

How does social media propaganda influence public perception and strategic outcomes in modern military conflicts?

April 18, 2026 | SnugLab Research | readme.snuglab.com

Executive Summary

Social media propaganda significantly influences public perception and strategic outcomes in modern military conflicts by fundamentally altering the nature of warfare from physical terrain to the cognitive and information domains. It achieves this by exploiting cognitive vulnerabilities through synthetic media and algorithmic amplification, leading to strategic fatigue and a degradation of an adversary's internal cohesion. While some argue it remains a secondary tactical tool, evidence suggests its low-cost, high-reach nature makes it a primary driver of strategic destabilization, though scalable defenses like pre-bunking offer some mitigation at the individual level.

Key Findings

Social Media Propaganda as a Strategic Driver in Cognitive Warfare

Social media propaganda has evolved beyond a mere tactical tool to become a primary driver of strategic outcomes in modern military conflicts, fundamentally shifting the focus from kinetic engagements to the cognitive and information domains [2, 5, 12]. This transformation is largely enabled by synthetic media, including AI-generated images, voice cloning, and deepfake technology, which allow for the creation of indistinguishable fake imagery and fabricated statements [5, 6, 8]. These tools facilitate "cognitive warfare," exploiting human psychological vulnerabilities, biases, and beliefs to achieve destabilization [2, 9]. Through tactics like "psychosensory warfare," these technologies induce fear and a loss of hope [2].

Strategically, these operations aim for "destabilization" by amplifying systemic distrust and uncertainty within populations [7]. The continuous exposure to unverifiable information leads to two primary psychological adaptations: widespread credulity (accepting vivid imagery at face value) or "blanket skepticism," which is a total loss of

trust in all information [6]. This capability establishes generative AI as a primary driver of strategic influence, moving beyond social media's traditional role as a tactical tool for reconnaissance and intelligence gathering [1, 5, 8]. The scale of identified organized social media manipulation campaigns has increased by 15% since 2019, indicating a growing threat to democracies [4].

Impact on Public Perception and Trust

The pervasive nature of social media propaganda directly influences public perception by distorting discourse, eroding trust in legitimate journalism, and creating societal divisions [5]. In "unconstrained" environments with high internet access, traditional psychological operations (PSYOPs) are less effective because they must compete with an unlimited number of narratives [3]. This environment fosters "blanket skepticism," where continuous exposure to disinformation leads to a total loss of trust in all information, making populations less susceptible to traditional influence methods [6]. Conversely, in "constrained" environments, such as parts of Somalia or Yemen, traditional methods like leaflets and posters remain more impactful [1, 3].

Digital propaganda, by polarizing societies and eroding the shared perception of truth, poses a significant threat to democratic institutions [5]. Strategic influence operations often employ "destabilization" strategies specifically designed to amplify this uncertainty and systemic distrust [7]. As the Oxford Internet Institute found, "Social media manipulation of public opinion is a growing threat to democracies around the world, according to the 2020 media manipulation survey from the Oxford Internet Institute, which found evidence in every one of the 80+ countries surveyed" [4].

Economic Asymmetry and Countermeasures

Social media propaganda creates an economic asymmetry where low-cost digital provocations can force high-cost institutional responses, leading to strategic fatigue and paralysis [15]. This "cognitive attrition," amplified by algorithmic manipulation that often operates below conscious awareness, degrades an adversary's decision-making capacity and internal cohesion [15]. This effectively hollows out the foundation for kinetic action, establishing the manipulation of the cognitive domain as the new "high ground" for conflict, replacing the traditional seizure of terrain [15].

While traditional methods of countering disinformation, such as "debunking," have proven less effective due to cognitive biases [3], emerging defensive strategies include "pre-bunking" and AI-driven detection [5, 8, 11]. Pre-bunking involves inoculating audiences against anticipated narratives before they are deployed [3, 11]. However, while pre-bunking is effective at the individual level, it does not sufficiently neutralize the economic advantage of digital propaganda due to the structural economic asymmetry caused by algorithmic amplification and the potential for overreliance on AI-driven interventions [10, 11, 12, 13, 14, 15].

Limitations in Measuring Direct Battlefield Impact

Despite the strategic shift towards cognitive warfare, direct empirical data linking specific deepfake deployment to measurable battlefield troop movements or diplomatic shifts is not available in the research [5, 6, 8]. However, related digital activities do provide insights:

- **Deepfakes and Social Tension:** In India, deepfakes have been used during elections to disseminate fake candidate imagery and amplify religious and ethnic divisions, leading to communal tensions and violence [5].
- **Open-Source Intelligence (OSINT):** In the Ukraine conflict, researchers use OSINT via social media to track troop movements and identify war crimes [1]. Similarly, Houthi forces in Yemen used social-media-enabled analysis of satellite imagery to uncover the positions of anti-Houthi forces, enabling a counterattack [1].
- **Intelligence Gathering:** As Stanford's research notes, "Military organizations, both state-sponsored and otherwise, can (and do) exploit this open-source intelligence to recalibrate their tactics and achieve strategic advantages" [1].

The research also does not provide a quantitative breakdown of the cost-benefit ratio between traditional psychological operations and low-cost algorithmic amplification campaigns, specifically comparing budget requirements versus estimated reach or engagement metrics. It also does not identify specific demographics most susceptible to "blanket skepticism" or provide statistical outcomes for digital literacy interventions [6].

Social Media Presence vs. Technical Capability

Social media activity is an unreliable metric for determining an actor's technical

cybersecurity competency [16, 18, 19]. It primarily reflects communication strategies and psychological manipulation rather than specialized engineering skills [15, 16]. While social media can be used for reconnaissance and as a delivery mechanism for malicious payloads, the discovery of threats via social media by third parties does not equate to the actor's inherent technical capability [15, 17, 18].

Implications

The findings indicate that modern military conflicts are increasingly fought in the cognitive and information domains, with social media propaganda serving as a powerful, low-cost strategic weapon. This shift necessitates a re-evaluation of traditional military doctrines, emphasizing the importance of information defense and resilience alongside kinetic capabilities. For governments and institutions, the implications include the urgent need to develop robust strategies to counter destabilization campaigns, protect public trust, and address the economic asymmetry that favors digital propaganda. This involves investing in advanced AI-driven detection and pre-bunking initiatives, while also fostering critical thinking and media literacy among populations to mitigate the effects of widespread credulity and blanket skepticism. The challenge lies in developing scalable defenses that can effectively neutralize the economic advantage of propaganda without creating new vulnerabilities through overreliance on AI.

Limitations and Caveats

This report is limited by the absence of specific empirical data linking deepfake deployment directly to battlefield troop movements or diplomatic shifts. While the strategic impact of synthetic media is evident in cognitive warfare, direct, measurable correlations with kinetic outcomes are not detailed in the provided research. Furthermore, the research does not offer quantitative cost-benefit analyses comparing traditional psychological operations with algorithmic amplification campaigns, nor does it identify specific demographics most susceptible to "blanket skepticism" or provide statistical outcomes for digital literacy interventions. The effectiveness of regulatory frameworks in reducing disinformation velocity during active kinetic operations also remains largely unexplored in the provided findings.

Sources

- [1] [edu] Tweets Tactics - fsi.stanford.edu - <https://fsi.stanford.edu/sipr/tweets-tactics>
- [2] [edu] Cognitive Warfare The Fight For Gray Matter In The Digital G - ndupress.ndu.edu - <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3853187/cognitive-warfare-the-fight-for-gray-matter-in-the-digital-gray-zone/>
- [3] [edu] Data As A Weapon Psychological Operations In The Age Of Irre - mwi.westpoint.edu - <https://mwi.westpoint.edu/data-as-a-weapon-psychological-operations-in-the-age-of-irregular-information-threats/>
- [4] [edu] 2021 01 13 Social Media Manipulation Political Actors Indust - ox.ac.uk - <https://www.ox.ac.uk/news/2021-01-13-social-media-manipulation-political-actors-industrial-scale-problem-oxford-report>
- [5] Download - granthaalayahpublication.org - <https://www.granthaalayahpublication.org/Arts-Journal/ShodhKosh/article/download/6445/5885/35875>
- [6] The Verification Crisis Synthetic Media And Disinformation I - trendsresearch.org - <https://trendsresearch.org/insight/the-verification-crisis-synthetic-media-and-disinformation-in-the-u-s-israel-iran-conflict/?srsId=AfmBOoo0yQWyugk4wFB4waP0L2pp15aDHo5bHOS9HmW94SIDcbc7b8LE>
- [7] [preprint] arxiv.org - <https://arxiv.org/abs/2508.01552>
- [8] [social] Global Information Warfare Cognitive Influence Signal Ivan O - linkedin.com - <https://www.linkedin.com/pulse/global-information-warfare-cognitive-influence-signal-ivan-o9ugf>
- [9] Winning Influence In The Cognitive Domain - smallwarsjournal.com - <https://smallwarsjournal.com/2026/03/06/winning-influence-in-the-cognitive-domain/>
- [10] [peer-reviewed] Psychological inoculation improves resilience against ... - Science - <https://www.science.org/doi/10.1126/sciadv.abo6254>
- [11] [peer-reviewed] AI-driven disinformation: policy recommendations for ... - PMC - <https://pmc.ncbi.nlm.nih.gov/articles/PMC12351547/>
- [12] [gov] Algorithmic transparency and assessing effects of ... - <https://www.commerce.senate.gov/services/files/62102355-DC26-4909-BF90-8FB068145F18>
- [13] [peer-reviewed] WE CAN TAKE ACTION - Confronting Health Misinformation - <https://www.ncbi.nlm.nih.gov/books/NBK572168/>
- [14] [edu] [PDF] Lewandowsky, S., & Van Der Linden, S. (2021). Countering - https://research-information.bris.ac.uk/ws/portalfiles/portal/263813879/FINAL_Revision_ERSP_inoc_paper_4SvdL.pdf
- [15] [edu] [PDF] Inoculating the Public Against Misinformation - Scholar Commons - <https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=7311&context=etd>
- [16] [peer-reviewed] Social media impact on societal security - PMC - NIH - <https://pmc.ncbi.nlm.nih.gov/articles/PMC11947725/>
- [17] [edu] [PDF] Relationship of Cyber Threat Intelligence and Critical Infrastructure ... - <https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=18306&context=dissertations>
- [18] [edu] Navigating Social Media Security: Protecting a Business Against ... - <https://techpro.smu.edu/blog/navigating-social-media-security-protecting-a-business-against-cyber-risks>
- [19] [PDF] Exploring the Impact of Social Media on Cyber security Threats and ... - <https://zenodo.org/records/17070464/files/Exploring%20the%20Impact%20of%20Social%20Media%20on%20Cybersecurity%20Threats%20and%20Mitigation%20Strategies.pdf?download=1>