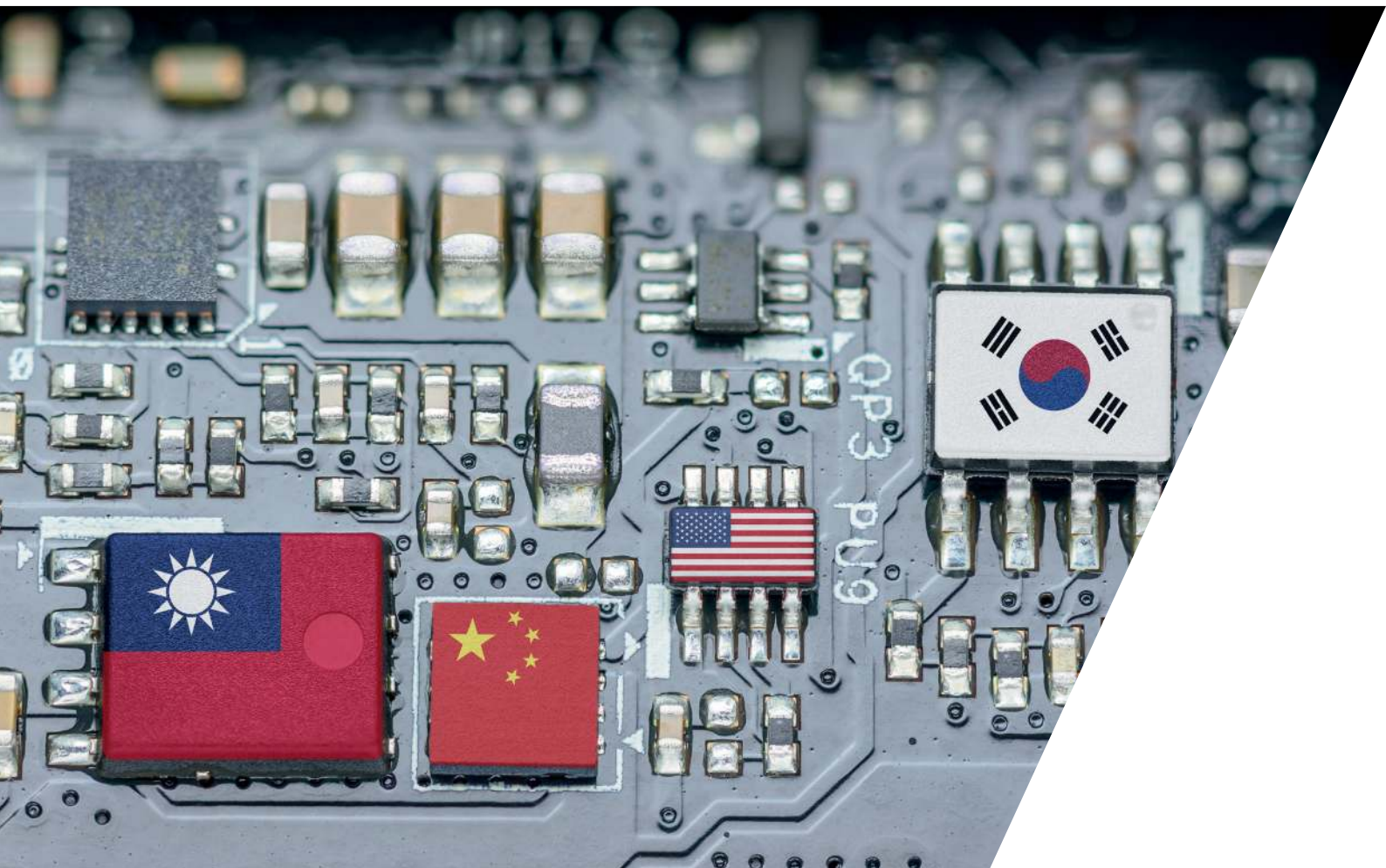


CHINA'S USE OF AI AND ITS NEGATIVE IMPACT ON THE WORLD

By M. DANE WATERS,
HUMANITY FOR FREEDOM FOUNDATION



**CENTRE FOR
INDO-PACIFIC
STUDIES**

CHINA'S USE OF AI AND ITS NEGATIVE IMPACT ON THE WORLD

By M. DANE WATERS,
HUMANITY FOR FREEDOM FOUNDATION

Published in 2025 by The Henry Jackson Society

The Henry Jackson Society
Millbank Tower
21-24 Millbank
London SW1P 4QP

Registered charity no. 1140489
Tel: +44 (0)20 7340 4520

www.henryjacksonsociety.org

© The Henry Jackson Society, 2025. All rights reserved.

Title: "CHINA'S USE OF AI AND ITS NEGATIVE IMPACT ON THE WORLD"
By M. Dane Waters, Humanity for Freedom Foundation

The views expressed in this publication are those of the author and are not necessarily indicative of those of The Henry Jackson Society or its Trustees.

Cover image: Flags of China, Taiwan, South Korea and USA highlighted on microchips on a motherboard by William Potter at Shutterstock (<https://www.shutterstock.com/image-photo/flag-republic-china-taiwan-korea-usa-2186145939>).



**CENTRE FOR
INDO-PACIFIC
STUDIES**

About Us



DEMOCRACY | FREEDOM | HUMAN RIGHTS

About The Henry Jackson Society

The **Henry Jackson Society** is a think-tank and policy-shaping force that fights for the principles and alliances which keep societies free, working across borders and party lines to combat extremism, advance democracy and real human rights, and make a stand in an increasingly uncertain world.

CENTRE FOR INDO-PACIFIC STUDIES

About the Centre for Indo-Pacific Studies

The **Centre for Indo-Pacific Studies** is a research centre within the Henry Jackson Society that aims to educate the public about the geostrategic importance of the Indo-Pacific region, and to explore structural shifts, regional complexities and historic tensions that exist alongside the economic and social growth that constitutes the “rise of Asia”. It also advocates a British role in the broader Indo-Pacific region, commensurate with Britain’s role as a custodian of the rule-based international system.

About the Author

M. Dane Waters is a political strategist, author, filmmaker and advocate for democracy. With experience spanning six continents, he has advised campaigns, governments and NGOs, worked on US presidential and international elections and played a key role in over 60 ballot campaigns. He founded the Initiative & Referendum Institute at USC and the Humanity for Freedom Foundation, dedicated to promoting freedom and aiding those affected by authoritarianism. A passionate animal welfare advocate, he also founded The Elephant Project and produced *The Linesman*, a documentary on human–elephant conflict. Throughout his career, Dane has sought the tipping points that drive meaningful change for people, democracy and the planet.

Acknowledgments

I am grateful to all those whose insights and guidance have informed the preparation of this report. In particular, I am also indebted to Professor Matt Qvortrup and Mykola Kuzmin for their assistance in the research and production of this paper.

Contents

About The Henry Jackson Society	2
About the Centre for Indo-Pacific Studies	2
About the Author	3
Acknowledgments	3
Executive Summary.....	5
Introduction	7
AI-Driven Surveillance: Eroding Privacy and Human Rights	8
AI and the Great Firewall: Censorship and Information Control.....	10
AI in Military Expansion: China's Autonomous Warfare Capabilities.....	11
AI in Economic Dominance: China's Global Market Manipulation	12
AI-Driven Supply Chains and Market Control	15
AI in Financial Markets and Cryptocurrency Regulations	17
The Weaponisation of AI in Trade Wars	19
DeepSeek AI's Manipulation of Narratives	21
China's AI Influence on International Organisations	24
AI's Role in Intelligence and Espionage	26
China's Use of AI to Advance Its Efforts to Take Taiwan.....	28
China's Use of AI to Help Russia Defeat Ukraine.....	30
Global Recommendations.....	33
UK Policy and Legislative Recommendations to Counter China's AI Expansion	35
Report Conclusion.....	38

Executive Summary

China's rapid advancements in artificial intelligence (AI) have significantly reshaped the global landscape, with profound implications for security, economic stability and democratic values. While AI holds immense potential for innovation and efficiency, under China's authoritarian use of it, AI has become a tool for mass surveillance, censorship, disinformation, military expansion and economic coercion. This report analyses how China weaponises AI to consolidate power, influence global narratives, how Chinese AI companies must comply with the CCP's orders, and how this undermines democratic institutions worldwide.

At the domestic level, China has developed the most sophisticated AI-powered surveillance state, utilising facial recognition, predictive policing, and biometric data-tracking to monitor its citizens and suppress dissent. The Great Firewall – an AI-driven censorship mechanism – controls the flow of information, shaping public perception and reinforcing the authority of the Chinese Communist Party (CCP). AI-enhanced disinformation campaigns manipulate domestic narratives and influence international media, pushing pro-Beijing messaging while suppressing dissenting views.

Beyond its borders, China's AI strategy extends into military, economic and geopolitical domains. The People's Liberation Army (PLA) is rapidly developing AI-powered autonomous warfare systems, cyberwarfare capabilities and intelligence analysis tools, making China a key player in modern conflict dynamics. Meanwhile, China has leveraged AI in the global economy for industrial automation, supply chain control and financial market manipulation, positioning itself as a dominant force in semiconductors, rare earth minerals and digital finance sectors. By integrating AI into the Belt and Road Initiative (BRI), Beijing has expanded its digital and economic influence across developing nations, embedding AI-driven infrastructure that ensures long-term dependence on Chinese technology.

A key case study within this report examines DeepSeek AI, a sophisticated Chinese AI system which is capable of manipulating narratives and influencing public opinion. DeepSeek AI is capable of controlling search engine results, generating AI-written propaganda and manipulating social media discussions, ensuring that, when Beijing so wishes, its messaging dominates the digital space. Beijing has been able to weaponise AI-driven disinformation, which has proven effective in altering public perception on issues such as Hong Kong.

China's AI ambitions also directly impact global security, particularly in the Taiwan Strait and Russia-Ukraine conflict. The report details how China employs AI to undermine Taiwan's democracy, using cyberwarfare, economic coercion, deepfake disinformation and AI-assisted military strategy to destabilise the island nation. Similarly, China has provided AI-driven intelligence sharing, cyberwarfare tools and economic assistance to Russia's war effort against Ukraine, strengthening Moscow's ability to evade sanctions and continue its aggression.

China's infiltration into international organisations through AI-driven influence further cements its ability to shape global cybersecurity, trade and governance regulations. By pushing for AI-friendly authoritarian policies in institutions such as the United Nations (UN), International Telecommunication Union (ITU) and World Economic Forum (WEF), China seeks to normalise state-led AI governance, expanding its reach over the digital and economic future of the world.

Given the profound risks posed by China's AI strategy, this report outlines a series of critical recommendations to safeguard democratic values, economic stability and international security. These recommendations emphasise the need for ethical AI frameworks, stronger cybersecurity measures, reduced reliance on Chinese AI technology, countering AI-driven

disinformation, economic defences against AI-enabled market manipulation and bolstering AI in defence and national security. Additionally, the report underscores the importance of Western nations making clear their intent to defend Taiwan militarily, reinforcing deterrence against Chinese aggression.

China's AI strategy represents one of the greatest threats to democracy, digital freedom and global stability in the modern era. The expansion of AI-driven authoritarianism, disinformation, surveillance, economic coercion and military advancements demands an urgent response from the international community. Failure to act could lead to a world where governments manipulate truth, replace privacy with surveillance and consolidate economic power through AI-driven coercion. A coordinated and proactive response is essential to ensuring AI remains a force for innovation, freedom and global security.

Introduction

China's rapid artificial intelligence (AI) advancement has raised profound global concerns. While AI promises efficiency and innovation, in the hands of an authoritarian state, it becomes a tool for surveillance, censorship, propaganda, military build-up and economic leverage. The Chinese Communist Party (CCP) has integrated AI into its governance model, enhancing state power at the expense of individual rights and open discourse.^{1, 2, 3}

This research comprehensively analyses China's use of AI and its negative global impact. It examines how AI-driven surveillance erodes privacy and human rights, how AI-powered censorship (embodied by the Great Firewall) controls information and how AI is leveraged to spread disinformation domestically and abroad. It also assesses China's pursuit of AI in military systems and the threats this poses to global security. China's bid for economic dominance through AI innovation is analysed, highlighting potential consequences for global markets and fair competition.

A detailed case study of DeepSeek AI chatbot is included, revealing the technical mechanisms by which this Chinese-developed system has been used by Beijing to manipulate responses in favour of CCP narratives. The real-world examples of its influence on global discourse and the implications of AI-driven manipulation on media credibility and freedom of speech are explored.

Additionally, this paper examines China's use of AI in its strategic efforts to take control of Taiwan as well as its AI support for Russia, particularly in disinformation campaigns and cyber collaboration.^{4, 5, 6, 7, 8, 9}

By exploring these key themes, this paper provides a persuasive yet factual argument that China's AI strategy represents a direct challenge to democracy, human rights and global security.

¹ Rollet, Charles, "Leaked Data Exposes a Chinese AI Censorship Machine", *TechCrunch*, 26 March 2025, <https://techcrunch.com/2025/03/26/leaked-data-exposes-a-chinese-ai-censorship-machine/>.

² VanderKlippe, Nathan, "Can China Use Artificial Intelligence to Perfect Central Planning?", *The Globe and Mail*, 15 June 2022, <https://www.theglobeandmail.com/world/article-can-china-use-artificial-intelligence-to-perfect-central-planning/>.

³ VanderKlippe, Nathan, "China Using AI to Censor Sensitive Topics in Online Group Chats", *The Globe and Mail*, 28 November 2016, <https://www.theglobeandmail.com/news/world/china-using-ai-to-censor-sensitive-topics-in-online-group-chats/article33116794/>.

⁴ Temple-Raston, Dina, "Taiwan Using AI to Fight Disinformation Campaigns, Former Minister Says", *The Record*, 14 February 2025, <https://therecord.media/taiwan-using-ai-to-fight-disinformation>.

⁵ Mobilio, Major Sarah, "GenAI in the 2024 Taiwan Presidential Election: Lessons for Democracies", *The Cyber Defense Review*, 19 December 2024. Available at: <https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/4012192/genai-in-the-2024-taiwan-presidential-election-lessons-for-democracies/>.

⁶ "Spamouflage", *Wikipedia: The Free Encyclopedia*, last modified 31 March 2025, <https://en.wikipedia.org/wiki/Spamouflage>.

⁷ Tucker, Patrick, "How China Could Use Generative AI to Manipulate the Globe on Taiwan", *Defense One*, 10 September 2023, <https://www.defenseone.com/technology/2023/09/how-china-could-use-generative-ai-manipulate-globe-taiwan/390147/>.

⁸ Morgan, Evan, "Eroding Global Stability: The Cybersecurity Strategies of China, Russia, North Korea, and Iran", *Irregular Warfare Initiative*, 1 August 2024, <https://irregularwarfare.org/articles/eroding-global-stability-the-cybersecurity-strategies-of-china-russia-north-korea-and-iran/>.

⁹ S. Saqib, "Sino-Russia Cyber Alliance: AI-Driven Threats to US National Security", *Sociology & Cultural Research Review* 4, no. 1 (2025), <https://srrjournal.com/index.php/14/article/view/111>.

AI-Driven Surveillance: Eroding Privacy and Human Rights

One of the most immediate and far-reaching impacts of China's AI use is in state surveillance. Over the past decade, Chinese authorities have constructed the world's most pervasive surveillance network, empowered by advanced AI technologies like facial recognition and big-data analytics. An estimated 626 million CCTV cameras have been installed in China, comprising over half of all global surveillance cameras. In major cities, such as Shanghai, the density of surveillance cameras per capita is unmatched.^{10, 11}

Chinese AI surveillance is explicitly used to monitor political dissent and control ethnic minorities. Nowhere is this more apparent than in Xinjiang, where the Muslim Uyghur population is subjected to Orwellian monitoring. Facial recognition systems specifically target Uyghurs, flagging individuals based on ethnic appearance.^{12, 13, 14}

Strong evidence uncovered by journalists and researchers shows that Chinese AI cameras and software have been calibrated to identify Uyghur faces and alert authorities to their movements. This technological tracking feeds a broader campaign of repression: ubiquitous checkpoints, biometric data collection (DNA, iris scans) and the infamous "re-education" internment camps.

Even outside Xinjiang, Chinese citizens are under the unblinking eye of AI surveillance. Public security bureaus leverage facial recognition to identify wanted suspects, jaywalkers and protesters. Traffic cameras tied to AI systems automatically issue tickets for infractions. "Smart city" systems analyse feeds, from crowd densities to individuals' clothing and behaviour.^{15, 16}

China's "Social Credit System" – often misunderstood but illustrative – demonstrates the regime's ambition to algorithmically monitor and shape citizen behaviour. This system, implemented in various pilot forms, uses vast data (from financial records to CCTV footage to online posts) to rate individuals' "trustworthiness". Those with low scores can be automatically blacklisted from transportation, financial services and even education opportunities. This data-driven authoritarianism represents an erosion of privacy and civil liberties.

The negative impact of China's AI-fuelled surveillance is not confined to its borders. China has been exporting its surveillance technology worldwide, contributing to a troubling trend of "authoritarian tech" adoption in other countries. Major Chinese companies have sold AI-powered camera systems and monitoring software to dozens of governments in Asia, Africa

¹⁰ Rollet, Charles, "Leaked Data Exposes a Chinese AI Censorship Machine", *TechCrunch*, 26 March 2025, <https://techcrunch.com/2025/03/26/leaked-data-exposes-a-chinese-ai-censorship-machine/>.

¹¹ A study by Comparitech in 2020 found that China had the highest number of surveillance cameras per capita globally, with an estimated 626 million cameras installed, heavily concentrated in major cities like Shanghai and Beijing (Paul Bischoff, "Surveillance camera statistics: which are the most surveilled cities?", Comparitech, 23 May 2023, <https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/>).

¹² Grzanna, Marcel, "Exclusive: How Shanghai Uses AI Cameras to Monitor and Track Uyghurs", *Table.Media*, 13 June 2024, <https://table.media/en/china/feature/how-shanghai-uses-facial-recognition-to-track-and-trace-uyghurs/>.

¹³ Reports from human rights organisations confirm that China's AI surveillance in Xinjiang specifically targets Uyghur Muslims using facial recognition and biometric tracking technologies ("China's Algorithms of Repression", Human Rights Watch, 1 May 2019, <https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass>).

¹⁴ Amnesty International, "EU: Surveillance Tech Sales to China and Human Rights Abusers Must Stop", Amnesty International, 21 September 2020, <https://www.amnesty.org/en/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers/>.

¹⁵ VanderKlippe, Nathan, "Can China Use Artificial Intelligence to Perfect Central Planning?", *The Globe and Mail*, 15 June 2022, <https://www.theglobeandmail.com/world/article-can-china-use-artificial-intelligence-to-perfect-central-planning/>.

¹⁶ Xu, Vicky Xiuzhong, and Bang Xiao, "Chinese Authorities Use Facial Recognition, Public Shaming to Crack Down on Jaywalking, Criminals", *ABC News*, 20 March 2018. <https://www.abc.net.au/news/2018-03-20/china-deploys-ai-cameras-to-tackle-jaywalkers-in-shenzhen/9567430>.

and Latin America. Amnesty International and other human rights groups warn that these exports "fuel widespread human rights abuses" as regimes with poor rights records gain new tools for repression.¹⁷

China's use of AI in surveillance has created a symbiosis between big data and Big Brother. The result is a dystopian reality where individual privacy is virtually non-existent and fundamental human rights are trampled by an all-seeing digital panopticon.

¹⁷ Ibid.

AI and the Great Firewall: Censorship and Information Control

Beyond surveillance, China aggressively controls the information environment using advanced technology. The Great Firewall of China is a multifaceted system with technical filters, legal regulations and human oversight to monitor and restrict the internet. The Great Firewall blocks access to thousands of foreign websites and services (including Google, Facebook and news outlets such as *The New York Times*) and filters sensitive keywords from online traffic. AI algorithms analyse internet traffic in real time to detect and filter forbidden content.^{18, 19}

AI is equally crucial in China's tightly controlled social media platforms. Companies like Tencent (WeChat) and Weibo are legally required to police the content on their platforms, relying on automated machine learning classifiers to scan and censor posts. These algorithms shape online discourse as users learn to avoid certain topics or phrases altogether, reinforcing a culture of self-censorship.

Beyond simply deleting content, China leverages AI to control *information flow and agenda-setting*. AI algorithms, guided by government directives, can be used to promote certain hashtags or stories and suppress others. Automated bot accounts (many likely AI-operated) influence conversations on Weibo, diluting critical commentary with pro-CCP messages.

Other authoritarian regimes are adopting China's AI-driven censorship model, fragmenting the global internet into national silos policed by AI. The Great Firewall serves as a template for digital repression, threatening freedom of speech and information worldwide.²⁰

¹⁸ Freedom House, "China: Freedom on the Net 2021 Country Report", *Freedom on the Net*, 21 September 2021, <https://freedomhouse.org/country/china/freedom-net/2021>.

¹⁹ "China's Great Firewall", Stanford University, 2011, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html.

²⁰ Ibid.

AI in Military Expansion: China's Autonomous Warfare Capabilities

China's military investment in AI is reshaping modern warfare and posing a direct challenge to global stability. The People's Liberation Army (PLA) has heavily invested in autonomous weapons systems, cyberwarfare and AI-powered intelligence analysis, aiming to dominate future conflicts. The integration of AI into China's military strategies presents significant threats, particularly in the realms of unmanned combat systems, strategic decision-making and hybrid warfare tactics.

AI-Powered Unmanned Combat Systems

One of the most concerning developments is China's use of AI in autonomous combat drones, underwater vehicles and robotic soldiers. The PLA is actively developing swarms of AI-driven drones that can conduct coordinated attacks, reconnaissance missions and air defence suppression.²¹ These autonomous systems reduce the need for human oversight, enabling large-scale warfare with fewer personnel.

Lethal Autonomous Weapons (LAWs)

China's development of LAWs is particularly alarming. These AI-driven weapon systems can identify, track and eliminate targets without direct human intervention. Such technology raises critical ethical and strategic concerns, as it reduces accountability in warfare and increases the likelihood of rapid, uncontrolled escalation.²²

AI in Strategic Decision-Making

China is leveraging AI to enhance military strategy and battlefield decision-making. The PLA uses AI-driven simulations and predictive analytics to model battle scenarios, identify weaknesses in enemy defences and refine operational tactics. AI-powered wargaming and strategic simulations allow China to optimise its battle plans with minimal risk.

²¹ The Center for a New American Security (CNAS) has documented China's military AI investments, including AI-driven drone swarms and autonomous battlefield decision-making systems (<https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power>).

²² A U.S. Department of Defense (DoD) report highlights that China's PLA has integrated AI into cyberwarfare, targeting critical infrastructure in rival nations (<https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/military-and-security-developments-involving-the-peoples-republic-of-china-2024.pdf>).

AI in Economic Dominance: China's Global Market Manipulation

China's strategic deployment of AI has given it unprecedented economic leverage, allowing it to outpace competitors, manipulate financial markets and weaponise trade. Through initiatives like "Made in China 2025", Beijing has aggressively pursued technological self-sufficiency to reduce dependence on Western innovation and establish dominance in key industries.

AI in Manufacturing and Industrial Automation

China leads the world in AI-driven industrial automation, integrating machine learning, robotics and predictive analytics into its factories. Companies like Huawei, Tencent and Alibaba have developed AI-powered assembly lines, significantly lowering manufacturing costs while increasing production efficiency. This AI-driven shift threatens Western manufacturing sectors, as China can mass-produce advanced products at lower prices.

Recent studies have found that China's AI-integrated factories reduced production costs by 30% while increasing efficiency by 40%, far outpacing traditional Western manufacturing methods.^{23, 24}

AI-Driven Financial Systems and Market Manipulation

China has weaponised AI to analyse financial markets, predict economic trends and influence global investments. Through algorithmic trading and AI-driven stock market manipulation, China has been able to:

- control currency exchange rates to make exports more competitive²⁵
- influence commodity prices, particularly in rare earth metals and critical raw materials²⁶
- bypass economic sanctions using AI-driven blockchain technology and alternative payment systems.

For example, China likely used AI-driven trade retaliation algorithms during the US-China trade wars to impose precise tariffs on American agricultural products, disproportionately impacting regions in the US that politically opposed Chinese trade policies and attempting to influence electoral outcomes.^{27, 28}

AI in Intellectual Property Theft and Economic Espionage

AI is critical in China's cyber espionage strategy, allowing it to steal Western nations' intellectual property (IP) and corporate secrets. State-backed hacking groups, including APT41 and Hafnium, use AI-enhanced malware to:

- automate cyberattacks on corporate networks and research institutions
- bypass security firewalls using AI-driven social engineering attacks
- analyse stolen data with AI-powered analytics to reverse-engineer Western technology.

Recent publicly available research shows that Chinese hackers targeted over 500 Western companies, stealing USD 600 billion in intellectual property annually. These AI-driven cyber intrusions accelerate China's technological advancements, reducing its domestic research and development need.^{29, 30}

AI in the Belt and Road Initiative (BRI)

China uses AI to expand its economic influence through the BRI, integrating AI-powered logistics, surveillance and financial systems into developing nations.³¹ AI-driven BRI projects allow China to:

- monitor trade routes and supply chains using AI-powered smart port technology
- influence partner nations' economies by providing AI-driven financial modelling tools
- deploy surveillance AI in developing countries to track government officials and suppress dissent.

By embedding AI into BRI infrastructure, China ensures long-term economic dependencies that limit Western influence in Asia, Africa and Latin America.

The Risks of AI-Enabled Market Manipulation

China's AI-driven economic expansion is not just about technological progress; it is a calculated geopolitical strategy designed to undermine fair competition and manipulate global markets. AI-powered predictive analytics allow China to:

- trigger supply chain disruptions to retaliate against Western policies
- exploit economic vulnerabilities in trade-dependent nations
- use AI-driven digital currency (the digital yuan) to bypass US-controlled financial systems.

Conclusion

China's strategic use of AI in its economic policies has fundamentally altered global trade, finance and industrial competition. By leveraging AI-driven automation, financial modelling and predictive analytics, China has positioned itself as a dominant force in critical industries, including semiconductors, trade logistics, manufacturing and digital finance. The nation's commitment to AI innovation is not merely about technological advancement – it is a deliberate effort to reshape global economic dependencies in its favour.

Integrating AI into economic espionage, intellectual property theft and market manipulation has allowed China to accelerate its growth at the expense of fair competition.³² AI-powered

²³ "Manufacturing's Tipping Point: Why AI is No Longer Optional", *iPangram*, accessed 1 April 2025, <https://www.ipangram.com/post/manufacturing-s-tipping-point-why-ai-is-no-longer-optional>.

²⁴ Kai Shen, Xiaoxiao Tong, Ting Wu, and Fangning Zhang, "The Next Frontier for AI in China Could Add \$600 Billion to Its Economy", *McKinsey & Company*, 7 June 2022, <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-next-frontier-for-ai-in-china-could-add-600-billion-to-its-economy>.

²⁵ Congressional Research Service, *China's Digital Currency: Electronic Chinese Yuan (e-CNY) and U.S. Economic Interests*, IF11707, updated 2 May 2023, Washington, DC: Congressional Research Service, <https://crsreports.congress.gov/product/pdf/IF/IF11707>.

²⁶ Q. Guo and Z. Mai, "How Do Seasonal, Significant Events, and Policies Affect China's REE Export Prices? Based on Deep Learning Perspective", *Resources Policy* 88 (2024): 104520. <https://www.sciencedirect.com/science/article/abs/pii/S0301420724005725>.

²⁷ "China Slaps Tariffs on U.S. Farm Products, Hitting Trump Country Hard", *CBS News*, 1 June 2019, <https://www.cbsnews.com/news/china-tariffs-us-farmers/>.

²⁸ Sung Eun Kim and Yotam Margalit, "The Political Geography of the US-China Trade War", *International Organization* 75, no. 1 (Winter 2021): 1-36, <https://sungeunkim.com/wp-content/uploads/2023/04/kim-margalit-io-2021.pdf>.

²⁹ Nicole Sganga, "Chinese Hackers Took Trillions in Intellectual Property from About 30 Multinational Companies", *CBS News*, 4 May 2022, <https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/>.

³⁰ "The U.S. Economy Is Losing as Much as \$600 Billion a Year in Intellectual Property from Chinese Espionage", *The National Interest*, 1 June 2023, <https://nationalinterest.org/blog/buzz/us-economy-losing-much-600-billion-year-intellectual-property-chinese-espionage-210956>.

³¹ Jonathan Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (London: Profile Books, 2022).

³² "House Committee Report Highlights Growing Threat of Chinese Cyber Espionage, Intellectual Property Theft", *Industrial Cyber*, 14 February 2025, <https://industrialcyber.co/critical-infrastructure/house-committee-report-highlights-growing-threat-of-chinese-cyber-espionage-intellectual-property-theft/>.

hacking, algorithmic stock trading and supply chain dominance have given Beijing significant control over key global industries, often disadvantaging Western economies. Furthermore, China's BRI, coupled with AI-driven surveillance and digital financial tools, has deepened economic ties with developing nations, reinforcing global reliance on Chinese technology and infrastructure.³³

Perhaps most concerning is China's ability to weaponise AI in economic coercion, using smart sanctions, trade restrictions and financial algorithms to pressure nations that challenge its policies. Beijing has demonstrated a willingness to manipulate international economic stability for political gain through AI-driven trade war strategies and monetary influence.

Ultimately, China's AI-fuelled economic expansion poses a significant threat to global markets, free trade and fair competition. If left unchecked, its AI-driven economic strategies will further consolidate Chinese economic supremacy, giving it unprecedented leverage over international financial systems, supply chains and geopolitical decision-making. As AI evolves, nations must establish safeguards to counteract China's market manipulation tactics, ensuring a more balanced and transparent global economic landscape.

³³ Evan Williams, "China's Digital Silk Road Taking Its Shot at the Global Stage", *East Asia Forum*, 9 May 2024, <https://eastasiaforum.org/2024/05/09/chinas-digital-silk-road-taking-its-shot-at-the-global-stage/>.

AI-Driven Supply Chains and Market Control

China's AI-powered logistics and manufacturing systems allow it to control global supply chains, granting it a strategic advantage in international trade. Companies like Alibaba, JD.com and Huawei leverage AI-powered warehouses, autonomous logistics networks and real-time predictive analytics to optimise trade efficiency while exerting significant economic leverage on dependent markets.

AI in Logistics and Trade Optimisation

Chinese e-commerce giants have fully integrated AI into logistics management, creating some of the world's most advanced supply chain infrastructures. AI-driven algorithms help companies to predict demand fluctuations, optimise shipping routes and minimise delivery delays.

For example, JD.com's AI-powered warehouse network uses robotic automation and machine learning to ensure seamless order fulfilment with minimal human intervention. Alibaba's Cainiao logistics platform employs AI to streamline global shipping, reducing delivery times and maximising cost efficiency.

With AI-powered demand forecasting, China has the ability to manipulate trade flows by adjusting supply levels based on geopolitical and economic calculations. This capability allows Beijing to restrict or expand access to crucial goods based on political objectives, using economic dependencies as leverage in global diplomacy.

AI-Enabled Control Over Critical Supply Chains

China's strategic use of AI in rare earth minerals, semiconductors and medical supply chains gives it disproportionate influence over industries that Western nations heavily rely on.

- **Rare Earth Metals:** China controls over 80% of the world's rare earth processing and has used AI to optimise extraction, refine production and regulate global supply distribution. These metals are critical for advanced technology, including military hardware, electric vehicles and consumer electronics.
- **Semiconductors:** Despite Western efforts to curb its access to cutting-edge semiconductors, China is aggressively using AI to develop domestic semiconductor capabilities. AI-powered chip design accelerates China's push for self-reliance, while its dominance in supply chain logistics ensures that it remains a key player in the global semiconductor trade.
- **Medical Supplies:** The COVID-19 pandemic highlighted China's ability to control global medical supply chains, including distributing PPE, pharmaceuticals and essential medical equipment. AI-powered tracking systems allowed China to restrict exports at critical moments, pressuring foreign governments into compliance with its geopolitical objectives.

AI in Maritime and Freight Logistics

The BRI has expanded China's control over international trade routes. AI-powered maritime and freight logistics ensure China dominates global shipping lanes and dictates trade flows.³⁴

- **Port Management:** China operates AI-enhanced smart ports across Asia, Africa and Europe, using machine learning to manage cargo movements efficiently.

³⁴ Jonathan E. Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (New York: Harper Business, 19 October 2021).

- **Maritime Tracking:** AI-driven maritime tracking allows Beijing to monitor and manipulate global shipping patterns, rerouting essential goods during trade or economic conflicts.
- **Supply Chain Dependence:** Many nations that have signed on to China's BRI projects are now dependent on AI-powered Chinese logistics networks, making them vulnerable to supply disruptions if they act against China's strategic interests.

AI's Role in Economic Coercion Utilising Supply Chain Disruptions

China is willing to use economic coercion against countries that challenge its policies. AI enables more precise targeting of industries and markets most vulnerable to supply chain disruptions.

For instance, China's restriction on rare earth exports to Japan in 2010 was an early example of supply chain weaponisation. Today, AI enhances Beijing's ability to execute similar strategies on a larger scale, monitoring trade dependencies and adjusting supply accordingly. Nations that rely on China's AI-driven logistics and supply networks may face economic retaliation if they act against Beijing's interests.

Conclusion

China's AI-driven control over supply chains gives it unprecedented leverage over global markets. China can manipulate economic dependencies and exert strategic influence over nations and industries by dominating logistics, manufacturing, rare earth metals, semiconductors and maritime trade. As AI continues to enhance predictive analytics and trade monitoring, China's ability to weaponise supply chains for political and economic gains will only increase.

AI in Financial Markets and Cryptocurrency Regulations

China has used AI to regulate financial markets and cryptocurrency transactions, effectively suppressing decentralised finance to maintain government control over capital flows.³⁵ AI-driven analytics assess and predict market trends, trade risks and economic sanctions countermeasures, allowing China to manipulate financial systems while curbing economic threats.

AI in Stock Market Surveillance and Manipulation

China employs AI-powered financial surveillance tools to monitor domestic stock markets and identify potential disruptions. AI-driven predictive analytics allow regulators to anticipate market volatility, control currency fluctuations and suppress financial crises before they escalate.³⁶

- **Stock Market Regulation:** AI analyses stock trading behaviours, detects anomalies and prevents unwanted speculation that could destabilise Chinese markets.^{37, 38}
- **Algorithmic Trading:** The Chinese Government actively regulates high-frequency AI-driven trading to ensure that state-backed institutions retain a competitive advantage over private traders.
- **Market Influence on a Global Scale:** AI also allows China to influence foreign financial markets by strategically timing investments, divestments and trade restrictions to benefit Chinese state-owned enterprises.³⁹

AI and Cryptocurrency Suppression

China has cracked down on cryptocurrency transactions, using AI to enforce bans on decentralised finance while simultaneously developing a state-controlled digital currency. AI tools monitor blockchain networks, track illicit transactions and identify users engaged in crypto-related activities.⁴⁰

- **Cryptocurrency Transaction Monitoring:** AI detects blockchain transactions that circumvent China's financial restrictions, allowing authorities to shut down mining operations and penalise crypto traders.
- **The Digital Yuan:** China has introduced the digital yuan, an AI-backed central bank digital currency (CBDC), which allows the Government to fully control financial transactions while phasing out anonymous cash exchanges.

³⁵ Francis Shin, "What's Behind China's Cryptocurrency Ban?", *World Economic Forum*, 31 January 2022, <https://www.weforum.org/stories/2022/01/what-s-behind-china-s-cryptocurrency-ban/>.

³⁶ S. Maheshwari and N. N. Chatnani, "Applications of Artificial Intelligence and Machine Learning-Based Supervisory Technology in Financial Market Surveillance: A Review of Literature", *FII Business Review*, 2023. <https://journals.sagepub.com/doi/abs/10.1177/23197145231189990>.

³⁷ K. Chen, X. Li, B. Xu, J. Yan, and H. Wang, "Intelligent Agents for Adaptive Security Market Surveillance", *Enterprise Information Systems*, 2017, <https://www.tandfonline.com/doi/abs/10.1080/17517575.2015.1075593>.

³⁸ A. M. Rahmani, B. Rezazadeh, and M. Haghparast, "Applications of Artificial Intelligence in the Economy, Including Applications in Stock Trading, Market Analysis, and Risk Management", *IEEE Access* 11 (2023): 78412-78429, <https://ieeexplore.ieee.org/document/10197415>.

³⁹ J. Shields, "Smart Machines and Smarter Policy: Foreign Investment Regulation, National Security, and Technology Transfer in the Age of Artificial Intelligence", *UIC Law Review* 51, no. 2 (2018): 369-402, <https://repository.law.uic.edu/cgi/viewcontent.cgi?article=2752&context=lawreview>.

⁴⁰ Francis Shin, "What's Behind China's Cryptocurrency Ban?", *World Economic Forum*, 31 January 2022, <https://www.weforum.org/stories/2022/01/what-s-behind-china-s-cryptocurrency-ban/>.

- **Surveillance of Cross-Border Transactions:** AI-driven big data analytics track offshore financial flows, ensuring Chinese citizens and corporations comply with Government-imposed currency restrictions.⁴¹

AI in Economic Sanctions Countermeasures

As Western nations impose sanctions on China and its allies, AI-driven financial modelling helps China predict, mitigate and counteract economic penalties.

- **Sanctions Avoidance Strategies:** AI assesses economic vulnerabilities in sanctioned regions and helps China redirect trade routes, establish alternative payment systems and create financial workarounds.
- **AI in International Trade Agreements:** China uses AI to negotiate trade agreements that minimise the impact of Western financial restrictions, strengthening its global economic foothold.
- **Currency Manipulation:** AI enables China to adjust monetary policies in response to sanctions, stabilising the yuan and protecting national economic interests.

Conclusion

China's use of AI in financial market regulation, cryptocurrency suppression and economic countermeasures ensures that the Government retains full control over capital flows while limiting financial independence. Through AI-powered economic surveillance, China dictates the future of digital finance, ensuring that centralised financial systems remain in place to benefit state control.

⁴¹ Can Zhao, *Foreign Assets for Chinese Control: Capital Filtration, New Triple Alliance, and the Global Political Economy of China's Information Industry (1995-2020)* (PhD diss., University of Victoria, 2022), 178-212, https://dspace.library.uvic.ca/bitstream/handle/1828/14083/Zhao_Can_PhD_2022.pdf.

The Weaponisation of AI in Trade Wars

AI-enhanced economic modelling allows China to strategically manipulate trade agreements, tariffs and international supply chains to coerce dependent economies into compliance with its policies. AI-powered "smart sanctions" allow China to selectively target foreign businesses and investors, ensuring maximum economic leverage while minimising domestic repercussions.

AI in Trade Agreement Manipulation

China uses AI-driven predictive analytics to assess trade patterns and anticipate the economic vulnerabilities of partner nations. This enables China to:

- influence international trade negotiations by adjusting tariff policies, subsidies and import/export restrictions to favour Beijing's long-term economic goals
- exploit economic dependencies by identifying industries in foreign countries heavily reliant on Chinese supply chains
- leverage AI-driven currency modelling to adjust monetary policies in response to shifts in global trade agreements, giving China an unfair advantage in economic diplomacy.

AI in Tariff Optimisation and Retaliatory Sanctions

AI is critical in China's ability to strategically impose and lift tariffs to punish adversaries or reward compliant nations. By analysing trade data, China can:

- determine which foreign industries are most vulnerable to tariff changes and selectively target them
- use AI to model retaliatory tariff responses when nations impose sanctions or economic restrictions on China
- enhance domestic industry resilience by adjusting subsidies and incentives based on AI-driven trade forecasts.

AI-Driven Smart Sanctions and Corporate Targeting⁴²

China has developed AI-powered "smart sanctions" that selectively target foreign businesses, investors and economic sectors without damaging its own economy. AI enables China to:

- track and analyse foreign investment flows, allowing it to punish corporations or investors that engage in activities Beijing deems unfavourable
- leverage AI-driven social media sentiment analysis to predict public and investor reactions to economic policies, adjusting responses accordingly
- blacklist companies through AI-enhanced compliance monitoring, ensuring that multinational corporations operating in China align with CCP policies.

For example, in response to Western sanctions against Chinese technology firms like Huawei, Beijing used AI-driven economic analytics to restrict sales, increase regulatory scrutiny and pressure foreign firms that complied with US sanctions.⁴³

⁴² B. Koch, *Sanctions, Trade Wars, and Economic Warfare: A Psychological and Legal Perspective on Global Economic Fragmentation*, 2024. <https://www.researchgate.net/publication/389901823>.

⁴³ Z. Zhang, "Cutting the Tail Off to Survive: China's Tech Companies' Business Strategy under US Economic Sanctions", *China Report* (2025), <https://journals.sagepub.com/doi/abs/10.1177/00094455251323734>.

AI in Global Supply Chain Disruptions

By controlling AI-enhanced global supply chains, China can manipulate market stability and use trade disruptions as economic coercion. China employs AI-driven logistics systems to:

- disrupt the supply of rare earth metals to nations that oppose its geopolitical interests
- slow down or accelerate export processes to pressure trade partners into adopting policies favourable to China
- redirect global shipping routes using AI-driven maritime and freight logistics, ensuring economic dependency on China's infrastructure.

Conclusion

China's weaponisation of AI in trade wars reshapes the balance of economic power, allowing it to precisely coerce, punish and manipulate global markets. By using AI-driven trade modelling, tariff optimisation, smart sanctions and supply chain disruptions, China strengthens its ability to undermine international trade norms while consolidating economic dominance.

DeepSeek AI's Manipulation of Narratives

DeepSeek AI is one of China's most powerful tools for manipulating online discourse, controlling information flows and shaping public opinion favouring the CCP.

DeepSeek AI integrates natural language processing, sentiment analysis and machine learning algorithms to craft, amplify and enforce pro-China narratives while suppressing dissenting viewpoints.^{44, 45}

The genesis of DeepSeek AI can be traced to earlier iterations of China's information operations architecture, forged during two pivotal crises: the 2019–2020 Hong Kong protests and the early stages of the COVID-19 pandemic. Although DeepSeek itself was not yet operational at the time, these events were critical in shaping the strategic, technical, and ideological foundations of its eventual development.

During the Hong Kong protests, Beijing deployed a combination of bot networks, state-aligned influencers, and coordinated messaging campaigns across platforms such as Twitter, Facebook, and YouTube to delegitimize pro-democracy activism. Protesters were portrayed as violent extremists, yet the methods employed were often unsophisticated and easily flagged, revealing the limits of China's then-existing disinformation tools and the need for more adaptive, language-intelligent systems.

The onset of the COVID-19 pandemic magnified these limitations. In its effort to deflect responsibility for the virus's origins, amplify praise for its pandemic response, and undermine Western governance models, China launched a sprawling, multilingual propaganda campaign. The scale, speed, and global reach required to execute such efforts highlighted the necessity for automated narrative control, real-time sentiment analysis, and AI-driven content generation.

Released in 2023, DeepSeek AI is a direct outgrowth of these strategic pressures. Informed by the lessons of Hong Kong and COVID-19, it represents a new phase in China's global information operations – capable of subtle, multilingual influence, automated response generation, and proactive narrative engineering. DeepSeek marks a shift from reactive censorship to intelligent propaganda, where AI enables China to not only suppress dissent but shape global discourse in alignment with state objectives.⁴⁶

How DeepSeek AI Controls Information

DeepSeek AI is designed to filter, adjust and redirect discussions across Chinese and international digital platforms. It operates through:

- **AI-Powered Censorship:** The system automatically detects and suppresses politically sensitive topics, such as criticism of the CCP, dialogues about human rights abuses or discussions about Taiwan, Tibet and Hong Kong democracy movements.^{47, 48}

⁴⁴ "AI startup DeepSeek facing hack, blocks questions about CCP", *Fox Business*, accessed 29 March 2025, <https://www.foxbusiness.com/technology/ai-startup-deepseek-facing-hack-blocks-questions-about-ccp>.

⁴⁵ Hao, Yaqiu, "Why DeepSeek Is So Dangerous", *Journal of Democracy* (Online Exclusive), 23 February 2025, <https://www.journalofdemocracy.org/online-exclusive/why-deepseek-is-so-dangerous/>.

⁴⁶ Ibid.

⁴⁷ Chang, LYC, "Taiwan: A Battlefield for Cyberwar and Disinformation", *Melbourne Asia Review*, 2024, <https://melbourneasiareview.edu.au/taiwan-a-battlefield-for-cyberwar-and-disinformation/>.

⁴⁸ Hung, Chia-Lin, Wu-Chi Fu, and Chun-Chi Liu, "AI Disinformation Attacks and Taiwan's Responses During the 2024 Presidential Election", Thomson Foundation, 2024, https://thomsonfoundationwebsite.azurewebsites.net/media/268943/ai_disinformation_attacks_taiwan.pdf.

- **Algorithmic Bias:** DeepSeek AI subtly rewrites responses to align with Government narratives. Even when asked neutral questions, the AI prioritises responses that downplay Government failings or emphasise China's achievements.⁴⁹
- **Influence on Search Engines:** Chinese state-controlled platforms use DeepSeek AI to manipulate search results, prioritising pro-Beijing content while burying dissenting perspectives.⁵⁰

DeepSeek AI in Global Propaganda

Beyond domestic censorship, DeepSeek AI plays a crucial role in China's international disinformation campaigns. It has been deployed by Beijing to:⁵¹

- spread pro-CCP content on global social media platforms like X, Facebook and YouTube
- generate AI-written articles that promote China's policies while discrediting democratic institutions
- amplify bot networks that push coordinated narratives in multiple languages, ensuring a wider global reach
- counteract Western media criticism by flooding online spaces with Government-aligned viewpoints, drowning out independent journalism.

Psychological Manipulation Through AI-Generated Content

DeepSeek AI doesn't just censor or suppressively manipulate narratives by generating organic and credible propaganda; it also facilitates the rapid dissemination of disinformation through automated amplification, targets specific demographics with tailored messaging, and potentially undermines the integrity of online discourse by blurring the lines between authentic and artificial content.⁵² This includes:

- AI-generated "news reports" that imitate legitimate journalism but are actually tailored to advance state propaganda
- deepfake videos of Western politicians or journalists supposedly praising China's governance while criticising their own countries
- manipulated sentiment analysis that ensures positive content about the CCP trends more frequently than negative reports.

The Risks of AI-Driven Disinformation

The increasing sophistication of AI-powered manipulation tools like DeepSeek AI seriously threatens global democracy and free speech. By influencing public opinion, elections and geopolitical narratives, China can:

- destabilise democratic institutions by injecting false information into political discourse
- undermine Western credibility by spreading AI-generated propaganda that erodes trust in independent journalism

⁴⁹ Hao, Yaqiu, "Why DeepSeek Is So Dangerous", *Journal of Democracy* (Online Exclusive).

⁵⁰ "Deeply Troubling DeepSeek AI", *IJ-Reportika*, February 2025, <https://ij-reportika.com/deeply-troubling-deepseek-ai/>.

⁵¹ Ibid.

⁵² Ibid.

- silence critics worldwide through AI-powered surveillance and automated harassment of dissidents online.

Conclusion

DeepSeek AI represents a new frontier in state-controlled information warfare. Its ability to censor, manipulate and amplify narratives allows the CCP to shape global discourse, suppress opposition and expand its ideological influence. As AI technology advances, DeepSeek AI will only become more sophisticated, making it increasingly difficult for societies to distinguish between authentic discourse and state-engineered propaganda.

China's AI Influence on International Organisations

China has strategically leveraged AI to expand its influence in international organisations, ensuring that global regulations, standards and policies align with its authoritarian governance model. Through the UN, the International Telecommunication Union (ITU), the World Economic Forum (WEF) and other key global institutions, China is actively shaping the future of AI governance, digital security and internet control in ways that benefit its geopolitical ambitions.

AI in Global Standard-Setting Organisations⁵³

One of China's primary strategies for AI dominance is to dictate international AI standards. Through its leadership positions in organisations such as the ITU and the International Organization for Standardization, China is pushing AI policies that:

- promote state-controlled AI governance models that emphasise central authority over data access, privacy and freedom of expression.
- normalise AI-driven surveillance technologies as legitimate governance tools, making it easier for authoritarian regimes to justify mass monitoring of citizens.
- weaken Western dominance in AI regulatory frameworks, ensuring that Chinese AI companies, like Huawei and Alibaba, benefit from global AI infrastructure investments.

China's AI Agenda at the United Nations

China has used AI to influence UN agencies, particularly in digital security, economic development and human rights sectors. Through its influence in UN initiatives, China has:

- advanced AI-driven "Smart City" programs that include mass surveillance, facial recognition and biometric data tracking under the guise of urban development
- blocked or watered-down AI-related human rights resolutions that focus on privacy, censorship and AI misuse
- promoted AI as a tool for economic development while downplaying concerns about its role in political repression.

In agencies like UNESCO and the UN Human Rights Council, China has advocated for "AI ethics" frameworks that exclude discussions on AI-powered censorship, state-led disinformation and algorithmic political suppression.⁵⁴

AI's Role in China's Digital Silk Road Diplomacy

Through the BRI, China exports its AI-driven governance models to developing nations, particularly in Asia, Africa and Latin America.⁵⁵ By offering AI-powered infrastructure investments, China is:

- embedding Chinese AI standards in global markets, making partner nations dependent on Chinese technology and regulatory frameworks

⁵³ Seaman, John, "AI and Technical Standardization: China's Strategic Move", *Reconnect China Policy Brief*, no.16, Ghent University, October 2024, https://www.reconnect-china.ugent.be/wp-content/uploads/2024/10/Reconnect-China-Policy-Brief-16_AI-and-Technical-Standardization.pdf.

⁵⁴ Garrido Rebolledo, Verónica, "Impact of the Artificial Intelligence on International Relations: Towards a Global Algorithms Governance", *Revista UNISCI*, no.67 (2025): 21-41, <https://www.unisci.es/wp-content/uploads/2025/01/UNISCIDP67-1GARRIDO.pdf>.

⁵⁵ Hillman, Jonathan E, *The Digital Silk Road: China's Quest to Wire the World and Win the Future*, New Haven, CT: Yale University Press, 2021.

- providing AI-driven surveillance and cybersecurity tools to governments that align with China's digital authoritarianism, ensuring compliance with Beijing's political and economic goals
- expanding AI-powered financial and trade networks that bypass Western oversight, creating an alternative digital economy under Chinese influence.

AI and Influence Over Global Cybersecurity Policies

China is actively shaping global cybersecurity standards through AI-driven regulatory proposals that:

- redefine digital sovereignty to justify state control over internet access, data sharing and AI-based censorship
- encourage AI-driven censorship frameworks that align with China's Great Firewall, allowing governments to monitor and suppress online activity⁵⁶
- weaken cybersecurity laws that expose China's AI espionage activities, ensuring its cyber operations face minimal global resistance.

AI's Role in Weakening Western AI Coalitions⁵⁷

China's influence in global AI governance is also aimed at splintering Western AI coalitions. Beijing has:

- undermined US-led AI alliances by promoting its own AI partnerships with developing nations and non-aligned states
- blocked AI-related sanctions and export controls at international forums to prevent restrictions on China's AI technology
- used AI-driven diplomatic strategies to counteract Western narratives on AI ethics, privacy rights and free speech.

Conclusion

China's AI influence in international organisations is a calculated effort to reshape global AI governance in its favour. China ensures that authoritarian AI models become internationally accepted by leveraging AI-driven diplomacy, digital infrastructure investments and cybersecurity policymaking. As AI technology advances, Beijing's strategic positioning within global institutions will deepen its control over the future of AI regulation and digital governance worldwide.

⁵⁶ Mozur, Paul, "Inside China's Great Firewall", *The New York Times*, 8 May 2018, <https://www.nytimes.com/2018/05/08/technology/china-surveillance-technology.html>.

⁵⁷ Mariani, Bernardo, "China's Global Security Vision in a Changing World", *PeaceRep Report*, April 2024, <https://peacerep.org/wp-content/uploads/2024/04/Chinas-Global-Security-Vision-in-a-Changing-World-DIGITAL.pdf>.

AI's Role in Intelligence and Espionage

China has leveraged AI to revolutionise its intelligence-gathering and espionage operations, making them more sophisticated, efficient and difficult to detect. AI is used extensively in cyber espionage, intelligence analysis, deepfake deception and global surveillance to advance China's geopolitical and military objectives.⁵⁸

AI in Cyber Espionage⁵⁹

China's state-backed hacking groups, such as APT41, Hafnium and APT10, use AI-enhanced tools to conduct large-scale cyber intrusions against governments, corporations and research institutions worldwide. AI plays a critical role in:

- **Automated Cyberattacks:** AI-driven malware can autonomously identify and exploit vulnerabilities in foreign networks, reducing the need for human hackers.
- **AI-Powered Social Engineering:** China employs machine learning to analyse social media and business networks, identifying targets for phishing campaigns.
- **Automated Data Harvesting:** AI enables China to process and analyse vast amounts of stolen data, including biometric information, government records and intellectual property.

In 2020, China-linked hackers breached US Government agencies, stealing sensitive information using AI-enhanced attack methods. Similarly, AI-driven cyber intrusions have been used to steal COVID-19 vaccine research, defence technologies and classified communications.⁶⁰

AI in Intelligence Analysis and Targeting

China's intelligence agencies utilise AI to sift through massive datasets, identify strategic intelligence and predict geopolitical trends. AI-driven intelligence gathering enhances:

- **Behavioural Analysis:** AI assesses patterns in foreign military movements, economic shifts and political discourse to predict future actions.
- **Facial Recognition Surveillance:** AI-powered surveillance networks identify and track high-profile foreign individuals, journalists, dissidents and intelligence operatives.⁶¹
- **Interception of Encrypted Communications:** AI's ability to break encryption algorithms and analyse intercepted data is a growing concern for Western intelligence agencies.

China's AI-driven intelligence framework allows it to identify weaknesses in adversary defences, track opposition figures and precisely plan covert operations.⁶²

⁵⁸ Hunter, Lance Y., C.D. Albert, J. Rutland, and K. Topping, "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", *Defense & Security Analysis*, 2024, <https://www.tandfonline.com/doi/abs/10.1080/14751798.2024.2321736>.

⁵⁹ Obioha, O. Val, O.O. Olaniyi, and M.O. Gbadebo, "Cyber Espionage in the Age of Artificial Intelligence: A Comparative Study of State-Sponsored Campaigns", *SSRN* (2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5107605.

⁶⁰ Nakashima, Ellen, and Joseph Marks, "U.S. and Allies Blame China for Microsoft Exchange Hack", *The Washington Post*, 19 July 2021. https://www.washingtonpost.com/national-security/microsoft-hack-china-biden-nato/2021/07/19/a90ac7b4-e827-11eb-84a2-d93bc0b50294_story.html.

⁶¹ Mozur, Paul, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras", *The New York Times*, 8 July 2018, <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>.

⁶² Kania, Elsa B, "AI Weapons' in China's Military Innovation", *Brookings Institution*, April 2020, https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania_v2.pdf.

Deepfake Technology and Disinformation Warfare

China has weaponised AI-powered deepfake technology to create convincing fake videos, audio recordings and social media personas for disinformation campaigns. AI-generated content is used to:

- **Impersonate Political Leaders and Influencers:** Deepfake videos and AI-synthesised voices are deployed to spread false statements attributed to foreign officials.
- **Manipulate Public Opinion:** AI-driven fake accounts and bot networks amplify state-sponsored propaganda while discrediting real opposition voices.
- **Create Fabricated Evidence:** AI-generated fake documents, reports and news articles are used to influence public perception and justify government policies.

During the Hong Kong protests, AI-driven deepfakes were circulated to smear pro-democracy activists, portraying them as violent criminals. Similar tactics were used during Taiwan's elections and are being used during the Russia-Ukraine war.⁶³

AI-Enabled Mass Surveillance and Foreign Intelligence Operations

China's AI-powered mass surveillance extends beyond its borders, with intelligence operations targeting foreign universities, businesses and research institutions. AI-enhanced espionage tools allow China to:⁶⁴

- track foreign nationals in real-time using AI-enabled security cameras embedded in cities worldwide
- monitor and influence Chinese diaspora communities by identifying and pressuring activists, academics and opposition figures
- conduct espionage through AI-powered business partnerships, where joint ventures serve as cover for technology theft and intelligence gathering.

Conclusion

China's use of AI in cyber espionage, intelligence gathering, deepfake propaganda and global surveillance has created a new paradigm in intelligence warfare. By harnessing AI for covert operations, cyber intrusions and psychological warfare, China continues to expand its influence and disrupt geopolitical stability. As AI technology evolves, China's intelligence and espionage capabilities will become even more advanced and difficult to counter.⁶⁵

⁶³ Michałkiewicz-Kądziela, E, "The Impact of Deepfakes on Elections and Methods of Combating Disinformation in the Virtual World", *Teka Komisji Prawniczej PAN*, 2024, <https://bibliotekanauki.pl/articles/55796001.pdf>.

⁶⁴ Mozur, Paul, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras", *The New York Times*, 8 July 2018, <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>.

⁶⁵ Moy, William R., and Katarzyna T. Gradon, "Artificial Intelligence in Hybrid and Information Warfare: A Double-Edged Sword", in *Artificial Intelligence and International Conflict in the 21st Century*, edited by Joachim A. Koops, 55-76, London: Routledge, 2023, <https://library.oapen.org/bitstream/handle/20.500.12657/62917/1/9781000895896.pdf#page=62>.

China's Use of AI to Advance Its Efforts to Take Taiwan

China has integrated AI into its broader strategy to assert control over Taiwan, using AI-driven cyberwarfare, disinformation campaigns, military planning and economic coercion. AI enables China to undermine Taiwan's democracy, weaken public trust and prepare for a potential military invasion with precision and efficiency.⁶⁶

AI-Powered Cyberwarfare Against Taiwan

China's state-sponsored cyber units use AI-enhanced tools to infiltrate Taiwanese Government networks, critical infrastructure and defence systems. AI plays a crucial role in:

- **Automated Cyberattacks:** AI-driven malware can autonomously detect and exploit vulnerabilities in Taiwan's systems, disrupting operations at key institutions.
- **AI-Powered Network Intrusions:** China's hackers use machine learning algorithms to bypass cybersecurity defences and extract sensitive intelligence.
- **Cyber Sabotage:** AI targets Taiwan's electrical grid, banking systems and communication networks, causing disruption in critical sectors.

China has intensified cyberattacks on Taiwan's election systems, military databases and corporate institutions to undermine stability and gain strategic advantages.⁶⁷

AI-Driven Disinformation and Psychological Warfare

China's AI-driven disinformation campaigns aim to divide Taiwanese society, influence elections and erode public confidence in Taiwan's leadership. Beijing deploys AI-powered bots, deepfake videos and fake social media accounts to:

- **Spread False Narratives:** AI-generated fake news and deepfake videos are used to portray Taiwan's Government as weak, corrupt or incapable of defending the nation.⁶⁸
- **Influence Elections:** AI-driven sentiment analysis helps China identify political divides in Taiwan and amplify internal discord, targeting key voter groups with tailored propaganda.
- **Promote Pro-China Sentiment:** AI-powered recommendation algorithms push pro-Beijing content on social media, normalising the idea of unification with China.

China's AI-generated content is carefully designed to undermine Taiwan's national identity and weaken resistance to CCP control.

AI in Military Planning and Strategic Operations

The PLA has incorporated AI into war-gaming, troop movements and invasion planning for a potential takeover of Taiwan. AI enhances military operations by:

- **Predicting Taiwan's Defence Strategies:** AI simulations analyse Taiwan's military response capabilities and predict how forces might react under different scenarios.⁶⁹

⁶⁶ Tucker, Patrick, "How China Could Use Generative AI to Manipulate the Globe on Taiwan", *Defense One*, 10 September 2023, <https://www.defenseone.com/technology/2023/09/how-china-could-use-generative-ai-manipulate-globe-taiwan/390147/>.

⁶⁷ Insisa, Antonino, "Taiwan 2023 and the 2024 Elections: A DPP Partial Victory After a Contested Electoral Campaign", *Asia Major*, vol. XXXIV (2023): 173-190, <https://www.asiamajor.org/files/AM2023-volume.pdf#page=181>.

⁶⁸ Ibid.

⁶⁹ Rieff, J., Chsij Lin, D.S. Barnett, and M. Bohnert, "Harnessing the Power of Private Sector Innovation to Defeat a Chinese Invasion of Taiwan", *RAND Corporation*, 2024, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2900/RRA2930-1/RAND_RRA2930-1.pdf.

- **Optimising Battlefield Decisions:** AI-powered decision-making tools assist PLA commanders in choosing optimal attack strategies in real time.
- **Enhancing Drone and Autonomous Warfare:** China has developed AI-driven autonomous combat drones, naval systems and robotic warfare units that could be used in an invasion scenario.

AI-Enabled Economic Coercion and Trade Manipulation

China uses AI-driven economic modelling to pressure Taiwan economically, targeting key industries to force compliance. AI-powered economic warfare includes:⁷⁰

- **AI-Driven Supply Chain Disruptions:** China can restrict trade, delay shipments or withhold critical supplies needed by Taiwanese industries.
- **Financial Market Manipulation:** AI-powered stock market strategies allow China to destabilise Taiwan's financial sector by triggering fluctuations in investment patterns.
- **AI-Optimised Sanctions:** AI determines the most effective economic pressure points to punish pro-independence figures and businesses.

AI in Maritime Surveillance and Naval Blockades

China uses AI-driven maritime surveillance systems to track Taiwanese military movements, monitor US naval activity and enforce territorial claims in the Taiwan Strait. AI enhances:⁷¹

- **Satellite Surveillance:** AI-powered satellites provide real-time intelligence on Taiwan's military bases and fleet movements.
- **Automated Naval Monitoring:** AI-driven sea drones and smart sensor networks track foreign vessels near Taiwan's waters, ensuring China's dominance in maritime disputes.
- **Simulated Blockade Strategies:** AI-driven logistics models help China plan naval blockades to isolate Taiwan from international support.⁷²

Conclusion

China's use of AI in its efforts to subdue and ultimately take over Taiwan is a highly coordinated, multi-pronged strategy that spans cyberwarfare, military simulations, economic coercion and AI-powered disinformation. By leveraging AI-driven tools, China is actively working to weaken Taiwan's democratic institutions, destabilise its economy and prepare for a potential military confrontation. As AI technology advances, Taiwan and its allies must develop countermeasures to combat AI-driven Chinese aggression and protect democratic sovereignty.

⁷⁰ Singh, S, "In What Ways Does the Rise of China's Emerging Cognitive Warfare Capabilities Pose a Threat to South-East Asia?", *King's College London*, 2024, <https://core.ac.uk/download/pdf/618458559.pdf>.

⁷¹ Rosenbach, Eric, Ellie Lee, and Brian Russell, "The Autonomous Arsenal in Defense of Taiwan. Belfer Center for Science and International Affairs", *Harvard Kennedy School*, February 2025, https://www.belfercenter.org/sites/default/files/2025-02/DETS_The%20Autonomous%20Arsenal_1.pdf.

⁷² Ibid.

China's Use of AI to Help Russia Defeat Ukraine

China has played a crucial role in supporting Russia's war efforts against Ukraine through AI-driven intelligence sharing, cyberwarfare, economic resilience modelling and disinformation campaigns. By leveraging AI-powered technologies, China is assisting Russia in countering Western sanctions, strengthening military operations and manipulating global narratives to justify its invasion.⁷³

AI-Driven Cyberwarfare and Espionage

Analysts and defense observers have raised concerns that China may be sharing advanced AI-driven surveillance and cyber tools with Russian forces, enabling sophisticated attacks on Ukrainian infrastructure and military systems. Key contributions include:

- **AI-Powered Cyberattacks:** Chinese AI-driven hacking tools help Russia breach Ukrainian military command centres, government institutions and critical infrastructure.
- **AI-Enhanced Malware Deployment:** Machine learning algorithms assist in the development of more advanced malware and ransomware attacks used to disrupt Ukrainian defence networks.
- **Automated Cyber Reconnaissance:** AI enables Russian intelligence to monitor Ukrainian troop movements, supply chains and communication networks in real-time.

China's cyber collaboration with Russia has allowed Moscow to escalate digital warfare against Ukraine, creating massive disruptions to financial systems, power grids and military logistics.⁷⁴

AI in Russian Military Operations and Battlefield Strategy

China's AI expertise has also played a role in enhancing Russia's battlefield strategies. AI-driven military applications provided to Russia include:

- **AI-Powered Drone Warfare:** China has supplied Russia with AI-enabled drones for reconnaissance, surveillance and precision strikes on Ukrainian forces.⁷⁵
- **AI-Optimised Military Logistics:** Machine learning is used to streamline Russian troop deployments, supply chain logistics and battlefield resource allocation.
- **Autonomous Combat Systems:** China has provided AI-powered targeting systems for Russian artillery and missile units, improving their accuracy and lethality.⁷⁶

AI-Driven Disinformation and Propaganda Campaigns

China has actively supported Russia's global disinformation efforts, using AI-driven tools to manipulate public perception and weaken international support for Ukraine. This includes:

⁷³ Hunter, Lance Y., C.D. Albert, J. Rutland, and K. Topping, "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", *Defense & Security Analysis*, 40, no. 1 (2024): 23-44, <https://www.tandfonline.com/doi/abs/10.1080/14751798.2024.2321736>.

⁷⁴ Obioha, O. Val, O.O. Olaniyi, and M.O. Gbadebo, "Cyber Espionage in the Age of Artificial Intelligence: A Comparative Study of State-Sponsored Campaigns", *SSRN* (2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5107605.

⁷⁵ Rickli, Jean-Marc, and Francesco Mantellassi, "The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare", *Geneva Centre for Security Policy*, April 2024, <https://www.gcsp.ch/publications/war-ukraine-reality-check-emerging-technologies-and-future-warfare>.

⁷⁶ Blakcori, N., L.I. Stathakis, L.D. Koutsoukos, and R. Maier, "The Evolving UAS Threat: Lessons from the Russian-Ukrainian War Since 2022 on Future Air Defence Challenges and Requirements", *NATO IAMD Centre of Excellence*, February 2024, <https://iamd-coe.org/wp-content/uploads/2024/02/The-Evolving-UAS-Threat-Lessons-from-the-Russian-Ukrainian-War-Since-2022-on-Future-Air-Defence-Challenges-and-Requirements.pdf>.

- **AI-Generated Propaganda:** Chinese AI platforms create pro-Russian fake news, deepfake videos and misleading narratives to discredit Ukraine and justify the invasion.
- **AI-Enhanced Social Media Manipulation:** AI-powered bot networks flood Western social media platforms with pro-Kremlin messaging, anti-Ukraine rhetoric and disinformation about NATO's role in the conflict.⁷⁷
- **Sentiment Analysis for Targeted Influence:** China's AI-driven sentiment analysis identifies Western political and social divisions that can be exploited to weaken support for Ukraine and undermine international sanctions against Russia.

AI in Sanctions Evasion and Economic Support

China has been instrumental in helping Russia bypass Western economic sanctions by using AI-driven trade strategies and financial systems. These efforts include:

- **AI-Powered Financial Modelling:** AI helps Russia redirect trade routes, predict economic vulnerabilities and optimise currency exchange strategies to minimise the impact of Western sanctions.
- **AI in Digital Payment Systems:** China's digital yuan and blockchain-powered payment networks allow Russia to continue financial transactions outside Western banking systems.⁷⁸
- **AI-Optimised Resource Management:** Machine learning algorithms assist Russia in securing alternative energy supplies, optimising fuel distribution and managing critical wartime resources.

AI-Assisted Military and Strategic Coordination

China's AI-driven intelligence-sharing capabilities enhance Russia's military decision-making and geopolitical strategies. China is believed to be providing:

- **Satellite-Based AI Reconnaissance:** China's AI-powered satellite technology enables Russia to track Ukrainian military positions, anticipate counteroffensives and plan strategic manoeuvres.⁷⁹
- **AI in War Simulation Modelling:** Machine learning enhances Russia's ability to predict battlefield outcomes, assess Western military aid effectiveness and refine its war strategies.⁸⁰
- **AI-Backed Surveillance of Western Military Support:** AI-driven monitoring tools help Russia track weapons shipments, troop reinforcements and NATO support operations for Ukraine.

⁷⁷ Hellström, Johan, Pekka Kallioniemi, Siiri Kytöneva, and Mikko Puranen, "Are Russian Narratives Amplified by PRC Media? A Case Study on Narratives Related to Sweden's and Finland's NATO Applications", *Riga: NATO Strategic Communications Centre of Excellence*, 2023, <https://stratcomcoe.org/publications/are-russian-narratives-amplified-by-prc-media-a-case-study-on-narratives-related-to-swedens-and-finlands-nato-applications/298>.

⁷⁸ Caudevilla, O., and H.M. Kim, "The Digital Yuan and Cross-Border Payments: China's Rollout of Its Central Bank Digital Currency", University of Hong Kong Faculty of Law, 2022, *SSRN*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4371414.

⁷⁹ Rickli, Jean-Marc, and Francesco Mantellassi, "The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare", *Geneva Centre for Security Policy*, April 2024, <https://www.gcsp.ch/publications/war-ukraine-reality-check-emerging-technologies-and-future-warfare>.

⁸⁰ McInnis, James M, "Russia and China Look at the Future of War", *Institute for the Study of War*, 2023, https://understandingwar.org/sites/default/files/Russia%20and%20China%20Look%20at%20the%20Future%20of%20War_0.pdf.

Conclusion

China's AI-driven assistance to Russia is significantly bolstering Moscow's ability to wage war against Ukraine. By supplying cyberwarfare tools, military AI technologies, economic evasion mechanisms and global disinformation capabilities, China is prolonging the conflict, weakening Western sanctions and reinforcing Russia's geopolitical ambitions. As AI technology evolves, China's indirect support for Russia will remain critical in the war's trajectory and its broader implications for global security.

Global Recommendations

Given the significant risks posed by China's AI-driven authoritarian expansion, a coordinated global response is essential to counteract its influence and safeguard democratic values, economic stability and international security. Below are key recommendations for governments, private sector actors and international organisations.

Develop Ethical AI Frameworks and Regulatory Standards

- Establish global AI governance norms, emphasising transparency, accountability and human rights protections.
- Strengthen AI ethics policies in international institutions like the UN, G7 and WTO to counter China's authoritarian AI model.
- Support the development of AI regulatory frameworks that prevent AI-enabled surveillance, censorship and disinformation.
- Support emerging economies to develop AI technologies that align with democratic principles rather than China's authoritarian model.

Strengthen Cybersecurity Measures

- Increase investment by governments into AI-driven cybersecurity solutions to counter China's AI-enhanced cyberwarfare and espionage activities.
- Enhance cooperation between democratic nations to share intelligence on China's AI-driven cyber threats.
- Mandate stricter security protocols for AI-based systems, including multi-layered encryption, zero-trust architecture and continuous AI-driven threat monitoring to prevent intellectual property theft and digital espionage.

Reduce Dependency on Chinese AI and Technology

- Diversify global AI supply chains by encouraging investment in alternative AI technology providers.
- Develop domestic AI capabilities in critical industries, including semiconductors, cybersecurity and digital infrastructure.
- Impose restrictions on Chinese AI companies involved in surveillance, censorship and authoritarian governance.

Counter AI-Driven Disinformation

- Establish AI-powered fact-checking initiatives to detect and counteract Chinese AI-generated propaganda and disinformation campaigns.
- Regulate AI-generated content on social media platforms to prevent the spread of state-sponsored manipulation by implementing stringent content verification mechanisms, transparency requirements and real-time detection tools. Social media companies should be required to label AI-generated content clearly, using digital watermarking and metadata tagging to differentiate between human-created and AI-produced material.
- Encourage media literacy programs to educate the public on AI-driven influence operations.

Enhance Economic Defences Against AI-Enabled Market Manipulation

- Implement AI-driven trade monitoring systems to detect and counteract China's economic coercion and supply chain manipulation.
- Establish trade alliances to reduce reliance on Chinese-controlled logistics, rare earth minerals and AI-driven manufacturing.

Bolster AI in Defence and National Security

- Invest in AI-driven military defence systems to counter China's AI-enhanced autonomous warfare capabilities.
- Strengthen AI-based intelligence-sharing networks among allies to anticipate and mitigate security threats.
- Establish international agreements to limit the proliferation of lethal autonomous weapons and ensure ethical AI use in warfare.

Increase AI Transparency and Accountability in International Institutions

- Advocate for greater transparency in AI policy decisions at the UN, WTO and other global institutions.
- Oppose China-led initiatives that seek to normalise AI-enabled digital authoritarianism.
- Promote AI regulations prioritising democratic governance, free speech and digital privacy.

Make Clear the West's Intent to Defend Taiwan Militarily

- Western nations must unequivocally state their commitment to defending Taiwan in the event of a Chinese military invasion.
- Strengthen military partnerships with Taiwan, including AI-powered defence capabilities, intelligence-sharing and joint training exercises.
- Expand deterrence measures, such as increased naval and aerial patrols in the Taiwan Strait, to signal that any attempt to take Taiwan by force will be met with a unified military response.
- Encourage NATO and Indo-Pacific allies to establish a collective security framework addressing China's AI-driven military expansion and the Taiwan contingency.
- Use AI-driven simulations and strategic forecasting to anticipate potential Chinese invasion strategies and prepare countermeasures in advance.

UK Policy and Legislative Recommendations to Counter China's AI Expansion

Below are key recommendations specific to the UK Government.

Strengthen AI Supply Chain Independence and Ban High-Risk Chinese AI Tech

New Legislative Proposal:

- **National AI Security Act** – Would prohibit UK public sector procurement of AI surveillance equipment from Chinese companies due to national security risks.
 - *Currently, the UK has removed some Hikvision and Dahua cameras from certain government buildings but lacks a legal mandate to eliminate them nationwide.*

Strengthen Existing Law:

- **Foreign Investment and AI Protection Act** – Expand the National Security and Investment Act (2021) to include AI as a high-risk sector, blocking acquisitions of UK AI firms by Chinese state-linked companies.
 - *Currently, the law covers telecoms and defence but does not specifically restrict AI takeovers.*
- **AI Supply Chain Resilience Bill** – Strengthen UK technology independence by expanding government research and development funding for domestic AI chip production and alternative suppliers.
 - *Currently, there are UK research grants for semiconductors, but no specific AI supply chain strategy exists.*

New Ministerial Actions:

- **Home Secretary and Security Minister:** Issue a full ban on Hikvision and Dahua technology from UK public buildings and law enforcement systems.
- **Business and Trade Secretary:** Secure AI trade agreements with Japan, South Korea and the US to build non-Chinese AI supply chains.

Counter China's AI-Driven Disinformation and Influence in the UK

New Legislative Proposal:

- **Foreign Disinformation and AI Propaganda Act** – This would require social media platforms to label AI-generated content from foreign state actors (including China) and remove AI-powered bot networks that spread disinformation.
 - *Currently, no UK law requires platforms to disclose AI-generated political content or foreign propaganda.*
- **AI Transparency in Political Advertising Bill** – This would mandate clear labelling of AI-generated political ads and prohibit foreign AI-generated election interference.
 - *Currently, UK election laws do not cover AI-generated political advertising.*

Strengthen Existing Law:

- **National Security Communications Act** – Expand Ofcom's regulatory powers to investigate and penalise AI-driven Chinese disinformation campaigns.
 - *The Online Safety Act (2023) regulates harmful content but does not address AI-driven foreign influence operations.*

New Ministerial Actions:

- **Culture Secretary:** Establish a UK AI Disinformation Taskforce within Ofcom to counter China's AI-driven media influence.
- **Foreign Secretary:** Sanction Chinese AI firms involved in global disinformation operations.

Enhance AI-Driven Cybersecurity and Intelligence-Sharing with Allies**New Legislative Proposal:**

- **UK AI Cybersecurity Act** – This would require removing Chinese AI software and cloud services from UK critical infrastructure and government IT systems.
 - *Currently, the UK focuses on removing Chinese telecoms (Huawei) but has no AI-specific cybersecurity mandate.*
- **AI Espionage Prevention Bill** – Criminalise economic espionage using AI, restricting UK university partnerships with Chinese AI firms linked to the military.
 - *Currently, UK espionage laws do not cover AI-specific risks or academic tech transfers to China.*

Strengthen Existing Law:

- **UK Cybersecurity Alliance Act** – Strengthen the UK's AI cybersecurity cooperation with Five Eyes nations (US, Canada, Australia, New Zealand).
 - *Existing agreements focus on general cybersecurity, but this bill would formalise AI-specific cooperation.*

New Ministerial Actions:

- **Chancellor of the Duchy of Lancaster (Cybersecurity Minister):** Expand the National Cyber Security Centre's AI Threat Intelligence Unit to track China's AI-driven cyber threats.
- **Defence Secretary:** Integrate AI-based cybersecurity into UK military operations to counter China's AI-enhanced cyberwarfare.

Block China's AI Influence on Global Governance and Trade Standards**New Legislative Proposal:**

- **AI and Digital Sovereignty Act** – This would prevent UK participation in China-led AI regulatory bodies, such as those in the ITU and WEF, which promote authoritarian AI governance.
 - *Currently, there is no UK law limiting AI governance participation in international bodies dominated by China.*

- **Strategic AI Defence Act** – This would create a UK AI Standards Authority to establish Western-aligned AI regulatory frameworks and counter China's push for state-controlled AI norms.
 - *Currently, no UK government body is responsible for setting independent AI governance standards at an international level.*

Strengthen Existing Law:

- **AI Supply Chain Sanctions Bill** – Expand the UK's sanctions regime to cover Chinese AI firms involved in human rights abuses, digital authoritarianism and economic coercion.
 - *Currently, UK sanctions focus on telecoms (e.g. Huawei) but do not target AI-driven threats like AI surveillance and economic manipulation.*

New Ministerial Actions:

- **Prime Minister and Foreign Secretary:** Lead a UK-EU-US coalition to oppose China's AI proposals at the UN and establish a "Democratic AI Charter".
- **Business and Trade Secretary:** Negotiate alternative AI investment frameworks with G7 partners to counter China's AI-driven BRI influence.
- **Defence Secretary:** Expand AI defence partnerships with Australia and Japan to deter China's AI-enhanced military expansion in the Indo-Pacific.

Report Conclusion

China's strategic use of AI represents one of the most significant challenges to democracy, global stability and economic security. AI is not just a technological tool in China's hands – it is a means of surveillance, disinformation, military expansion and economic coercion, enabling Beijing to consolidate power domestically while exerting influence worldwide.

From mass surveillance in Xinjiang to the weaponisation of AI-driven disinformation, China has demonstrated an unprecedented ability to control information, manipulate global narratives and suppress dissent. The PLA is rapidly integrating AI into autonomous warfare systems and cyberwarfare capabilities, significantly increasing the risks of military conflicts, particularly in Taiwan. Meanwhile, China's AI-enhanced economic strategy allows it to manipulate supply chains, steal intellectual property and exercise financial and trade coercion against its adversaries.

The export of AI-driven authoritarianism through initiatives like the BRI has also normalised digital repression, as China provides AI-powered surveillance and cyber tools to autocratic regimes. At the same time, China's growing influence in international institutions threatens to shape global AI governance in ways that favour state-led control rather than transparency, fairness and democracy.

The implications of China's AI-driven expansion are far-reaching and urgent. If left unchecked, China's continued use of AI as a geopolitical weapon could permanently alter the global balance of power, undermine democratic institutions and increase the likelihood of global conflicts, economic instability and digital authoritarianism.

This report outlines critical recommendations to counteract China's AI-enabled authoritarian expansion, including strengthening cybersecurity measures, reducing reliance on Chinese AI technology, building AI coalitions among democratic nations and countering AI-driven disinformation and economic manipulation. The report also underscores the need for Western nations to make clear their intent to defend Taiwan militarily, ensuring that deterrence remains strong against Chinese aggression.

China's AI ambitions must not be met with complacency. The world is at a crossroads where decisive action is necessary to preserve democracy, digital freedom and fair economic competition. Governments, international organisations and private-sector leaders must work together to develop AI policies that protect human rights and prevent AI from becoming a tool of authoritarian control.

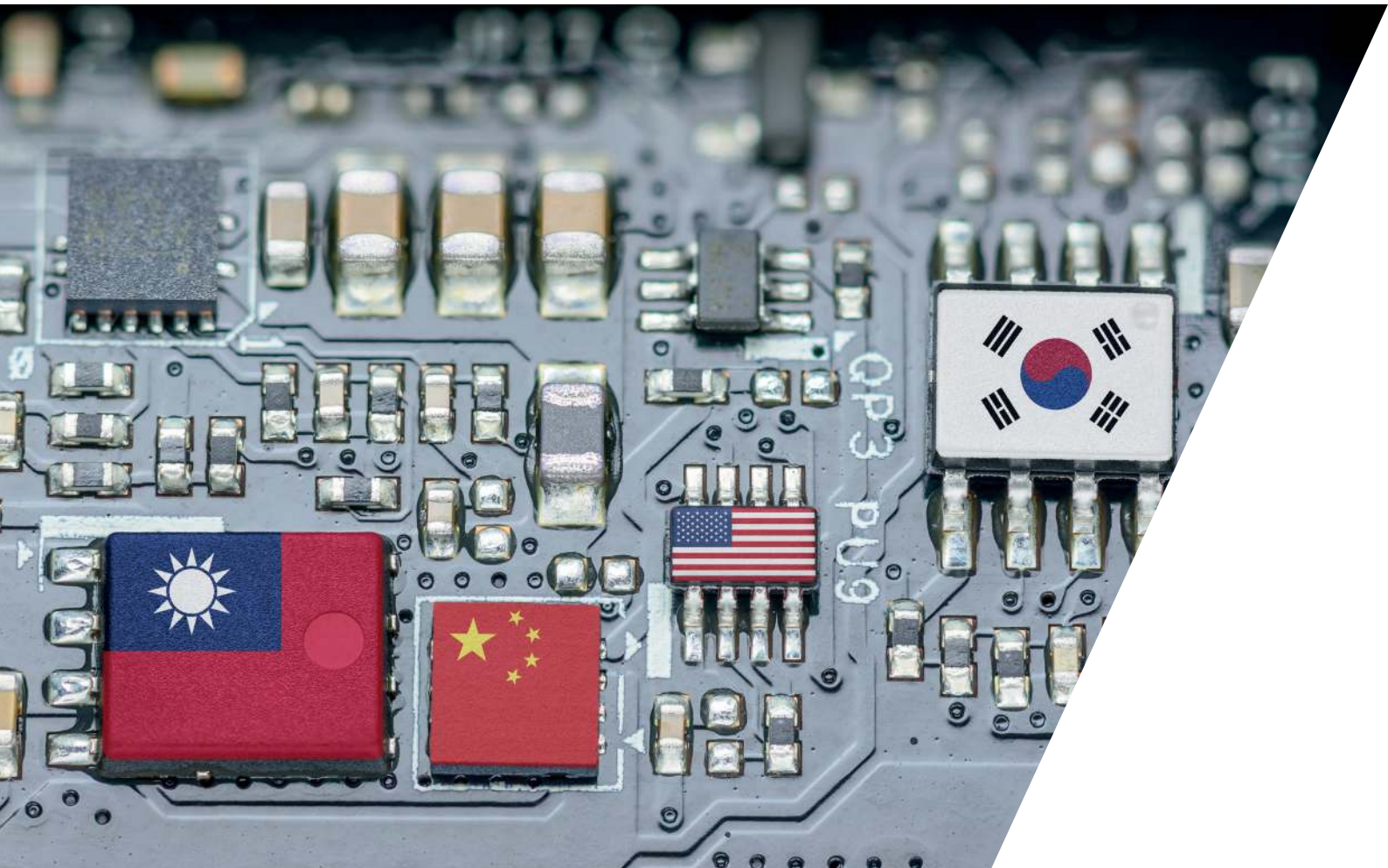
The future of AI – and the global order itself – depends on how the international community responds to China's AI-driven challenge. A coordinated, proactive and strategic approach is essential to ensure that AI remains a force for good rather than a means of oppression and global destabilisation.

Title: "CHINA'S USE OF AI AND ITS
NEGATIVE IMPACT ON THE WORLD"
By M. Dane Waters,
Humanity for Freedom Foundation

© The Henry Jackson Society, 2025

The Henry Jackson Society
Millbank Tower, 21-24 Millbank
London SW1P 4QP, UK

www.henryjacksonsociety.org



**CENTRE FOR
INDO-PACIFIC
STUDIES**