Hybrid CoE Paper 29

Artificial Intelligence and Foreign Information Manipulation: Chinese and Russian approaches

Hybrid CoE

Heidi Hanhijärvi – March 2026

Hybrid CoE Papers are finalized analyses of a topic related to hybrid threats, based on one or more research questions. They may be either conceptual analyses or based on a concrete case study with empirical data.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 www.hybridcoe.fi

ISBN 978–952–7591–36–9 (web)
ISBN 978–952–7591–37–6 (print)
ISSN 2670–2053 (web)
ISSN 2814–7227 (print)

March 2026

Cover photo: Master1305 / Shutterstock.com

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) is an autonomous, network-based international expert organization dedicated to addressing hybrid threats. Hybrid CoE's mission is to enhance the security of its 35 Participating States, the European Union and NATO by providing expertise, training, and networks to counter hybrid threats. Its core values are excellence, integrity and respect. The Centre is located in Helsinki, Finland.

Responsibility for the views expressed in this paper ultimately rests with the authors.

Contents

Summary

Influence networks linked to China and Russia have actively used foreign and domestic artificial intelligence (AI) tools to boost their existing operational tactics since at least 2022. AI technology can act as a force multiplier for disinformation, electoral interference, and the spread of technology that reflects authoritarian standards and values. Such tools provide information manipulation actors with enhanced cost-efficiency, scale and personalization in content production, while promoting a distorted worldview due to their biased or deficient training data.

There is a gap between Russia's AI ambitions and its capabilities, at least in the short term. Russia-linked influence actors are using AI tools available on the open market to broaden their information manipulation toolbox, but they are unable to devote significant resources to developing their own AI systems. Meanwhile, China's world-leading national AI capabilities already provide China-linked influence actors with the ability to use domestic AI tools for operational support, data gathering and content personalization to target individual users online. It is highly likely that this trend will continue, with China-linked actors further developing their capabilities and skills, and Russia lagging behind. Russia's cooperation with China could be an important enabler of its future AI capabilities. In the context of foreign information manipulation, however, the two countries appear to echo each other only when their distinct interests are aligned.

Developments in AI technology present practitioners in the Euro-Atlantic region with threats and risks from hybrid threat actors, alongside opportunities to harness AI to support countermeasures. The growth in AI-powered foreign information manipulation requires liberal democracies urgently to combine new technological solutions with conventional countermeasures to effectively safeguard democratic processes and the global information environment's integrity.

1 Introduction

This paper analyses China's and Russia's artificial intelligence (AI) ambitions, national capabilities and use cases in the context of their information manipulation targeting foreign countries. The paper combines desk research and roundtable discussions during an expert workshop organized by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in September 2025. The data collection for this report was concluded in September 2025.

The key research question this paper addresses is: *How have China and Russia integrated AI technologies into their respective foreign information manipulation strategies, national capability development and operations?* The analysis is structured as follows. The following sections provide an actor-specific analysis of China and Russia, providing an insight into both countries' ambitions, national capabilities and use cases of AI tools in information manipulation targeting foreign countries. The paper highlights both countries' integration of AI technologies into their strategic approaches, capability development and information manipulation efforts in distinct ways. In the final two sections the paper compares Chinese and Russian approaches, identifies emerging dynamics, and discusses the implications of AI-facilitated information manipulation for countermeasures.

The weaponization and manipulation of information are among the hallmarks of hybrid threats.[1] By exploiting division in societies and creating confusion and disorder in the information domain, hybrid threat actors aim to undermine democratic processes and decision-making capabilities in target countries. Since 2013–2014, around the Revolution of Dignity and the Annexation of Crimea, Russia has renewed its influence efforts in the information domain and employed continuous multiplatform and multilanguage disinformation campaigns.[2] Chinese foreign information manipulation efforts have received less attention than Russian influence operations; however, China has also recognized the value of these deniable, low-cost and low-risk efforts in the information domain. Over the last decade Chinese disinformation and propaganda efforts have harnessed new technologies to become increasingly sophisticated, aggressive and widespread.[3]

Russia's information warfare has been aggressive and open to experimentation while aiming to preserve its regime, contribute to the re-establishment of its Soviet-era sphere of influence and erode trust in democratic

[1] Georgios Giannopoulos et al., 'The Landscape of Hybrid Threats: A Conceptual Model', EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978–92–76–29819–9, doi:10.2760/44985, JRC123305, 32.

[2] See e.g. European Parliament Research Service, 'Russia's strategy for Latin America: Strengthening ties in the light of the 16th BRICS Summit in Kazan (Russia)', European Parliament, October 2024 https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762473/EPRS_BRI(2024)762473_EN.pdf; VIGINUM, 'African Initiative: From Public Diplomacy to Covert Influence Operations', Premier Ministre, Secrétariat général de la défense et de la sécurité nationale, VIGINUM, Technical Report, June 2025, https://www.sgdsn.gouv.fr/files/files/Publications/20250612_TLP-CLEAR_VIGINUM_FCDO_EEAS_Technical_Report_African_Initiative_EN.pdf.

[3] Sarah Cook et al., 'Authoritarian Expansion and the Power of Democratic Resilience', in *Beijing's Global Media Influence*, ed. Sarah Cook, Angeli Datt, Ellie Young, B. C. Han (Freedom House, 2022). https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience/country-reports.

institutions in target countries. Meanwhile, China's information manipulation has traditionally aimed to increase its discourse power[4] on the global stage, silencing dissent and promoting its positive reputation and geopolitical objectives through long-term efforts. Both Russia and China aim to weaken the alleged hegemony that the United States and its allies have held in global power structures, promote a multipolar world order, and erode democratic processes in foreign countries.[5]

For the purpose of this publication, information manipulation can be defined as a phenomenon encompassing three criteria: "a coordinated campaign, the diffusion of false information or information that is consciously distorted, and the political intention to cause harm".[6] Electronic warfare, cyber threats and other broader foreign influence efforts have been excluded from this analysis. This paper therefore focuses on specific forms of information manipulation – propaganda and disinformation – to better understand China's and Russia's ambitions, capabilities and uses of AI tools in deliberately spreading biased, misleading or false information to promote a political cause or to harm a social group, organization or country.[7]

There is no commonly shared definition of AI, which is in part due to the broad range of applications included in the category of AI systems.[8] This paper adopts an open definition of AI which has been proposed by the European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG): "Systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals."[9] This includes machine learning and its

[4] From a Chinese perspective discourse power is perceived as an actor's ability to shape the international order to reflect their interests and values. See Kenton Thibaut, 'Chinese Discourse Power: Ambitions and Reality in the Digital Domain', Atlantic Council, August 2022, https://www.atlanticcouncil.org/in-depth-research-reports/report/chinese-discourse-power-ambitions-and-reality-in-the-digital-domain/, 4.

[5] Tamás Matura, 'Sino-Russian Convergence in Foreign Information Manipulation and Interference: A Global Threat to the US and Its Allies', Center for European Policy Analysis (CEPA), 30 June 2025, https://cepa.org/comprehensive-reports/sino-russian-convergence-in-foreign-information-manipulation-and-interference/.

[6] Jean-Baptiste Jeangène Vilmer et al., 'Information Manipulation: A Challenge for Our Democracies', Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces of France, August 2018, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf, 21.

[7] Propaganda refers to the biased or misleading spread of information to advance a political cause. Disinformation has been defined as the deliberate spread of false information to harm a social group, organization or country. See Claire Wardle et al., 'Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making', Council of Europe Report DGI (2017) 09, 27 September 2017, https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html.

[8] Haroon Sheikh et al., 'Artificial Intelligence: Definition and Background', in *Mission AI. Research for Policy*, (Cham: Springer, 2023), 15–41, 18.

[9] High-Level Expert Group on Artificial Intelligence, 'A Definition of AI: Main Capabilities and Scientific Disciplines', European Commission, 8 April 2019, https://ec.europa.eu/newsroom/ dae/document.cfm?doc_id=56341.

subset deep learning.[10] Generative AI models such as large language models (LLMs) are a subcategory of machine learning. They can create new content, including images, video, audio and text based on suggestions, also known as prompts.

[10] In general terms machine learning refers to a field focusing on developing computers and machines that can automatically adapt their performance in specific tasks based on given data; deep learning utilizes layered artificial neural networks to capture complex relationships in unstructured data. For a detailed discussion of machine learning, deep learning and generative AI see e.g. Faisal Kalota, 'A Primer on Generative Artificial Intelligence', *Education Sciences*, Volume 14, Issue 2 (2024): 172–187.

2 China

2.1 China’s AI and information manipulation ambitions

The political and military elites of the People’s Republic of China (PRC) view AI as a foundational part of future social and political superstructures.[11] The PRC relies on AI technologies to empower growth and competitiveness in both the civil and military sectors. The development of AI capabilities that will surpass those of the United States is a core priority for China.[12]

The PRC communicated its AI ambitions nearly a decade ago in the 2017 State Council’s New Generation Artificial Intelligence Development Plan (AIDP).[13] The AIDP envisions the growing use of AI technologies in the spheres of economic productivity, governance and national defence through three distinct goals for China: to catch up with leading AI technologies by 2020; to achieve "major breakthroughs" by 2025; and to become "a major AI innovation centre in the world" by 2030.[14] The 2015 Chinese government "Made in China 2025" plan supports the AIDP’s implementation, particularly by aiming to boost China’s own semiconductor production by 70 per cent by 2025.[15]

Under the leadership of Xi Jinping there has been a steady push in China towards more aggressive political influence activities, including information manipulation efforts targeting foreign countries.[16] The core objective of the Chinese Communist Party (CCP) is maintaining regime stability, hence ensuring that the domestic and global information environments are favourable to the regime. Through information manipulation China also seeks to increase its ability to set the agenda in international arenas (discursive power) and promote China’s reputation as a powerful state.[17]

[11] Qi Haotin, ‘China’s Evolving AI Development’, in *The AI Wave in Defence Innovation*, ed. Micheal Raska and Richard Bitziner (Abingdon: England Routledge, 2023), 137–155, 137.

[12] Liana Edgar, ‘Generative AI and Disinformation: Analysing China’s Strategy Amidst US Investment and Export Controls,’ *San Diego International Law Journal*, Volume 26, Issue 1, (2025): 147–178, https://digital.sandiego.edu/ilj/vol26/iss1/5, 149; Office of the Director of National Intelligence, ‘Annual Threat Assessment of the U.S. Intelligence Community’, Office of the Director of National Intelligence, March 2025, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf, 147.

[13] China State Council, ‘New Generation Artificial Intelligence Development Plan’, Order no. 35. 8 July 2017. For a full English translation see e.g. Graham Webster et al., ‘Full Translation: China’s "New Generation Artificial Intelligence Development Plan" (2017)’, Standford University, 1 August 2017, https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

[14] Insikt Group, ‘Measuring the US-China AI Gap’, Recorded Future Threat Analysis, May 2025, https://go.recordedfuture.com/hubfs/reports/ta-2025–0508.pdf, 24.

[15] Ibid., 33; Center for Security and Emerging Technology, ‘Notice of the State Council on the Publication of "Made in China 2025"’, Translation via Center for Security and Emerging Technology, 10 March 2022, https://cset.georgetown.edu/publication/notice-of-the-state-council-on-the-publication-of-made-in-china-2025/.

[16] For a comprehensive overview of united front work and China’s influence activities under Xi Jinping see Anne-Marie Brady, ‘Magic Weapons: China’s Political Influence Activities Under Xi Jinping’.

[17] Dexter Roberts, ‘China’s Disinformation Strategy: Its Dimensions and Future’, Atlantic Council, December 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/12/CHINA-ASI-Report-FINAL-1.pdf, 4.

Over the last decade state-linked Chinese actors have adopted an information manipulation and influence strategy which aims to manipulate public opinion, amplify polarization on key societal issues, and silence and attack individuals and entities through mass distribution of pro-Chinese content online, inauthentic social media accounts, targeted disinformation, cyberbullying and harassment.[18] Particularly since 2019 and the Covid-19 pandemic Chinese state-linked actors' information manipulation strategies have become more aggressive and have focused on covert action, indicating that Beijing's influence operations are moving closer to Moscow's.[19]

China's foreign propaganda and disinformation efforts involve CCP organs, state agencies, the People's Liberation Army (PLA), and public and private companies. The United Front Work Department and the International Liaison Department are among the central CCP influence actors, while the Ministry of State Security, Ministry for Foreign Affairs, and Taiwan Affairs Office are examples of state bodies involved in foreign information manipulation.[20] Chinese social media companies provide data and new technologies for influence activities abroad.[21] Although it is difficult to ascertain the exact roles of these actors, they generally direct the work of a vast network of companies, non-state actors, celebrities, influencers and other individuals spreading pro-Chinese propaganda and disinformation in a manner that ensures adherence to the regime's narratives.[22]

These complex networks enable pro-Chinese information manipulation to reach diverse audiences and complicate attribution efforts. Chinese information manipulation efforts occur in an information and media ecosystem that is tightly controlled by party-state agencies, and which gives prominence to the CCP's narratives, outlets and platforms.[23] China does not separate its information and influence strategies and

[18] Sarah Cook et al., 'Beijing's Global Media Influence 2022: Authoritarian Expansion and Power of Democratic Resilience', Freedom House, Country Report, September 2022, https://freedomhouse.org/sites/default/files/2022–09/BGMI_final_digital_090722.pdf.

[19] Office of the Director of National Intelligence, 'Annual Threat Assessment of the U.S. Intelligence Community', Office of the Director of National Intelligence, 5 February 2024, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf, 12. Russia's information warfare strategy is discussed in more detail below.

[20] The 'Three Warfares' strategy is discussed in more detail below. For further information about the Chinese ecosystem involved in information manipulation and influence operations abroad see e.g. Anne-Marie Brady, 'Magic Weapons: China's Political Influence Activities Under Xi Jinping'; Anne-Marie Brady, *Marketing Dictatorship: Propaganda and Thought Work in Contemporary China*, (New York: Rowman and Littlefield, 2009); Paul Charon and Jean-Baptiste Jeangène Vilmer, 'Chinese Influence Operations: A Machiavellian Moment', Institute for Strategic Research (IRSEM), French Ministry for the Armed Forces, October 2021, https://www.irsem.fr/report.html.

[21] Paul Charon and Jean-Baptiste Jeangène Vilmer, 'Chinese Influence Operations. A Machiavellian Moment', 15–16.

[22] Office of the Director of National Intelligence, 'Annual Threat Assessment of the U.S. Intelligence Community', 5, 8.

[23] Gary King et al., 'How Censorship in China Allows Government Criticism but Silences Collective Expression', *American Political Science Review*, Volume 107, Issue 2, (2013): 326–343, https://tinyurl.com/y35r5qn8; Steven

activities between peace- and wartime, instead using an integrated approach.[24]

The "Three Warfares" concept, introduced in the 2003 Political Work Guidelines of the People's Liberation Army, is key to understanding Chinese information manipulation, though the concept describes only part of the CCP's broader ambitions to influence foreign actors.[25] The "Three Warfares" strategy aims to shape public opinion domestically and internationally, influence foreign decision makers' approach to China, and create a beneficial legal environment for Chinese action. The PLA contains special units dedicated to the implementation of this strategy, including information and psychological warfare efforts.[26] China has emphasized the value of pre-emptive psychological and information operations particularly when attacking an opponent with technologically superior capabilities.[27]

Since at least 2018 PLA researchers have expressed a desire to use AI technologies to advance social media manipulation, with the goal of shaping public opinion in foreign countries.[28] This includes using AI to assist social media manipulation by more efficiently creating inauthentic content, analysing and reacting to online users' sentiments in real time, and long-term astroturfing.[29] However, PLA researchers have expressed concerns about the potential impact of using AI tools with Western "biases" coded into them.[30]

China's interest in using AI technologies is also evident in a new concept of information

Lee Myers and Paul Mozur, 'China is Waging a Disinformation War Against Hong Kong Protesters', The New York Times, 13 August 2019, https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html.

[24] Ibid.

[25] The civil-military distinction does not exist in its conventional form in China. The PLA is an important part of the party state structure, and the CCP regime has actively asserted control over the military. For more detailed information about the role of the PLA in the Chinese ecosystem see e.g. Alex Bulanov et al., 'The Politics of the Military in China: The CCP and PLA', *Copenhagen Journal of Asian Studies*, Volume 16, (2002): 11, http://dx.doi.org/10.13140/RG.2.2.10116.24966; Timothy Heath et al., 'Political Legitimacy and the People's Liberation Army', RAND, Research Report, 22 January 2025, https://www.rand.org/pubs/research_reports/RRA2751-1.html; Peter Mattis, 'China's "Three Warfares" in Perspective', War on the Rocks, January 2018 https://warontherocks.com/2018/01/chinas-three-warfares-perspective/.

[26] Elsa Kania and John Costello, 'The Strategic Support Force and the Future of Chinese Information Operations'.

[27] James Yin and Phillip Taylor, 'Information Operations from an Asian Perspective: A Comparative Analysis', *Journal of Information Warfare*, Volume 7, Issue 1: 1–23, https://www.jstor.org/stable/26486727, 13.

[28] William Marcellino et al., 'The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0: Next-Generation Chinese Astroturfing and Coping with Ubiquitous AI', RAND Corporation, September 2023, https://www.rand.org/pubs/perspectives/PEA2679-1.html, 16.

[29] Astroturfing aims to create an impression of organic support for specific issues online. Marko Kovic et al. define online astroturfing as 'the dissemination of deceptive opinions by imposters posing as autonomous individuals on the Internet with the intention of promoting a specific agenda'. See Marko Kovic et al., 'Digital Astroturfing in Politics: Definitions, Typology, and Countermeasures', *Studies in Communication Sciences*, Volume 18, Issue 1 (2018): 69–85, http://dx.doi.org/10.24434/j.scoms.2018.01.005, 71.

[30] William Marcellino et al., 'The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0: Next-Generation Chinese Astroturfing and Coping with Ubiquitous AI', 17.

manipulation known as "algorithmic cognitive warfare".[31] The emerging framework of algorithmic cognitive warfare reflects the PLA's broader recognition of algorithms' and social media's impact on shaping international public opinion. In particular, Beijing took note of the impact Russia's cognitive warfare had on shaping global opinions in the context of its full-scale invasion of Ukraine in 2022.[32] In recent years Chinese actors have increasingly moved from flooding platforms with pro-Chinese content towards using algorithms to influence individual users online. Chinese scholars envision a crucial role for AI technologies in various stages of algorithmic cognitive warfare, but AI is also likely to be particularly important in the collection and analysis of vast quantities of precise user data, an essential requirement of future algorithmic cognitive warfare.[33]

2.2 China's national AI capabilities

In 2020 China was ranked second in AI capabilities worldwide. It has since continued rapidly to gain ground on the global leader, the United States, both in AI capabilities and in readiness to adopt AI technologies in specific sectors.[34] The United States still leads the production of AI models in quantity,[35] but China leads in the number of AI-related research papers and patents. In accordance with the PRC's AIDP and the "Made in China 2025" strategies China has made significant investments in its domestic semiconductor[36] industry and its overall self-sufficiency objectives.[37] Despite these investments, economic espionage and attempts at evading export controls, the Chinese domestic semiconductor industry still lags at least five years behind that of the US.[38]

[31] Cognitive warfare has appeared in Chinese scholarship since 2010. It is central to PLA military thinking, as it aims to shape the enemy's beliefs through tailored messaging. Cognitive warfare penetrates various domains of activity while abolishing all existing boundaries between war and peacetime, as well as soldiers and civilians. See Libby Lange, 'Decoding China's AI-Powered "Algorithmic Cognitive Warfare"', Special Competitive Studies Project, November 2024, https://www.scsp.ai/resource/decoding-chinas-ai-powered-algorithmic-cognitive-warfare/, 2.

[32] Ibid., 4

[33] Ibid., 6–8.

[34] Simon Porcher, 'Measuring Artificial intelligence capabilities and readiness', *Academy of Management Proceedings, 2020*, http://dx.doi.org/10.5465/AMBPP.2020.13168abstract, 13168; Eduardo Baptista, 'China Leads the World in Adoption of Generative AI, Survey Shows', Reuters, 10 July 2024, https://www.reuters.com/technology/artificial-intelligence/china-leads-world-adoption-generative-ai-survey-shows-2024–07–09/.

[35] Nestor Maslej et al., 'The AI Index 2025 Annual Report', AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA, April 2025, 3.

[36] Semiconductors are the foundation that makes all modern computing, including artificial intelligence, possible. They power the hardware that runs AI models, enable faster and more efficient AI computations, and help scale AI infrastructure.

[37] Ardi Janjeva et al., 'China's Quest for Semiconductor Self-Sufficiency: The Impact on UK and Korean Industries', The Alan Turing Institute, Center for Emerging Technology and Security, Briefing Paper, December 2024, https://cetas.turing.ac.uk/sites/default/files/2024–12/cetas_briefing_paper_-_chinas_quest_for_semiconductor_self-sufficiency_-_the_impact_on_uk_and_korean_industries.pdf, 14–18.

[38] Insikt Group, 'Measuring the US-China AI Gap', 9, 24–25; Kyle Chan, 'Hearing on "Made in China 2025 – Who is Winning?"', Testimony before the U.S.-China Economic and Security Review Commission, 6 February, 2025, https://www.uscc.gov/sites/default/files/2025–02/Kyle_Chan_Testimony.pdf.

China's centralized economic and political systems facilitate rapid AI development. The large AI industry and various technology companies have been the main drivers of China's AI development, and the close relationship between the state and private sectors enables the PRC to transfer private-sector innovations to the government sphere to advance national security interests.[39] Strict government control of the private sector facilitates information manipulation targeted at foreign countries, as China's private sector is already a global leader in many AI-facilitated persuasion technologies.[40] The PRC can also adopt strategically ambiguous regulatory frameworks for AI, which benefits the regime's information manipulation efforts.[41] The rigid government structure and censorship regime both enable and constrain the types of data China's AI sector can harness in AI development. Its authoritarian nature and centralized structure mean that the Chinese government has access to vast datasets that can be used to train AI models for surveillance and information manipulation. The PRC has been able to leverage detailed user data collected by the CCP and Chinese companies since the introduction of the 2017 national intelligence and cybersecurity laws.[42] China's centralized system also allows flexibility in setting priorities, pursuing goals and rapid testing of AI applications in real-world settings, regardless of potential ethical and moral concerns.[43] However, although companies within the Chinese AI ecosystem can leverage large datasets and build on foreign AI innovations, their growth is likely constrained by the need to adhere to the CCP's strict censorship requirements.[44]

In 2025 Chinese company DeepSeek released its own high-performing generative AI model, DeepSeek-R1, which closed the performance gap between Chinese and American AI models and was the first Chinese-coded generative AI tool created for an international user market.[45] The DeepSeek chatbot has been described as a "disinformation machine" due to its strong propensity to repeat false information[46] and

[39] Qi Haotin, 'China's Evolving AI Development', 138.

[40] Daria Impiombato et al., 'Persuasive Technologies in China: Implications for the Future of National Security', 4.

[41] For example, China's Interim Measures for Generative AI Service Management restrict AI-generated disinformation from the perspective of content providers but allow room for the government to create and use misleading content with generative AI to target foreign countries. For more information see Liana Edgar, 'Generative AI and Disinformation: Analysing China's Strategy Amidst US Investment and Export Controls', 150, 164.

[42] Dylan Buck, 'China in the Asia-Pacific Cyber Domain'.

[43] Lance Y. Hunter et al., 'The Military Application of Artificial Intelligence Technology in the United States, China, and Russia and the Implications for Global Security', 223.

[44] Daniel Sprick, 'Aligning AI With China's Authoritarian Value System', The Diplomat, 3 February 2025, https://thediplomat.com/2025/02/aligning-ai-with-chinas-authoritarian-value-system/; Hanna Dohmen, 'Assessing China's AI Development and Forecasting Its Future Tech Priorities', Atlantic Council, Strategic Insights Memo, 18 September 2024, https://www.atlanticcouncil.org/content-series/strategic-insights-memos/assessing-chinas-ai-development-and-forecasting-its-future-tech-priorities/.

[45] Ibid., 96.

[46] Macrina Wang et al., 'Chinese Chatbot Phenom is a Disinformation Machine', NewsGuard, 30 January 2025, https://www.newsguardtech.com/special-reports/deepseek-ai-chatbot-china-russia-iran-disinformation/.

vulnerability to exploitative measures.[47] The tendency of Chinese chatbots to reflect CCP narratives underlines the CCP's strategic goal of gradually shaping the global information environment in its favour. [48] In addition to DeepSeek's model the Chinese AI ecosystem has continued to deliver other high-performing generative AI models in 2025.[49] Despite these advances, Chinese frontier AI models' performance is three to six months behind competitors in the United States.[50]

2.3 China-linked actors' use of AI tools in information manipulation targeting foreign countries

The use of AI tools has enabled pro-Chinese influence networks to target a wider spectrum of audiences. China-linked networks have used generative AI tools to translate and tailor content to better suit local audiences. Generative AI technology has not only aided in breaking language and cultural barriers but in targeting different age cohorts. Information manipulation actors linked to China have used AI tools to boost existing operational tactics, including content production, astroturfing, impersonation and manipulating algorithms.[51] AI technologies have also been used to generate and manipulate images, memes, audio, videos, deepfakes and various forms of text, ranging from social media posts and comments to keywords.[52]

The most obvious examples of China-linked actors using AI tools in information manipulation efforts are from operations targeting Taiwan, dissidents, diaspora communities and the United States with AI-generated and manipulated visual content. For example, Spamouflage, a disinformation network which has operated thousands of inauthentic accounts across platforms since 2017 under the guidance of China's Ministry of Public Security, has actively shared AI-generated news anchors as part of disinformation campaigns targeting Taiwanese officials, and memes falsely accusing a Taiwanese presidential candidate of embezzlement. Spamouflage also attempted to amplify divisive narratives by impersonating

[47] Attack success rates have also been found to be high in some Western AI models like Llama 3.1, GPT-4.0 and Gemini 1.5 Pro. Nevertheless, one of the leading American reasoning models, OpenAI's O1, has shown a much stronger ability to detect malign attacks than DeepSeek. See e.g. Paul Kassianik and Amin Karbasi, 'Evaluating Security Risk in DeepSeek and Other Frontier Reasoning Models', Cisco, 31 January 2025, https://blogs.cisco.com/security/evaluating-security-risk-in-deepseek-and-other-frontier-reasoning-models.

[48] Charlene Lin and McKenzie Sadeghi, 'Chinese AI Models Register a 60 Percent Fail Rate in NewsGuard Audit of Pro-China Claims', NewsGuard, 25 July 2025, https://www.newsguardtech.com/special-reports/chinese-ai-models-60-percent-fail-rate-pro-china-claims/.

[49] Including the MiniMax M1 open-source reasoning model, which appears to compete with global leaders like DeepSeek R1, OpenAI o3 and Gemini 2.4 Pro in efficiency and performance.

[50] Insikt Group, 'Measuring the US-China AI Gap', 1.

[51] William Marcellino et al., 'The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0: Next-Generation Chinese Astroturfing and Coping with Ubiquitous AI', 11.

[52] Ibid.; Ben Nimmo, 'AI and Covert Influence Operations: Latest Trends', OpenAI, May 2024, https://downloads.ctfassets.net/kftzwdyauwt9/5IMxzTmUclSOAcWUXbkVrK/3cfab518e6b10789ab8843bcca18b633/Threat_Intel_Report.pdf; Kenton Thibaut, 'Trends in China's US election interference illustrate its longer game', Atlantic Council, DFR Lab, 4 November 2024, https://dfrlab.org/2024/11/04/china-us-election-interference/.

American voters online with AI-generated avatars, images, fake personas and memes during the United States midterm elections in 2022 and the presidential elections in 2024.[53]

Pro-Chinese disinformation actors are increasingly using videos with AI-generated voiceovers which are disseminated through online platforms.[54] In such cases AI tools have been used to generate persuasive pro-Chinese and anti-US content, including mimicking an American accent and using an artificially generated avatar. Similar tactics were also used to create audio recordings to damage the reputation of election candidates during the Taiwanese elections in 2024.[55]

Pro-Chinese disinformation accounts are continuously sharing various forms of AI-generated, manipulated and translated[56] texts. Examples include the creation of social media comments criticizing Chinese dissidents, and long-form articles in Spanish containing anti-US narratives, which were successfully planted in mainstream media outlets in Latin America.[57] Other targets included the Paris Olympics,[58] US Senators,[59] and social media platforms, where Open AI tools were used to generate seemingly authentic engagement in English, Chinese and Urdu.[60]

By generating and manipulating vast amounts of AI spam content, pro-Chinese actors attempt to manipulate search engine results and social media platforms, with the goal of silencing critical narratives and creating an impression of widespread organic engagement. Chinese-origin

[53] For more information about Spamouflage see Microsoft Threat Intelligence, 'Same Targets, New Playbook: East Asia Threat Actors Employ Unique Methods', Microsoft, April 2024, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-East-Asia-Report.pdf and The Graphika Team, 'The #Americans: Chinese State-Linked Influence Operations Spamouflage Masquerades as U.S. Voters to Push Divisive Online Narratives Ahead of 2024 Election', Graphika report, September 2024, https://public-assets.graphika.com/reports/graphika-report-the-americans.pdf.

[54] In December 2023 a network of more than 30 pro-Chinese YouTube accounts that had succeeded in drawing more than 120 million views was uncovered and linked to a Chinese company probably directed by Chinese governmental actors. See Jacinta Keast, 'Shadow Play: A Pro-China Technology and Anti-US Influence Operation Thrives on YouTube', Australian Strategic Policy Institute (ASPI), Policy Brief Report No. 77/2023, 14 December 2023, https://www.aspi.org.au/report/shadow-play/).

[55] Microsoft Threat Intelligence, 'Same Targets, New Playbook'.

[56] Generative AI tools have reportedly been used by CCP-linked actors to translate social media content and long-form articles to Chinese, English, Japanese, Korean, Spanish and Urdu. For more information see Ben Nimmo, 'AI and Covert Influence Operations: Latest Trends'; Ben Nimmo et al., 'Disrupting Malicious Uses of Our Models: An Update February 2025', Open AI, February 2025, https://cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf.

[57] Ben Nimmo et al., 'Disrupting Malicious Uses of Our Models: An Update February 2025'.

[58] VIGINUM, 'Challenges and Opportunities of Artificial Intelligence in the Fight Against Information Manipulation', 7.

[59] Darren Linvill and Patrick Warren, 'Hub Brief: Spamouflage Targeting of US Senator Marco Rubio', Clemson University Media Forensic Hub, 14 October 2024, https://regmedia.co.uk/2024/10/21/clemson_university_spamouflage_targeting_senator_marco_rubio.pdf.

[60] Ben Nimmo et al., 'Disrupting Malicious Uses of AI: June 2025', Open AI, June 2025, https://cdn.openai.com/threat-intelligence-reports/5f73af09-a3a3–4a55–992e-069237681620/disrupting-malicious-uses-of-ai-june-2025.pdf.

actors have used AI tools to amplify favourable narratives about sensitive subjects such as the treatment of Uyghurs in Xinjiang and the Hong Kong protests.[61] Most AI-facilitated Chinese-origin operations have had a very limited impact and have garnered minimal organic engagement, though they have operated on multiple platforms in a coordinated manner.

The use of influencer networks in spreading pro-Chinese propaganda and disinformation in contested areas like the Xinjiang region and Tibet is a common tactic in Chinese information manipulation. Influencers' posting patterns and behaviour are controlled by Chinese agencies known as Multi-Channel Networks (MCN), which are directed by the CCP and strictly controlled by its censorship regime.[62] The use of influencer networks is particularly helpful in generating large volumes of seemingly organic misleading content about contested issues to manipulate AI search engine algorithms into eventually favouring pro-Chinese narratives. China-linked operations have also used AI tools for astroturfing and managing numerous inauthentic accounts to avoid bot detection systems on social media platforms.[63]

Public reporting from technology companies shows that pro-Chinese actors are using Western AI tools for operational support to research advice on debugging code, social media analysis, political and social topics, and public social media activity, for example.[64] Actors linked to China have sought advice on how to collect real-time data about dissidents and then share the data with Chinese government authorities.[65] OpenAI's reporting indicates that Chinese-origin threat actors have used the company's tools to generate internal documents with detailed instructions and feedback on how to run future information operations.[66] At the same time China's strong national AI capabilities provide China-linked actors with new avenues for monitoring, analysing and targeting individual users online, as well as more broadly reshaping the global information environment.

[61] Lance Y. Hunter et al., 'Artificial Intelligence and Information Warfare in Major Power States: How the US, China, and Russia are Using Artificial Intelligence in Their Information Warfare and Influence Operations', 252–253.

[62] Bang Xiao, 'Leaked files reveal how China is using AI to erase the history of the Tiananmen Square massacre', ABC News, 3 June 2025, https://www.abc.net.au/news/2025–06–04/beijing-ai-and-censors-erase-tiananmen-square-massacre/105370772; Ryan Fergus et al., 'Frontier Influencers: The New Face of China's Propaganda', Australian Strategic Policy Institute (ASPI), International Cyber Policy Center, Policy Brief Report No. 65/2022, https://www.aspi.org.au/report/frontier-influencers/, 36–40.

[63] Jeff Kao et al., 'How China is Using Social Media Propaganda to Whitewash the Repression of the Uyghurs', Scroll.in (June 25 2021) https://scroll.in/article/998385/how-china-isusing-social-media-propaganda-to-whitewash-the-repression-of-the-uyghurs; Lance Y. Hunter et al., 'Artificial Intelligence and Information Warfare in Major Power States: How the US, China, and Russia are Using Artificial Intelligence in Their Information Warfare and Influence Operations', 253; Andrew Greene, 'Beijing-based 'Green Cicada' AI network uncovered on social media, fears of US Election disruption', ABC News, 13 August 2024, https://www.abc.net.au/news/2024–08–13/green-cicada-beijing-ai-network-uncovered-social-media-x/104219752.

[64] Google Threat Intelligence Group, 'Adversarial Misuse of Generative AI', Google Cloud, 30 January 2025, https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai.

[65] Ben Nimmo et al., 'Disrupting Malicious Uses of Our Models: An Update February 2025'.

[66] Ben Nimmo et al., 'Disrupting Malicious Uses of AI: June 2025.'

Further cases have emerged that point to pro-Chinese influence networks also using domestic AI tools for operational support. Leaked documents from the Chinese technology company GoLaxy have revealed that China has used the company's AI technology to monitor public sentiment and create information operations targeting Taiwan and Hong Kong.[67] GoLaxy, which is tightly intertwined with the Chinese government security apparatus and military, has combined data mining with generative AI technology across social media platforms to monitor specific users' sentiments and generate customized content at scale. This technology enables GoLaxy to engage in adaptive real-time conversations with individual users online, making the technology "a highly efficient propaganda engine".[68]

• • •

The above analysis provides China-specific findings for the paper's research question: *How have China and Russia integrated AI technologies into their respective foreign information manipulation strategies, national capability development and operations?* China has prioritized the strategic value of AI technologies for more than a decade, striving to become the global leader in the AI sector. China has specifically acknowledged the role AI tools play in achieving the country's foreign information manipulation objectives such as shaping global opinion in China's favour. The country's strong AI capabilities support its strategic objectives and will enable increasingly sophisticated foreign information manipulation efforts in the future. The analysis of China-linked and AI-enabled foreign information manipulation efforts underlines that AI tools already assist in generating and manipulating various forms of content, targeting specific parts of the population and boosting operational tactics. Simultaneously, influence actors affiliated with China continue to utilize open-market AI tools and traditional methods of foreign information manipulation, showcasing that AI technologies have yet to comprehensively transform their operational tactics.

[67] Julian Barnes, 'China Turns to A.I. in Information Warfare', The New York Times, 6 August 2025, https://www.nytimes.com/2025/08/06/us/politics/china-artificial-intelligence-information-warfare.html.

[68] Brett Goldstein and Brett V. Benson, 'The Era of A.I. Propaganda Has Arrived, and America Must Act', The New York Times, 5 August 2025, https://www.nytimes.com/2025/08/05/opinion/china-ai-propaganda.html.

3 Russia

3.1 Russia's AI and information manipulation ambitions

In 2017 President Vladimir Putin declared that whichever country led in AI development would "become the ruler of the world".[69] Like China, Russia perceives itself to be in competition with the United States over narratives and technological developments, and it is motivated by a fear of falling behind its rivals. Russian state-affiliated groups view AI technologies as crucial tools in amplifying and generating large volumes of misleading content.[70]

In 2019 the Russian government announced a dedicated National Strategy for the Development of Artificial Intelligence by 2030. The strategy, which focuses on the commercial use of AI, presents plans for increasing the Russian share of the global AI market by 2024, focusing on domestic AI development and attaining global leadership in certain AI-related areas by 2030.[71] The national AI strategy is generally vague, and its implementation is largely left to businesses, as the AI sector in Russia relies heavily on state-owned companies such as Sberbank, Yandex,[72] Mail.ru Group[73] and Gazprom Neft.[74]

Information manipulation efforts, including offensive information warfare targeting foreign countries, have been central to the Kremlin's peace- and wartime activities for more than a century.[75] Russia sees superiority in the broad multidomain and multidimensional application of information warfare as an essential enabler of victory during both open conflict and notional peacetime.[76] Information operations are used alongside and occasionally in reinforcement of a wide range of other activities and measures such as intelligence operations, kinetic attacks, electronic warfare and diplomatic initiatives.[77]

The concept of information warfare in Russia is inherently connected with preserving regime security.[78] In seeking to project its influence

[69] Associated Press, 'Putin: Leader in Artificial Intelligence Will Rule World', AP News, 1 September 2017, https://apnews.com/article/bb5628f2a7424a10b3e38b07f4eb90d4?utm_source=copy&utm_medium=share.

[70] Claudia Wallner et al., 'Emerging Insights: Russia, AI and the Future of Information Warfare', the Royal United Services Institute, June 2025, https://static.rusi.org/russia-ai-and-the-future-of-disinformation-warfare.pdf, 5.

[71] Stephanie Petrella et al., 'Russia's Artificial Intelligence Strategy: The Role of State-Owned Firms', Orbis Volume 65, Issue 1, (2020): 75–100, https://doi.org/10.1016/j.orbis.2020.11.004, 83–84.

[72] Sberbank and Yandex have created some of Russia's pioneering AI initiatives, GigaChat and YandexGPT.

[73] The Mail.ru Group was rebranded as VK in 2021.

[74] Stephanie Petrella et al., 'Russia's Artificial Intelligence Strategy: The Role of State-Owned Firms', *Orbis* Volume 65, Issue 1, (2020): 75–100, https://doi.org/10.1016/j.orbis.2020.11.004, 80.

[75] Bryan Nakayama, 'Democracies and the Future of Offensive (Cyber-Enabled) Information Operations,' *Cyber Defense Review*, Volume 7, Issue 3 (2022): 49–65, https://www.jstor.org/stable/48682322; Lance Y. Hunter et al., 'Artificial Intelligence and Information Warfare in Major Power States: How the US, China, and Russia are Using Artificial Intelligence in Their Information Warfare and Influence Operations', 259.

[76] S. G. Chekinov and S. A. Bogdanov, *Прогнозирование характера и содержания войн будущего: проблемы и суждения* (Forecasting the nature and content of the wars of the future: problems and judgements), Voennaia Mysl' (Military Thought), No. 10, 2015, pp. 44–45.

[77] K. Mshvidobadze, 'The Battlefield On Your Laptop', Radio Free Europe/Radio Liberty, 21 March 2011, http://www.rferl.org/articleprintview/2345202.html.

[78] Gavin Wilde and Justin Sherman, 'No Water's Edge: Russia's Information War and Regime Security', Carnegie Endowment for International Peace, 2022, https://carnegie-production-assets.s3.amazonaws.com/static/files/No_Waters_Edge-Russias_Information_War_and_Regime_Security_11.pdf.

in its neighbourhood and the global arena since the collapse of the Soviet Union, Russia has adopted a new guiding concept called "information confrontation", which is often used interchangeably with the concept of information warfare. Information confrontation generally depicts continued conflict in the information domain, consisting of tools ranging from psychological operations and support, the use of information technologies, intelligence, and electronic warfare to weaken adversaries.[79]

Over the last decade Russia has further emphasized the importance of developing its own technological capacities while making its information manipulation efforts abroad more aggressive to confuse and distort adversaries' information environments.[80] Beyond regime survival the overarching goals of Russian information confrontation abroad are to regain Russia's dominance in the post-Soviet/imperial sphere of influence, and to erode Western democratic processes, values and societies. Russian actors' online information manipulation efforts have had varying degrees of success.[81] They are often uncoordinated and unevenly resourced, which is reflected in an emphasis on large volumes of manipulated content and active, yet often amateurish, experimentation with new tactics and tools.[82] However, the elusive and complex nature of Russian information manipulation efforts complicates the effectiveness of collective responses. For example, widespread media coverage of relatively low-impact disinformation campaigns can inadvertently overestimate and bolster the perception of Russia as an influence actor.[83] Leaked documents show that Russian disinformation actors consider Western media attention a "metric of success", which guides their choice of future tactics.[84]

The Russian government employs a vast network of state and non-state actors to spread propaganda and disinformation, making attribution to the Kremlin more

[79] For further information about Russian strategic thinking on the concept of information confrontation see e.g. Michelle Grisé et al., 'Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation', RAND Corporation, 2022, https://www.rand.org/pubs/research_reports/RRA198–8.html

[80] Ibid., 9–10.

[81] It is challenging to study the true influence of Russian information warfare targeting foreign countries due to the complex nature of disinformation. Nevertheless, indicators such as narrative repetition and opinion poll data can be used to study the impact of Kremlin disinformation. For more detailed information about studying the success and impact of Russian disinformation campaigns see Aiden Hoyle and Josef Šlerka, 'Hybrid CoE Working Paper 29: Cause for Concern: The Continuing Success and Impact of Kremlin Disinformation Campaigns', The European Centre of Excellence for Countering Hybrid Threats, March 2024, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-29-cause-for-concern-the-continuing-success-and-impact-of-kremlin-disinformation-campaigns/.

[82] Claudia Wallner et al., 'Emerging Insights: Russia, AI and the Future of Information Warfare', the Royal United Services Institute, June 2025, https://static.rusi.org/russia-ai-and-the-future-of-disinformation-warfare.pdf, 5.

[83] Lilly Bilyana, 'Russian Information Warfare: Assault on Democracies in the Cyber Wild West', (Annapolis, MD: Naval Institute Press, 2022), 153–154.

[84] James Pamment and Darejan Tsurtsumia, 'Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency', Psychological Defence Agency (MPF), MPF Report Series 8/2025, https://mpf.se/psychological-defence-agency/publications/archive/2025–05–15-beyond-operation-doppelganger-a-capability-assessment-of-the-social-design-agency, 20.

challenging. Instead of a highly coordinated network, the main actors involved in Russian information manipulation have a tense history and relationships fraught with rivalries, often resulting in overlapping and contrasting efforts.[85] Within the government Russia's military intelligence agency (General Staff Main Directorate, GRU), the Russian Foreign Intelligence Service (SVR), the Russian military's Information Operations Troops (VIO) and the Federal Security Service (FSB) play an integral role in employing information manipulation abroad.[86]

Russia outsources much of its overseas information manipulation efforts to external actors who are tasked with creating and spreading propaganda and disinformation. Some of the most effective outsourced contractors are the Internet Research Agency (also known as the troll factory) and the autonomous non-profit organization (ANO) Dialogue.[87] Among the seemingly independent actors that are in effect controlled by or aligned with the Kremlin are Russian media outlets and press agencies such as the Africa Initiative, think tanks, social media platforms, influencer networks, IT companies, PR agencies, and individual journalists and bloggers.[88]

The Social Design Agency is among the most prolific pro-Kremlin actors. It has developed the Doppelganger, Undercut and Matryoshka operations, all of which have had global reach.[89] Individual actors are also key to pro-Russian information manipulation efforts, exemplified by John Mark Dougan, an American fugitive actively involved in disinformation operations known as CopyCop and Storm-1516, which have focused on discrediting Ukraine, electoral processes and political leaders in Europe.[90]

[85] For a comprehensive analysis of the role of non-state actors in Russian hybrid warfare see Eginhards Volāns et al., 'Handbook on the Role of Non-state Actors in Russian hybrid threats', Hybrid CoE Paper 27, https://www.hybridcoe.fi/publications/handbook-on-the-role-of-non-state-actors-in-russian-hybrid-threats/.

[86] Gavin Wilde and Justin Sherman, 'No Water's Edge: Russia's Information War and Regime Security', 9.

[87] Ibid.

[88] Alya Shandra and Robert Seely, 'The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine', Royal United Services Institute (RUSI), July 2019, https://static.rusi.org/201907_op_surkov_leaks_web_final.pdf, 80; Bret Schafer et al., 'The Russian Propaganda Nesting Doll: How RT is Layered Into the Digital Information Environment', Alliance for Securing Democracy, May 2024, https://securingdemocracy.gmfus.org/wp-content/uploads/2024/05/Laundromat-Paper.pdf, 5; LSM, 'Russian Social Media Networks VKontakte, Odnoklassniki to Be Blocked in Latvia', *LSM.lv*, 12 May 2022, https://eng.lsm.lv/article/features/media-literacy/russian-social-media-networks-vkontakte-odnoklassniki-to-be-blocked-in-latvia.a456465/; U.S. Department of State, 'Alerting the World to RT's Global Covert Activities', *U.S. Department of State*, 13 September 2024, https://www.state.gov/alerting-the-world-to-rts-global-covert-activities/; VIGINUM, 'African Initiative: From Public Diplomacy to Covert Influence Operations'.

[89] Martin Laine and Anastasia Morozova, 'Leaked Files from Putin's Troll Factory: How Russia Manipulated Western Elections', *Vsquare*, September 14 2024, https://vsquare.org/leaked-files-putin-troll-factory-russia-european-elections-factory-of-fakes/.

[90] Insikt Group, 'Russia-Linked CopyCop Expands to Cover US Elections, Target Political Leaders', Recorded Future, Insikt Group, Cyber Threat Analysis Russia, 24 June 2024, https://go.recordedfuture.com/hubfs/reports/cta-ru-2024–0624.pdf; VIGINUM, 'Analysis of the Russian Information Manipulation Set Storm-1516', Premier Ministre, Secréteriat général de la défense et de la sécurité nationale, VIGINUM, Technical Report, May 2025, https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf.

3.2 Russia's national AI capabilities

Russia's development of AI technologies in the military domain dates to Soviet scientific research in the 1960s.[91] However, Russia fell well behind the United States and China in the AI sector after the collapse of the Soviet Union.[92] Financial and resource limitations (including sanctions) are among the main obstacles to Russia's AI sector.

Russia faces further challenges due to restricted access to AI talent, research, infrastructure, innovation and hardware.[93] Russia's AI sector relies on state-controlled companies, which partly explains the scant government resources allocated to AI development. Russia's private sector is affected by low economic growth, few incentives for venture funding, a risk-averse culture and political control.[94] Due to its small electronics industry, Russia is highly dependent on foreign hardware, including semiconductors, and Western sanctions further hamper access to relevant supply chains.[95]

In recent years Russia has expanded technological cooperation with China and the BRICS countries, which may help it evade future sanctions and other constraints on its AI sector.[96] Russia's international partnerships, especially its relationship with China, could be an important enabler of its future AI capabilities.

Russia's authoritarian system facilitates access to big data domestically and abroad, which is crucial for training AI models. For example, Russian government legislation requires relevant service providers, including social media platforms and telecommunications companies, to store user data for three years and allow the FSB to access them.[97] Access to big data is key for Russia's AI sector, especially given its access to Western depositories of anonymized data has been hampered since its full-scale invasion of Ukraine. Access to data depositories is central for training algorithms, as Russia is among the few countries that are currently developing their own generative AI models.[98]

[91] Sergey Sukhankin, 'Russia Capitalizes on Development of Artificial Intelligence in Its Military Strategy', The Jamestown Foundation: Eurasia Daily Monitor, 3 March 2025, https://jamestown.org/program/russia-capitalizes-on-development-of-artificial-intelligence-in-its-military-strategy/.

[92] Ibid.

[93] Tortoise Media, 'The Global AI Index: Country Profiles', Tortoise Media, 2024, https://www.tortoisemedia.com/data/global-ai#data.

[94] Stephanie Petrella et al., 'Russia's Artificial Intelligence Strategy: The Role of State-Owned Firms', 78.

[95] Ibid., 79.

[96] Reuters, 'Putin orders Russian government and top bank to develop AI cooperation with China', Reuters, 1 January 2025, https://www.reuters.com/technology/artificial-intelligence/putin-orders-russian-government-top-bank-develop-ai-cooperation-with-china-2025–01–01/; Gleb Bryanski, 'Russia teams up with BRICS to create AI alliance, Putin says', Reuters, 11 December 2024, https://www.reuters.com/technology/artificial-intelligence/russia-teams-up-with-brics-create-ai-alliance-putin-says-2024–12–11/.

[97] Alina Polyakova, 'Weapons of the Weak: Russia and AI-Driven Asymmetric Warfare', Brookings Institute, 15 November 2018, https://www.brookings.edu/research/weapons-of-theweak-russia-and-ai-driven-asymmetric-warfare/.

[98] Gleb Bryanski and Elena Fabrichanya, 'Russia Will Boost AI Clout Despite West's Sanctions, Sberbank First Deputy CEO Says',' Reuters, 12 December 2024, https://www.reuters.com/technology/artificial-intelligence/russia-will-boost-global-ai-clout-despite-western-sanctions-sberbank-first-2024–12–12/.

3.3 Russia-linked actors' use of AI tools in information manipulation targeting foreign countries

Russia-linked actors have mostly used AI tools to amplify existing tactics such as producing inauthentic content at scale and spreading content to reach broader audiences and fuel polarization. Since early 2025 Russia-linked actors have also attempted to influence the training data of the AI models available on the market, thus seeking to confuse the global information environment.

AI-generated and manipulated disinformation content has ranged from inauthentic images, audio, videos and deepfakes to various text formats such as plagiarized news articles, social media comments and posts.[99] Inauthentic images created or manipulated by generative AI tools have mostly been used by pro-Russian disinformation actors to create emotionally appealing visuals to amplify polarizing narratives about domestic issues in the target country or region. Media organizations using AI-generated content include RIA Novosti,[100] Tsargrad, Russia Today and Sputnik. In some cases AI-generated or manipulated images have been used by Russia-linked disinformation actors to mislead viewers about events. For example, they shared AI-generated images of graffiti in Paris during the 2024 Olympic Games and manipulated images depicting the conflicts in Gaza and Ukraine.[101]

Pro-Russian actors have continuously used generative AI tools to produce profile pictures for inauthentic social media profiles.[102] In 2024 it was also revealed that the Russian CopyCop disinformation network had created fake journalist personas with generative AI tools for its network of hundreds of inauthentic news websites with the goal of boosting the legitimacy of the disinformation operation.[103]

[99] See e.g. Insikt Group, '"Operation Undercut" Shows Multifaceted Nature of SDA's Influence Operations', Recorded Future, 26 November 2024, https://go.recordedfuture.com/hubfs/reports/TA-RU-2024–1126.pdf; Ben Nimmo, 'AI and Covert Influence Operations: Latest Trends'; VIGINUM, 'Analysis of the Russian Information Manipulation Set Storm-1516', Premier Ministre, Secrétariat général de la défense et de la sécurité nationale, VIGINUM, May 2025, https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf; VIGINUM, 'Challenges and Opportunities of Artificial Intelligence in the Fight Against Information Manipulation'.

[100] EUvsDisinfo, 'How Russia uses AI to dehumanise Ukrainians', EuvsDisinfo, 7 February 2025, https://euvsdisinfo.eu/how-russia-uses-ai-to-dehumanise-ukrainians/.

[101] Dan Milmo, 'Russia Targets Paris Olympics with Deepfake Tom Cruise Video', The Guardian, 3 June 2024, https://www.theguardian.com/technology/article/2024/jun/03/russia-paris-olympics-deepfake-tom-cruise-video; Rolf Fredheim, 'Virtual Manipulation Brief: Verified Propagandists and the Hamas-Israel War', NATO Strategic Communications Centre of Excellence, Virtual Manipulation Brief 2023/02, 14 December 2023; Oksana Poluliah, 'How AI-Generated Content Distorts Truth About War and Russian War Crimes: Detecting and Analyzing AI-Generated Images', StopFake.org, 11 December 2024, https://www.stopfake.org/en/how-ai-generated-content-blurs-the-truth-about-war-and-russian-war-crimes-detecting-and-analyzing-ai-generated-images/.

[102] See e.g. Ben Nimmo et al., 'Disrupting Malicious Uses of AI: June 2025'.

[103] Steven Lee Myers, 'From Russia, Elaborate Tales of Fake Journalists', The New York Times, 18 March 2024, https://www.nytimes.com/2024/03/18/business/media/russia-fake-journalists.html; Insikt Group, 'Russia-Linked CopyCop Expands to Cover US Elections, Target Political Leaders'.

Most of the imagery used by these operations was medium to low quality.

Audio, video and deepfake content generated or manipulated with AI tools is a common feature of pro-Russian disinformation operations targeting foreign countries. Pro-Russian actors have used voice cloning and generative AI tools to imitate influential political figures and erode trust in political processes, institutions and leadership.[104] AI tools have been used to transform text-based content into voiceovers, showcased by a network of more than 40 accounts that used text-to-speech software to spread pro-Kremlin narratives about the European Parliament elections and Ukraine in the spring of 2024.[105]

Pro-Russian actors have used AI-generated video and deepfake content widely to impersonate influential figures and organizations and create false "testimonies" by alleged whistleblowers.[106] The disinformation operation Matryoshka has been among the most active users of deepfake video content, including a video series of fake "experts" repeating Russian propaganda narratives about Ukraine[107] and numerous AI-generated videos which have targeted Germany and the United States by mimicking authentic news organizations.[108]

The Doppelganger, CopyCop and Matryoshka disinformation operations have been among the most active users of generative AI tools to generate and manipulate content for inauthentic news sites mimicking legitimate media organizations. These operations have used generative AI tools to translate, plagiarize and edit articles from authentic news sites and create misleading articles about divisive issues such as the war in Ukraine and the

[104] In 2023 pro-Russian accounts spread an AI-generated audio file which falsely claimed to be a call between Ukrainian president Zelensky and his wife discussing corruption and criticizing the West. In 2024 pro-Kremlin networks shared an AI-generated audio file of former United States president Obama falsely crediting the assassination attempt on President Trump to the Democratic party.

[105] Coalter Palmer and Natalie Huet, 'TiKTok Content Farms Use AI Voiceovers to Mass-Produce Political Misinformation', NewsGuard, 11 July 2024, https://www.newsguardtech.com/special-reports/tiktok-content-farms-use-ai-voiceovers-to-mass-produce-political-misinformation/.

[106] The use of deepfake videos continues to be a regular operating method for pro-Kremlin actors aiming to undermine the Ukrainian leadership, as exemplified by numerous incidents of deepfakes claiming to portray president Zelensky.

[107] The Insider, 'Fake AI Versions of World-Renowned Academics Are Spreading Claims that Ukraine Should Surrender to Russia', The Insider, 13 December 2024, https://theins.ru/en/news/277174#:~:text=The%20use%20of%20AI%20was,the%20request%20of%20The%20Insider.

[108] Institute for Strategic Dialogue, 'Coordinated Disinformation Network Uses AI, Media Impersonation to Target German Election,', Institute for Strategic Dialogue, Digital Dispatches, 13 February 2025, https://www.isdglobal.org/digital_dispatches/coordinated-disinformation-network-uses-ai-media-impersonation-to-target-german-election/; Steven Lee and Stuart A. Thompson, 'Falsehoods Fuel the Right-Wing Crusade Against U.S.A.I.D', The New York Times, 7 February 2025, https://www.nytimes.com/2025/02/07/business/usaid-conspiracy-theories-disinformation.html.

Israel-Gaza conflict.[109] Pro-Russian disinformation operations have generated social media posts and comments in various languages with the aid of generative AI tools to boost misleading content and create an impression of authentic engagement. Networks of pro-Russian bloggers are increasingly using generative AI tools to create and spread Kremlin-aligned blogposts at scale.[110]

Russian actors have sought to amplify misleading content with the aid of AI tools, including automating content production on fake news websites and coordinating large networks of inauthentic accounts on different social media platforms.[111] Much of this activity has been conducted alongside older forms of machine learning similar to Google Translate. Russia Today has used an AI-enhanced software package to spread disinformation at scale,[112] and AI models or automation tools have been used to synchronize thousands of social media posts targeting Moldova.[113]

AI tools have enabled pro-Russian disinformation operations to flood information environments with pro-Russian narratives and obfuscate the origin of misleading content through information laundering. These efforts aim to erode trust in legitimate sources of information among the public in target countries by creating widespread confusion about what is or is not factual in online spaces. Despite their significant efforts, most AI-facilitated pro-Russian disinformation campaigns have been unable to reach significant organic audiences online.

Private-sector reporting on pro-Russian influence networks indicates that actors involved in creating and spreading Russian

[109] See e.g. Insikt Group, 'Malign Influence Threats Mount Ahead of US 2024 Elections', Recorded Future, Threat Analysis, 14 August 2024, https://go.recordedfuture.com/hubfs/reports/ta-2024–0813.pdf; Insikt Group, 'Russia-Linked CopyCop Expands to Cover US Elections, Target Political Leaders'; Ben Nimmo, 'AI and Covert Influence Operations: Latest Trends', OpenAI, May 2024, https://downloads.ctfassets.net/kftzwdyauwt9/5IMxzTmUclSOAcWUXbkVrK/3cfab518e6b10789ab8843bcca18b633/Threat_Intel_Report.pdf; Ben Nimmo and Michael Flossman, 'Influence and Cyber Operations: An Update', OpenAI, 9 October 2024, https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf.

[110] Craig Langford, 'The new wave of Russian disinformation blogs', UK Defence Journal, 18 May 2025, https://ukdefencejournal.org.uk/the-new-wave-of-russian-disinformation-blogs/.

[111] U.S. Department of Justice, 'Press Release: Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm', U.S. Department of Justice, 9 July 2024, https://www.justice.gov/archives/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners?mkt_tok=NjU5LVdaWC0wNzUAAAGUQsh-v6PZk3bC3Ukn-gmL-tJ8PetQwhh3b266qjQ47gdpxbbWQ8GB5-CDDCYJz27n2dZ-a8P_7zAz3LbcZnsNdfWGJ6866P6lrtvlsH4IUcUcPw; European External Action Service, 'Memo: Known Information Interference Operations During the June 2024 Elections for the European Parliament', European External Action Service, October 2024, https://ec.europa.eu/commission/presscorner/api/files/attachment/879707/Mem.

[112] Joint Cybersecurity Advisory, 'State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity', U.S. Federal Bureau of Investigation (FBI) and Cyber National Mission Force (CNMF), 9 July 2024, https://www.ic3.gov/CSA/2024/240709.pdf.

[113] Victoria Olari, 'Telegram Network Seeks to Manipulate Moldova's Local Political Discourse', The Atlantic Council, DFRLab, 6 March 2025, https://dfrlab.org/2025/03/06/telegram-network-moldova/.

disinformation are continuously leveraging public AI models without significant concern for operational security. Russia-linked accounts have reportedly used Western generative AI tools to research general news and events, and find information about building an AI chatbot and creating tools for interacting with LLMs.[114] Overall, Russia-linked influence networks continue actively to experiment with and instrumentalize AI tools that are available on the market for both content generation and operational support.

In early 2025 reports emerged that a Russian disinformation actor known as the Pravda network[115] had infiltrated the training data of some of the most popular AI chatbots, resulting in contamination of the content.[116] Although it is difficult to prove that manipulating LLM training data is the Pravda network's official strategy, its main operating method is to generate thousands of inauthentic articles daily for its vast network of fake websites.[117] The content on the networks' websites is largely unappealing to human readers, suggesting that the network focuses on manipulating the information environment with AI spam instead of attaining organic attention online. The Pravda network's websites have been cited as sources by Wikipedia articles, X community notes and chatbots, implying that the network has successfully manipulated search engine results, flooded web crawlers and manipulated LLM training data.[118]

• • •

In conclusion, an analysis of Russian strategies, capabilities and AI-enabled foreign information manipulation efforts suggests that there is currently a gap between Russia's ambitions and national capabilities. Russia perceives a strategically significant role for AI technologies in foreign information manipulation, but severe constraints hinder it from leveraging national capabilities. Despite Russia lagging behind in the global AI race, its strategic prioritization and long-term experience in aggressive foreign information manipulation enable Russia-affiliated influence actors to effectively integrate foreign AI tools into their efforts to boost their existing operational tactics.

[114] Google Threat Intelligence Group, 'Adversarial Misuse of Generative AI'.

[115] The Pravda network operates more than 200 fake websites which target countries around the globe through mostly English language content but also minority languages like Irish and Welsh, which have a much smaller online presence and are thus more vulnerable to online manipulation attempts.

[116] McKenzie Sadeghi and Isis Blachez, 'A Well-Funded Moscow-based Global "News" Network Has Infected Western Artificial Intelligence Tools Worldwide With Russian Propaganda', NewsGuard Special Report, 6 May 2025, https://www.newsguardrealitycheck.com/p/a-well-funded-moscow-based-global?utm_source=post-email-title&publication_id=2106147&post_id=158454200&utm_campaign=email-post-title&isFreemail=true&r=4an210&triedRedirect=true&utm_medium=email; Ange Lavoipierre and Michael Workman, 'Pro-Russian influence operation targeting Australia in lead-up to election with attempt to "poison" AI chatbots', ABC News, 2 May 2025, https://www.abc.net.au/news/2025–05–03/pro-russian-push-to-poison-ai-chatbots-in-australia/105239644.

[117] Joseph Menn, 'Russia Seeds Chatbots with Lies. Any Bad Actor Could Game AI the Same Way', The Washington Post, 17 April 2025, https://www.washingtonpost.com/technology/2025/04/17/llm-poisoning-grooming-chatbots-russia/.

[118] Valentin Châtelet and Amaury Lesplingart, Russia-linked Pravda Network Cited on Wikipedia, LLMs, and X,' Atlantic Council, DFRLab, 12 March 2025, https://dfrlab.org/2025/03/12/pravda-network-wikipedia-llm-x/.

Pro-Russian AI-enabled foreign information manipulation efforts have for the most part received limited organic online engagement, yet their volume and aggressive nature have considerable potential to influence target societies. In addition to using generative AI tools available on the open market, Russia-linked influence actors continue to rely heavily on more rudimentary measures, indicating that AI tools have thus far constituted only an addition to the Russian information manipulation toolkit.

4 Conclusion

Both China and Russia are heavily focusing on and investing in AI technologies. Both are using AI in their information manipulation efforts overseas and have integrated AI technology into their strategic thinking and capability development. The rapid pace of AI development risks providing Russia and China with even more varied and sophisticated information manipulation tools in the future, some of which are discussed in the next section.

To date, AI technology has formed one part of China and Russia's information manipulation targeting foreign countries, with generative AI tools having the biggest impact. China is ahead of Russia in capability development, but this has not limited the scale and impact of Russia's foreign information manipulation. Russian activity may be cruder and easier to attribute, but it can still undermine confidence and trust within Western societies.

Both countries continue to combine AI tools with traditional information manipulation tactics, indicating the impact of these new capabilities currently remains limited. For Russia developing domestic AI models and capabilities is not a necessity for AI-facilitated information manipulation due to a strategy that emphasizes creating chaos and confusion in target countries through continuous experimentation with and expansion of their information manipulation toolkit. In contrast, Chinese-origin networks are increasingly using AI technology not just to generate and manipulate misleading content at scale but for data mining, monitoring and targeting individuals online.

Despite some similarities in their information manipulation efforts, it should not be assumed that the two countries are in practice either willing or able to cooperate in foreign influence activities. Their relationship is opportunistic, motivated by short-term considerations rather than long-term shared interests. Chinese and Russian actors currently appear only to echo each other when their distinct interests are aligned.

5 Policy implications

AI tools bring both opportunities and risks for practitioners working to counter propaganda and disinformation. Russia's and China's integration of AI technology into their information manipulation strategies, capability development and operations underlines the urgency of combining new technological solutions with conventional countermeasures to effectively safeguard democratic processes and the integrity of the global information environment.

- **Key risks for policymakers**

China is rapidly developing world-leading AI capabilities and seeking to overtake the US as the leading AI country. Over the coming months we should also expect to see increased dependence on Chinese AI infrastructure and tools. There are already indications that leading firms within the BRICS countries have begun to shift to Chinese, Russian and Emirati models instead of US ones.

Rapid developments in the AI sector could provide information manipulation actors with **more varied and sophisticated tools, including agentic AI technology.** Agentic AI could revolutionize how machines make decisions, act and learn independently.[119] Due to the enhanced autonomy, adaptability and efficiency agentic AI provides users, hybrid threat actors may use this novel technology to automate various stages of information manipulation efforts, ranging from content production to the operation of inauthentic accounts.

The increasing and more varied use of AI technology in information manipulation risks making misleading content more widespread, personalized and difficult to detect and attribute.[120] It is therefore essential for practitioners to understand the development of AI technologies and ensure that adequate countermeasures are implemented.

Both China and Russia have sought to shape **AI governance norms.** China has been especially keen to take a leadership role in AI ethics and standard setting to gain leverage in the global AI market, promote positive narratives about its domestic innovations and shape the future of AI development.[121] For Russia the focal point in AI development and governance is the BRICS framework, where it continues to spearhead novel cooperation initiatives like the AI Study Group and BRICS AI Alliance Network.[122] Increased collaboration in the AI sector has already pushed organizations in the BRICS countries to adopt Russia's Code of AI Ethics and prioritize the use of Chinese and Russian AI technology over Western competitors' models.[123]

[119] San Murugesan, 'The Rise of Agentic AI: Implications, Concerns, and the Path Forward', *IEEE Intelligent Systems*, Volume 40, Issue 2, (2025): 8–14, https://doi.org/10.1109/MIS.2025.3544940, 8–9.

[120] VIGINUM, 'Challenges and Opportunities of Artificial Intelligence in the Fight Against Information Manipulation', 14–17.

[121] Jing Cheng and Jinghan Zeng, 'Shaping AI's Future? China in Global AI Governance', *Journal of Contemporary China*, Volume 32, Issue 143: 794–810, http://dx.doi.org/10.1080/10670564.2022.2107391, 804, 808.

[122] Ivana Stradner and Emily Hester, 'Russia Aims to Ride the BRICS to AI Victory'.

[123] XVI BRICS Summit, 'Kazan Declaration: Strengthening Multilateralism for Just Global Development and Security', BRICS Russia 2024, 23 October 2024, http://static.kremlin.ru/media/events/files/en/RosOySvLzGaJtmx2wYFv0lN4NSPZploG.pdf.

China's and Russia's influence in the global governance of AI technology can tangibly influence the kind of AI systems that will be developed and how AI tools can be leveraged. Developing **comprehensive regulation and robust norms** is a key part of ensuring that governments and technology companies have sufficient safeguards in place to tackle malign use and the generation of biased, harmful or misleading content, and to protect the information ecosystem against increasing volumes of manipulation attempts more broadly.

- **Key opportunities for policymakers**

AI technology provides a wide range of methodologies for monitoring, detecting and documenting misleading information. Attribution can occur more quickly and easily from this. **AI technology is not, however, a silver bullet that can address information threats alone.** The best results of fact checking still emerge from a combination of AI tools and human judgement, and continuous human oversight and model development generally play a crucial role in the effective deployment of AI technology in countering information manipulation.[124]

A whole-of-society approach to countering information manipulation is more important than ever. Much of the expertise in the malign and positive uses of AI technology is found in private companies, so it is crucial to break down silos between the private, public and non-governmental sectors to ensure that practitioner communities have the most up-to-date information about information threats. Cross-sectoral cooperation is also key to the development and deployment of improved tools for countering information manipulation.

Information sharing and collaboration across governments are essential. Countries in the Euro-Atlantic region should be learning more from each other and from other countries (such as Taiwan) which continue to deal with large volumes of AI-generated content. Although there is no one-size-fits-all solution to countering information manipulation, a wealth of information is available to policymakers about best practice. It could be used more effectively.[125]

[124] Hamid Reza Saeidnia et al., 'Artificial Intelligence in the Battle Against Disinformation and Misinformation: A Systematic Review of Challenges and Approaches,' *Knowledge and Information Systems*, Volume 67, (2025): 3139–3158, http://dx.doi.org/10.1007/s10115–024–02337–7, 3145–3149.

[125] Robert Kupiecki et al., 'The Current State of Detection and Response to FIMI', Secure Automated Unified Framework for Exchange (SAUFEX), Research Report, 2025, https://saufex.eu/research; Jakub Kalenský and Heidi Hanhijärvi, 'Countering-Disinformation in the Euro-Atlantic: Strengths and Gaps', Hybrid CoE Research Report 15 (The European Centre of Excellence for Countering Hybrid Threats, October 2025), https://www.hybridcoe.fi/publications/countering-disinformation-in-the-euro-atlantic-strengths-and-gaps/.

Contributors

The author is enormously grateful for the help and support received during the drafting of this paper from the colleagues listed below. Their engagement, expertise and attendance at an expert workshop in September 2025 shaped this publication's content and conclusions.

- Megan Hughes, Research Associate, Centre for Emerging Technology and Security
- Alexander Babuta, Director, Centre for Emerging Technology and Security
- Daria Impiombato, Senior Analyst, Mercator Institute for China Studies (MERICS)
- Andreas Edevald, Senior Analyst, Swedish Psychological Defence Agency
- Ingrid Bicu, Research Associate, Universidad Pontificia de Salamanca

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats