poll for the first time since the fall of the Nazi regime in 1945.

Bibliografia

- Africa Center for Strategic Studies (2023, June 21). Tracking Russian Interference to Derail Democracy in Africa. https://africacenter.org/spotlight/russia-interference-undermine-democracy-africa/.

- Central Intelligence Agency (1983). CIA Manual for Psychological Operations in Guerrilla Warfare. Taycan.

- Hasselbach, C. (2024, July 9). German support for Ukraine under pressure from populists. Deutsche Welle. https://www.dw.com/en/german-support-for-ukraine-under-pressure-from-populists/a-70138863.

- Iashchenko, I. (2023, September 18). Russian disinformation about the Ukrainian conflict since 2014: fact-checking and recurring patterns. Aspen Online. https://aspeniaonline.it/russian-disinformation-about-the-ukrainian-conflict-since-2014-fact-checking-and-recurring-patterns/.

- IISS, International Institute of Strategic Studies (2015, February). The Military Balance 2015. https://www.iiss.org/publications/the-military-balance/the-military-balance-2015/.

- McKew, M. K. (2017, September/October). The Gerasimov Doctrine. Politico Magazine. https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/.

- NATO (2016, July, 2017). The "Lisa case": Germany as a target of Russian disinformation. NATO Review. https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html.

- OCCRP. (2023, February 3). Kremlin-Linked Group Arranged Payments to European Politicians to Support Russia's Annexation of Crimea. OCCRP. https://www.occrp.org/en/investigation/kremlin-linked-group-arranged-payments-to-european-politicians-to-support-russias-annexation-of-crimea.

- Popescu, O. (2024, December 10). Romania's election crisis: A stark warning for NATO nations on Russian meddling. European Council on Foreign Relations. https://ecfr.eu/article/romanias-election-crisis-a-stark-warning-for-nato-nations-on-russian-meddling/.

- Reuters (2025, January 2025). Russian disinformation targets German election campaign, says think-tank. Reuters. https://www.reuters.com/world/europe/russian-disinformation-targets-german-election-campaign-says-think-tank-2025-01-20/.

- Sauer, P. (2024, October 12). 'Russia's dirty money will hijack our democratic process': how tiny Moldova fears Kremlin is fixing EU referendum. The Guardian. https://www.theguardian.com/world/2024/oct/12/moldova-fears-kremlin-fixing-eu-referendum-russia/.

- Select Committee on Intelligence United States Senate (2019). Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views. 116th Congress, 1st Session, Senate, Report 116-XX. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

- US Cyber Command (2024, September 3). Russian Disinformation Campaign "DoppelGänger" Unmasked: A Web of Deception. USCYBERCOM Public Affairs. https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/.

- Weisskircher, M. (2025). Far-right movement-party activism as strategy: Germany's 'peace movement' during Russia's war against Ukraine. Acta Politica, 60(1): 118-138. https://link.springer.com/article/10.1057/s41269-024-00378-y.

- Wither, J. (2016, January). Making Sense of Hybrid Warfare. Connections the Quarterly Journal, 15(2): 73-87. https://www.researchgate.net/publication/301237833_Making_Sense_of_Hybrid_Warfare.