International Journal of Advanced Scientific Research
www.allscientificjournal.com
ISSN: 2456-0421
Received: 24-04-2026, Accepted: 25-05-2026, Published: 09-06-2026
Volume 11, Issue 2, 2026, Page No. 102-110

# Hybrid warfare and information operations: The role of cyber-propaganda in modern conflicts

**Müzaffer Dinçay Tevfikür Rahman**
Researcher, Global Research and Analysis Lab (GRAL), Romania
**DOI:** https://doi.org/10.66856/ijasr.2026.11.2.11050

**Abstract**
The contemporary security landscape has been fundamentally reshaped by the emergence of hybrid warfare—a doctrine that deliberately fuses conventional military force with cyberattacks, economic coercion, espionage, and, crucially, large-scale information operations. This paper examines the structural integration of cyber-propaganda within hybrid warfare strategies, analyzing how state and non-state actors exploit the digital information environment to weaken public trust, manufacture political instability, and assert narrative dominance during armed conflict. Drawing on case studies from the Russian-Ukrainian war, Chinese pressure campaigns against Taiwan, and broader Euro-Atlantic influence operations, the paper maps the evolving taxonomy of cyber-propaganda—from website spoofing and coordinated inauthentic social-media behavior to AI-generated deepfakes and algorithmic manipulation. Particular attention is given to Russia's Operation Doppelganger, China's cognitive warfare doctrine, and the role of advanced persistent threat (APT) groups in synchronizing cyberattacks with disinformation cycles. The paper further evaluates the institutional and legal countermeasures adopted by NATO, the European Union, and individual democratic states, arguing that effective resilience requires integrated whole-of-society responses combining technological detection, media literacy, legal frameworks, and proactive strategic communication. The analysis concludes that cyber-propaganda has transitioned from a peripheral instrument of statecraft to a decisive operational variable of twenty-first-century warfare, with profound implications for democratic governance, civil-military relations, and international security architecture.

**Keywords:** Hybrid warfare, information operations, cyber-propaganda, disinformation, cognitive warfare, influence operations, Russia, China, NATO, deepfakes

## Introduction

The character of warfare is changing. Where twentieth-century conflict was largely defined by the mass deployment of armored formations, air superiority, and nuclear deterrence, the opening decades of the twenty-first century have produced a far more ambiguous and multi-domain form of coercion. Hybrid warfare—a strategy that combines conventional military capabilities with cyberattacks, economic pressure, espionage, proxy forces, and information operations—has repositioned the cognitive domain as a principal battlefield. Within this domain, cyber-propaganda occupies a pivotal place, enabling belligerents to attack the minds of adversaries before a single shot is fired, to sustain psychological pressure throughout a conflict, and to contest the narrative long after formal hostilities subside.

The theoretical foundations of this shift are not entirely novel. Sun Tzu's injunction to subdue the enemy without fighting, Soviet-era concepts of 'active measures,' and Cold War psychological operations all anticipated elements of contemporary information warfare. What is genuinely new is the scale, speed, precision, and technical sophistication with which digital communications technologies now allow these operations to be conducted. The internet, social media platforms, generative artificial intelligence (AI), and ubiquitous smartphone penetration have collectively created an information environment of unprecedented reach, where fabricated content can be produced in seconds, distributed to millions within minutes, and algorithmically amplified far beyond any organic human network.

The strategic salience of these capabilities has been dramatically demonstrated across multiple contemporary theaters. Russia's full-scale invasion of Ukraine in February 2022—and the years of preparatory information operations that preceded it—offered the most extensively documented case of cyber-propaganda integrated within a comprehensive hybrid warfare campaign. Simultaneously, China has deployed a sophisticated information warfare architecture against Taiwan combining cyber intrusions, AI-generated disinformation, fake news websites, and coordinated social-media influence to weaken public cohesion and undermine democratic institutions without yet resorting to kinetic conflict. Beyond these primary cases, influence operations linked to state actors have proliferated across European elections, disrupted critical infrastructure narratives, and sought to erode the cohesion of the NATO alliance.

This paper proceeds in seven sections. Following this introduction, Section Two develops a theoretical and definitional framework for hybrid warfare and information operations. Section Three offers a detailed analysis of cyber-propaganda's structural components and operational mechanics. Section Four examines the Russia-Ukraine conflict as a paradigmatic case study. Section Five analyzes Chinese information warfare against Taiwan. Section Six surveys the broader Euro-Atlantic disinformation ecosystem, with particular attention to Operation Doppelganger and AI-enabled influence operations. Section Seven evaluates the countermeasures and resilience frameworks developed in response. The paper concludes

with reflections on the future trajectory of cyber-propaganda and its implications for democratic security.

## Theoretical Framework

### Defining Hybrid Warfare

The concept of hybrid warfare resists a single authoritative definition, having been employed by scholars, practitioners, and policymakers with varying degrees of precision. The term was popularized in its contemporary form following Russia's annexation of Crimea in 2014, when analysts observed a campaign that seamlessly combined covert military deployment (the so-called 'little green men'), economic pressure through energy dependency, cyber intrusions against Ukrainian government systems, and sustained information operations designed to justify the intervention and fragment Ukrainian national identity (Galeotti, 2016; Renz, 2016) [11, 33]. NATO's subsequent working definition captures the essential elements: hybrid warfare involves the use of 'a wide range of overt and covert military, paramilitary, and civilian measures...employed in a highly integrated design' (NATO, 2015) [25].

What distinguishes hybrid warfare from earlier models of irregular or asymmetric conflict is its deliberate exploitation of the 'gray zone'—the contested space between peace and war where the thresholds for conventional military response are deliberately kept below the level that would trigger Article 5 collective defense obligations or other formal international security mechanisms. As the Center for European Policy Analysis has observed, hybrid operations are designed to be 'adaptive, continuous, and hard to attribute, keeping the target off-balance' (CEPA, 2025) [1, 6]. Each individual instrument—a cyberattack, an energy supply disruption, a disinformation campaign—may appear manageable in isolation; their combined and synchronized application is designed to overwhelm democratic societies' capacity to detect, attribute, and respond effectively.

By 2025, hybrid warfare has matured into what analysts describe as a fully integrated 'battlespace spanning AI, autonomy, economic coercion, and cognitive warfare' (HybridSec, 2025) [18, 19]. The strategic logic is coherent: by avoiding a direct kinetic confrontation that would trigger conventional deterrence mechanisms, hybrid actors can impose substantial costs on adversaries while maintaining plausible deniability and keeping escalation below critical thresholds.

### Information Operations and the Cognitive Domain

Within this hybrid framework, information operations (IO) refer to the integrated employment of electronic warfare, psychological operations, military deception, operational security, and computer network operations to influence the information environment. The doctrinal category of 'influence operations' specifically targets the perceptions, beliefs, and decision-making of both foreign audiences and domestic populations. As Marsili (2024) [23] notes, these operations fall under the broader concept of 'information warfare' and represent a component of national power—the aggregate of all resources available to a state in pursuing national objectives.

Cognitive warfare, a more recent conceptual development, extends this framework by targeting the cognitive processes of individual human beings rather than physical infrastructure or institutional decision-making alone. NATO's Allied Command Transformation has defined cognitive warfare as operations aimed at affecting the neural processes, perceptions, reasoning, and behaviors of individuals at scale. The fusion of AI, social media algorithms, and behavioral data analytics has given cognitive warfare tools a precision and reach that earlier psychological operations could not approach. As research published in the journal Frontiers in Human Neuroscience has demonstrated, targeted social-media content can reliably alter risk perception, moral judgments, and political preferences within relatively short exposure periods.

Cyber-propaganda sits at the intersection of these concepts, denoting the deliberate use of digital communications technologies—including social media platforms, search engine optimization, bot networks, fabricated news websites, and AI-generated synthetic media—to advance political or military objectives through the manipulation of information. Unlike traditional propaganda, which required state or quasi-state broadcasting infrastructure, cyber-propaganda can be produced and distributed at low cost by relatively small teams, amplified through automated systems, and targeted at specific demographic or psychographic segments of the population.

## Structural Components of Cyber-Propaganda Perations

### The Information Operations Kill Chain

Modern cyber-propaganda campaigns exhibit a recognizable operational architecture that can be mapped onto an 'information operations kill chain' analogous to the cyber kill chain model developed in the physical cybersecurity domain. This architecture comprises five interdependent phases: narrative development, content production, distribution infrastructure, amplification mechanisms, and effect assessment.

Narrative development involves the strategic identification of societal fault lines—economic anxieties, ethnic or sectarian tensions, political polarization, distrust of institutions—that can be exploited and amplified through targeted messaging. Sophisticated state-level operators conduct detailed sociological and psychographic research on target populations to identify the narratives most likely to resonate. Russia's Social Design Agency (SDA), the primary organizational vehicle behind the Doppelganger campaign, developed detailed strategy papers analyzing the specific vulnerabilities of French, German, Ukrainian, and American audiences before designing tailored content packages for each market (CORRECTIV, 2024) [3, 13].

Content production in contemporary operations increasingly relies on generative AI. Large language models can produce politically targeted articles in multiple languages at scale; AI voice-cloning technology can fabricate audio attributed to political leaders; deepfake video generators can produce convincing synthetic footage of events that never occurred. The World Economic Forum has documented that during the 2024-2025 electoral cycle, cloned voices and visual persona deepfakes became 'a more prevalent risk and a live feature of democratic politics,' with verified incidents in Slovenia, Romania, Ireland, and the Netherlands (WEF, 2026).

Distribution infrastructure encompasses the networks of websites, social media accounts, and content distribution systems used to publish and circulate disinformation content. The Doppelganger operation typifies this approach through its systematic creation of cloned versions of

legitimate Western news outlets—fabricated replicas of Spiegel, Le Monde, Fox News, and the Washington Post designed to deceive audiences about the provenance of false articles (DFRLab, 2024). These fake sites are coupled with bot networks and paid social-media advertising to ensure initial distribution, while traffic distribution systems (TDS) such as the Kehr.io service is used to redirect audiences and evade platform content moderation (Qurium, cited in INTRINSEC, 2025) [20].

Amplification mechanisms exploit the algorithmic logic of social media platforms—which prioritize emotionally provocative, novel, and socially validating content—to achieve organic distribution far beyond the initial seeding. Research by Vosoughi *et al*. (2018) [44] in Science demonstrated that false news stories spread approximately six times faster than true ones on Twitter/X, driven primarily by human retweet behavior rather than bots. This structural feature of digital information platforms means that even modestly resourced disinformation operations can achieve disproportionate influence if their content is sufficiently emotionally resonant.

**Integration with Kinetic and Cyber Operations**

A defining characteristic of mature hybrid campaigns is the deliberate synchronization of information operations with cyberattacks and kinetic military action. Mandiant's analysis of Russian threat actor APT44 (Sandworm) documented a consistent pattern of coordinating the timing of cyber operations against Ukrainian critical infrastructure with missile and drone strikes, such that digital disruptions amplified the psychological impact of physical attacks and vice versa (Mandiant/Google Cloud, 2024) [7, 16, 22]. The October 2022 Sandworm attack on a Ukrainian energy substation—which deployed the Industroyer2 malware to trip circuit breakers and cause power outages—coincided precisely with a mass Russian missile strike on infrastructure across Ukraine, a synchronization designed to maximize both physical damage and psychological effect.

This integration reflects a broader doctrinal evolution in Russian military thought. The concept of 'reflexive control,' developed within Soviet and post-Soviet military theory, holds that the primary objective of modern warfare is to cause the adversary to make decisions favorable to one's own side by feeding them carefully curated information and shaping their perceptual environment. Under this doctrine, information operations are not ancillary to military action but constitute its essential precondition and complement.

**Case Study I: Russia's Hybrid Warfare in Ukraine**

**Preparatory Information Operations (2014–2022)**

Russia's information warfare against Ukraine did not begin with the full-scale invasion of February 2022 but rather constituted a sustained, years-long campaign of narrative preparation. Following the 2014 Revolution of Dignity and annexation of Crimea, Russian state and state-affiliated media systematically advanced a set of core narratives designed to delegitimize Ukrainian statehood, portray Ukrainian political leadership as Western puppets or fascists, and construct a revisionist historical framework in which Ukraine was an artificial nation inseparable from Russia. These narratives were amplified through RT (Russia Today), Sputnik, and an extensive network of third-party websites and social-media accounts operating under the broader framework of what researchers have called Russia's 'firehose of falsehood' approach—producing high volumes of contradictory content designed not to persuade but to confuse and overwhelm (Paul & Matthews, 2016) [30].

Between 2014 and 2022, Russian cyber operations against Ukraine served both intelligence collection and infrastructure disruption functions while simultaneously generating content for information operations. The BlackEnergy attacks on the Ukrainian power grid in December 2015 and December 2016—the first confirmed cases of cyberattacks causing power outages to civilian populations—were followed by intensive Russian media coverage that undermined confidence in Ukrainian state institutions and foreshadowed the vulnerability of Ukrainian infrastructure (SANS ICS, 2016). The 2017 NotPetya attack, described by the CIA as a Russian military operation and by Wired magazine's Andy Greenberg as the most destructive cyberattack in history, caused an estimated $10 billion in global economic damage while generating a narrative of Ukrainian state incapacity (Nakashima, 2018) [24].

**Full-Scale Invasion: Synchronized Hybrid Campaign (2022–2025)**

The February 24, 2022, invasion inaugurated the most intensively documented case of hybrid warfare in the modern era. Within hours of the invasion's launch, Russian cyber operators deployed WhisperGate and HermeticWiper malware against Ukrainian government, financial, and media organizations, defacing websites and destroying data in parallel with the opening military offensive. According to the National Security Archive's analysis, these attacks targeted government websites and critical infrastructure to create confusion, undermine trust, and amplify the psychological impact of the opening military strikes (NSA, 2023).

Over the subsequent three years, Russia's primary cyber operational unit in Ukraine—Sandworm (formally designated APT44 by Google's Mandiant in April 2024) [22] [16]—was responsible for nearly all disruptive and destructive cyberattacks in the theater. Mandiant's comprehensive assessment documented six distinct operational phases ranging from pre-invasion pre-positioning, through multiple disruption-focused phases targeting energy, water, heating, and transportation systems, to a more recent refocus toward cyber-espionage as Russian military strategy shifted toward a war of attrition (Mandiant, 2024) [22]. APT44's deployment of new wiper variants including SwiftSlicer (2023) and ZEROLOT (2024-2025), as well as the Infamous Chisel malware targeting Ukrainian military Android devices, demonstrated a continuous evolution of both tools and tactics (PicusSecurity, 2026) [31].

The information operations dimension of Russia's campaign was equally sophisticated. Russian state and affiliated media maintained a prolific output of disinformation targeting both Ukrainian domestic audiences and the Western publics whose political support was essential to Ukraine's defense effort. Key narratives included claims of Ukrainian government corruption and dysfunction, allegations of neo-Nazi ideology among Ukrainian military forces, disinformation about Western weapons falling into terrorist hands, and repeated assertions that NATO's support for Ukraine was dragging the world toward nuclear war. The Doppelganger campaign—the most extensively documented coordinated inauthentic behavior operation linked to

Russia—specifically targeted Western audiences with content designed to undermine support for Ukraine and amplify political polarization within NATO member states.

According to Leiden University research published in January 2025 [21, 26, 27], hybrid operations linked to Russia rose sharply from 13 documented incidents in 2023 to 44 in 2024, while the U.S. Helsinki Commission recorded 150 hybrid operations from February 2022 to November 2024 (CyberPeace Institute, 2025) [2, 5, 41]. This escalation reflects not a loss of effectiveness but rather a deepening commitment to hybrid methods as Russian conventional military operations stalled in the face of Ukrainian resistance and Western material support.

**Narrative Warfare and the Battle for Western Opinion**

A particularly significant dimension of Russian information operations was their targeting of Western democratic publics. Understanding that Ukraine's military survival depended on sustained Western political will to provide financial and military assistance, Russian operators invested heavily in campaigns designed to erode that support. The Doppelganger operation deployed cloned versions of major Western news outlets—including fake replicas of Germany's Spiegel, France's Le Monde, and the United States' Washington Post and Fox News—to publish fabricated articles advancing narratives favorable to Russian interests (DFRLab, 2024). The operation's four core message themes were consistent: that sanctions against Russia were ineffective and self-destructive; that Western publics were suffering economically as a result of supporting Ukraine; that Russophobia was an irrational and dangerous ideology; and that Ukraine itself bore responsibility for the conflict.

The operational sophistication of the Doppelganger campaign was demonstrated by its adaptation and persistence in the face of countermeasures. Despite being sanctioned by the European Union and the United States, the campaign continued operating through the use of cloaking services, new domain registrations, and exploitation of European-based internet infrastructure. A CORRECTIV investigation published in July 2024 [3] revealed that Doppelganger was partly relying on European and German companies to spread its propaganda, raising serious questions about the governance of the internet infrastructure used by disinformation operations (CORRECTIV, 2024) [3, 9, 13]. The U.S. Department of Justice seized 32 internet domains linked to the campaign in September 2024, with the DOJ affidavit revealing that the operation was directed from Putin's inner circle through Sergei Kiriyenko, head of the Kremlin's domestic policy directorate (DOJ, 2025).

**Case Study II: China's Cognitive Warfare Against Taiwan**

**Doctrinal Foundations of Chinese Information Warfare**

China's approach to information warfare is grounded in the concept of 'Three Warfares' (san zhong zhanfa)—public opinion warfare, psychological warfare, and legal warfare—formally incorporated into the People's Liberation Army's (PLA) political work regulations in 2003. These doctrinal frameworks reflect the CCP's strategic objective of achieving political and military objectives against Taiwan through 'winning without fighting,' minimizing the need for kinetic conflict by exhausting Taiwanese political will, fragmenting domestic cohesion, undermining alliances with democratic partners, and making resistance appear futile (Smallwarsjournal, 2025) [38]. China's political warfare against Taiwan is explicitly a whole-of-party, whole-of-state, and whole-of-military effort, coordinated by the United Front Work Department, the Cyberspace Administration of China, and the PLA's Strategic Support Force.

Drawing directly on the lessons of Russia's experience in Ukraine—which the PLA has studied intensively—China's military strategy now establishes a joint and multi-domain doctrine that prioritizes the integration of cyber operations, information operations, and electronic warfare within a unified operational framework (FPRI, 2025). The PLA's recent reorganization created new cyber and information warfare structures specifically designed to operationalize this integrated doctrine.

**Scale and Persistence of Chinese Cyber Operations**

The quantitative scale of Chinese cyber operations against Taiwan is extraordinary. Taiwan's National Security Bureau reported that cyberattacks targeting Taiwan's key infrastructure rose 6% in 2025 from the previous year to an average of 2.63 million attacks per day—a figure representing a 113% increase compared to 2023 and reflecting an exponential escalation in the intensity of Chinese cyber pressure (TechRepublic, 2026) [39]. Energy and emergency rescue/hospital sectors experienced the most significant year-on-year surge, reflecting a strategic prioritization of attacks on infrastructure whose disruption would most severely damage civilian morale and public confidence in the government's capacity to protect its citizens.

Taiwan's National Security Bureau characterized this campaign as a form of hybrid warfare combining information-system intrusions with traditional military exercises, attempting to disrupt military capabilities and pre-position for potential conflict (Techi, 2026). The cyber operations are closely coordinated with Chinese military actions around Taiwan: China carried out 40 joint military exercises around the island in 2025, with many cyberattacks timed to coincide with these maneuvers to compound psychological pressure and test response times.

**Cognitive Warfare Tactics Against Taiwan**

Taiwan's 2024 and 2025 presidential elections served as major focal points for Chinese cognitive warfare operations. In the lead-up to the 2024 election, China deployed AI-generated disinformation campaigns—including deepfakes and synthetic narratives—designed to discredit Democratic Progressive Party candidate Lai Ching-te, portraying him as a 'separatist' who would inevitably provoke war with China. These campaigns reportedly employed generative AI to create false personas and deepfakes suggesting that 'reunification' viewpoints were more widespread within Taiwan than they actually were (Smallwarsjournal, 2025) [38].

Taiwan's National Security Bureau's analysis of Chinese cognitive warfare tactics in 2025 identified five primary operational categories: the deployment of fake websites by entities linked to China's Central Publicity Department and Ministry of Public Security; the hijacking of Taiwanese social media accounts through cyber intrusions; the use of rented overseas servers as proxies to spread fabricated disinformation; the coordinated amplification of divisive

narratives through bot networks; and the exploitation of cultural and linguistic similarities between mainland China and Taiwan to make Chinese-origin propaganda less distinguishable from authentic domestic discourse (Globalsecurity.org, 2026).

China's information operations against Taiwan are also integrated with broader infrastructure sabotage operations. In February 2023, Chinese vessels severed undersea cables near the Matsu Islands, leaving residents without internet access for more than 50 days. A similar operation in January 2025 targeted the Trans-Pacific Express Cable System, with Chinese-linked entities employing sophisticated vessel-tracking obfuscation to conceal their involvement (GeopoliticalMonitor, 2025) [12]. These physical infrastructure attacks are designed to amplify the effects of cyber operations and information campaigns by creating information vacuums that can be filled with Chinese-originated narratives.

## The Euro-Atlantic Information Battlefield: AI, Elections, and Democratic Resilience

### Operation Doppelganger: Anatomy of a Global Influence Network

Operation Doppelganger, established in 2022 by Russia's Social Design Agency under Kremlin direction, represents the most extensively documented coordinated foreign influence operation targeting Western democracies. The operation has targeted Ukraine, Germany, France, the United States, Italy, Israel, and multiple other countries, with the overarching aim of serving Kremlin narratives—primarily by weakening Western support for Ukraine and amplifying political polarization within NATO member states (Wikipedia, Doppelganger entry).

Meta classified Doppelganger as an advanced persistent threat (APT) in its Q2 2024 threat report and reported that approximately $105,000 was invested in advertising on its platform alone—a remarkably low investment for an operation that achieved documented distribution to hundreds of thousands of users. Bavarian intelligence data covering the period from May 2023 to July 2024 documented 7,983 Doppelganger campaigns generating 828,842 clicks across a monitored sample that represented only a fraction of the operation's full scope (EU DisinfoLab, 2024) [8].

The German Federal Foreign Office's June 2024 [13] technical report described Doppelganger as 'one of the largest and most sophisticated disinformation campaigns spreading pro-Russian narratives and disinformation discovered to date worldwide.' The campaign operated in multiple languages, maintained an evolving repertoire of distribution tactics to circumvent platform content moderation, and demonstrated a capacity for rapid narrative adaptation in response to breaking news events (German Federal Foreign Office, 2024) [13].

### AI-Enabled Disinformation: Deepfakes and Electoral Interference

The 2024-2025 period marked a qualitative threshold in the deployment of AI-generated synthetic media for influence operations. As the World Economic Forum documented in its March 2026 [45] analysis, deepfake technology crossed a critical threshold in this period, eliminating earlier tell-tale glitches and becoming accessible to anyone with a smartphone. Evidence from multiple national elections confirmed that cloned voices and visual persona deepfakes had become standard tools of electoral interference (WEF, 2026).

In December 2024, Romania's Constitutional Court took the extraordinary step of annulling the first round of the country's presidential election after intelligence surfaced evidence of a months-long influence campaign—involving AI-generated content and Russian-linked social-media amplification—designed to boost a nationalist, pro-Russian candidate (Selejan-Gutan, 2024; PMC, 2025) [32]. In Ireland's 2025 presidential election, a deepfake video falsely depicted the eventual winner withdrawing his candidacy, including fabricated footage of national broadcasters confirming the news, released just days before polling day (WEF, 2026). The Netherlands saw approximately 400 AI-generated synthetic images deployed to attack political candidates during the same electoral cycle.

The Indian subcontinent also emerged as a significant theater of AI-enabled information warfare following the April 2025 Pahalgam terrorist attack in Kashmir. Within hours of the attack, which killed 26 civilians, Telegram and X were flooded with synthetic narratives: deepfake videos depicted senior military officials discussing alleged 'false flag' operations; AI-generated images fabricated militant figures and military victories; and religious iconography was weaponized to escalate communal tensions. India's Press Information Bureau identified seven major instances of misinformation during the crisis, with evidence pointing to coordinated activity by Pakistan-linked actors reportedly aided by China (ORF, 2026; GlobalTaiwan, 2025) [14].

### Social Media Platforms as Structural Enablers

A persistent challenge in addressing cyber-propaganda is the role of commercial social media platforms as structural amplifiers of disinformation content. The algorithmic logic of engagement-maximizing content recommendation systems systematically privileges content that generates strong emotional reactions—outrage, fear, moral indignation—which also happens to be the primary emotional register of effective disinformation. Research on the 2016 and subsequent U.S. elections documented that false news stories spread significantly faster than true ones on Twitter/X, with human retweet behavior—not bot activity—being the primary driver of this differential spread.

The European Union's Digital Services Act (DSA), which entered full enforcement in 2024 [9], created the first comprehensive regulatory framework requiring major platforms to conduct risk assessments for their contribution to information manipulation and to take proportionate mitigation measures. Early enforcement actions under the DSA targeted X (formerly Twitter) over concerns about its decision to reduce trust and safety staffing while hosting disinformation from state-linked accounts. The effectiveness of the DSA framework remains contested, with critics arguing that the enforcement mechanisms are too slow to address the speed at which disinformation campaigns can spread and adapt.

## Countermeasures, Policy Responses, and Resilience Frameworks

### NATO's Strategic Communications Architecture

The NATO alliance has developed a progressively more sophisticated institutional architecture for countering information warfare over the past decade. The NATO

Strategic Communications Centre of Excellence (StratCom COE), established in Riga in 2014, serves as the primary research and coordination hub for the Alliance's information operations countermeasures. In 2024, the Centre published NATO's first strategic communications fundamentals doctrine, formalizing a shared framework for communication professionals across the Alliance and marking a significant step toward doctrinal coherence on information warfare (NATO ACT, 2025) [26, 27].

On July 10, 2024, NATO unveiled an updated AI strategy that explicitly highlighted the dangers of AI-enabled disinformation and information operations, signaling a recognition that generative AI had fundamentally altered the threat landscape (RUSI, 2024) [28]. The NATO Parliamentary Assembly's 2025 [26, 27] committee report on Chinese disinformation emphasized the urgency of bolstering efforts to counter PRC information manipulation operations, noting that the emergence of AI tools and the popularity of TikTok were exacerbating risks to Allied populations and institutions (NATO PA, 2025) [26, 27].

The NATO Parliamentary Assembly has also called for decisive coordinated action on cyberattacks and disinformation, urging Allied governments to improve threat awareness through monitoring, proactive communication, and public education, while preventing the spread of disinformation through legislation and strengthening institutional resilience (NATO PA, 2024) [28]. This represents a significant evolution from earlier NATO positions that treated information operations primarily as a communications challenge rather than a security threat requiring coordinated defensive action.

**EU Policy Framework and Digital Resilience**

The European Union has developed the most comprehensive multilateral framework for addressing information manipulation of any major international institution. The EU's approach to hybrid threats and disinformation has been progressively strengthened through multiple instruments: The Action Plan against Disinformation (2018), the European Democracy Action Plan (2020), the Digital Services Act (2022, enforced 2024) [7, 8, 9], and the Foreign Information Manipulation and Interference (FIMI) framework developed by the EU External Action Service. The EU's Strategic Agenda 2024-2029 explicitly identifies 'hybrid threats and disinformation' as priority security challenges (European Council, 2024) [8, 9].

The FIMI framework is particularly significant because it moves beyond the terminology of 'disinformation'—which implies a focus on the falsity of specific content—to address the structural and systemic manipulation of the information environment regardless of whether individual pieces of content are technically false. This conceptual shift recognizes that influence operations can be highly effective using selectively true information, strategic omissions, amplification of authentic but marginal voices, and narrative framing rather than outright fabrication.

**National-Level Responses: Taiwan's Model**

Taiwan has developed what many securities analysts regard as the most sophisticated national-level framework for countering hybrid warfare threats among democratic states. Facing over 2.4 million cyberattacks daily in 2024, Taiwan institutionalized cyber threat intelligence-sharing with the United States and other partners, passed the Organization Act of the Administration for Cyber Security under the Ministry of Digital Affairs in 2022, and launched a national cybersecurity strategy incorporating public-private partnership mechanisms (GlobalTaiwan, 2025) [14].

Taiwan's Ministry of Digital Affairs has also developed innovative rapid-response mechanisms for countering disinformation, including a government-affiliated fact-checking infrastructure that operates at the speed of social media rather than the traditional news cycle. The 'humor over rumor' approach pioneered by former Digital Minister Audrey Tang employed creative, accessible counter-narratives designed to be shared virally in competition with disinformation content—a recognition that the most effective counter-disinformation interventions must compete on the same emotional and aesthetic terrain as the disinformation they seek to rebut.

**Media Literacy and Societal Resilience**

Beyond institutional and technical countermeasures, researchers and policymakers have increasingly emphasized the importance of building societal resilience against information manipulation through media literacy education, prebunking interventions, and strengthened civic epistemics. Finland's model of comprehensive media literacy education—integrated across the curriculum from primary school through university and incorporated into vocational training for all public sector employees—has been widely cited as a benchmark for building population-level resistance to disinformation. Finland consistently ranks among the most resilient European societies to information manipulation in cross-national surveys.

Prebunking—the technique of exposing people to weakened forms of disinformation arguments in order to build cognitive resistance, analogous to vaccine inoculation against disease—has been validated through randomized controlled experiments as an effective method for reducing susceptibility to novel disinformation content. Research by van der Linden *et al*. (2022) [43] demonstrated that brief prebunking interventions significantly reduced the perceived accuracy of disinformation in experimental populations, with effects persisting for multiple weeks. Google's deployment of prebunking advertisements targeting key vulnerable demographics in European elections represents the first large-scale application of this research outside controlled laboratory settings.

**Discussion: The Future of Cyber-Propaganda in Hybrid Warfare**

The foregoing analysis supports several major conclusions about the trajectory of cyber-propaganda within hybrid warfare and its implications for international security.

First, the integration of cyber-propaganda with kinetic and cyber operations is deepening rather than stabilizing. The evidence from Ukraine demonstrates that sophisticated state actors have developed doctrines, organizational structures, and technical capabilities specifically designed to synchronize information operations with physical attacks. This synchronization is not merely tactical—producing simultaneous psychological and physical effects—but also operational, using cyber operations to set conditions for information campaigns and using information operations to pre-shape the psychological environment in which kinetic actions will be received.

Second, generative AI has introduced a qualitative discontinuity in the threat landscape. The democratization of

synthetic media production—deepfakes, AI-generated text, voice cloning—has eliminated the technical barriers that previously limited sophisticated influence operations to well-resourced state actors. The convergence of increasingly capable and accessible AI tools with the algorithmic amplification logic of social media platforms creates a structural tendency toward information environment degradation that will be extraordinarily difficult to reverse through regulatory or technical countermeasures alone.

Third, the geographic scope of information warfare is expanding. While the Russia-Ukraine conflict and Chinese operations against Taiwan have been the primary analytical focus of this paper, the evidence reviewed here points to a broader globalization of information warfare methods and technologies. The use of AI-generated disinformation in the aftermath of the 2025 Pahalgam attack in India, the documented Chinese assistance to Pakistani information operations, and the proliferation of Doppelganger-style infrastructure across multiple theaters all indicate that the operational models pioneered by Russia and China are being adopted by a widening range of state and non-state actors.

Fourth, the cognitive domain has become a decisive strategic theater in its own right, not merely an adjunct to physical operations. The Romanian electoral annulment, the Irish deepfake incident, and the documented impact of influence operations on Western political support for Ukraine all demonstrate that information operations can achieve strategic-level effects—altering government policy, changing electoral outcomes, fragmenting alliances—without any kinetic military action. This has profound implications for how states conceptualize national security and for the adequacy of existing legal and institutional frameworks that remain primarily calibrated to physical threats.

Fifth, the challenge for democracies is fundamentally structural as well as operational. The very features that make democratic societies resilient in many respects—free speech, open information environments, independent media, competitive politics—also create structural vulnerabilities to information manipulation. Authoritarian states face no such dilemma: they can suppress domestic disinformation while projecting it outward, creating an asymmetric advantage. Effective democratic resilience must therefore be built not through restricting freedom of expression but through strengthening the epistemological foundations of public discourse—media literacy, institutional credibility, fact-checking infrastructure, and prebunking at scale.

## Conclusion

This paper has examined the structural integration of cyber-propaganda within contemporary hybrid warfare, demonstrating through detailed case analysis of Russia's campaign against Ukraine, China's cognitive warfare against Taiwan, and broader Euro-Atlantic influence operations that information warfare has moved from the periphery to the center of modern conflict. The evidence reviewed establishes that cyber-propaganda is not merely one instrument among many within the hybrid toolkit but rather the connective tissue that gives hybrid warfare its distinctive character—enabling belligerents to achieve strategic-level effects below the threshold of kinetic conflict, to shape the political and psychological environment in which military operations unfold, and to sustain pressure on adversaries across domains and timescales that conventional military power cannot reach.

The emergence of generative AI as an operational platform for influence operations represents the most significant recent development in this trajectory. By dramatically reducing the cost and technical barrier to sophisticated synthetic media production, AI has opened the cognitive domain to a far wider range of actors while simultaneously increasing the difficulty of detection and attribution. The documented deployment of AI-generated deepfakes in national elections across Romania, Ireland, the Netherlands, India, and Taiwan within a single two-year period signals that this is not a future threat but a present operational reality.

The countermeasures reviewed in this paper—NATO's strategic communications doctrine, the EU's FIMI framework and Digital Services Act, Taiwan's institutional resilience architecture, and media literacy and prebunking programs—represent meaningful progress but remain inadequate to the scale and sophistication of the threat. Effective democratic resilience against hybrid information warfare will require integrated whole-of-society strategies that combine technical detection and attribution capabilities with legal frameworks, institutional strengthening, proactive strategic communication, and long-term investment in the media literacy and epistemic infrastructure of democratic publics.

Ultimately, the contest over information represents a contest over the cognitive sovereignty of democratic citizens—their capacity to form accurate beliefs about the world and to act on those beliefs in ways that reflect their genuine values and interests rather than the manipulated perceptions engineered by adversarial actors. Protecting that sovereignty is not merely a security imperative but a foundational requirement of democratic governance in the twenty-first century.

## References


1. Center for European Policy Analysis (CEPA). The hybrid threat imperative: Deterring Russia before it is too late, 2025. https://cepa.org/comprehensive-reports/the-hybrid-threat-imperative-deterring-russia-before-it-is-too-late/
2. Commission on Security and Cooperation in Europe (Helsinki Commission). Russia's shadow war on NATO, 2024. https://www.csce.gov/hearings/russias-shadow-war-on-nato/
3. CORRECTIV. Inside Doppelganger: How Russia uses EU companies for its propaganda, 2024. https://correctiv.org/en/fact-checking-en/2024/07/22/inside-doppelganger-how-russia-uses-eu-companies-for-its-propaganda/
4. CORRECTIV. Doppelganger: CORRECTIV investigations bring Russian propaganda campaign to a halt. European Digital Media Observatory, 2024. https://edmo.eu/publications/doppelganger-correctiv-investigations-bring-russian-propaganda-campaign-to-a-halt/
5. CyberPeace Institute. Cyber dimensions of hybrid warfare, 2025. https://cyberpeaceinstitute.org/news/cyber-dimensions-of-a-hybrid-warfare/
6. Defense Feeds. How Russia's hybrid warfare is transforming the war in Ukraine, 2025.

https://defensefeeds.com/analysis/conflicts/russias-hybrid-war/
7. Digital Forensic Research Lab (DFRLab). Doppelganger: How Russia mimicked real news sites and created fake ones to target US audiences. Atlantic Council, 2024. https://dfrlab.org/2024/09/18/doppelganger-us-election/
8. EU DisinfoLab. Doppelganger hub, 2024. https://www.disinfo.eu/doppelganger-hub/
9. European Council. Strategic agenda 2024–2029, 2024. https://www.consilium.europa.eu/
10. Foreign Policy Research Institute (FPRI). China's cyber playbook for the Indo-Pacific, 2025. https://www.fpri.org/article/2025/08/chinas-cyber-playbook-for-the-indo-pacific/
11. Galeotti M. 'Hybrid war' and 'little green men': How it works and how it doesn't. In A. Pikulicka-Wilczewska & R. Sakwa (Eds.), Ukraine and Russia: People, politics, propaganda and perspectives E-International Relations, 2016, 156–164.
12. Geopolitical Monitor. 'War without harm': China's hybrid warfare playbook against Taiwan, 2025. https://www.geopoliticalmonitor.com/war-without-harm-chinas-hybrid-warfare-playbook-against-taiwan/
13. German Federal Foreign Office. Technical report on an analysis of the Doppelgänger disinformation campaign, 2024. https://www.auswaertiges-amt.de/resource/blob/2682484/2da31936d1cbeb9faec49df74d8bbe2e/technischer-bericht-desinformationskampagne-doppelgaenger-1--data.pdf
14. Global Taiwan Institute. Lessons for India: How Taiwan handles Chinese political warfare, 2025. https://globaltaiwan.org/2025/07/lessons-for-india/
15. GlobalSecurity.org. Analysis of China's cognitive warfare tactics against Taiwan in 2025. Taiwan National Security Bureau, 2026. https://www.globalsecurity.org/intell/library/reports/2026/2025-china-cognitive-warfare-tactics-against-taiwan_nsb_20260110.pdf
16. Google Cloud / Mandiant. Sandworm disrupts power in Ukraine using a novel attack against operational technology, 2024. https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/
17. Google Cloud / Mandiant. APT44: Unearthing Sandworm, 2024. https://cloud.google.com/blog/topics/threat-intelligence/
18. HybridSec. State of hybrid conflict: Fall 2025, 2025. https://hybridsec.org/blog/hybrid-warfare-stateof2025/
19. HybridSec. Hybrid warfare 2025: Blurring the lines between war and peace, 2025. https://hybridsec.org/blog/hybrid-warfare-2025-trends/
20. INTRINSEC. Doppelganger: New disinformation campaigns spreading on social media through Russian networks, 2025. https://www.intrinsec.com/en/doppelganger-new-disinformation-campaigns-spreading-on-social-media-through-russian-networks/
21. Leiden University. Research: Europe increasingly targeted by Russian sabotage, 2025. https://www.universiteitleiden.nl/en/news/2025/01/research-europe-increasingly-targeted-by-russian-sabotage
22. Mandiant. APT44: Unearthing Sandworm [Security report]. Google Cloud, 2024.
23. Marsili M. Navigating the risks of hybrid warfare: Cyber, cognitive, and information threats at the brink of conflict. IX Media International Scientific Conference. ResearchGate, 2024. https://www.researchgate.net/publication/385751572
24. Nakashima E. Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. The Washington Post, 2018.
25. NATO. Hybrid warfare [Background document]. NATO Headquarters, 2015.
26. NATO Allied Command Transformation (ACT). Shaping the future of strategic communications in NATO, 2025. https://www.act.nato.int/article/stratcom-coe-2025/
27. NATO Parliamentary Assembly (NATO PA). Chinese disinformation report—Teitelbaum (011 CDSRCS), 2025. https://www.nato-pa.int/document/2025-chinese-disinformation-report-teitelbaum-011-cdsrcs
28. NATO Parliamentary Assembly (NATO PA). NATO assembly calls for decisive action on cyberattacks and disinformation, 2024. https://www.nato-pa.int/news/nato-assembly-calls-decisive-action-cyberattacks-and-disinformation-stronger-partnerships
29. Observer Research Foundation (ORF). Algorithms of falsehood: The challenges of governing AI-generated disinformation, 2026. https://www.orfonline.org/expert-speak/algorithms-of-falsehood-the-challenges-of-governing-ai-generated-disinformation
30. Paul C, Matthews M. The Russian 'firehose of falsehood' propaganda model. RAND Corporation, 2016. https://www.rand.org/pubs/perspectives/PE198.html
31. Picus Security. Inside Sandworm: Decade of cyber sabotage and espionage activity, 2026. https://www.picussecurity.com/resource/blog/inside-sandworm-decade-of-cyber-sabotage-and-espionage-activity
32. PMC / Springer. The fundamental rights risks of countering cognitive warfare with artificial intelligence. AI & Society, 2025. https://pmc.ncbi.nlm.nih.gov/articles/PMC12500826/
33. Renz B. Russia and 'hybrid warfare.' Contemporary Politics,2016:22(3):283–300. https://doi.org/10.1080/13569775.2016.1201316
34. Romandash A. Hybrid warfare: Ukraine, Russia, and Western lessons (Policy Brief No. 209). Centre for International Governance Innovation, 2025. https://www.cigionline.org/documents/3540/PB_no.209.pdf
35. Royal United Services Institute (RUSI). The need for a strategic approach to disinformation and AI-driven threats, 2024. https://www.rusi.org/explore-our-research/publications/commentary/need-strategic-approach-disinformation-and-ai-driven-threats
36. RUSI. Russia, AI and the future of disinformation warfare, 2025. https://static.rusi.org/russia-ai-and-the-future-of-disinformation-warfare.pdf
37. Sensity AI. The role of deepfakes in cognitive warfare, 2026. https://sensity.ai/blog/the-role-of-deepfakes-in-cognitive-warfare/
38. Small Wars Journal / Arizona State University. China's political warfare: The fight for Taiwan on the information battlefield, 2025.

https://smallwarsjournal.com/2025/02/19/chinas-political-warfare-the-fight-for-taiwan-on-the-information-battlefield/
39. TechRepublic. China launched 2.6M daily cyberattacks on Taiwan in 2025, 2026. https://www.techrepublic.com/article/news-china-cyberattacks-taiwan/
40. The Record / Recorded Future News. Russian hackers target 20 energy facilities in Ukraine amid intense missile strikes, 2024. https://therecord.media/russian-hackers-target-energy-facilities-ukraine
41. The Record / Recorded Future News. Russia's Sandworm hackers deploying wipers against Ukraine's grain industry, 2025. https://therecord.media/russia-sandworm-grain-wipers
42. US. Department of Justice. Justice Department disrupts covert Russian government-sponsored foreign malign influence operation, 2025. https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence
43. van der Linden S, Roozenbeek J, Compton J. Inoculating against fake news about COVID-19. Frontiers in Psychology,2022:11:566790. https://doi.org/10.3389/fpsyg.2020.566790
44. Vosoughi S, Roy D, Aral S. The spread of true and false news online. Science,2018:359(6380):1146–1151. https://doi.org/10.1126/science.aap9559
45. World Economic Forum (WEF). How cognitive manipulation and AI will shape disinformation in 2026, 2026. https://www.weforum.org/stories/2026/03/how-cognitive-manipulation-and-ai-will-shape-disinformation-in-2026/