

# The Weaponization of Truth: Analyzing Misinformation as a Pillar of Fifth-Generation Warfare (5GW)

<sup>1</sup>Mehran Hayat, <sup>\*2</sup>Nazni Noordin

<sup>1</sup>School of Business and Social Sciences, Albukhary International University, Malaysia

<sup>2</sup>Faculty of Administrative Science and Policy Studies, Universiti Teknologi MARA, Malaysia

\*Corresponding Author

DOI: <https://dx.doi.org/10.47772/IJRISS.2026.1026EDU0174>

Received: 15 March 2026; Accepted: 20 March 2026; Published: 08 April 2026

## ABSTRACT

The landscape of modern conflict has shifted from the traditional battlefield of steel and lead to the invisible digital domains of the mind. In this new era, known as Fifth-Generation Warfare (5GW), the most powerful weapon is no longer a missile but a narrative. Traditional defense mechanisms are often ill-equipped to counter the rapid and viral spread of state-sponsored disinformation. This targets the nation's social and psychological fabric rather than its physical borders. This paper examined how misinformation serves as a core strategic tool in 5GW, specifically focusing on the "Weaponization of truth," in which facts are distorted to create chaos. Utilizing secondary data analysis, this paper explored cognitive warfare through the lens of two modern case studies: the high-stakes tensions between Iran and Israel and the long-standing rivalry between India and Pakistan. By analyzing these conflicts, this paper demonstrated how propaganda is used to manipulate public perception and trigger political instability. The findings highlight the urgent need for "cognitive security" frameworks, new ways for societies to protect themselves in an age of post-truth geopolitics. Ultimately, this paper argues that understanding the psychological impact of digital lies is essential for maintaining peace in a hyper-connected world.

**Keywords:** Fifth-Generation Warfare (5GW), Cognitive Security, Digital Propaganda, India- Pakistan Conflict, Iran-Israel Relations.

## INTRODUCTION

War has historically been understood as a form of physical confrontation conducted on defined battlefields and involving conventional military forces. However, the nature of conflict has evolved significantly in recent decades. With the rapid expansion of digital technologies, the arena of warfare has increasingly shifted towards informational and cognitive domains, where digital devices play a central role in shaping and disseminating strategic narratives. This is what experts call Fifth-Generation Warfare (5GW).

In this new era, the goal is not just to destroy an enemy's army, but to destroy their ability to tell what is true. By "weaponizing the truth," states can now create chaos and division without ever firing a single shot (Khan et al., 2025). This transformation is captured in the concept of 5GW, which extends beyond the asymmetric tactics of Fourth-Generation Warfare (4GW) (Scherling, 2026). While 4GW was about using violence to send a message, 5GW is about using information to change reality itself. It is "mental warfare" targeting the collective mind of a population (Puurunen, 2025; Krishnan, 2022).

Within this evolving landscape, misinformation has emerged as a central strategic instrument (Khan, 2025). Rather than relying solely on physical force, state and non-state actors increasingly use manipulated narratives to influence public opinion, shape political outcomes, and destabilize societies (Tweissi, 2025). Saleem et al. (2026) argue that these dynamics are evident in contemporary conflicts such as the Iran-Israel rivalry and the India-Pakistan relationship, where digital platforms serve as key arenas of competition.

Despite a growing body of research on misinformation and cybersecurity, existing studies do not sufficiently conceptualize misinformation as a structured and strategic component of 5GW. They often focus on technological mechanisms, such as algorithms and bots, while overlooking the strategic intent behind narrative construction and deployment (Shafie, 2022).

The problem is that when people can no longer distinguish between a genuine report and a state-sponsored lie, the social fabric of a country begins to tear (Wardle, 2024). This paper addressed this gap by examining misinformation as a core pillar of 5GW. Through a comparative analysis of the Iran–Israel and India–Pakistan conflicts, the study explored how narratives are constructed and weaponized to achieve cognitive and political objectives in contemporary geopolitical environments.

## LITERATURE REVIEW

### The Theoretical Framework of Fifth-Generation Warfare (5GW)

The shift from 4GW to 5GW reflects a transformation in conflict from the physical domain to the informational and cognitive domains. Scherling (2026) argues that 5GW blurs the boundaries between war and peace, extending conflict beyond traditional battlefields into the realm of perception and influence. Building on this, Puurunen (2025) conceptualizes 5GW as mental warfare, aimed at disrupting cognitive processes rather than destroying physical infrastructure.

Krishnan (2022) suggests that victory is achieved when a population can no longer independently distinguish between authentic and manipulated narratives. Furthermore, Mukherjee (2025) highlights the strategic role of narrative construction, where actors actively shape perceptions to advance political objectives. Together, these perspectives position 5GW as a form of conflict centered on controlling interpretation rather than territory.

### The Weaponization of Truth

The weaponization of truth in 5GW extends beyond the simple spread of false information, operating instead as a structured process of narrative construction and manipulation. Khan et al. (2025) conceptualize disinformation as a cycle of creation, dissemination, and amplification, in which information is strategically designed to remain partially grounded in truth to enhance credibility and emotional impact.

The dynamics of digital communication environments reinforce this process. Broda and Strömbäck (2024) argue that online platforms facilitate the formation of echo chambers, where selective exposure to information limits critical engagement and shields misleading narratives from correction. In such environments, emotionally charged content is more likely to gain visibility and influence public perception.

Furthermore, algorithmic systems play a crucial role in accelerating the spread of disinformation. As highlighted by Khan (2025) and Bakirov and Suleimenov (2025), digital platforms prioritize engagement-driven content, enabling state and non-state actors to amplify selective narratives and exploit existing social and political divisions. In this context, information becomes a strategic tool for shaping interpretations of reality and achieving geopolitical objectives.

This process, as shown in Figure 1, represents the strategic cycle of disinformation within the 5GW framework. The process begins with the creation phase, in which information is selectively distorted while preserving elements of truth to ensure credibility. This is followed by dissemination through digital platforms targeting specific audiences. The amplification stage is driven by algorithmic systems that prioritize engagement, allowing narratives to spread rapidly and form echo chambers. The cumulative effect of this cycle is cognitive paralysis, where the target population becomes unable to distinguish between authentic and manipulated information.

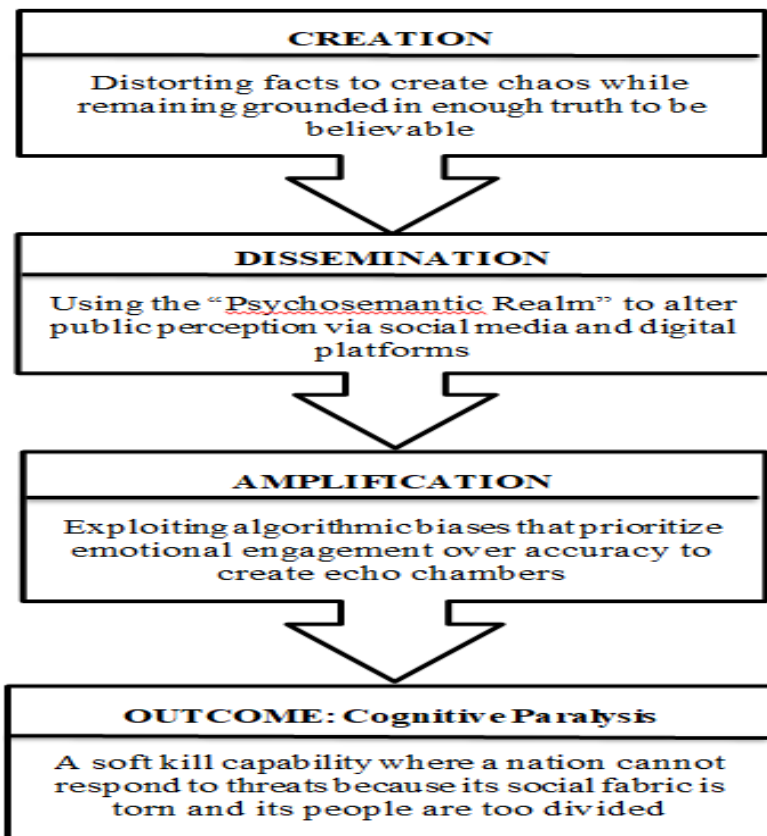


Figure 1: The strategic structure of Disinformation in Fifth-Generation Warfare (5GW)

### Cognitive Warfare and the Mechanics of Deception

A central dimension of 5GW is its ability to influence perceptions through cognitive and psychological means. Shafie (2022) describes this as the “psychosemantic realm,” where language, symbols, and narratives are strategically used to shape how individuals interpret reality. In this context, communication itself becomes a tool of conflict, allowing actors to bypass traditional military defenses and directly target the public consciousness.

Building on this, Mukherjee (2025) highlights the role of narrative warfare, where the objective is to construct persuasive interpretations of events that align with strategic interests. Rather than relying on physical force, actors seek to influence beliefs and expectations, shaping how societies understand both threats and outcomes.

This approach reflects a broader shift toward cognitive dominance as a strategic objective. Bakirov and Suleimenov (2025) emphasize the importance of cognitive sovereignty, referring to a state’s ability to protect its population from external manipulation. When this capacity is weakened, prolonged exposure to competing narratives can lead to social distrust and fragmentation, reducing a nation’s ability to respond effectively to crises. In this sense, cognitive warfare functions as a soft mechanism of destabilization, operating through psychological influence rather than direct confrontation.

### Case Study Analysis: Iran vs Israel in the Digital Domain

The ongoing rivalry between Iran and Israel provides a useful case for analyzing 5GW. Tweissi (2025) notes that this conflict has moved beyond simple proxy wars into a total information war. Both states use high-level strategic deceptions to manage domestic and international perceptions. For example, the use of “leaked” intelligence, whether real or fabricated, is intended to create a sense of dread.

Khan (2025) points out that in the Iran- Israel context, misinformation is often used to signal strength or weakness to the international community without the risks associated with conventional military strikes. The literature suggests that, for these two actors, the narrative of strikes is often more important than the strikes themselves. By controlling the flow of information, they can manage the escalation of the conflict, using digital tools to

achieve psychological victories that traditional weapons cannot. This demonstrates a transition towards perception management as a form of deterrence, where the goal is to convince the adversary that they have already lost the battle for international opinion (Krishnan, 2022).

### **Case Study Analysis: India vs Pakistan and the media battlefield**

In South Asia, the India-Pakistan conflict has been “digitized” in a way that directly impacts civilian populations, turning social media into a front-line trench. Saleem et al. (2026) conducted a phenomenological study showing how misinformation during border tensions creates widespread anxiety and radicalization among civilians. This is a classic 5GW outcome: destabilizing the home front through psychological pressure.

Zahra and Shahid (2025) explore how media stances in this region are often shaped by state-sponsored narratives that upload historical grievances to the digital age to trigger social distrust. The literature indicates that both nations have moved toward a permanent state of “Hybrid War,” where the objective is to cause the opponent to implode through internal social conflict.

As Shafie (2022) points out, the “psychosemantic” nature of these digital campaigns ensures that, even in the absence of physical fighting, the war continues in the public's minds. By using the framework provided by Khan et al. (2025), we can see that the India-Pakistan information war is a sophisticated cycle of creating alternative truths that challenge the political stability and national narrative of the opposing state.

### **Digital Sovereignty and the Role of Non-State Platforms**

A crucial, often-overlooked element in the 5GW literature is the role of platforms themselves. Hameed (2025) discusses how digital escapism and gaming behaviors are increasingly used as vectors for conflict narratives. In a world where people spend more time in digital spaces than in physical environments, these spaces become the primary arena for indoctrination. Khan (2025) warns that corporate control over information flows means states no longer have total information sovereignty.

Instead, states must negotiate with or manipulate technology giants to ensure their narratives reach the public. This adds a layer of complexity to 5GW, as the “weapon” (the platform) is often owned by a third party. Bakirov and Suleimenov (2025) argue that this lack of control makes countries vulnerable to “narrative hijacking”, where an external enemy uses a country’s own social media infrastructure to spread dissent. This makes the “weaponization of truth” a pervasive, 24/7 operation beyond the reach of traditional international law.

### **Global Governance and the Future of Truth**

The final pillar of the literature addresses the international community's struggle to keep up with these rapid developments. Wardle (2024) released a conceptual analysis showing that the overlap between hate speech, misinformation, and 5GW is making traditional peacekeeping almost impossible. If people on the ground do not trust the truth provided by international bodies, peace cannot be maintained.

Mukherjee (2025) concludes that the world is entering an era of “Post-Truth Geopolitics”, where the most successful states will be those that can defend their “Information Ecosystem”. The consensus from this scholar is that unless international law evolves to define “Information Aggression” as a form of warfare, the weaponization of truth will continue to undermine global stability. The ultimate challenge for modern states, as Surjatmodjo et al. (2024) conclude, is building “Cognitive Resilience,” teaching populations to identify and resist weaponized narratives before they cause social collapse.

## **METHODOLOGY**

This study adopted a qualitative research design, grounded in systematic secondary data analysis, to examine the role of misinformation as a strategic tool in 5GW. Data were collected from peer-reviewed journal articles, policy reports, and academic databases such as Scopus, Google Scholar, and ResearchGate, focusing on literature published between 2022 and 2026 to ensure relevance to recent developments in digital warfare and the evolving nature of disinformation strategies.

The selection of Iran-Israel and India-Pakistan as case studies was purposive and theoretically informed. These cases were chosen due to their high levels of digital engagement, ongoing geopolitical tensions, and documented use of information warfare strategies, making them suitable for examining the operational dynamics of disinformation in 5GW.

The analysis was conducted through thematic coding, in which instances of disinformation in both case studies were categorized into the three stages of the disinformation cycle: creation, dissemination, and amplification. Relevant examples from the literature were systematically examined and compared to identify recurring patterns and strategic similarities in how narratives are constructed and deployed by state and non-state actors.

A key limitation of this study is its reliance on secondary data, which restricts access to real-time or classified information on operations and may limit the depth of insights into ongoing strategic practices. However, this limitation is mitigated through the triangulation of multiple academic and policy sources, enhancing the credibility and reliability of the findings by ensuring consistency across diverse sources.

## ANALYSIS AND DISCUSSION

The analysis revealed a fundamental shift from kinetic to non-kinetic warfare, where the primary arena of conflict is no longer physical territory but the cognitive domain of populations. Within the 5GW framework, misinformation serves as a strategic instrument to shape perceptions rather than to achieve immediate physical destruction (Saleem et al., 2026). This transformation blurs the traditional boundaries between war and peace, as well as between combatants and civilians, making information itself a central weapon.

A key implication of this shift is the increasing role of civilians as active participants in conflict. During the 2019 Pulwama–Balakot crisis between India and Pakistan, for example, social media platforms were flooded with unverified videos, recycled war footage, and nationalist hashtags such as #IndiaStrikesBack and #PakistanZindabad, which intensified public sentiment on both sides.

A similar pattern has been observed during subsequent border tensions, where archival images and videos from unrelated conflicts were recirculated and reframed as current events, contributing to widespread confusion among civilian audiences. This illustrated how digital platforms enable ordinary users to amplify strategic narratives, turning the “home front” into a critical battlefield where misinformation can escalate tensions in real time.

The Iran–Israel case further demonstrated how disinformation functions as a tool of strategic signaling and perception management. For instance, repeated reports of alleged cyberattacks, such as the 2020 cyber incident targeting Iran’s Shahid Rajaei port and subsequent claims of retaliatory operations, were accompanied by conflicting narratives across media outlets and online platforms. In many cases, “leaked” intelligence and anonymous sources were used to create ambiguity, allowing both states to project strength without direct military escalation.

Similarly, recurring reports of covert cyber operations and alleged retaliatory actions are often circulated through unofficial or anonymous channels. This reflects a shift toward perception-based deterrence, where narrative control becomes more influential than physical action.

In both cases, the effectiveness of misinformation is reinforced by platform dynamics. Algorithm-driven amplification promotes emotionally charged and sensational content, often regardless of its accuracy. The rapid spread of misleading clips during crises, such as old combat footage reshared during India–Pakistan tensions or edited images circulated in Iran–Israel narratives, demonstrates how the disinformation cycle of creation, dissemination, and amplification operates in practice. These mechanisms create echo chambers that reinforce bias and limit critical engagement with opposing viewpoints.

Figure 2 illustrates the relative reach and dissemination of different types of information across digital platforms. The figure suggests that misleading and false information tends to achieve greater visibility than verified content. This pattern is largely influenced by algorithmic systems that prioritize engagement-driven material, allowing

emotionally charged narratives to spread more rapidly. As a result, misinformation reaches broader audiences, reinforcing echo chambers and amplifying its psychological impact. This supports the argument that digital platforms play a critical role in enabling the weaponization of truth in 5GW.

Figure 2: Comparative Reach of Verified and Misleading Information

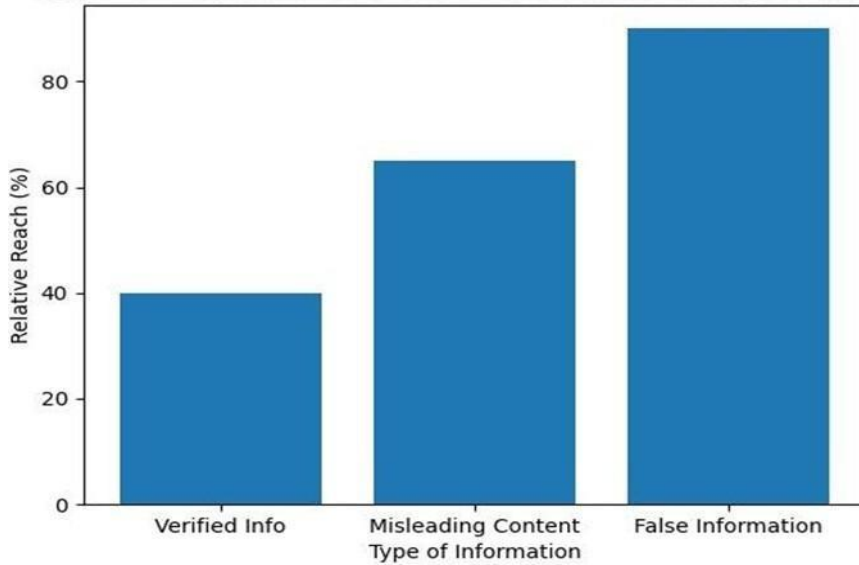


Figure 2: Comparative reach of verified and Misleading Information in Digital Environments Source: Author’s illustration based on existing literature

The concept of the “weaponization of truth” is central to these dynamics. Rather than relying solely on fabricated information, actors often distort real events to construct persuasive yet misleading narratives. For example, selectively edited videos or miscaptioned images shared during conflict periods can frame defensive actions as aggressive moves or exaggerate military success.

This strategy contributes to “cognitive paralysis,” where individuals struggle to distinguish between credible information and manipulation. This strategic blending of fact and distortion enhances credibility while simultaneously undermining the audience’s ability to critically evaluate information, reinforcing the conditions necessary for cognitive paralysis.

Ultimately, these findings highlight that control over information and narrative construction has become a decisive factor in contemporary conflict. The erosion of shared reality weakens public trust and complicates institutional decision-making, increasing vulnerability to both internal instability and external influence. As demonstrated through these examples, the operationalization of misinformation in 5GW is not abstract but actively shapes real-world conflicts, emphasizing the urgent need for cognitive resilience and adaptive security response.

### Policy Implications and Recommendations

The findings of this study demonstrate that the strategic use of disinformation in 5GW contributes directly to cognitive paralysis, a condition in which individuals and societies become unable to distinguish between credible information and manipulation. This erosion of shared reality weakens public trust, disrupts decision-making processes, and increases vulnerability to both internal instability and external influence. Addressing this challenge requires developing comprehensive cognitive security strategies that directly target the mechanisms by which disinformation operates.

At the national level, governments should prioritize digital literacy initiatives to strengthen the public’s ability to critically evaluate information. By enhancing analytical awareness, such programs can reduce susceptibility to manipulated narratives and limit the spread of disinformation within civilian populations. In parallel, regulatory frameworks must be strengthened to ensure greater accountability from social media platforms, particularly regarding algorithmic amplification that disproportionately promotes emotionally charged and

misleading content. These measures are essential in disrupting the disinformation cycle that leads to cognitive paralysis.

At the international level, there is a need to establish clearer legal and normative frameworks to define and regulate “information aggression” as a component of modern conflict. Strengthening international cooperation can help coordinate responses to cross-border disinformation campaigns and reduce their destabilizing effects. Furthermore, the development of early warning systems capable of detecting coordinated narrative manipulation would enable states to respond proactively or prevent the escalation of cognitive disruption into broader social or political crises. Collectively, these measures build cognitive resilience, which is critical for countering the long-term effects of disinformation in 5GW.

## CONCLUSION

The weaponization of truth represents a fundamental transformation in contemporary conflict, where influence over perception has become as important as physical power. This study has demonstrated that disinformation functions not merely as a byproduct of digital communication but as a structured and strategic pillar of 5GW, designed to manipulate cognition and reshape collective understanding.

Through a comparative analysis of the Iran-Israel and India-Pakistan conflicts, the study showed how digitally mediated narratives are deliberately constructed and amplified to influence both domestic and international audiences. In both cases, disinformation operates as a tool of psychological pressure, shaping public interpretation and reinforcing strategic objectives without direct military confrontation. These findings highlight the emergence of cognitive paralysis as a critical outcome of 5GW, where the erosion of shared reality limits a society’s ability to respond effectively to threats.

Collectively, the findings emphasized the growing significance of safeguarding the information landscape. Enhancing media awareness, optimizing accountability, and developing international arrangements to address information warfare are important measures toward developing cognitive stability. As international communication continues to increase through online platforms, interpretation and addressing the weaponization of truth will remain significant for maintaining political stability and international peace.

Future research should incorporate empirical, data-driven methods to better measure the real-world impact of misinformation in 5GW. Comparative studies across different geopolitical contexts would also help validate and extend this study’s findings. Additionally, further work is needed to develop effective strategies to counter disinformation and strengthen cognitive resilience.

## REFERENCES

1. Bakirov, A., & Suleimenov, I. (2025). Theoretical bases of methods of counteraction to modern forms of information warfare. *Computers*, 14(10), 410. <https://doi.org/10.3390/computers14100410>
2. Broda, E., & Strömbäck, J. (2024). Misinformation, disinformation, and fake news: Lessons from an interdisciplinary, systematic literature review. *Annals of the International Communication Association*, 48(2), 139–166. <https://doi.org/10.1080/23808985.2024.2323736>
3. Hameed, M. (2025). Digital escapism amid conflict: Media and gaming behaviors in the shadow of war. *EXCLI Journal*, 24, 774–776. <https://doi.org/10.17179/excli2025-8592>
4. Khan, A. M. (2025). 5th generation warfare and the erosion of traditional state power: Analyzing non-kinetic strategies in modern conflict. *International Journal of Social Sciences Bulletin*, 3(3), 915–924. <https://doi.org/10.5281/zenodo.15.344786>
5. Khan, S. B., Nabil, Z., & Kazmi, S. A. H. (2025). The weaponization of misinformation in hybrid warfare. *JCS Journal for Current Sign*, 3(3), 1280–1308. <http://currentsignreview.com/index.php/JCS/article/view/331>
6. Krishnan, A. (2022). Fifth generation warfare, hybrid warfare, and grey zone conflict: A comparison. *Journal of Strategic Security*, 15(4), 14–31. <https://doi.org/10.5038/1944-0472.15.4.2013>
7. Mukherjee, J. (2025). Exploring narrative warfare as a tool of psychological influence in contemporary geopolitics. *Khazanah Sosial*, 7(3), 553–563. <https://doi.org/10.15575/ks.v7i3.49640>
8. Puurunen, M. (2025). From information to cognition: Mental warfare from the Russian perspective (JYU

- Reports No. 64). University of Jyväskylä. <https://doi.org/10.17011/jyureports/64>
9. Saleem, J., Hameed, S., Shehzad, M. N., Shahzad, R. B., Ali, N., Aftab, M. M., Khan, S., Asif, A., Amna, I., & Khan, H. Z. (2026). Exploring civilian minds and lives during the 2025 India-Pakistan conflict: A phenomenological study in Lahore, Pakistan. *BMJ Open*, 16(2), 17–32. <https://pmc.ncbi.nlm.nih.gov/articles/PMC12927282/>
  10. Scherling, J. S. (2026). Fog of war: The role of fake news in initiating and prolonging conflict. *Frontiers in Communication*, 11. <https://doi.org/10.3389/fcomm.2026.1790164>
  11. Shafie, R. S. (2022). The psychological realm of social media warfare affecting public diplomacy. *Proceedings*, 82(1), 97. <https://doi.org/10.3390/proceedings2022082097>
  12. Surjatmodjo, D., Unde, A. A., Cangara, H., & Sonni, A. F. (2024). Information pandemic: A critical review of disinformation spread on social media and its implications for state resilience. *Social Sciences*, 13(8), 418 . <https://doi.org/10.3390/socsci13080418>
  13. Tweissi, B. (2025). Iran vs. Israel: How deception and the information war shaped public perceptions. Arab Center for Research and Policy Studies. <https://www.dohainstitute.org/en/Lists/ACRPS-PDFDocumentLibrary/iran-vs-israel-how-deception-and-the-information-war-shaped-public-perceptions.pdf>
  14. Wardle, C. (2024). A conceptual analysis of the overlaps and differences between hate speech, misinformation and disinformation. United Nations Department of Peace Operations. [https://peacekeeping.un.org/sites/default/files/report\\_a\\_conceptual\\_analysis\\_of\\_the\\_overlaps\\_and\\_differences\\_between\\_hate\\_speech\\_misinformation\\_and\\_disinformation\\_june\\_2024\\_update.pdf](https://peacekeeping.un.org/sites/default/files/report_a_conceptual_analysis_of_the_overlaps_and_differences_between_hate_speech_misinformation_and_disinformation_june_2024_update.pdf)
  15. Zahra, S., & Shahid, M. (2025). Narratives in conflict: Media framing and propaganda during the 2025 India-Pakistan war. *Review Journal of Social Psychology & Social Works*, 3(2), 838. <https://socialworksreview.com/index.php/Journal/article/view/240>