IE University IE International Policy Review (IPR)
Journal **7 Issue 1** (2026)
https://ipr.blogs.ie.edu/

AI, Ethics, and Propaganda: The United Kingdom's Ethical Dilemma in Responding to China's Use of AI-Driven Information Warfare

Aden Couture

School of Politics, Economics and Global Affairs, IE University, Madrid, Spain.
Bachelor of International Relations

E-mail: acouture.ieu2024@student.ie.edu

Published January 2026

Editor: Marie-Louise Palumbo, IE University

Abstract

Transforming the dimensions of information warfare, artificial intelligence (AI) has improved both the precision and reach of narrative manipulation at an ever-increasing pace. As authoritarian powers use machine learning, deepfakes, and automated propaganda to shape perceptions, liberal democracies face a key challenge: how to protect and defend against such tactics without compromising their ethical and legal standards. Exploring the world of AI propaganda and information warfare, this article examines a key dilemma through the case of the United Kingdom's response to China, framed within the domain of 'security on land', while focusing on the defence of the domestic informational environment as a core element of military security. Moreover, emphasising that the UK's commitment to transparency and accountability strengthens democratic legitimacy while inevitably creating a vulnerability when faced with states that are not bound by such ethical and legal constraints, such as China. Asymmetry is shown through the analysis of the balance between authoritarian efficiency and democratic restraint, where moral integrity affords long-term legitimacy. Still, it limits the ability to respond rapidly and effectively. From innovation to education, through a qualitative examination, this paper concludes that the United Kingdom must align its ethics with strategy to move forward and maintain its influence in the world of information warfare.

Keywords: AI-Driven Propaganda; Democratic Ethics; Strategic Asymmetry; Disinformation; UK–China Relations; Information Security

1. Introduction

The world of international relations has changed considerably since the advent of artificial intelligence, as information itself has become a weapon. The rapid integration of AI into propaganda marks a new phase in warfare, in which algorithms, rather than armies, shape public perception and confer political legitimacy. Defined by its use of machine learning and automation, as AI continues to evolve, 'the challenge of discerning genuine content from fabricated material will only intensify'.[1] This

[1] Shahla Nasiri and Armin Hashemzadeh, "The Evolution of Disinformation from Fake News Propaganda to AI-driven

is a significant concern where propaganda is in action, as political and military objectives are increasingly targeted.

This article addresses the area of 'security on land', focusing on how states protect their domestic informational environment from the rising threat of AI-enabled manipulation as public trust erodes and moral cohesion weakens. Unlike cyberattacks that target systems, information warfare is a method that targets the human cognitive domain, meaning the minds and emotions of citizens. Democratic societies, such as the United Kingdom, face a distinct challenge within the realm of information warfare: how to respond effectively to hostile information operations without undermining the ethical and democratic principles that underpin their legitimacy.

China has emerged as the foremost practitioner of AI-driven propaganda, which, according to the U.S. Department of Defense, the PLA (People's Liberation Army) is moving towards 'next-generation combat capabilities' that it defines as 'intelligentized warfare'.[2] China's core focus on control over data, perception, and communication as tools of warfare seeks strategic advantage through the management of information, disregarding ethical implications to gain global influence and internal power. However, in contrast, the *UK Defense Artificial Intelligence Strategy* highlights its focus on maintaining trust and a 'clear commitment to lawful and ethical AI use', guided by responsibility and transparency.[3] The difference between state policies on AI-driven information warfare is evident, exposing a clear normative divide: China uses AI to control information, whereas the UK uses it to protect its integrity.

This, therefore, brings up the research question driving this article: *To what extent can the United Kingdom uphold ethical standards in information operations while effectively responding to China's use of AI-driven propaganda?*

Spanning from 2017 to 2025, the timeframe used in this paper corresponds to China's AI propaganda expansion and the UK's strategic adaptation. This study both examines and compares the strategy and ethics behind the evolution of AI as a tool for information warfare between both states, proposing policy measures to enhance democratic resilience without compromising integrity.

2. Background: AI, Propaganda, and the Transformation of Information Warfare

The evolution and usage of information in the world of militarisation predates the digital era; yet, its rapid acceleration is due to the diffusion of networked technologies and the integration of AI into both military and political strategies. With its growing grip on global military regimes, the combination of conventional force, psychological, and cyber components, also known as hybrid warfare, has become a hallmark of modern conflict. Missy Cummins, a former U.S. Navy pilot and now professor at Duke University, argues that advances in

Narratives as Deepfake," *Journal of Cyberspace Studies* 9, no. 1 (2025): 229–250.

[2] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China: Annual Report to Congress* (2024), 8.

[3] Ministry of Defence, "Defence Artificial Intelligence Strategy," Department of Health, June 17, 2022.

commercial AI have outpaced military development. This has resulted in what she considers a "metaphorical arms race",[4] reshaping how states integrate AI into strategic operations, completely transforming modern conflict into reliance on algorithmic control, perception, and information.

Highlighted by Russia's hybrid operations in Crimea, the post-2014 period represented the power and importance of digital propaganda in modern warfare and military strategy. China closely studied these examples, incorporating similar tactics into its formerly defined 'Three Warfares' framework. Originally adopted in 2003, the PLA introduced this strategy under three categories: Psychological, Media, and Legal Warfare, all of which pushed China's advancement towards modernised operations.[5] Since its development in the early 2000s, it has evolved from a political and ideological lens into an integrated component of informationised warfare, now emphasising the use of emerging technologies such as AI and social media manipulation.[6] The introduction of AI into the Chinese military framework has significantly enhanced its capabilities, enabling the state to automate message amplification, analyse sentiment, and generate synthetic media on a large scale.

Domestically, China's information strategy reveals the close integration of AI into its propaganda ecosystem. Under the Cyberspace Administration of China (CAC), machine-learning systems are used to monitor discourse, tailor information, and identify and prevent dissent. Codified in the Provisions on the Governance of the Online Information Content Ecosystem (2019), this approach requires online platforms to implement content management mechanisms, which include algorithmic recommendation models and manual intervention systems, which "cultivate a positive, healthy, and upward-oriented network culture".[7] Moreover, this system has a clear focus on the control of society, upholding "mainstream value orientation".[8]

Operating under a civil-military fusion, this framework utilises technologies originally developed for civilian purposes, such as facial recognition and data analytics, to serve state security objectives. This unethical use of AI concerns democratic states as China simultaneously aims to become THE global leader of AI by 2030, "making China the world's primary AI innovation center", according to the 2017 New Generation Artificial Intelligence Development Plan.[9]

Outside of China, external influence has expanded AI-enabled influence networks that target global audiences.

[4] Missy Cummings, *Artificial Intelligence and the Future of Warfare* (London: Chatham House for the Royal Institute of International Affairs, 2017), 1.

[5] Morgan Martin, "China's Three Information Warfares," *U.S. Naval Institute Proceedings*, March 3, 2021.

[6] China Aerospace Studies Institute, *Review of In Their Own Words: Science of Military Strategy*, 2020, accessed November 14, 2025.

[7] "网络信息内容生态治理规定" [Provisions on the Governance of the Online Information Content Ecosystem], Central Cyberspace Affairs Commission, 2019.

[8] Central Cyberspace Affairs Commission, *Provisions on the Governance of the Online Information Content Ecosystem*.

[9] "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)," *DigiChina*, October 2021.

In an attempt to exert soft power, China has employed a range of tactics, from controlling Youtube influencers to launching marketing campaigns and utilising propaganda to counter the spread of anti-Chinese messages.[10] One key hallmark of this control was investigated by Graphika, an advanced cyber threat intelligence and social media analysis platform, which labelled it the "Spamouflage Dragon".[11] This pro-Chinese propaganda network not only targets users with fake accounts, but also real social media influencers, promoting Chinese culture while criticising democratic movements such as those in Hong Kong. This extensive web of coordinated accounts uses synthetic media, deepfakes, and bot amplification to promote pro-Beijing narratives, a significant threat to Western states such as the United Kingdom. Operating during times of crisis, such as the Covid-19 pandemic,[12] these systems aim to disseminate coordinated disinformation across global platforms, highlighting China's sophisticated evolution from traditional propaganda to algorithmic persuasion in the digital age.

On the other hand, the United Kingdom's strategic approach to AI in defence and communication contrasts that of China, promoting the key values of ethical governance and transparency. Published under the 2019 - 2022 Conservative government, the UK Defense Artificial Intelligence Strategy, as briefly explored in the introduction, highlights fairness, accountability, responsibility, transparency, and reliability. As stated in this strategy framework, "Our vision is that, in terms of AI, we will be the world's most effective, efficient, trusted and influential Defence organisation for our size"[13], truly pushing the belief in the compatibility between trust, security, and AI evolution in state strategy.

Meanwhile, complementing this AI diffusion is the Online Safety Act of 2023, which simultaneously protects children and adults online by imposing duties on social media companies and search services[14]. As of 25 July 2025, platforms have a legal duty to protect children online, requiring them to mitigate algorithmic harm[15]. Furthermore, the National AI Strategy of 2021 somewhat mirrors China's developmental plans mentioned previously, yet specifically emphasises investment, innovation, and the protection of values[16], in perhaps a less realistic way, focusing on multilateral cooperation.

The UK's model of protecting society through trust emphasises its democratic values, privileging restraint, legality, and cooperation. However, its institutional structure remains complex, as responsibility for AI-related governance is distributed across various distinct governmental departments, creating bureaucratic inertia

[10] Patrick Warren, Darren Linvill, Leland Fecher, Jayson Warren, and Steven Sheffield, *The 5-Year Spam: Tracking a Persistent Chinese Influence Operation*, 2023, 1–3.
[11] Graphika, *Spamouflage Breakout*, 2021, accessed November 14, 2025.
[12] Graphika, *Spamouflage Breakout*.
[13] Ministry of Defence, "Defence Artificial Intelligence Strategy."
[14] Department for Science, Innovation and Technology, "Online Safety Act," GOV.UK, July 24, 2025, accessed November 14, 2025.
[15] Department for Science, Innovation and Technology, "Online Safety Act."
[16] GOV.UK, "National AI Strategy," December 18, 2022, accessed November 14, 2025.

that hinders change at a slower rate compared to China.[17] This plural framework allows oversight and ethical scrutiny, yet creates fragmentation and extremely slow policy coordination between the civil and defense domains.

Together, the developments and strategies of both China and the UK illustrate and define how AI has transformed the nature of information warfare in the modern age, moving from a tool of strategic communication to a central instrument of state power. Both states recognise the security implications of these technologies, yet embody fundamentally different philosophies of control. While China integrates AI into state-directed information management, the UK emphasises ethics and legal principles. Establishing the context for analysis, this divide will be examined in terms of how these contrasting models generate asymmetries of influence and raise profound questions on the balance between ethical restraint and strategic necessity in the digital age.

3. Analysis: Asymmetry Between Authoritarian Efficiency and Democratic Restraint

The clear asymmetry between China's authoritarian efficiency and the United Kingdom's ethical restraint is what lies at the heart of this paper's analysis. Defining the information warfare landscape, the evolution of machine learning and automated persuasion has transformed this battle for power into a moral hazard. The ability for the weaponisation of information not only lies within a state's data and algorithms, but in the ethics that govern their use.

At its core, the most pressing problem is how democracies can defend themselves in a world where authoritarian states face no moral limits or obligations. Michael Walzer, a leading political theorist and key voice in modern Just War theory, described in Just and Unjust Wars (2015) that the rules of 'jus in bello', the justice of conduct in war, also apply to actions short of war.[18] Demanding both proportionality and discrimination, these rules mean that even indirect forms of conflict must not harm civilians or cross moral boundaries. According to Walzer, in this regard, within the information domain, democratic states, such as the UK, must counter manipulation and disinformation without abandoning truth and public trust. Ethical restraint in this case, therefore, becomes not a limitation but rather a source of legitimacy

This asymmetry that occurs between the two systems begins with governance. As previously noted, the *New Generation Artificial Intelligence Development Plan* (2017) combines the powers of civilian and military AI development, positioning it as a "new focus of international competition".[19] Laying out clear and eager milestones, such as an AI core industry worth 1 trillion Renminbi (RMB, or Chinese Yuan) by 2030, there is a call for "deep military-civil integration".[20] Evolving into a

[17] Jennifer Kretchmar, "Bureaucratic Inertia," EBSCO Information Services, 2021, accessed November 14, 2025.

[18] Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (New York: Basic Books, 2006), 16.

[19] "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)."

[20] "Full Translation: China's 'New Generation Artificial Intelligence Development Plan.'"

system governed in a centralized form, this plan is under direct control of the Central Cybersecurity and Informationization Commission, chaired by Xi Jinping, and executed through the Cyberspace Administration of China, a hybrid party-state regulator overseeing content, data, and cybersecurity.[21] This produces a tightly structured vertical coordination system between all political, military, and industrial players. This, therefore, allows for rapid policy iteration, yet prioritises speed, cohesion, and oversight above transparency and accountability.

In contrast to the Chinese system, the UK's *Defense Artificial Intelligence Strategy* (2022) has a far more dispersed authority and control structure. Under the control of the Ministry of Defense (MoD), the Department for Science, Innovation, and Technology (DSIT), and Ofcom, ethical oversight is deeply embedded.[22] This, however, as mentioned previously, creates a term known as 'bureaucratic inertia', defined as the tendency for large organisations to resist change due to slow, inflexible procedures.[23] This distinction from China's fast-paced system places the UK in second place and allows Chinese dominance in the AI information warfare sphere of influence. China seeks power and control; meanwhile, the UK seeks defense and rule. Focusing on detection, attribution, and public education through the National Cyber Security Centre (NCSC) and the 77th Brigade, a specialist force that protects the UK from information warfare, British interests are clearly set on protecting its people and values.[24]

As reported by the European External Action Service (EEAS), regimes such as China operate within a largely hidden digital ecosystem, where 79.5% of channels are estimated to be covert or non-attributed.[25] This means that authoritarian states can deploy AI-generated content and influence that poses a minimum risk of detection. This is a significant dilemma for democratic states such as the UK, as the article states that these key players in global information warfare "exploit anonymity, making it difficult to trace operations and shielding them from dancing exposure or legal accountability", a structural advantage that is hard to compete with.[26] Chinese information strategy can use propaganda at scale through fabricated news sites and inauthentic networks that the UK cannot do. This ethical divergence lies at the heart of this article, particularly in the UK's strategic challenge: responding effectively to AI-driven Chinese information warfare while upholding democratic norms, civil liberties, and legitimacy.

This, overall, leads to a central paradox: the same ethical restraints that restrict the UK's operational reach, also enhance its strategic influence. Transparency and legality strengthen British leadership, presenting itself as a strong

[21] Roger Creemers, *The Regulation of Generative AI in China* (SSRN, May 2024), 2.
[22] Ministry of Defence, *Defence Artificial Intelligence Strategy*.
[23] Kretchmar, "Bureaucratic Inertia."

[24] "77th Brigade – Information Operations," British Army, 2019, accessed November 14, 2025.
[25] European External Action Service, *Report on FIMI Threats 3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the Architecture of FIMI Operations* (March 2025).
[26] European External Action Service, *Report on FIMI Threats*.

democratic state; however, ethics alone cannot guarantee resilience. Revealing this clash not only between the UK and China, but also wider democratic and authoritarian strategies, it is clear that the future strength of the UK depends on transforming ethical governance into an operational asset. There must be alignment between moral integrity and strategic precision.

To conclude this analysis, the significance and depth of the strategic gap between the UK and China can be defined by three asymmetries:

- Pace: Chinese AI-driven information operations act rapidly and spontaneously through centralised authority; the UK responds slowly, acting under legal and bureaucratic review.
- Risk tolerance: China can tolerate and accept reputational costs associated with influence exposure; the UK cannot, as such costs threaten its democratic legitimacy.
- Information control: China uses AI to shape information; the UK uses AI to stabilise it.

4. Policy Recommendations: Aligning Ethical Principles With Strategic Necessity

The current UK policy framework provides a powerful normative foundation; however, it remains strategically weak in contrast to the rapidly expanding Chinese AI-enabled information warfare. Ethically sound, the principles embedded within the *Defense Artificial Intelligence Strategy* (2022) provide a democratically legitimate strategy; however, it suffers from institutional fragmentation and slow decision-making.[27] The Parliamentary Office of Science and Technology (POST) has furthermore stated concerns regarding the lack of a skilled cyber workforce, emphasising the "need for the UK to improve skills, security, technologies and offensive capability".[28] This highlights the weak response in contrast to China's hostile influence. At the same time, we have seen how China's centralised, civil-military fusion, under the 2017 *New Generation AI Development Plan*, allows for rapid response and innovation.[29] This asymmetry requires a clear shift in UK AI information-warfare strategy, moving towards a more integrated and technologically advanced model whilst maintaining its ethical roots.

To begin, the creation of a 'National Information Security Command' (NISC) would be a key step in the direction of structural reform, improving speed, efficiency, and authority. Closely following the already established National Cyber Security Centre (NCSC) as a key hub for technical authority and rapid threat assessment, the NISC would integrate the current division of tasks between the MOD, GCHQ, DSIT, and Foreign Office under one single strategic command body.[30] Its scope would cover real-time threat analysis, coordination of information operations, and oversight of ethical compliance, allowing for a seamless response to China whilst maintaining democratic standards.

[27] Ministry of Defence, *Defence Artificial Intelligence Strategy*.
[28] Dylan Sherman and Simon Brawley, "AI, Disinformation and Cyber Security," POST, January 29, 2025.
[29] "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)."
[30] National Cyber Security Centre, accessed November 14, 2025.

Such a plan mirrors the set, vertical coordination that has been described previously in China's Cyberspace Administration, which operates under the Central Cybersecurity and Informatization Commission to synchronise data governance, propaganda and security policy.[31] That being said, while the UK cannot replicate authoritarian control, it can adopt comparable organisational coherence while maintaining and embedding ethical and legal advisors. This would ensure a rapid response from the NISC that aligns with democratic values, all while minimising bureaucratic inertia.[32] This policy would enable the state to match China's operational speed without compromising transparency.

Secondly, the UK must prioritise technological capability as the backbone of information defence. From AI forensics to content authentication, this sphere must become a national security priority, given the speed and scale of China's infrastructure. Advanced digital tools capable of authenticating content origin and detecting synthetic manipulation should receive increased investment from both the public and private sectors, as recommended by the OECD, allowing authorities to identify deepfakes and inauthentic networks at a far greater scale.[33] Accelerating development, the UK should focus on formalising partnerships between the NCSC, private firms, and the Alan Turing Institute, the nation's centre of research and innovation for AI.[34] These partnerships would not only guide the UK towards a more innovative information domain but could also be used to counter the skilled workforce shortage by including educational institutions. The combination of governmental, private, and educational sectors would allow for significant improvements in innovation and capability, all while supporting the continuous training of new workers.

Thirdly, to maintain credibility, the UK must not solely rely on defensive innovation. Developing ethical offensive capabilities–defined as proportionate, legally authorised actions that expose, attribute, and counter foreign hostile information operations–is essential and necessary for publicly challenging aggressive propaganda while not mirroring authoritarian tactics. These measures would target foreign adversarial influence campaigns and exclude domestic persuasion, which therefore ensures compliance with democratic norms and civil liberties. From debunking mechanisms to targeted campaigns, the UK could involve a wide variety of strategies that would hold it up in the ever-evolving world of information warfare.

Together, these recommendations would align both ethics and strategy. By integrating institutions and enhancing technology, the United Kingdom can safeguard its information environment without compromising the democratic values it must uphold.

---

[31] "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)."

[32] Kretchmar, "Bureaucratic Inertia."

[33] OECD, "AI Principles," 2024, accessed November 14, 2025.

[34] "Our Strategy," The Alan Turing Institute, 2023, accessed November 14, 2025.

5. Conclusion

As artificial intelligence has evolved in the digital era, it has transformed into an active instrument of strategic power. As explored throughout this article, the United Kingdom and China highlight two opposing strategies for navigating this transformation. The Chinese model emphasises centralised, civil-military fusion, enabling a rapid and efficient system of AI-driven information warfare. On the other hand, the UK has taken a far more ethical approach, focusing on the principles of transparency, legality, and legitimacy, yet limiting operational agility. This division produces a clear asymmetry, where China uses AI to shape and control information, while the UK uses it to protect and stabilise its information environment.

Analysing the key differences, this article has demonstrated that this asymmetry is spread across three key dimensions: the pace of response, the tolerance for reputational risk, and the purpose of information control. China, acting as an unconstrained operational model, allows for manipulation to take place on a significant scale with speed, whereas the UK's heavy oversight generates slow, bureaucratic decision-making. Yet this comparison also reveals a clear paradox, where the UK's ethics that limit its operations also act as a strategic asset, providing democratic strength and legitimacy.

The policy recommendations stated in this paper move towards an aligned path, including a unified National Information Security Command (NISC), as well as investment to bridge the gap between ethical commitment and strategic necessity. Ultimately, the future strength and resilience of the United Kingdom depends on its ability to integrate morals and strategy. Ethical constraint must be transformed into a source of resilience in an era where information itself has become a weapon.

Bibliography

British Army. 2019. "77th Brigade – Information Operations." https://www.army.mod.uk/learn-and-explore/about-the-army/formations-divisions-and-brigades/field-army-troops/77th-brigade-information-operations/.

Central Cyberspace Affairs Commission. 2019. "网络信息内容生态治理规定 [Provisions on the Governance of the Online Information Content Ecosystem]." https://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm.

China Aerospace Studies Institute. 2020. *Review of In Their Own Words: Science of Military Strategy*.

Creemers, Roger. 2024. *Review of The Regulation of Generative AI in China*. SSRN. https://doi.org/10.2139/ssrn.

Cummings, Missy. 2017. *Artificial Intelligence and the Future of Warfare*. London: Chatham House.

Department for Science, Innovation and Technology. 2025. "Online Safety Act." GOV.UK. https://www.gov.uk/government/collections/online-safety-act.

DigiChina. 2021. "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)." https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

Graphika. 2021. *Spamouflage Breakout.* https://graphika.com/reports/spamouflage-breakout.

GOV.UK. 2022. "National AI Strategy." https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version.

Kretchmar, Jennifer. 2021. "Bureaucratic Inertia." EBSCO Research Starters. https://www.ebsco.com/research-starters/social-sciences-and-humanities/bureaucratic-inertia.

Martin, Morgan. 2021. "China's Three Information Warfares." *U.S. Naval Institute Proceedings*, March 3. https://www.usni.org/magazines/proceedings/2021/march/chinas-three-information-warfares.

Ministry of Defence. 2022. "Defence Artificial Intelligence Strategy." https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy.

National Cyber Security Centre. n.d. "About the NCSC." https://www.ncsc.gov.uk.

Nasiri, Shahla, and Armin Hashemzadeh. 2025. "The Evolution of Disinformation from Fake News Propaganda to AI-driven Narratives as Deepfake." *Journal of Cyberspace Studies* 9 (1): 229–250. https://doi.org/10.22059/jcss.2025.387249.1119.

OECD. 2024. "AI Principles." https://www.oecd.org/en/topics/sub-issues/ai-principles.html.

Sherman, Dylan, and Simon Brawley. 2025. "AI, Disinformation and Cyber Security." Parliamentary Office of Science and Technology (POST).https://post.parliament.uk/ai-disinformation-and-cyber-security/.

The Alan Turing Institute. 2023. "Our Strategy." https://www.turing.ac.uk/about-us/our-strategy.

U.S. Department of Defense. 2024. *Military and Security Developments Involving the People's Republic of China: Annual Report to Congress.* https://media.defense.gov.

Walzer, Michael. 2006. *Just and Unjust Wars: A Moral Argument with Historical Illustrations.* 4th ed. New York: Basic Books.

Warren, Patrick, Darren Linvill, Leland Fecher, Jayson Warren, and Steven Sheffield. 2023. *The 5-Year*

Spam: Tracking a Persistent Chinese Influence Operation. Clemson University Media Forensics Hub.