Original Study **Open Access**

Maurice Dawson*, Abdul Hadi Khan, Cedric Nartey

Weaponising the mind: AI, cyberspace and the future of psychological operations

DOI 10.2478/jms-2025-0011
Received: June 01, 2025; Accepted: October 10, 2025

Abstract: Psychological operations have historically played a decisive role in shaping the outcome of conflicts, leveraging media and ideology to influence minds rather than battlefields. As warfare transitions into a multidomain environment, artificial intelligence (AI) has emerged as both a catalyst and a complicating factor in modern influence strategies. This paper traces the evolution of psychological warfare from World War II (WWII) to present-day disinformation campaigns, highlighting how adversaries exploit democratic transparency to undermine public trust. Drawing upon historical case studies and recent developments – including election interference, deepfake technologies and AI-enhanced sentiment analysis – the research demonstrates how AI-driven psychological operations now operate across physical, digital and emotional boundaries. The authors argue that the integration of cyberpsychology and AI into the psychological operations toolkit marks a strategic inflection point. Without a coherent, ethically grounded doctrine, liberal democracies risk ceding influence to adversaries who wield digital propaganda with increasing sophistication.

Keywords: Artificial Intelligence, Information Operations, Psychological Warfare

1 Introduction: Psychological warfare in World War II (WWII)

Psychological warfare – using communication to sway attitudes, emotions and decision-making – gained unprecedented traction during WWII. Although its roots stretch far back into history, the global conflict marked a turning point where propaganda became central to both military strategy and home-front morale (see Table 1).

Each country approached the practice differently. The Soviet Union leveraged cultural pride and historical symbolism to rally its citizens and undermine its enemies. At home, the message was tightly regulated; abroad, the Soviets invoked revered German historical figures and exploited internal Nazi divisions to undermine trust in leadership (Linebarger 1954). Japan, in contrast, invested in shaping overseas perceptions, especially in the United States, where it fine-tuned news placements and disguised propaganda as cultural or educational material. These efforts proved more successful during wartime than in the years before it began (Linebarger 1954).

The radio played a crucial role during this era. With its immediacy and broad reach, it eclipsed print as the most effective tool for psychological influence. Propaganda also took many forms beyond media – civilians received food, gifts and humane messages; prisoners were treated with courtesy and subjected to ideological engagement. These strategies reveal how profoundly the battle for hearts and minds became intertwined with the broader war effort.

2 Contrasting soviet approaches to propaganda

Soviet psychological tactics were sharply divided by the audience. Internally, information flow was tightly controlled – state censors managed the message to avoid dissent and ensure ideological uniformity. For external consumption, particularly targeting Nazi forces, Soviet broadcasts adopted a more strategic tone. These transmissions referenced respected German cultural and historical figures to fracture enemy unity and morale. Black radio – disguised as coming from other sources – was one of several tools the Soviets employed to sow doubt among their enemies (Linebarger 1954, pp. 82–88).

***Corresponding author: Maurice Dawson,** Center for Cyber Security and Forensics Education, Illinois Institute of Technology, Chicago, IL, USA, E-mail: mdawson2@illinoistech.edu
Abdul Hadi Khan and Cedric Nartey, Center for Cyber Security and Forensics Education, Illinois Institute of Technology, Chicago, IL, USA

Tab. 1: Key moments in WWII psychological operations

Year	Event	Summary
1939	War begins	Psychological operations are formally integrated into military strategy, signalling a shift towards ideological as well as kinetic warfare (Linebarger 1954, p. 3).
1941	Japan targets US opinion	Japan initiates preemptive influence campaigns targeting the US population to erode trust in American foreign policy (Linebarger 1954, pp. 83–84).
1942	Soviet propaganda ramps up	The USSR intensifies radio efforts to penetrate German troop morale using historical references and nationalist sentiment (Linebarger 1954, pp. 82–88).
1943	Japan influences US media	Japanese propagandists successfully placed articles in US news outlets, masking disinformation as cultural education (Linebarger 1954, pp. 84–86).
1943	China engages POW	Chinese Communist forces convert psychological warfare into personal outreach, treating Japanese prisoners with dignity and political education (Linebarger 1954, pp. 86–87).
1944	Allies expand black radio	Covert radio stations disguised as enemy sources gain momentum, broadcasting demoralising messages across Axis territories (Linebarger 1954, p. 90).
1945	Allied radio reaches Japan	Widespread standard-wave radio broadcasts from US stations on Saipan reach millions of Japanese civilians (Linebarger 1954, p. 127).
1945	End of organised US Psywar	Agencies such as the OWI and the OSS dissolved after the war, marking the end of centralised US psychological warfare operations (Linebarger 1954, pp. 138–140).

OSS, Office of Strategic Services; OWI, Office of War Information; POW, Prisoner of War; WWII, World War II.

3 Japan's methods for shaping US public opinion

Japan was highly calculated in its approach to psychological operations directed at the United States. It successfully placed articles in American media that appeared informative or cultural while subtly shaping narratives in Japan's favour. These campaigns were more refined and practical during the war than in peacetime. Additionally, Japanese operatives used 'black propaganda' throughout Asia, embedding disinformation in professional-quality publications. Their messaging avoided overt political content, instead focusing on themes that resonated with humanitarian or intellectual curiosity, making it more palatable to foreign readers (Linebarger 1954, pp. 83–86).

4 Political warfare and psychological operations

Political warfare and psychological operations remain essential instruments of statecraft, particularly in the strategic space between open warfare and covert operations. These tools operate across a continuum – from shaping perceptions among allies to undermining adversaries – and are pivotal in contests of influence, legitimacy and national resolve (Lord, 1989). As articulated in historical assessments, the effectiveness of political warfare hinges not merely on the capacity to project narratives but on the integration of psychological, informational, diplomatic and economic tools within a coherent national strategy (George and Smoke 1989).

However, despite their utility, the United States has often lacked a consistent institutional framework to sustain such efforts. Bureaucratic fragmentation and the absence of unified interagency planning have historically undercut the implementation of psychological–political operations. George and Smoke (1989) contend that without a deliberate and adaptive organisational structure – one capable of fusing intelligence with communications strategy – psychological operations are likely to remain reactive and piecemeal.

The contemporary relevance of these challenges is evident in recent disinformation campaigns targeting American elections. Adversaries such as Russia have demonstrated an adeptness at exploiting political fractures within the US body politic. As noted by the House Select Committee, Russia's influence operations during the 2020 election echoed – and in some cases directly parroted – political rhetoric from prominent American figures to sow doubt about electoral integrity (House of Representatives, Congress 2022). These efforts, which included the use of social media manipulation and the dissemination of fabricated news content, were not isolated acts of interference but rather components of a broader psychological strategy aimed at eroding public trust and democratic cohesion.

Importantly, political warfare is not confined to enemy populations. Influence operations are frequently designed to reach neutral states and even domestic audiences. These efforts, whether overt or covert, aim

to reinforce strategic narratives, delegitimize alternative perspectives and secure favourable alignment among key stakeholders (George and Smoke 1989). Yet the lack of a sustained national political warfare doctrine hampers the US ability to shape the global information environment proactively. Adversaries with centralised propaganda mechanisms and fewer bureaucratic constraints often outpace the United States in both agility and strategic coherence.

To remain competitive in this evolving domain, the United States must invest in cross-domain coordination between civilian and military actors, build institutional memory for political and psychological campaigns and refine feedback mechanisms that incorporate real-time audience analysis. As the 6th January Committee emphasised, psychological operations – when deployed externally – can be mirrored and turned inward by foreign actors exploiting the openness of American discourse (House of Representatives, Congress 2022). Strengthening national capacity for political warfare is not only a matter of defending democratic institutions but also a strategic imperative in an era marked by contested influence and hybrid conflict.

5 Foreign disinformation targeting US democracy

Foreign adversaries – most notably Russia and China – have engaged in persistent disinformation efforts aimed at US audiences. These influence campaigns are not only long-standing but also intensify during key democratic events such as national elections. These moments present a strategic opportunity to exploit social divisions and erode trust in American democratic institutions (House of Representatives, Congress 2022).

During the lead-up to and aftermath of the 2020 election, Russian actors actively circulated narratives designed to undermine confidence in the electoral process. Interestingly, much of the content used by Russian outlets echoed and amplified statements already made by President Trump. This included his claims about mail-in ballots, election fraud and the legitimacy of the results. US intelligence agencies noted that Russian operations leveraged Trump's rhetoric to further influence their goals (House of Representatives, Congress 2022).

This strategy was not novel. Similar tactics were prepared by Russian operatives in 2016 in anticipation of a Hillary Clinton victory. When Trump won, those plans were shelved, only to resurface in 2020 targeting President Biden and the Democratic Party (House of Representatives, Congress 2022). These efforts were carried out in part by Project Lakhta, the Kremlin-backed organisation previously known for operating the Internet Research Agency. Using fake social media accounts, fabricated news platforms and even recruiting unwitting individuals from countries like Ghana and Mexico, these campaigns delivered targeted messages to Americans across the political spectrum (House of Representatives, Congress 2022).

Despite public awareness and intelligence warnings, these disinformation tactics continue to evolve. The most recent Annual Threat Assessment concluded that Moscow is likely to maintain and even expand these operations in future elections, possibly by forging deeper ties with individuals in US media and politics who can serve as conduits for messaging (House of Representatives, Congress 2022).

6 Politics and information warfare

After reviewing the article by Tismaneanu and Cioflâncă (2016), several important lessons about modern propaganda and information warfare emerged, particularly in how these tools are utilised in today's digital landscape. One of the most striking points is that propaganda no longer comes in obvious forms, such as old posters or state-run broadcasts. It now blends seamlessly with real news and social media content, often making it difficult to distinguish between information intended to inform and content meant to influence or mislead. This tactic is employed by both governments and independent groups, often to shape public opinion, create division or erode trust in democratic institutions. The digital environment has made these efforts faster, broader and more complex to trace, which raises serious concerns about how modern societies protect their public discourse.

Another takeaway is the challenge faced by open democracies. Because of their commitment to free speech and transparent governance, they become easier targets for disinformation campaigns. Tismaneanu and Cioflâncă (2016) explain that, unlike authoritarian states, democracies do not typically control narratives through censorship, making it easier for malicious actors to spread confusion or polarising messages. The solution is not censorship, though. Instead, the authors emphasise the need for better media literacy, ethical journalism and coordinated policy responses that strengthen trust in institutions without compromising on civil liberties. What became clear through the reading is that understanding information warfare today requires more than just technical

awareness – it demands a thoughtful response grounded in education, governance and international cooperation.

7 US Army civil affairs and psychological operations

US Army Civil Affairs involves engaging with the civilian population (U.S. Army Civil Affairs and Psychological Operations Command [USACAPOC] (n.d.)). They collaborate with the community to enhance stability, empower local governments and improve the quality of life for residents (Civil Affairs Association (n.d.)). Psychological operations support national security objectives at tactical, operational and strategic levels. However, operational psychological operations are conducted at a smaller scale, with even tactical psychological operations even more limited (Civil-Military Cooperation Centre of Excellence [CIMIC-COE] (n.d.); U.S. Army Special Operations Forces [USASOF] (n.d.)).

8 Psychological warfare

Psychological warfare has become an increasingly decisive factor in determining the success of military operations, both historically and in modern geopolitical conflicts. Its strategic application minimises the reliance on conventional force by targeting the morale, perceptions and cohesion of adversaries. For instance, during Operation Desert Storm, coalition forces employed psychological tactics such as aerial leaflet distribution, which played a crucial role in inducing mass surrenders among Iraqi soldiers – more than 100,000 surrendered without major confrontation (Newitz 2024). These outcomes underscore the effectiveness of psychological operations in saving lives and reducing physical combat.

The implications of such tactics extend far beyond the battlefield. Psychological warfare serves as a force multiplier, complementing kinetic strategies while also functioning as a powerful tool of influence in its own right. Modern instances, such as China's large-scale military drills near Taiwan following diplomatic tensions, demonstrate how the psychological component can shift the strategic balance without engaging in direct combat (Hung & Hung, 2022). Furthermore, the Arab Spring exemplified how psychological influence, delivered through social media platforms, can destabilise regimes and alter national trajectories without traditional warfare (Van Niekerk et al., 2011). This evolution reveals that the psychological dimension of conflict is not only enduring but increasingly sophisticated in its integration with digital technologies and global communication networks.

9 Cyber warfare

In the digital age, cyberwarfare has emerged as a formidable domain of conflict, capable of producing strategic outcomes without the need for conventional weapons. Unlike traditional warfare, cyber operations can target a nation's infrastructure, information systems and public trust with relative anonymity and global reach. Dawson (2021) notes that cyberattacks have increasingly focused on critical sectors such as healthcare, energy and defence, with threat actors exploiting software vulnerabilities and leveraging social engineering to compromise national assets. The integration of artificial intelligence (AI) into cyber operations only amplifies these risks by enabling real-time decision-making and adaptive threats that traditional defences are ill-equipped to counter.

The weaponisation of cyberspace has created a paradigm shift where national security is no longer solely dependent on physical assets but also on digital resilience and information dominance. According to Oerlemans and Langenhuijzen (2025), one of the greatest challenges facing democratic nations is balancing national security interests with civil liberties when using open-source intelligence and commercial data for cyber operations. The blurred boundary between state-sponsored cyberwarfare and criminal or ideological attacks further complicates attribution and response, leaving governments to operate in a domain with evolving norms and limited regulatory frameworks. These dynamics make it imperative for nations to establish cross-sector partnerships and shared intelligence strategies.

10 Review of AI tools and their uses in PSYOPS

In examining the intersection of AI and psychological operations, it becomes evident that many tools originally designed for educational or communication enhancement can be repurposed for military and even nefarious strategic applications (see Table 2). Natural language processing (NLP) tutors, for instance, were developed to support language learning and real-time dialogue analysis. However, when adapted for defence purposes, they can serve to prepare operatives for combat.

Tab. 2: AI tools and their uses in psychological operations

AI tool	Potential use for military operations	Nefarious use for psychological operations	APA in-text citation
NLP tutors	Language training for operatives, real-time translation and psychological assessments during interrogations	Deploying deceptive bots to mimic authentic language use, spreading tailored propaganda	Woo and Choi (2021)
Intelligent personal assistants (e.g. Alexa)	Operational language immersion, training support and real-time feedback for mission-critical communications	Eavesdropping or psychological conditioning through suggestive responses in conversations	Woo and Choi (2021)
Neural network-based dialogue systems	Simulated foreign language dialogue training, operational debriefing support and psychological profiling	Manipulating dialogues in digital forums to steer public perception or sow discord	Woo and Choi (2021)
AI grammar correction tools	Improved clarity and accuracy in official communications and training materials across multilingual units	Altering educational or official materials to disseminate disinformation	Woo and Choi (2021)
AI-powered sentiment analysis systems	Monitoring of public sentiment in occupied areas or during foreign operations to inform narrative control	Analysing emotional responses to seed unrest or amplify fear in targeted populations	Islam et al. (2024)

AI, artificial intelligence; NLP, natural language processing.

11 AI use in misinformation

AI techniques facilitate the effortless reproduction of images by malicious individuals, hence enabling them to influence public sentiment. For instance, in Figure 1A, the graphic advocating for Stevenson was employed to solicit votes. Nonetheless, ChatGPT was prompted to modify the photograph to persuade the individual to support Nixon. Additional prompts included preserving the colour branding and image dimensions while modifying phrases and names slightly to ensure they are not readily identifiable or discernible from Figure 1A. The outcome was Figure 1B, which was a direct result of the specified prompt.

Text is a domain where AI can adeptly alter important terms, facilitating the proliferation of misinformation and deception. These writings can replicate the original while preserving the author's style and tone, including features such as copyrights and governmental headings in the document.

12 Election deep fakes

Deepfakes represent one of the most compelling applications currently available. These are digitally changed films, photos or sounds that seem authentic but have been modified using AI. Deep fakes can make an individual or entity appear to talk or perform acts they never actually did. As this technology continues to evolve, it will become increasingly complex for people to distinguish between reality and fabrication.

In the lead-up to the 2024 elections, emerging technologies such as deepfakes and AI-generated memes began to play a more insidious role in public discourse. Rather than simply entertaining or informing, these tools were increasingly weaponized to manipulate perception, foster division and distort truth. Experts have warned that the sophistication of AI-driven content blurs the lines between factual and fabricated media, making it difficult for the average citizen to distinguish between authenticity and deception. The article highlighted how political operatives and foreign actors can exploit these technologies to subtly reshape narratives and sow confusion across digital platforms, particularly targeting swing-state populations and vulnerable demographics (NPR 2024).

13 Envisioning the future of psychological operations

Today, the US Army has a role, 37F Psychological Operations Specialist, where a soldier becomes a persuasion expert (GoArmy (n.d.)). It is the responsibility of Psychological Operations (PSYOP) specialists to assess and produce targeted information designed to influence and engage specific audiences. Utilising a range of communication channels, these specialists disseminate essential information and deliver support to civilian populations, military personnel and governmental entities both within the United States and internationally (Department of Defense (n.d.)). Since warfare now has a fifth domain, namely cyber, psychological operations, those associated with this field must integrate cyber tools into their toolkit to achieve true success.

Fig. 1: (A) Original political party photo. (B) AI misinformation created photo. AI, artificial intelligence.

The new field of cyberpsychology is a branch of psychology that studies the impact of human behaviour and psychological processes. This field examines how technology, such as the Internet and social media, influences groups, individuals and society. Today, cyberpsychology is evolving rapidly in tandem with advances in AI. AI-powered applications such as virtual humans, affective computing and deepfake technologies are being deployed in persuasive messaging, behaviour modification and emotional manipulation – fields critical to modern psychological operations. These technologies raise ethical questions about privacy, consent and the weaponization of digital experiences. Virtual environments and AI agents can replicate or manipulate affective states, potentially being harnessed for psychological warfare or ideological influence (Ancis 2020).

14 Conclusion

As technology advances, so too does the capacity to manipulate cognition and perception at scale. This research highlights a growing reality: AI is not only reshaping the mechanics of psychological operations but also redefining the ethical and strategic frameworks within which such operations are conducted. From Cold War-era black propaganda to the algorithmically tailored disinformation of today, psychological warfare has evolved into a hybrid tool of persuasion and disruption. What once relied on loudspeakers and leaflets now thrives through machine-generated speech, deepfake videos and social media echo chambers.

Yet this transformation brings new dilemmas. Democracies, constrained by legal norms and civic values, are often at a disadvantage compared with more authoritarian regimes in this domain. The convergence of AI and psychological operations demands urgent reassessment of institutional capabilities, doctrinal clarity and cross-sector collaboration. Without these, the battle for influence in cyberspace may be won not by those with the most truth, but by those with the most data and the best algorithms. Navigating this terrain requires not just technical innovation but a renewed commitment to defending cognitive sovereignty in the age of algorithmic persuasion.

References

Ancis, J. R. (2020). The age of cyberpsychology: An overview. *Technology, Mind, and Behavior, 1*(1). doi: 10.1037/tmb0000009

Civil Affairs Association. (n.d.). *What is Civil Affairs?* Retrieved 1 June 2025, Available at https://www.civilaffairsassoc.org/what-is-civil-affairs

Civil-Military Cooperation Centre of Excellence. (n.d.). 2.6 U.S. Civil Affairs. *CIMIC Handbook*. Retrieved June 1, 2025, Available at https://www.cimic-coe.org/handbook-entries/welcome-to-the-cimic-handbook/ii-fundamentals/2-6-us-civil-affairs/

Dawson, M. E. (2021). *Cyber Security in the Age of Critical Infrastructure Protection and Artificial Intelligence. Postdoctoral thesis*, Universidade Fernando Pessoa. Available at https://bdigital.ufp.pt/entities/publication/5e93c236-588a-4564-bfb6-982d33fe11b4

Department of Defense. (n.d.). *37F Psychological Operations Specialist. Credentialing Opportunities On-Line (COOL)*, Retrieved June 1, 2025, Available at https://www.cool.osd.mil/army/moc/index.html?moc=37f&tab=overview

George, A. L., & Smoke, R. (1989). Deterrence and foreign policy. *World Politics, 41*(2), 170-182.

GoArmy. (n.d.). *37F Psychological Operations Specialist. U.S. Army*. Retrieved June 1, 2025, Available at https://www.goarmy.com/careers-and-jobs/ground-forces/languages-code/37f-psychological-operations-specialist

House of Representatives, Congress. (2022). Final Report of the Select Committee to Investigate the January 6th Attack on the United States Capitol. [Government]. Government Publishing Office. Available at https://www.govinfo.gov/app/details/GPO-J6-REPORT/

Hung, T. C., & Hung,T. W. (2022). How China's cognitive warfare works: a frontline perspective of Taiwan's anti-disinformation wars. *Journal of Global Security Studies, 7*(4), ogac016.

Islam, M. S., Kabir, M. N., Ghani, N. A., Zamli, K. Z., Zulkifli, N. S. A., Rahman, M. M., & Moni, M. A. (2024). Challenges and future in deep learning for sentiment analysis: a comprehensive review and a proposed novel hybrid approach. *Artificial Intelligence Review, 57*(3), 62.

Linebarger, P. M. A. (1954). *Psychological Warfare*, 2nd edn. New York: Duell, Sloan and Pearce.

Lord, C. (1989). The psychological dimensions in national strategy. In C. Lord & F. R. Barnett (Eds.), *Political warfare andpsychological operations: Rethinking the US approach* (pp. 13–27). Washington, DC: National Defense University PressPublications.

Newitz, A. (2024). Psychological tactics in military history. *Journal of Modern Conflict Studies, 12*(1), pp. 45-58.

NPR. (2024). *Deepfakes, memes and artificial intelligence pose new threats for elections*. Available at https://www.npr.org/2024/12/21/nx-s1-5220301/deepfakes-memes-artificial-intelligence-elections

Oerlemans, J. J., & Langenhuijzen, S. (2025). Balancing national security and privacy: Examining the use of commercially available information in OSINT practices. *International Journal of Intelligence and CounterIntelligence, 38*(2), pp. 579-597. doi: 10.1080/08850607.2024.2387850

Tismaneanu, V., & Cioflâncă, C. (2016). Propaganda and information warfare in the digital age. *Journal of Media Studies, 31*(4), pp. 241-254. doi: 10.1515/jms-2016-0184

U.S. Army Civil Affairs and Psychological Operations Command. (n.d.). *USACAPOC(A) homepage*. U.S. Army Reserve. Retrieved 1 June 2025, Available at https://www.usar.army.mil/USACAPOC/

U.S. Army Special Operations Forces. (n.d.). *Civil Affairs*. GoArmySOF. Retrieved 1 June 2025, Available at https://www.goarmysof.army.mil/CA/

Van Niekerk, B., Pillay, K., & Maharaj, M. (2011). The Arab Spring| Analyzing the role of ICTs in the Tunisian and Egyptian unrest from an information warfare perspective. *International Journal of Communication, 5*, 11.

Woo, Y., & Choi, Y. (2021). AI in academia: An overview of selected tools and their areas of application, Available at https://arxiv.org/abs/2111.04455