

Crowdsourced Intelligence vs. AI Propaganda: The Challenges of Global Governance in the Age of Digital Warfare

**Pragati Khanna¹, Harsh Dixit², Jannet Emma Tonateni Fransisco³, Varsha Dhio Dora⁴,
Trisha Dev⁵**

**1BA Programme (Political Science and Philosophy), Lakshmibai College, University Of
Delhi, New Delhi, Delhi-110052, India**

**2B.A. Political Science (Hons.), Department of Political Science, Seth Anandram
Jaipuria**

College, University of Calcutta, Kolkata, West Bengal-700005, India

**3Masters in Management Department of Administration & Management STADIO
Higher**

Education, 24 Wagner Street, 10005, Namibia

**4M.A Public Policy, Programme of Public Policy, University of Madras, Chennai, Tamil
Nadu, 600075, India**

**5M.A. Economic, Department of Economics, Manipal University, Jaipur,
Rajasthan 303007, India**

Corresponding author: Pragati Khanna, Email Id: pragatikhanna813@gmail.com

Corresponding Author's Contact Number: +91 9650284598

Abstract

Artificial Intelligence has fundamentally changed the modern digital operation, whereby creating a constant struggle between what is perceived to be true and the human reality. This study uses a qualitative, exploratory-descriptive study using secondary data from academic journals, policy documents and institutional reports to examine the interaction between crowdsourced Open-Sourced Intelligence (OSINT) and Artificial Intelligence (AI) driven propaganda in modern warfare, alongside the global governance challenges that arise from their interaction. Findings reveal that there is a serious tension within the digital information ecosystem: whilst generative Artificial Intelligence promotes public opinions to spread disinformation and misinformation that is persuasive and may manipulate political processes, crowdsourced intelligence offers real-time verification and transparency. There are Regulatory Frameworks such as the European Union's AI Act and Digital Services Act that serve as blueprints to counter AI-driven manipulation from technical solutions to the adoption of human-centered governance models. Ultimately, the study demonstrates that it is important to maintain digital information integrity by balancing computational tools with collaborative human verification to foster resilience against any revolving threats in digital security and global governance.

Keywords

Artificial Intelligence, Open-Source Intelligence (OSINT), Crowdsourced Verification, AI-Driven Propaganda, Digital Warfare, Global Governance, Disinformation, Epistemic Sovereignty.

Introduction

Artificial intelligence (AI) has transformed the way information is gathered, studied, and shared during digital conflicts. AI-enabled Open-Source Intelligence (OSINT) can help people handle large amounts of publicly available information, while machine learning and natural language processing have made it possible to perform more tasks across the

intelligence cycle (Ghioni et al., 2024; O’Browne et al., 2024). At the same time, AI-generated content, automated bots and deepfakes have made it easier to create and share false information, causing concerns about information integrity and trust in what people see (Marigliano et al., 2024; Goldstein et al., 2024). OSINT and crowdsourced intelligence should not be seen as the same thing. OSINT means intelligence that comes from information available to the public, while crowdsourced intelligence comes from a group of people, including citizens, journalists, researchers and others in civil society. Crowdsourced verification is more specific, referring to group efforts to check whether information is accurate. These practices can support openness and accountability, while AI-enabled propaganda can create and spread false narratives faster and more widely (La Barbera et al., 2024; Marigliano et al., 2024). These changes have made the digital information environment harder to assess and govern, especially when false narratives move quickly. The cross-border nature of AI-driven information operations also creates challenges for governance, particularly in relation to accountability, regulation, international cooperation, and human oversight (Emery-Xu et al., 2025; Fitz-Gerald & Padalko, 2026). Even though existing research looks at AI-enabled OSINT, AI governance, crowdsourced verification, and digital propaganda, the way these areas connect is not well understood. This study therefore examines how crowdsourced intelligence and AI propaganda work together in digital warfare and considers the governance challenges that arise from this relationship.

Literature Review

The convergence of artificial intelligence (AI), Open-Source Intelligence (OSINT), and digital communication has transformed intelligence gathering, information warfare, and global governance. Ghioni et al. (2024) demonstrate that AI-enabled OSINT is already changing the way analysts collect and process public data, but questions remain regarding transparency, privacy, accountability, and ethics. Similarly, O’Browne et al. (2024) highlight how machine learning and natural language processing are enhancing each stage of the intelligence cycle while also presenting potential pitfalls such as algorithmic bias, the reliability of data sources, and insufficient human oversight. In the realm of governance, Emery-Xu et al. (2025) tackle the global regulatory challenges associated with the rapid

development of AI, arguing that a coordinated approach is required to ensure innovation, security, and accountability at the multinational level. Complementing these findings, Marigliano et al. (2024) provide an illustrative example of how bots and AI-fueled digital propaganda during the Russia-Ukraine conflict have been used to shape public opinion. Overall, the existing literature addresses different aspects of AI-enabled intelligence and information warfare, but limited attention has been given to the role of crowdsourced intelligence in relation to AI propaganda. Artificial intelligence has become widely accepted by younger generations and continues to play a major role in shaping the digital information space. The abuse of artificial intelligence created unprecedented problems in society: deepfakes, social bot accounts, automated manipulation, disinformation, and propaganda. The ability for AI to be used in digital warfare to spread misinformation to intentionally sway public opinion, ruin individual and company reputations, influence elections, and diminish public trust in government and democratic institutions. These studies show the ability for AI-powered propaganda to become a threat to society, governments, and world peace. As Fitz-Gerald and Padalko (2026) point out, improved AI governance and social resilience are critical components for addressing the risks of artificial intelligence and misinformation. Policymakers need to establish governance frameworks focused around transparency, accountability, ethical AI, digital literacy, and responsible technology development. Regulatory approaches like the European Union's Artificial Intelligence Act and Digital Services Act can act as policy blueprints for mitigating online manipulation and long-term threats from new AI technology. While there are many risks to AI, it's important to note that generative AI, such as large language models (LLMs) and deep generative models, have powerful tools that can be leveraged for good or bad intentions. When it comes to cyber security, AI will act as both a sword and a shield, creating new possibilities for defense and cyber attacks. Growing technical capacity outstripping governance mechanisms makes human-AI collaborations and crowdsourced intelligence all the more crucial. We should not leave it up to AI systems to shape our information environments. Humans should use their intelligence, critical thinking skills, ability to fact-check and collaborate with one another in the public interest to crowdsource propaganda and disinformation detection and response as another tool in our collective arsenal. Crowdsourced intelligence can help build social resilience when citizens, researchers, civil society groups, and governments verify information

and jointly discover new risks. Furthermore, in order to take into account new global threats, technological developments, and evolving patterns of digital warfare, AI governance

frameworks and intelligence models must be continuously updated. This approach has the potential to advance global cooperation, cybersecurity, democratic resilience, information integrity, and world peace in an increasingly AI-driven society. Digital warfare has transformed the information environment by enabling both crowdsourced intelligence and AI-generated propaganda to influence public opinion, policymaking, and international security. Crowdsourced intelligence relies on citizens and journalists to collect, verify, and to circulate information, which often strengthens transparency and rapid crisis response. In contrast, AI-generated propaganda exploits AI to produce persuasive disinformation that manipulates public perception and undermines democratic processes (Goldstein et al., 2024). Digital technologies have also increased the complexity of cybersecurity threats, information warfare, and cross-border regulation, creating a greater need for international cooperation and adaptive governance frameworks (Silva, 2025). Furthermore, the integration of AI into digital communication has intensified concerns regarding misinformation and ethical governance, emphasizing the need for regulatory mechanisms that balance technological innovation with information integrity (Imam, 2025). Collectively, these studies suggest that while crowdsourced intelligence can enhance accountability and resilience, the rapid advancement of AI propaganda presents significant challenges for global governance, which requires coordinated international policies to safeguard information. Research on information in the digital age is beginning to see how crowdsourced verification and artificial intelligence propaganda are interlinked issues. Authors like La Barbera and others look at how crowdsourced fact-checking can help fight misinformation at scale (2024). But the use of people to check facts was met with mixed reviews, as some believe it works and others were a bit apprehensive. Gao, Zhang and Rui (2025) examined how community notes on social media are used to reduce false information. This approach was more about enabling many people to contribute to content moderation, as it was better for dealing with the volume of digital discussion today while still allowing people to speak their mind. Meanwhile, scholars

studying propaganda look at the other side of the issue, thinking about false information in terms of computational power. In 2025, Mustafa, Luczak-Roesch and Johnstone studied how computational propaganda exploits platforms and new technologies to disperse false information at a rapid pace, and how large language models play an important role in spreading false information, as they can automatically generate misleading content.

Osimen, Newo and Fulani (2024) discovered a link between the use of artificial intelligence in warfare and propaganda in terms of security among countries. They observed that the employment of AI in weapons development has generated a kind of competition among nations, with ambiguous consequences for international security and humanitarian laws. So the main question this research aims to answer is how the world can balance the need for crowdsourcing to stop misinformation against the propaganda driven by artificial intelligence.

Research Gap

There are currently multiple approaches available in the literature to study modern information warfare: some focus on decentralized crowdsourced truth-seeking, while others focus on centralized automated disinformation. However, the interaction between these two phenomena has not been systematically studied at a global level. The pace of human (or hybrid human/machine) fact-checking is nowhere near the pace of AI propaganda generation. Much research has focused on local/regional regulation schemes, but little work has explored how decentralized crowdsourced truth-seeking and AI disinformation could be incorporated within a flexible, global governance framework. We propose to move beyond narrow technological or regulatory solutions toward more holistic models of governance that capture the interplay of crowdsourced truth and machine-generated lies.

Methodology

1. Research Approach

This study adopts a qualitative research approach to examine the relationship between crowdsourced intelligence and AI propaganda in digital warfare and its implications for governance. It interprets existing research on intelligence, propaganda, misinformation, and governance rather than measuring variables or testing causal relationships (Ghioni et al., 2024; Fitz-Gerald & Padalko, 2026).

2. Research Design

The study follows an exploratory-descriptive design based entirely on secondary evidence. Relevant literature was identified on artificial intelligence, OSINT, crowdsourced intelligence, digital propaganda, information warfare, digital warfare, and governance. Literature on crowdsourced verification and computational propaganda was considered (La Barbera et al., 2024; Mustafa et al., 2025).

3. Data Sources

The study uses secondary sources, including peer-reviewed articles, journals, books, and reports from reputable organizations. Sources were selected based on specific criteria as relevant, authentic, credible, and recent. The literature covers AI-enabled OSINT, crowdsourced verification, computational propaganda, misinformation, and international AI governance (O’Browne et al., 2024; Gao et al., 2025; Emery-Xu et al., 2025).

4. Analytical Framework

The study’s framework is based on comparative analysis of the reviewed literature. The research question was broken down into themes. These include intelligence, verification, propaganda, misinformation, governance, and digital security. It focuses on similarities and differences among the themes. The findings were synthesized to demonstrate how crowdsourced intelligence and AI propaganda practices coexist and their implications for governance (Marigliano et al., 2024; O’Browne et al., 2024).

5. Nature of Study

The study is qualitative, exploratory, and descriptive in nature. It focuses on interpreting findings of previous studies. The study did not engage in experimental research to establish cause-and-effect relationships between the variables. Instead, it integrated the phenomena to analyze their effect on the research problem (Emery-Xu et al., 2025; Fitz-Gerald & Padalko, 2026).

Analysis

The current digital warfare ecosystem brings together a decentralized, open source intelligence (OSINT) movement led by everyday people and a centralized, automated propaganda system driven by artificial intelligence (AI) (Ghioni et al., 2024; Marigliano et al., 2024). Although much of the literature on these topics tends to treat them as separate areas of study, there is some evidence that a qualitative analysis of OSINT and AI propaganda provides insight into the dynamics between information verification and information manipulation in modern global governance (Emery-Xu et al., 2025; Silva, 2025).

1. The Dual Impact of AI in Modern Digital Warfare

AI can act as a double-edged sword, bolstering both intelligence gathering efforts and the scale of propaganda operations (Balasubramanian et al., 2025; O’Browne et al., 2024). Intelligence Gathering: OSINT and the analysis of cyber threats are enhanced through machine learning and natural language processing technologies, which enable the swift analysis of vast amounts of information (Ghioni et al., 2024; O’Browne et al., 2024). This allows for the quick discovery, validation, and comprehension of new information throughout the intelligence process, ultimately facilitating real-time decision-making (Balasubramanian et al., 2025; O’Browne et al., 2024).

Propaganda: In parallel with intelligence gathering, the proliferation of generative AI technologies such as large language models (LLMs), generative deep neural networks, deepfakes, and automated bots has resulted in increased volume of targeted misinformation (Goldstein et al., 2024; Marigliano et al., 2024). With the support of AI, propaganda may be fine-tuned by humans to be almost as convincing as real propaganda (Goldstein et al., 2024),

as was the case with Russian propaganda during the Russia-Ukraine war (Marigliano et al., 2024).

2. OSINT and AI Propaganda: Dynamics

The interaction between OSINT and AI propaganda may be qualitatively described as an ongoing battle between verification and manipulation (Fitz-Gerald & Padalko, 2026; Goldstein et al., 2024).

Verification vs. Manipulation: Open source intelligence enables citizens, journalists, and other members of the public to collect, validate, and disseminate real-time information (Ghioni et al., 2024). This grassroots approach to information-gathering helps promote transparency, accountability, and resilience by providing additional, independent channels for validating information to contest dominant or fabricated accounts of events (Fitz-Gerald & Padalko, 2026; Ghioni et al., 2024). However, coordinated, state-sponsored AI propaganda campaigns can seek to deliberately alter the direction of discourse, intervene in political processes and elections, damage reputations, and undermine public faith in institutions (Imam, 2025; Marigliano et al., 2024).

The Core Interplay: The relationship between OSINT and AI propaganda thus mirrors the larger dynamic between decentralized verification and centralized manipulation (Ghioni et al., 2024; Goldstein et al., 2024). Whereas crowdsourced OSINT acts as a grassroots, distributed form of verification, AI-driven propaganda functions as a centralized, technologically mediated form of deception (Goldstein et al., 2024; O’Browne et al., 2024). This interaction suggests that contemporary digital warfare relies less on the creation of content itself than on the power to establish the credibility, accuracy, and influence of information in a shared global governance system (Emery-Xu et al., 2025; Silva, 2025).

3. AI as opportunity, threat and political manipulation

The literature reveals different ways through which AI could be beneficial to the young generation while also threatening human well-being and democratic societies. This

contradiction proves that AI is not intrinsically good or bad, but its impact depends on how it is designed, regulated, and adopted (Fitz-Gerald & Padalko, 2026; UNESCO, 2024). Deepfakes, bots, and fake news could distort the outcome of political events and sway public opinion. Given the extensive reach of social media, AI-generated disinformation could rapidly spread and affect millions of people. Such challenges to political processes pose a significant risk to democratic governance (Fitz-Gerald & Padalko, 2026; UNESCO & UNDP, 2025).

4. AI and mistrust reputation

The widespread use of fake news and deepfakes could trigger a high level of distrust among the general population. People may become skeptical about the credibility of institutions and question the authenticity of information and democratic processes. Consequently, AI could undermine democracy by fueling social polarization, mistrust, and uncertainty in political leadership (UNESCO, 2024; UNESCO, 2026). Deepfakes and AI-manipulated visuals could damage the reputation of politicians and ordinary citizens. Such challenges to personal integrity could compel individuals to invest more resources in protecting their digital identity, reputation, and public perception (Fitz-Gerald & Padalko, 2026; UNESCO & UNDP, 2025).

5. The need for governance

The literature emphasizes the importance of effective governance in countering the identified risks. Governments need to implement appropriate policies and laws to regulate the use of AI in society. Moreover, policymakers must acknowledge that AI is not an end in itself but a tool that requires responsible, transparent, and accountable adoption (Fitz-Gerald & Padalko, 2026; UNESCO, 2026).

6. The EU as a role model

The analysis of the EU AI Act and Digital Services Act (DSA) shows that the European Union has taken a leading regulatory approach towards addressing AI-related and digital-platform risks. The EU AI Act, for example, includes transparency requirements

concerning AI-generated and manipulated content, including deepfakes. Other jurisdictions could consider similar approaches to enhance transparency, accountability, and security on digital platforms (Fitz-Gerald & Padalko, 2026; European Commission, 2026).

7.Cybersecurity risks

Generative AI and large language models could transform cybersecurity while simultaneously creating new vulnerabilities. The same technology can empower defenders to identify and respond to threats while also providing malicious actors with more advanced tools for launching sophisticated cyberattacks (UNESCO, 2026).

Complementarity

The literature does not necessarily promote the replacement of human intelligence with artificial intelligence. On the contrary, it supports the view that AI should function as a complementary technology that serves human-centred objectives while maintaining human oversight, accountability, and decision-making (UNESCO, 2024; European Commission, 2026).

Peace and international security

Since disinformation, cyberattacks, and AI-enabled manipulation can have cross-border implications, countering these risks requires coordinated responses from policymakers around the globe. In this regard, international collaboration is critical for developing resilient AI governance frameworks and addressing emerging global AI challenges (Fitz-Gerald & Padalko, 2026; Cass-Beggs & Samson, 2026).

Constant updates

Since AI technology develops faster than traditional legislative processes, policymakers need to regularly review and update existing legal frameworks. AI governance should therefore remain adaptive and flexible enough to respond to emerging risks and technological

developments (Fitz-Gerald & Padalko, 2026; European Commission, 2026). The EU AI Act itself follows a phased implementation approach, with different requirements coming into force over time, illustrating the need for regulatory frameworks to evolve alongside technological developments.

Discussion

The qualitative analysis reveals that there is a clear conflict between decentralized, crowdsourced OSINT and the use of AI in the automated dissemination of propaganda in today's digital conflicts. At one extreme of the spectrum, crowdsourced OSINT efforts rely on volunteers, including ordinary people, independent journalists, academics, and civil society organizations, to collect, verify, and share verifiable information online (Ghioni et al., 2024; La Barbera et al., 2024). These collaborative networks contribute to transparency and civic resilience, providing a reliable alternative to official government sources and fake news. In contrast, the widespread availability of generative AI, automated bot accounts, and highly realistic deepfakes allows bad actors to produce customized disinformation at a massive scale and at high velocity (Goldstein et al., 2024; Marigliano et al., 2024; Mustafa et al., 2025). These AI-powered tools distort the information environment, undermine public confidence in core democratic institutions, and manipulate social media platforms to influence the attitudes of populations in other countries (Imam, 2025). Thus, current digital conflicts are no longer about producing a greater number of pieces of content than the opposition, but rather about determining what constitutes credible information, establishing the legitimacy of the dominant narrative, and securing epistemic sovereignty in the context of global governance (Emery-Xu et al., 2025; Silva, 2025).

Conclusion

In this paper the relations between crowdsourced intelligence and artificial intelligence propaganda and digital warfare are studied. Our study contributes to the expanding research on open-source intelligence, the governance of artificial intelligence and digital propaganda as a matter of global governance (Ghioni et al., 2024; Marigliano et al., 2024). The study

findings unveiled the paradoxical nature of automated deception and verification as the impact of artificial intelligence on digital propaganda (Balasubramanian et al., 2025). Artificial intelligence can assist crowdsourced intelligence with the overall speed of information collection and verification processes (O’Browne et al., 2024). In contrast, automated deception tools enable the production of disinformation out of the verification capacity of crowdsourced intelligence (Goldstein et al., 2024; Mustafa et al., 2025). This results in a wider contest about truth, reliability, and authenticity, raising questions about epistemic sovereignty and management (Emery-Xu et al., 2025; Silva, 2025). Crowdsourced Open Source Intelligence is one approach to resolving centralized manipulation and generating social resilience (La Barbera et al., 2024), but it cannot replace effective management, which should also cover the risks of generative AI (UNESCO, 2026). The best approach is to combine human and machine intelligence, as proposed by UNESCO (2024) and the European Commission (2026).

The EU’s AI Act and Digital Services Act are notable examples of approaches to hybrid warfare regulation; nevertheless, since the development of artificial intelligence significantly exceeds legislative practices, this issue will always be actual and will require active policy innovations (Fitz Gerald & Padalko, 2026; Cass Beggs & Samson, 2026). Consequently, further research is needed to consider the regulation of hybrid wars from the perspective of multiple countries. Ultimately, the present findings demonstrate the complex nature of the interaction between human and artificial intelligence, which remains critical to social integrity, international relations, and security.

Reference

Balasubramanian, P., Liyana, S., Sankaran, H., Sivaramakrishnan, S., Pusuluri, S., Pirttikangas, S., & Peltonen, E. (2025). Generative AI for cyber threat intelligence: Applications, challenges, and analysis of real-world case studies. *Artificial Intelligence Review*, 58, Article 336.

Cass-Beggs, D., & Samson, P. (2026). A global framework for emerging global AI challenges. In A. Fitz-Gerald, V. Ganesh, J. Nathwani, M. Niazi, & M. S. Herdem (Eds.), *Foundational principles of AI governance and policy* (pp. 195–212). Springer.

Emery-Xu, N., Jordan, R., & Trager, R. (2025). International governance of advancing artificial intelligence. *AI & Society*, 40, 3019–3044.

European Commission. (2026). AI Act service desk: Resources and implementation timeline. <https://ec.europa.eu/>

Fitz-Gerald, A., & Padalko, H. (2026). Artificial intelligence and disinformation: Building societal resilience in the age of manipulation and propaganda. In A. Fitz-Gerald, V. Ganesh, J. Nathwani, M. Niazi, & M. S. Herdem (Eds.), *Foundational principles of AI governance and policy* (pp. 181–193). Springer.

Gao, Y., Zhang, M. M., & Rui, H. (2025). Can crowdchecking curb misinformation? Evidence from Community Notes. *Information Systems Research*, 37(2), 1242–1258. <https://doi.org/10.1287/isre.2024.1609>

Ghioni, R., Taddeo, M., & Floridi, L. (2024). Open source intelligence and AI: A systematic review of the GELSI literature. *AI & Society*, 39, 1827–1842.

Goldstein, J. A., Chao, J., Grossman, S., Stamos, A., & Tomz, M. (2024). How persuasive is AI-generated propaganda? *PNAS Nexus*, 3(2), 1–7. <https://doi.org/10.1093/pnasnexus/pgae034>

Imam, M. (2025). The threats of AI and disinformation in times of global crises. *Bulletin of Islamic Research*, 3(4), 635–650. <https://doi.org/10.69526/bir.v3i4.394>

La Barbera, D., Maddalena, E., Soprano, M., Roitero, K., Demartini, G., Ceolin, D., Spina, D., & Mizzaro, S. (2024). Crowdsourced fact-checking: Does it actually work? *Information Processing & Management*, 61(5), Article 103792. <https://doi.org/10.1016/j.ipm.2024.103792>

Marigliano, R., Ng, L. H. X., & Carley, K. M. (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, Article 170.

Mustafa, H., Luczak-Roesch, M., & Johnstone, D. (2025). Conceptualizing the evolving nature of computational propaganda: A systematic literature review. *Annals of the International Communication Association*, 49(1), 45–60.
<https://doi.org/10.1093/anncom/wlaf001>

O'Browne, T., Abedin, M., & Chowdhury, M. J. M. (2024). A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications. *International Journal of Information Security*, 23, 2911–2938.

Osimen, G. U., Newo, O., & Fulani, O. M. (2024). Artificial intelligence and arms control in modern warfare. *Cogent Social Sciences*, 10(1), Article 2407514.
<https://doi.org/10.1080/23311886.2024.2407514>

Silva, S. (2025). Artificial intelligence and international relations: Navigating opportunities and challenges in global governance. *JANUS.NET, e-Journal of International Relations*, 16(2), 22–39. <https://doi.org/10.26619/1647-7251.16.2.2>

UNESCO.(2024).Examining media and information literacy responses to generative AI: A UNESCO policy brief. UNESCO, & UNDP. (2025). Artificial intelligence, freedom of expression and elections: Safeguarding democratic processes.