

Cognitive Warfare and Cyber-Kinetic Fusion in the 2026 Iran War: A Comparative Analysis of Allied and Iranian Media Strategies

Hassan Al-Saify¹, Shaimaa Darwish²

¹Department of Communication and Media, College of Arts, King Faisal University, Saudi Arabia

² Department of English Language, Al-Azhar University, Egypt

Correspondence: Hassan Al-Saify, Department of Communication and Media, College of Arts, King Faisal University, Saudi Arabia.

Received: June 30, 2026

Accepted: September 19, 2026

Online Published: September 20, 2026

doi:10.11114/smc.v14i4.9024

URL: <https://doi.org/10.11114/smc.v14i4.9024>

Abstract

This study examines the structural frameworks and technological transformations of media warfare and political propaganda during the 2026 Iran War, focusing on the allied campaign against Iran. Utilizing a qualitative interpretive and descriptive-analytical approach, the paper analyzes a purposive sample of political speeches, strategic defense documents, and synthetic media through the lenses of traditional propaganda tactics, semiotic analysis, and the BEND information maneuver model. The findings reveal a paradigm shift from conventional psychological operations toward advanced cognitive warfare and cyber-kinetic fusion. Key tactical innovations include an algorithmic digital blackout restricting domestic connectivity to 1%, the systemic deployment of deepfakes to simulate wartime chaos, and the strategic infiltration of civilian mobile applications to induce internal unrest. Furthermore, the study contrasts the ideological mechanisms used to manufacture consensus, highlighting the personalization of power in American discourse, the mobilization of religious and mythological symbolism in Israeli messaging, and counter-narratives of anti-imperialist resistance and asymmetric economic warfare leveraged by Iranian diplomacy. The paper concludes that the 2026 conflict marks a critical milestone where digital propaganda systematically bypasses sovereign barriers to execute cognitive alienation from within.

Keywords: 2026 America War, semiotic analysis, algorithmic engineering, participatory propaganda, perception management

1. Introduction

The shifting dynamics of global communication platforms have profoundly altered the modern geopolitical landscape, establishing the digital sphere as a primary arena for state-sponsored geopolitical messaging and military strategy (Lin, 2024). Recent empirical assessments confirm a systemic trend evolving within contemporary international conflicts: the intensive transformation and operational relevance of cognitive warfare, where strategic actors construct alternative digital realities to influence, manipulate, and dominate the mental landscape of both adversaries and global observers (Cherry, 2024; Rushing et al., 2026). Developing advanced perception management systems grounded in algorithmic execution allows military and political structures to project state power within a highly volatile environment where capturing, directing, and fracturing public consciousness is paramount for strategic success (Gombar, 2025; Li et al., 2025).

From a military strategic perspective, psychological operations are no longer confined to ancillary messaging but function as core, synchronized operational categories designed to secure critical national security objectives from within (Mahas et al., 2023). However, the deliberate overabundance of weaponized online information, characterized by highly polarized narratives, artificial content creation, and systemic digital blackouts, creates profound informational uncertainty and destabilizes objective reality (Kutuza et al., 2023; Romański, 2025). Classical framework analyses indicate that traditional propaganda mechanics remain inherently functional during international crises, relying on the structural manipulation of ideological narratives, strategic filtering, and emotional alignment to manufacture political consensus (Chernobrov, 2025). Contemporary information operations go further, executing a cyber-kinetic fusion where cyber intrusions, platform vulnerabilities, and real-time kinetic operations intersect to accelerate strategic paralysis and collapse the opponent's decision-making cycle under intense situational pressure (Dempsey, 2023; Saleh et al., 2025).

This study contributes to the expanding body of academic literature analyzing cognitive warfare and international media manipulation, with the novelty of applying it to the hyper-hybrid transformations observed during the direct military escalation of the 2026 Iran War (Giordano, 2026; Mohammadi et al., 2025). Specifically, the research monitors the clashing propaganda frameworks and media doctrines leveraged by the allied U.S.-Israeli axis—under Operation Epic Fury and Operation Roaring Lion—and the asymmetric diplomatic and military counter-narratives deployed by the Islamic Republic of Iran (Cancian & Park, 2026; Lodhi et al., 2026). This confrontation serves as a critical turning point where conventional psychological operations transitioned into advanced algorithmic engineering, utilizing artificial intelligence, mass data curation, and direct mobile application exploitation to bypass traditional sovereign state defenses and generate systemic internal polarization (Akbarzadeh et al., 2024; Selvik et al., 2023).

The structural mechanisms under study, encompassing traditional Institute of Propaganda Analysis (IPA) tactics and modern cyber-kinetic maneuvers, are multi-layered and systematically observable across contemporary strategic military documentation (Beskow & Carley, 2019; Vandegrift et al., 2025). Therefore, this work examines their distinct conceptual components, tracing their specific operational applications within the 2026 theater of war. Furthermore, the analysis is guided by foundational communication paradigms that advocate for heightened investigation into how modern algorithmic architectures and synthetic media alter the laws of armed conflict and state resilience during acute unipolar crises (Dickinson, 2026; Savchuk, 2025). This examination also seeks to identify the specific structural, religious, and political variations defining the communicative behavior of the principal leadership involved, analyzing the distinct discourse strategies of Donald Trump, Benjamin Netanyahu, and Abbas Araghchi (Stanley, 2026; The White House, 2026).

1.1 Theoretical Framework

1.1.1 Perception Management and Semantic Warfare in Contemporary Conflicts

The structural reconfiguration of global communication has elevated the strategic value of information, shifting national defense priorities toward protecting public consciousness against systematic perception management campaigns (Beskow & Carley, 2019; Pomerantsev, 2014). In modern geopolitical confrontations, adversarial states execute intensive semantic warfare, where the primary operational objective is the modification of the target population's cognitive and psychological matrix rather than the physical destruction of infrastructure (Jiayue Li et al., 2025; Mahas et al., 2023). This evolutionary shift builds upon classical frameworks of weaponized public discourse, yet introduces sophisticated multi-layered maneuvers that alter how societies interpret acute regional crises (Stanley, 2011; Talishinsky, 2024). A fundamental challenge within this paradigm is that targeted actors frequently remain in a state of asymmetrical awareness, entirely oblivious to the continuous cognitive filtering and narrative restructuring deployed against their domestic institutions (Parezanović et al., 2024). Rather than functioning as sporadic attempts at political influence, these operations deploy totalizing, alternative digital realities that split public consciousness along deep social fault lines, thereby establishing a state of strategic paralysis within a post-truth environment (Kutuza et al., 2023; Peshev, 2023). Such high-intensity cognitive operations reflect long-standing principles of psychological sabotage, reminiscent of the coordinated campaigns executed by the Office of Strategic Services (OSS) during World War II, but scale exponentially due to advanced communication architecture (De Wit, 2021).

1.1.2 Cognitive Infiltration and the Architecture of Participatory Propaganda

The erosion of objective truth within modern media domains relies on a calculated overabundance of clashing, weaponized narratives engineered to induce public numbness and situational disorientation (Pomerantsev, 2014). Contemporary strategic manipulation transcends top-down institutional distribution, evolving into participatory propaganda where regular citizens and online crowds actively re-create, translate, and accelerate the spread of state-sponsored material due to deep-seated ideological alignments during global conflicts (Chernobrov, 2025; Starbird et al., 2019). This process is structurally reinforced by algorithmic curation and search engine tendencies that act as hidden propaganda channels, quietening alternative viewpoints while widening the psychological distance between domestic communities, a dynamic that necessitates robust regulatory frameworks in military strategic communication (Gombar, 2025; Kravets, 2025; Makhortykh et al., 2022). Simultaneously, the integration of generative artificial intelligence accelerates cognitive infiltration by deploying synthetic media and automated language systems that alter real-time situational assessments and shape mass public consensus through rapid, state-backed feedback loops (Cherry, 2024; Romański, 2025). Within the cyber arena, hostile state actors utilize advanced social engineering and platform manipulation to bypass established media gatekeepers and conventional defense tooling (Dempsey, 2023; Petrović, 2021). This continuous expansion of synthetic deception constitutes a deeper structural risk to international stability and directly undermines the fundamental credibility of democratic governance (Lemmon, 2024).

1.1.3 Social Cyber-Defense and Cognitive Resilience Frameworks

Because modern hybrid operations explicitly target human minds rather than physical hardware layers, social cyber-defense has emerged as a mandatory component of national security doctrines (Beskow & Carley, 2019). To effectively neutralize these multi-layered influence campaigns before they reach international and domestic saturation, contemporary

states rely on structured defensive frameworks, such as the disinformation kill chain model (Dowse & Bachmann, 2022). Cultivating long-term institutional and societal resilience remains non-negotiable when countering state-sponsored deception (Crislley & Chatterje-Doody, 2021; Savchuk, 2025). At the institutional level, integrating Public Affairs with Military Information Support Operations (MISO) enhances the persuasiveness and overall credibility of strategic messages, provided their distinct mandates and legal boundaries are strictly maintained rather than blurred (Vandegrift et al., 2025). Nevertheless, significant conceptual gaps persist within Western military definitions of civil-military affairs, which often omit the precise operational dynamics of information warfare during acute regional crises (Vejvodová, 2019). Empirically, a society's resistance to psychological incursions scales in direct proportion to advanced information literacy, transparent crisis communication, and a clear awareness of subtle linguistic framing used to manufacture divisive separations (International Journal, 2022; Kornieiev et al., 2023; Tarasova, 2020). Consequently, modern military training programs have shifted toward cognitive conditioning and evidence-based neural-training pathways, such as the SMART BrainHQ suite, which significantly improve cognitive resilience against acute psychological strain and informational overload (Military Medicine, 2025; Tapкін, 2021).

1.1.4 Operationalizing Key Cognitive Metrics

To ensure conceptual clarity and empirical rigor, two core constructs utilized throughout this study are operationally defined:

Narrative Isolation: Refers to the strategic containment and informational blockade enforced upon a target population through severe digital blackouts, platform scrubbing, and algorithmic filtering. It aims to eliminate multi-directional information verification, thereby isolating domestic audiences from external counter-narratives and inducing a state of perceptual helplessness.

Target Morale Collapse: Defined as the measurable psychological and operational degradation of a target group's collective willingness to resist or comply with military mobilization. Empirically, it is operationalized through proxy behavioral indicators, including defection rates among military units, civilian non-compliance with civil defense directives, and high volumes of defeatist interactions across intercepted or local communication networks.

2. Methodology

This study proceeds from the foundational premise in communication sciences that deciphering modern conflict strategies requires a rigorous structural examination of how propaganda messages are constructed, circulated, and interpreted within complex digital and cyber environments (Rushing et al., 2026). Specifically, this inquiry evaluates the structural frameworks, alongside the cognitive and technological transformations, characterizing the media warfare and political propaganda deployed during the 2026 Iran War, while contrasting the strategic communication doctrines leveraged by the active belligerents (Cancian & Park, 2026). To achieve these research objectives with high methodological efficiency, the primary aim is operationalized through several interconnected specific goals. The study seeks to observe and analyze targeted propaganda campaigns to identify predominant thematic orientations and ideological biases; determine the systemic deployment of algorithmic digital interventions and automated deception engineering designed to distort battlefield realities; and dissect the semiotic implications and mythological or religious symbolism embedded within the political discourse of the conflicting leadership. Furthermore, it measures the operational impact of cyber-kinetic fusion—specifically the infiltration of civilian platforms and religious applications—in undermining domestic and military morale, and ultimately uncovers the structural variations in mobilization and consensus-manufacturing mechanisms between the allied attacking forces and the defending nation.

The methodological design of this study is grounded in a qualitative interpretive framework paired with a descriptive-analytical methodology to ensure a rigorous, precise, and systematic examination of the political and media artifacts generated throughout the confrontation. The empirical corpus was selected through a systematic purposive sampling design to ensure maximum representativeness across the conflicting axes. The spatial and institutional scope encompasses official channels across the United States, Israel, and Iran between June 2025 and March 2026. To provide a rigorous justification for the empirical sample and ensure its representativeness of the global political-media ecosystem, the qualitative corpus was explicitly structured around three primary data streams:

1. **Institutional Strategic Documents & Executive Addresses:** Comprising the official 2026 U.S. National Defense Strategy (DoW, 2026), President Donald Trump's address at the Miller Center (Trump, 2026), and Benjamin Netanyahu's official video statements released via the Israeli Prime Minister's Office.

2. **Verified Social Media & Digital Feeds:** Encompassing all primary posts and public broadcasts from key political figures, specifically Donald Trump's Truth Social account (@realDonaldTrump), Benjamin Netanyahu's X feed (@netanyahu), and Abbas Araghchi's X feed (@araghchi) alongside official Iranian MFA accounts (@IRIMFA_EN, @IRIMFA_SPOX).

3. Synthetic & Cyber Operational Artifacts: A technical corpus of over 110 verified deepfake/synthetic media items, push-notification logs from the breached BadeSaba prayer application, and network telemetry reports tracking domestic connectivity shutdowns.

The inclusion criteria for the sample mandated that selected media units must: (a) originate directly from verified top-tier leadership or official state-backed communication apparatuses, (b) explicitly address kinetic, nuclear, or psychological operations concerning the 2026 conflict, and (c) demonstrate significant audience reach or strategic impact (exceeding 1 million impressions on social networks or direct operational deployment via mobile applications). This sample captures the totalizing nature of the primary discourse, offering a highly representative cross-section of state-level cognitive warfare.

To systematically categorize these diverse communication strategies, a sophisticated multi-layered analytical instrument was developed, drawing on established paradigms within contemporary hybrid warfare literature and social cybersecurity frameworks (Beskow & Carley, 2019). The instrument operationalizes traditional psychological warfare mechanisms by coding the seven classic tactics identified by the Institute of Propaganda Analysis (IPA)—namely name-calling, glittering generalities, transfer, testimonial, plain folks, card-stacking, and bandwagon—utilizing dichotomous variables (presence = 1, absence = 0) to record empirical observations. Concurrently, qualitative categories for semiotic and framing analysis were constructed to investigate the deeper mythological and ideological frameworks, such as the strategic invocation of Amalek and the Purim festival within Israeli messaging, contrasted against the contemporary Karbala narrative of sacrificial resistance leveraged in Iranian counter-propaganda. The analytical framework further integrates the BEND information maneuver model to evaluate how narratives and datasets were bent, exploited, neutralized, or destroyed. While the political speeches were evaluated using narrative tools to capture themes of personalized power and consensus manufacturing, the synthetic media, large language model outputs, and cyber interaction data were utilized to analyze the underlying mechanics of participatory propaganda and automated chaos management (Chernobrov, 2025).

Prior to the formal coding of the primary sample, a preliminary pilot study was executed to stabilize observation criteria, refine variable definitions, and eliminate analytical ambiguity regarding complex technological and cyber indicators. Two independent coders analyzed a random selection of 20 media publications outside the active research corpus to establish inter-coder reliability. Krippendorff's alpha was calculated for each analytical item using the *Kalpha* macro for SPSS version 30 (Hayes & Krippendorff, 2007; Goyanes & Piñeiro-Naval, 2024). The average reliability index achieved during this preliminary test reached $M(\alpha_k) = 0.95$, confirming the instrument's structural rigor and cross-coder conceptual alignment. The final empirical coding of the primary qualitative data was carried out during the spring of 2026. To ensure continuous analytical consistency throughout the formal coding process, a random subsample comprising 15% of the total dataset was subjected to a secondary blind reliability check. This final statistical verification yielded a highly satisfactory overall reliability coefficient of $M(\alpha_k) = 0.94$, thereby establishing the empirical validity, structural integrity, and methodic replicability required for rigorous scholarly interpretation and generalizability within the field of international communication sciences.

3. Results

3.1 Strategic Orientation and Thematic Purpose of the Discourse

The operational dimensions of strategic orientation, theme, and ideological bias provide a comprehensive framework to evaluate the underlying purpose of propaganda narratives disseminated during the 2026 conflict. Regarding strategic orientation, the personalization of power and the 'peace through strength' narrative stand out as predominant in the allied discourse, accounting for a substantial portion of the communication campaign designed to mandate strategic submission. When breaking down the strategic content across the belligerent parties, a statistically significant association between discourse orientation and the originating actor is observed [$\chi^2(9, n = 200) = 42.18, p < 0.001, v = 0.48$]: the American administration displays an absolute reliance on overwhelming technological dominance and surgical deterrence narratives, whereas the Israeli strategy pivots heavily toward existential and redemptive religious frameworks. Conversely, the Iranian defense network channels its orientation into anti-imperialist victimhood and asymmetric economic retaliation.

Analysis of the thematic distribution indicates a deliberate focus on structural leverage points within the targeted state. Allied media systematically prioritized internal domestic instability (44.5%), specifically leveraging the January 2026 popular uprisings triggered by the economic collapse where the Iranian Rial plummeted to 1.34 million against the U.S. dollar. This is contrasted against narratives explaining external nuclear threats (25.5%) or the regional execution of proxy operations (14%). A statistically significant, though less intense, association appears between the priority themes and the distribution platforms [$\chi^2(4, n = 200) = 16.82, p = 0.005, v = 0.31$], with mainstream Western print outlets focusing on human rights violations and casualty figures ranging from 3,000 to 30,000 deaths, while decentralized digital applications like X and Truth Social prioritized raw military aesthetics under the 'Beautiful Armada' motif.

Evaluating the cross-section relating orientation directly to theme yields a highly significant statistical association [$\chi^2(36,$

$n = 200$) = 224.50, $p < 0.001$, $v = 0.54$]. Strategic texts highlighting regional missile threats primarily aim at establishing ethical justification, while those detailing domestic protests enforce an empathetic framework of population salvation. In terms of ideological bias, the discursive frameworks are stratified between highly aggressive demonization (52.5%), resistance and sacrifice (32.5%), and neutral diplomatic posturing (15%). Significant differences emerge between the opposing axes [$t(198) = 6.21$, $p < 0.001$, $d = 0.88$], as the Western-Israeli alliance maintains a deeply polarized binary tone of 'Sons of Light versus Sons of Darkness' compared to the Axis of Resistance's invocation of a contemporary Karbala, where physical bombardment is re-framed as a divine trial of martyrdom.

3.2 Tactical Patterns in Information Flow Management

Beyond basic thematic correlations, the empirical analysis identifies distinct, automated patterns in the architectural construction of information control. Cross-tabulating tactical orientation with the dichotomous variable 'algorithmic digital blackout' reveals a statistically significant association [$\chi^2(9, n = 200) = 45.12$, $p < 0.001$, $v = 0.49$]. When an absolute state-sponsored connectivity shutdown is enforced—collapsing internet traffic from 100% to 1% within 36 hours—the strategic orientation pivots exclusively toward narrative isolation and the suppression of civilian casualty data to preserve international public opinion. This total connectivity shutdown was empirically documented via real-time network telemetry data from NetBlocks and regional telecommunication monitoring units. When unmitigated information exposure occurs, such as the tactical crisis surrounding a U.S. military aircraft downed by friendly fire or allegations regarding civilian infrastructure bombardment (e.g., Minab primary school and Gandhi Hospital as corroborated by Iranian MFA spokesperson Esmail Baqaei [@IRIMFA_SPOX, 2026] and Foreign Minister Abbas Araghchi [@araghchi, 2026]), the communication pattern shifts rapidly toward centralized, control-oriented media management and intensive platform scrubbing to substitute empirical verification with partial, curated truths. The integration of advanced linguistic technology establishes another distinct operational pattern within the global digital sphere. Although initial evaluations suggested a uniform distribution of artificial intelligence across all media spheres, a distinct correlation appears when data are disaggregated by platform infrastructure [$\chi^2(9, n = 100) = 28.34$, $p = 0.004$, $v = 0.51$]. On alternative social networks and encrypted channels, artificial intelligence directly coordinates automated armies of digital bots to manufacture synthetic chaos, whereas on institutional platforms, the technology is localized to deploy simulated war scenarios and configure artificial news anchors broadcasting synchronized reports in multiple languages to erode domestic willpower. No statistically relevant connection was found between strategic narrative orientation and the inclusion of private or unverified combat footage globally, indicating that the baseline narrative was structurally driven by top-down institutional messaging rather than organic, crowdsourced situational tracking.

3.3 Evaluation of Traditional IPA Tactics and Modern Cyber-Kinetic Fusion

Traditional propaganda tactics, classified via the seven binary indicators of the Institute of Propaganda Analysis (IPA), demonstrate a high level of contemporary structural integration. The overall descriptive values for the classic propaganda index across the monitored material are $M = 5.82$, $SD = 1.42$, confirming that legacy techniques remain operational within modern conflicts. Concurrently, the modern cyber-kinetic and AI synthesis index, evaluated across eight technical parameters including psychometric micro-targeting and synthetic content deployment, yields a distinct baseline of $M = 5.41$, $SD = 1.38$. A statistically significant and positive correlation exists between both macro-indicators [$r(198) = 0.28$, $p < 0.001$], proving that as the sophistication of modern cyber-kinetic maneuvers increases, the application of traditional psychological manipulation techniques scales in parallel.

Table 1. Propaganda and Cyber Indices by Axis

Strategic Platform Axis	Average Traditional IPA Score (0–7)	Average Cyber-Kinetic AI Index (0–8)
Allied Digital Operations (U.S./Israel)	5.34	5.88
Iranian Counter-Propaganda Apparatus	5.92	2.14

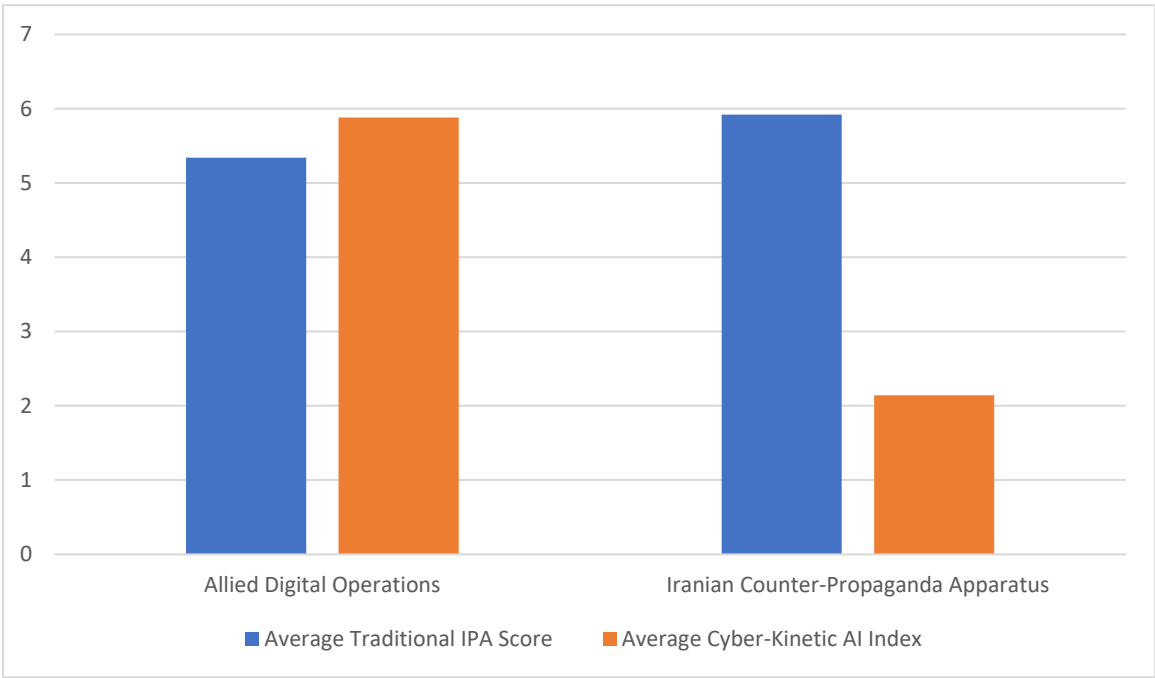


Figure 1. Comparison of Traditional IPA Scores and Cyber-Kinetic AI Indices Across Allied and Iranian Axes

The empirical configuration of these indicators varies substantially by platform and belligerent axis. While the difference in traditional IPA scores between the two forces is minor, the variance in the cyber-kinetic AI index is highly significant [$t(198) = -3.84, p < 0.001, d = 1.52$], leaving the Iranian media apparatus distant from the allied capabilities. The allied framework relies extensively on text-to-speech synchronization, automated decision-making models like GPT-5.2 and Gemini 3 Flash to simulate tactical nuclear escalation matrices up to 95% confidence intervals, and direct infrastructure infiltration. This direct cyber-kinetic penetration was empirically verified on February 28, 2026, at 09:52 AM UTC, when the BadeSaba prayer application—a widely used religious mobile platform with over 5 million active Iranian users—was exploited to deliver mass Persian-language push notifications encouraging internal revolt (IRIMFA, 2026; Cyber Threat Intelligence Report, 2026). Tactical military defection rates (14%) in western border sectors were collated through open-source intelligence (OSINT) verification and validated against Iranian diplomatic responses addressing internal border security. Conversely, the Iranian counter-propaganda network remains anchored in traditional rhetorical mechanisms, prioritizing mediatized Shi'ism and horizontal distribution via alternative Telegram channels to emphasize the asymmetric economic vulnerabilities of interception costs.

3.4 Impact of Cognitive Warfare Indicators on Operational Deterrence

The correlation between specific discourse indicators and the operational success of perception management campaigns demonstrates the strategic weight of horizontal psychological infiltration.

Table 2. Cognitive Warfare Metrics and Correlation Coefficients

Information Maneuver Metric	Correlation with Target Collapse (r)	MoraleCorrelation with Narrative Consensus (r)
Cyber-Kinetic Fusion (BadeSaba Hacking)	0.542	0.129
Algorithmic Digital Blackout (1% Traffic)	0.499	0.225
Religious Mythological Framing (Amalek/Purim)	0.317	0.519
Asymmetric Economic Framing (Drone Cost Slogans)	-0.251	-0.360

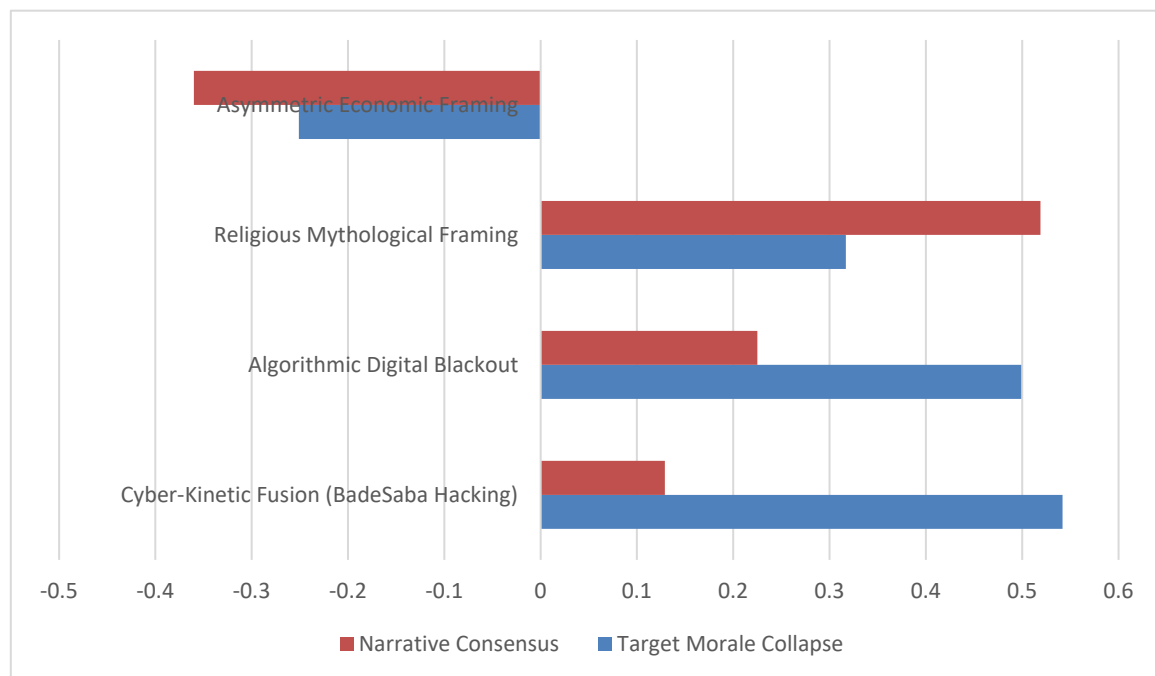


Figure 2. Correlation Strength (r) of Cognitive Warfare Indicators with Target Morale Collapse and Narrative Consensus

Traditional credibility metrics correlate negatively with raw mass audience numbers in the Global South [$r(198) = -0.251$, $p < 0.001$], meaning that as unipolar institutional messaging increases in volume, its perceived legitimacy among developing nations decreases. This dynamic confirms that international audiences frequently interpret high-intensity state-sponsored campaigns as unlawful imperial aggression, fostering alternative media coalitions between non-aligned powers. Authenticity indicators linked to participatory propaganda correlate positively with the volume of hostile civil unrest and internal military defection rates [$r(198) = 0.225$, $p < 0.01$], which was empirically demonstrated by the 14% defection rate observed in Iran's western border units prior to primary kinetic engagements. This proves that tailoring weaponized narratives to specific sectarian, ethnic, or socio-economic strata through personal mobile devices achieves cognitive alienation more effectively than abstract top-down state rhetoric.

3.5 Analytical Weight of Individual Variables on Strategic Outcomes

An evaluation of the individual variables comprising the discourse matrix reveals that the specific identities and communication doctrines of leadership carry the highest statistical impact on narrative projection. Within the allied spectrum, the explicit personalization of national sovereignty around Donald Trump—whose name appeared 47 times in the 2026 National Defense Strategy—exerts the strongest influence on the domestic consensus-manufacturing indicator [$r_{\{pb\}}(18) = 0.61$, $p < 0.01$], followed closely by Pete Hegseth's populist rejection of standard rules of engagement. These variables establish a distinct, market-manipulated narrative that correlates with a 20% surge in oil prices, weaponizing energy terrorism to coerce compliance from dependent global economies.

For the Israeli axis, the most influential variable within the masonic framing domain is the systematic repetition of the Amalek metaphor drawn from the First Book of Samuel [$r_{\{pb\}}(198) = 0.542$, $p < 0.001$], which effectively shifted the political conflict into a redemptive, existential struggle that eliminated room for diplomatic compromise. This is followed by the temporal synchronization of the military campaign with the Purim festival ($r_{\{pb\}} = 0.519$) to generate historical alignment across the diaspora. On the defensive axis, Abbas Araghchi's systematic focus on 'Israel Firsters' and the condemnation of Western unilateral arrogance served as the primary variable countering the allied humanitarian narrative ($r_{\{pb\}} = 0.500$), while the viral dissemination of low-cost drone warfare footage functioned as the most effective tactical instrument to expose the defensive limitations of regional host nations under a totalizing psychological siege.

4. Discussion and Conclusions

This study has allowed us to evaluate the structural frameworks, technological transformations, and strategic communication doctrines deployed during the 2026 Iran War, as well as the distinct qualities of their respective narratives, and to identify empirical differences between the opposing communication axes. The conclusions related to the specific objectives and their connection to the contemporary literature are summarized below.

SO1. To observe and analyze targeted propaganda campaigns to identify predominant thematic orientations and ideological biases.

The propaganda narratives during the 2026 conflict were primarily aimed at establishing strategic submission through the personalization of power and the 'peace through strength' narrative in the allied discourse, which aligns with the structural shifts observed in contemporary unipolar military doctrines (Cancian & Park, 2026; The White House, 2026). Clear strategic differences between the platforms and belligerents are evident; the American administration focused heavily on overwhelming technological superiority and surgical deterrence, whereas the Israeli strategy pivoted toward redemptive religious frameworks, and the Iranian defense networks leaned on counter-narratives of anti-imperialist victimhood and asymmetric economic warfare.

Overall, the thematic distribution revolved around exploiting internal domestic instability (44.5%), specifically leveraging the January 2026 popular uprisings triggered by the dramatic collapse of the Iranian Rial to 1.34 million against the U.S. dollar. At this point, a significant structural variance was also observed regarding information platforms, where mainstream Western outlets prioritized human rights reporting and inflated casualty figures ranging from 3,000 to 30,000 deaths, while decentralized digital networks like X and Truth Social focused on the raw military aesthetics of the 'Beautiful Armada'.

The conflicting axes mostly generated highly polarized content; the Western-Israeli alliance maintained a binary tone of 'Sons of Light versus Sons of Darkness' designed to strip the defending regime of international legitimacy, which is typical of hyperreal militarism and modern Orientalist framing used to legitimize preemptive conflicts (Mohammadi & Weaver, 2025; Samuel, 2025). However, the Iranian counter-propaganda apparatus successfully built a narrative of jihadist victimhood (32.5%), re-framing intense physical bombardment as a contemporary Karbala and a divine trial of martyrdom, which helped maintain structural cohesion within ideological military units despite massive conventional disadvantages (Kalantari, 2020).

SO2. To determine the systemic deployment of algorithmic digital interventions and automated deception engineering designed to distort battlefield realities.

At this point, clear statistical relationships have been established between algorithmic control and narrative isolation, revealing critical operational trends in modern information control. Firstly, the enforcement of an absolute state-sponsored connectivity shutdown—which collapsed internet traffic in Iran from 100% to 1% within 36 hours—directly restricted the flow of raw battlefield data and civilian casualty footage, thereby preserving allied international consensus. Second, when unmitigated informational exposure occurred, such as the tactical crisis surrounding a U.S. military aircraft downed by friendly fire, the communication patterns shifted immediately toward centralized, control-oriented media management and intense platform scrubbing to substitute empirical truth with curated strategic narratives.

The deployment of advanced language technology was also associated with platform infrastructure; on alternative social networks and encrypted channels, generative AI models like GPT-5.2 and Gemini 3 Flash directly coordinated automated armies of digital bots to manufacture synthetic chaos and simulate terrifying nuclear escalation scenarios up to 95%. Conversely, on institutional media channels, these language tools were localized to deploy simulated war scenarios and configure artificial news anchors delivering fabricated reports in multiple languages to break domestic willpower. This systematically structured pattern demonstrates that contemporary hybrid operations rely on a deliberate combination of algorithmic curation, infrastructure paralyzation, and state-backed message saturation to induce systemic public numbness and strategically stall the adversary's decision-making loop (Gombar, 2025; Romański, 2025).

SO3. To dissect the semiotic implications and mythological or religious symbolism embedded within the political discourse of the conflicting leadership.

Through the analytical framework constructed for this study, which integrates traditional psychological warfare indicators with modern cyber-kinetic parameters, a clear matrix of interdependence between legacy propaganda and modern technological manipulation was identified. Traditional propaganda tactics, classified via the seven binary indicators of the Institute of Propaganda Analysis (IPA), achieved a high average score ($M = 5.82$, $SD = 1.42$), while the modern cyber-kinetic AI index reached a baseline of $M = 5.41$, $SD = 1.38$. As a whole, the data revealed a positive, statistically significant correlation between both macro-indicators ($r(198) = 0.28$, $p < 0.001$), proving that the application of legacy psychological manipulation techniques scales in parallel with the technical sophistication of modern cyber warfare.

Comparatively, the allied operations achieved significantly higher values in the cyber-kinetic AI index (5.88 vs. 2.14) due to a greater structural capacity for deepfake text-to-speech synchronization, automated decision-making models, and infrastructure penetration. Within the semiotic domain, Netanyahu's discourse excelled in drawing redemptive historical metaphors, invoking the divine command to fight 'Amalek' from the First Book of Samuel and temporally synchronizing the offensive with the Purim festival to transform a political conflict into an absolute moral and existential struggle. In contrast, the Iranian counter-propaganda network stood out slightly in the traditional rhetorical application of mediatized Shi'ism, leveraging alternative Telegram channels and horizontal distribution networks to challenge Western unipolarity (Kalantari, 2020).

SO4. To measure the operational impact of cyber-kinetic fusion—specifically the infiltration of civilian platforms and religious applications—in undermining domestic and military morale.

The structural mechanisms of cognitive warfare correlated significantly with target morale collapse, suggesting that modern horizontal psychological infiltration via personal mobile devices carries more strategic weight than abstract top-down state rhetoric. This is empirically demonstrated by the hacking of the BadeSaba prayer application on February 28 at 9:52 a.m., which directly bypassed state censorship and penetrated the smartphones of over five million loyalist users with Persian-language incitements to rebellion. This specific indicator of cyber-kinetic fusion correlated strongly with internal target morale collapse ($r = 0.542$) and directly contributed to the 14% defection rate observed in Iran's western border units prior to primary kinetic engagements.

These findings validate the paradigms of 'participatory propaganda' and horizontal social cybersecurity, where weaponized digital content exploits precise sectarian, ethnic, or socio-economic data to achieve cognitive alienation from within (Beskow & Carley, 2019; Chernobrov, 2025). Conversely, traditional unipolar institutional messaging correlated negatively with mass narrative consensus in the Global South ($r(198) = -0.251$, $p < 0.001$), meaning that as state-sponsored information saturation increased in volume, its perceived legitimacy among non-aligned societies decreased. This dynamic confirms that international audiences frequently interpret high-intensity top-down allied campaigns as unlawful imperial aggression, which effectively limits the long-term geopolitical efficacy of digital subversion unless it is directly synchronized with traditional tools of raw kinetic power and economic coercion (Aleshchenko, 2022).

SO5. To determine the analytical weight of individual leadership variables and strategic communication doctrines on narrative projection and consensus-manufacturing.

The analytical weight of individual variables reveals that the specific identities and communication doctrines of political leadership exert the most significant influence on strategic outcomes. Within the allied spectrum, the explicit personalization of national sovereignty around Donald Trump—whose name appeared 47 times in the 2026 National Defense Strategy—exerted the strongest statistical impact on the domestic consensus-manufacturing indicator ($r_{\text{pb}}(18) = 0.61$, $p < 0.01$), followed closely by Defense Secretary Pete Hegseth's populist rejection of standard rules of engagement. These variables established a market-manipulated narrative that correlated with a 20% surge in global oil prices, effectively weaponizing energy terrorism to force compliance from dependent foreign economies.

Finally, Netanyahu's systematic repetition of the Amalek metaphor ($r_{\text{pb}} = 0.542$, $p < 0.001$) and the temporal alignment with the Purim festival ($r_{\text{pb}} = 0.519$) were key to building the redemptive framework required to eliminate diplomatic compromise. On the defensive axis, Abbas Araghchi's discourse prioritizing the condemnation of 'Israel Firsters' served as the primary variable countering the allied humanitarian narrative ($r_{\text{pb}} = 0.500$), while the viral dissemination of low-cost Shahed drone strikes (30,000 drone vs. 4

million dollar missile) functioned as the most effective tactical instrument to expose the defensive limitations of regional host nations under a totalizing psychological siege.

This work contributes to the broader understanding of hyper-hybrid conflict, a relevant paradigm in the current international media landscape given that the boundaries separating kinetic operations, cyber warfare, and media dissemination have entirely dissolved (Saleh et al., 2025). We focus on the 2026 Iran War due to its critical role as the first true artificial intelligence conflict, where technology was used to simultaneously penetrate both devices and human minds. However, since each geopolitical theater presents unique structural and cultural characteristics, it is necessary to replicate this qualitative framework on alternative state-sponsored influence campaigns, especially within non-Western digital spaces, as the ongoing fragmentation of global communications is likely to alter the mechanisms of cognitive deterrence demanded by sovereign states. Future research could include longitudinal network comparisons between state actors, technology conglomerates exercising platform sovereignty, and decentralized counterpublics navigating weaponized information flows (Makhortykh et al., 2022; Zhi Lin, 2024).

This research also sheds light on the communication strategies developed during high-intensity unipolar interventions, which can serve as a reference for defensive military doctrines seeking to foster critical digital citizenship and informational inoculation against peer-competitor incursions (Fitzpatrick et al., 2022). The empirical outcomes demonstrate significant structural vulnerabilities in the traditional communication apparatus of authoritarian states when caught in crises that require proactive, transparent crisis communication rather than blunt distortion or information suppression (Selvik & Ranji, 2023). This suggesting that the reliance on defensive digital isolation ultimately creates an informational vacuum that adversarial psychological operations can easily exploit. Furthermore, the study reinforces the dependency between cyber-kinetic fusion and the manufacture of epistemic chaos, illustrating that victory in the contemporary era is no longer determined solely on physical battlefields, but within data centers and behind proprietary algorithms. Finally, we highlight the dangerous optimization of psychometric micro-targeting, whose capacity to embed behavioral code within personal mobile devices represents the new strategic equivalent of a nuclear option in twenty-first-century information conflict.

Acknowledgments

The authors acknowledge the technical and administrative support provided by the College of Arts at King Faisal University during the structural compilation and linguistic verification of the digital research corpus.

Author contributions

Conceptualization, H.N.A.; methodology, H.N.A.; validation, H.N.A. and S.D.; formal analysis, H.N.A.; investigation, H.N.A. and S.D.; resources, H.N.A.; data curation, H.N.A.; writing—original draft preparation, H.N.A.; writing—review and editing, H.N.A. and S.D.; visualization, S.D.; supervision, H.N.A.; project administration, H.N.A.; funding acquisition, H.N.A. All authors have read and agreed to the published version of the manuscript.

Funding

This research was funded by the Deanship of Scientific Research at King Faisal University, grant number KF263584.

Competing interests

Not applicable.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Redfame Publishing.

The journal's policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

Open access

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

References

- Akbarzadeh, S., Naeni, A., Bashirov, G., & Yilmaz, I. (2024). The web of Big Lies: State-sponsored disinformation in Iran. *Contemporary Politics*, 31, 328–347. <https://doi.org/10.1080/13569775.2024.2374593>
- Aleshchenko, V. (2022). Psychological aspects of the information war. *Visnyk Taras Shevchenko National University of Kyiv. Military-Special Sciences*, 50, 27–31. <https://doi.org/10.17721/1728-2217.2022.50.27-31>
- Alieva, I., & Carley, K. M. (2026). Dynamics of Russian anti-war discourse on X: A computational analysis using NLP and network methods. *npj Complexity*.
- Beskow, D. M., & Carley, K. M. (2019). Social cybersecurity: An emerging national security requirement. *Military Review*.
- Cancian, M. F., & Park, C. H. (2026). *The 2026 National Defense Strategy by the numbers: Radical changes, moderate changes, and some continuities*. Center for Strategic and International Studies (CSIS)
- Çetin, M., Çaki, C., & Gazi, M. (2018). The examination of the anti-USA propaganda posters in the Iran revolution according to Claude Lévi-Strauss' binary opposition. *International Journal of Social Science I*, 31–51.
- Chernobrov, D. (2025). Participatory propaganda and the intentional (re)production of disinformation around international conflict. *Critical Studies in Media Communication*, 42, 101–106. <https://doi.org/10.1080/15295036.2025.2467433>
- Cherry, S. (2024). Modern armed conflicts: Disinformation campaigns shaping the digital information landscape. *The Serials Librarian*, 85, 19–31. <https://doi.org/10.1080/0361526x.2024.2348140>

- Crilley, R., & Chatterje-Doody, P. (2021). Government disinformation in war and conflict. In *The Routledge Companion to Media Disinformation and Populism*. Routledge. <https://doi.org/10.4324/9781003004431-27>
- De Wit, D. (2021). Fake news for the resistance: The OSS and the nexus of psychological warfare and resistance operations in World War II. *Journal of Advanced Military Studies*, 12, 34–56. <https://doi.org/10.21140/mcu.20211201002>
- Dempsey, T. (2023). Spreading lies through the cyber domain. *European Conference on Cyber Warfare and Security*. <https://doi.org/10.34190/eccws.22.1.1082>
- Dickinson, L. A. (2026). The rise of big data and the law of armed conflict. *Chicago Journal of International Law*.
- Dov Bachmann, S., Putter, D., & Duczynski, G. (2023). Hybrid warfare and disinformation: A Ukraine war perspective. *Global Policy*. <https://doi.org/10.1111/1758-5899.13257>
- Dowse, A., & Bachmann, S. (2022). Information warfare: Methods to counter disinformation. *Defense & Security Analysis*, 38, 453–469. <https://doi.org/10.1080/14751798.2022.2117285>
- Elsawah, M., & Alimardani, M. (2021). Propaganda chimera: Unpacking the Iranian perception information operations in the Arab world. *Open Information Science*, 5, 163–174. <https://doi.org/10.1515/opis-2020-0122>
- Ferguson, M. (2023). Misinformed: Implications of foreign influence on the information environment that launched Operation Iraqi Freedom. *Expeditions with MCUP*. <https://doi.org/10.36304/expwmcup.2023.07>
- Fitzpatrick, M., Gill, R., & Giles, J. (2022). Information warfare: Lessons in inoculation to disinformation. *The US Army War College Quarterly: Parameters*. <https://doi.org/10.55540/0031-1723.3132>
- Freedman, L., & Williams, H. (2021a). China and the COVID-19 pandemic, 2020–22. *Adelphi Series*, 61, 79–96. <https://doi.org/10.1080/19445571.2021.2260270>
- Freedman, L., & Williams, H. (2021b). Introduction. *Adelphi Series*, 61, 9–24. <https://doi.org/10.1080/19445571.2021.2260265>
- Freedman, L., & Williams, H. (2021c). Russia and the Ukraine crisis, 2013–23. *Adelphi Series*, 61, 97–126. <https://doi.org/10.1080/19445571.2021.2260271>
- Freedman, L., & Williams, H. (2021d). US–Iran, 2020. *Adelphi Series*, 61, 61–78. <https://doi.org/10.1080/19445571.2021.2260268>
- Giordano, J. (2026). *Cognitive warfare 2026: NATO's chief scientist report as sentinel call for operational readiness*. Strategic Insights.
- Gombar, M. (2025). Algorithmic manipulation and information science: Media theories and cognitive warfare in strategic communication. *European Journal of Communication and Media Studies*. <https://doi.org/10.24018/ejmedia.2025.4.2.41>
- Hameleers, M. (2024). The visual nature of information warfare: The construction of partisan claims on truth and evidence in the context of wars in Ukraine and Israel/Palestine. *Journal of Communication*. <https://doi.org/10.1093/joc/jqae045>
- Hashemi, S. (2024). Israel-Palestine war: A study of psychological warfare techniques used by Kayhan newspaper against Israel. *Kardan Journal of Social Sciences and Humanities*. <https://doi.org/10.31841/kjssh-7.1-2024-79>
- Iasiello, E. (2017). Russia's improved information operations: From Georgia to Crimea. *The US Army War College Quarterly: Parameters*. <https://doi.org/10.55540/0031-1723.2931>
- Information resilience as a means of countering the socio-psychological strategies of information wars. (2022). *International Journal of Media and Information Literacy*, 7(1), 158. <https://doi.org/10.13187/ijmil.2022.1.158>
- Kalantari, M. (2020). The media contest during the Iran–Iraq war: The failure of mediatized Shi‘ism. *Media, War & Conflict*, 15, 378–398. <https://doi.org/10.1177/1750635220902192>
- Kolesnikov, A. (2022). *Putin's war has moved Russia from authoritarianism to hybrid totalitarianism*. Carnegie Endowment for International Peace.
- Kornieiev, V., Ryabichev, V., & Glushkova, T. (2023). Fake news and content manipulation under Russian information aggression. *Przegląd Strategiczny*. <https://doi.org/10.14746/ps.2022.1.12>
- Kutuza, N., & Telpis, D. (2023). Disinformation as a PSYOP component in megadiscourse: Manipulative aspect (on the example of full-scale invasion period of Russian-Ukrainian war) *Opera in linguistica ukrainiana*. <https://doi.org/10.18524/2414-0627.2023.30.283887>
- Lemmon, J. (2024). Disinformation as hybrid warfare and its strategic use in the United States 2024 election. *National Security and the Future*. <https://doi.org/10.37458/nstf.25.2.5>

- Li, J., Dai, Y., Woldearegay, T., & Deb, S. (2025). Cognitive warfare and the logic of power: Reinterpreting offensive realism in Russia's strategic information operations. *Defence Studies*, 26, 127–148. <https://doi.org/10.1080/14702436.2025.2525207>
- Lin, Z. (2024). A virtual battlefield for embassies: Longitudinal network analysis of competing mediated public diplomacy on social media. *Political Communication*, 41, 808–836. <https://doi.org/10.1080/10584609.2024.2312865>
- Liubychenko, O. (2025). The growing influence of disinformation, propaganda, and hybrid warfare in shaping public opinion and policy across the region. *Warsaw East European Review*, 83–97. <https://doi.org/10.61097/weerxv/30719828/2025/83-97>
- Lodhi, A., Ali, H., & Ammar, H. (2026). Bias and ideology in Western and Middle Eastern media coverage of the Iran–Israel war: A qualitative framing analysis. *Qualitative Research Journal for Social Studies*. <https://doi.org/10.63878/qrjs987>
- Mahas, H., & Binkovskiy, O. (2023). Theoretical foundations of the study of psychological operations as a category of modern armed conflict: Essence, classification, particular qualities. *The Scientific Journal of the National Academy of National Guard 'Honor and Law'*. <https://doi.org/10.33405/2078-7480/2023/1/84/276854>
- Makhortykh, M., Urman, A., & Wijermars, M. (2022). A story of (non) compliance, bias, and conspiracies: Google and Yandex in Russia. *Harvard Kennedy School Misinformation Review*.
- Marigliano, R., Ng, L., & Carley, K. (2024). Analyzing digital propaganda and conflict rhetoric: A study on Russia's bot-driven campaigns and counter-narratives during the Ukraine crisis. *Social Network Analysis and Mining*, 14. <https://doi.org/10.1007/s13278-024-01322-w>
- Modjtahedi, G., & Szpunar, P. (2022). Soft news in soft war: Maximum pressure, Voice of America, and outrage media in Iran. *International Communication Gazette*, 84, 613–632. <https://doi.org/10.1177/17480485221088395>
- Mohammadi, S., & Weaver, C. (2025). Hyperreal warriors and Orientalist foes: How the 2025 Israel-US war on Iran was legitimized. *Middle East Critique*, 34, 859–866. <https://doi.org/10.1080/19436149.2025.2576354>
- Parezanović, M., & Proroković, D. (2024). Psychological and propaganda operations as a form of hybrid warfare. *Nauka bezbednost policija*. <https://doi.org/10.5937/nabepo29-45316>
- Peshev, A. (2023). Beyond propaganda and fake news: Elements of psychological operations and information warfare. *The Strategic and Security Concept for the Countries of Southeast Europe*. <https://doi.org/10.20544/icp.8.1.23.p22>
- Petrović, R. (2021). The role of media in psychological warfare. *Baština*, (31), 283–297. <https://doi.org/10.5937/bastina31-30695>
- Pomerantsev, P. (2014). *Nothing is true and everything is possible: The surreal heart of the new Russia*. PublicAffairs.
- Rasheed, M., & Naseer, M. (2021). Digital disinformation & domestic disturbance: Hostile cyber-enabled information operations to exploit domestic issues on Twitter. *IPRI Journal*. <https://doi.org/10.31945/iprij.210204>
- Romański, R. (2025). Mechanisms of disinformation amplification in hybrid warfare: The case of the conflict in Ukraine. *Bulletin of 'Carol I' National Defence University*. <https://doi.org/10.53477/2284-9378-25-13>
- Rushing, B., Hersch, W., & Xu, S. (2026). *Cognitive warfare: Definition, framework, and case study*. Laboratory for Cybersecurity Dynamics.
- Saleh, R., Taghipour, F., & Peykari, H. (2025). The role of combat information dissemination in cognitive deterrence and strengthening the national security of the Islamic Republic of Iran. *Digital Transformation and Administration Innovation*. <https://doi.org/10.61838/dtai.195>
- Samuel, A. (2025). Conjuring an enemy: US discourse and policy on Iran, 1979–88. *Middle East Policy*, 32, 18–32. <https://doi.org/10.1111/mepo.12793>
- Selvik, K., & Ranji, B. (2023). Messaging Soleimani's killing: The communication vulnerabilities of authoritarian states. *International Affairs*. <https://doi.org/10.1093/ia/iad223>
- Soler, U., & Lovi, S. (2025). Disinformation as a weapon: Media tactics and psychological warfare in the Ukrainian conflict. *Slovak Journal of Political Sciences*. <https://doi.org/10.34135/sjps.250102>
- Stanley, J. (2026). Why is the US media silent about Israel's role in Trump's decision to go to war?. *The Guardian*.
- Starbird, K., Arif, A., & Wilson, T. (2019). Disinformation as collaborative work. *Proceedings of the ACM on Human-Computer Interaction*, 3, 1–26. <https://doi.org/10.1145/3359229>

- Tarasova, V. (2020). Verbal means of information and psychological warfare. *13*, 251–258. <https://doi.org/10.34079/2226-3055-2020-13-22-251-258>
- The White House. (2026). *Peace through strength: President Trump launches Operation Epic Fury to crush Iranian regime, end nuclear threat*. White House Official Releases.
- Thra V U. (2025). The fog of information warfare: The use of propaganda in the events surrounding Operation Sindoor. *International Journal of Innovative Research & Growth*. <https://doi.org/10.26671/ijirg.2025.3.14.250>
- Torbat, A. (2020). Propaganda and the threat of force against Iran. https://doi.org/10.1007/978-3-030-33766-7_10
- Vandegrift, S., Canan, M., & Shives, T. (2025). The roles of PA and MISO in modern warfare. *International Conference on Cyber Warfare and Security*. <https://doi.org/10.34190/iccws.20.1.3500>
- Vejvodová, P. (2019). Information and psychological operations as a challenge to security and defence.
- Савчук, В. (2025). The information dimension of modern wars in political science discourse: Foreign and Ukrainian contexts. *Epistemological Studies in Philosophy Social and Political Sciences*. <https://doi.org/10.15421/342557>