

China's Digital Authoritarianism: A Realist Approach

Melanie Bui

Can a mastery gospel of Orwellian state genuinely exist in the modern world where technology has reshaped every fabric of society? Statista reports that there are 5.52 billion internet users worldwide in 2024 ^[1], and the average person spends six hours and 36 minutes online ^[2]. 250 million users were reported using Artificial Intelligence (AI) technology ^[3]. In 2024, global investment in artificial intelligence surpassed \$184 billion in US dollars and is projected to reach \$632 billion in 2028^[4]. Those promising numbers indicate that digital platforms have become an indispensable part of human life. A 2022 Pew Study^[5] demonstrated that digital technologies empower individuals by breaking down information barriers, empowering society, protecting human rights, and promoting a positive impact on democracy. However, one-third of countries in the world are now living under authoritarianism ^[6]. While traditional authoritarian regimes often maintain their legitimacy via patron-client and repress dissent, modern autocratic regimes even expand their control to cyberspace. In 2023, the White House released a fact sheet to introduce the term “authoritarian counterrevolution” ^[7] since digital authoritarianism is becoming a phenomenon. Digital authoritarianism is described as the pervasive use of technologies to “surveil, repress, demagogue the public and manipulate foreign populations” ^[8]. The Chinese Communist Party is leading in the development of advanced authoritarian tools, such as surveillance, censorship, facial recognition, and police churn through data ^[9]. With a staggering \$1 trillion investment in generative AI in the upcoming years ^[10], it is of utmost importance to realize that many states use AI to maintain social control and suppress dissents. Using a Realist perspective focusing on China's use of digital authoritarianism, this paper argues that China's digital authoritarianism exemplifies how technology has become a sharpened sword for consolidating state power.

Realism framework

Realism is the oldest theory in international relations, providing a pragmatic lens to analyze state behavior in an anarchic global system. Grounded in principles articulated by Morgenthau in 1948 and then expanded upon by Jervis in 1998, Realism emphasizes power, security, and the pursuit of national interest as the core driving forces of state actions.

In his book "Politics among Nations: The Struggle for Power and Peace", Morgenthau frames international politics as a competition for power. He argues that states act rationally to pursue their national interest, which is intrinsically tied to power. This explains why China's AI governance prioritizes state control over technological liberalization, ensuring AI serves political interests rather than market-driven growth.

China's approach to AI governance reflects a deeply ingrained philosophy of centralized control. The Chinese term for artificial intelligence, "人工智能" (rén gōng zhì néng), literally translates to "artificial intelligence," emphasizing AI as a human-made extension ultimately serving state interests. This perspective aligns with the ancient proverb "活到老, 学到老" ("what is learned young endures for life"), underscoring the Chinese Communist Party's belief that technologies must be shaped and controlled early before they mature productively (Sheehan, 2023)^[11]. China's deployment of advanced tools like surveillance systems and censorship exemplifies this mindset, consolidating domestic authority and projecting power abroad, in line with Morgenthau's third principle that national interest is defined by power. (Morgenthau, 1984, p.5)^[12]

As policy must arise from political analysis (Morgenthau, 1984, p.15)^[13], this assumption emphasizes the need for policies to prioritize national interest. China's strict regulation of the AI governance framework reflects the Realist strategy when it is designed to serve the CCP's agenda. Such a calculated strategy enables the state to maintain its power and mitigate the potential perils of advanced technologies. Hence, Morgenthau's insistence on power-centric decision-making is evident in these policies, crafted to strengthen state authority and secure the regime's longevity.

Jervis expands on the classical realism framework by highlighting the role of competition in an anarchic international system, where states constantly maneuver to safeguard and prioritize sovereignty over global cooperation (Jervis, 1998, p.971)^[14]. The geopolitical implications of China's digital authoritarianism are alarming. Many autocratic regimes have adopted China's tactics for developing and deploying AI models, challenging liberal democratic values of transparency and accountability.

Using the Realist lens, China's digital authoritarianism is not merely a domestic control mechanism but also a part of a broader strategy to assert its place in international order. Leveraging technology allows China to reinforce its sovereignty, mitigate external threats, and assert global dominance.

China's Digital Authoritarian Framework

Beijing is the world's first binding regulation on AI technology^[14]. Area of regulations including 2021 algorithmic recommendation^[15], 2022 provisions on deep synthesis^[16], and 2023 draft measure on generative AI^[17]. Overall, China AI governance frameworks have to maintain the CCP's legitimacy through information control while at the same time addressing the endogenous and exogenous impacts of AI on Chinese people. Despite total spending on AI technology in China is projected to reach \$7 billion^[18], it is notable that the goal of becoming an AI superpower comes in third place. Contrary to the US's pro-innovation approaches^[19], China's AI policy focuses more on restriction than on promoting innovations.

Algorithms, alongside data and computing power, form a critical component of the AI triad. China's action on targeting recommendation algorithms demonstrates that pro-innovations is not a core of its governance framework. In response to national security concerns about Western influence, China's AI governance integrates censorship and surveillance, blocking over 800 websites and automating content suppression on social media to ensure public discourse aligns with the state ideology ^[20]. On social media platforms, AI algorithms function as thought police, monitoring and removing posts or accounts that are deemed violating "community standards". List of "sensitive topics" including Tibetan independence, Tiananmen massacre, and everything the CCP deemed dangerous to its legitimacy. China also created Chinese versions of Google (Baidu), WhatsApp (WeChat), Paypal (Alipay), X (Weibo), and Amazon (Taobao) for better control due to the fear that any Chinese citizens who use the global version might smear the CCP. The Cyberspace Administration of China (CAC) is in charge of controlling online content. The first emerging algorithm control appeared in 2017 on TikTok platform, where user feeds were dominated by addictive algorithms ^[21]. The party perceived TikTok phenomena as a threat to public discourse and wanted to curb both the use and misuse of such algorithms. After that, the CAC released the auditing model called the registry algorithm webpage, where 30 algorithms are registered ^[22]. Developers are required to explain the rationale behind their algorithms and submit them to the website ^[23]. Once their algorithm is successfully registered, a limited filling version of it will be announced to the public.

The third area of governance is generative AI, which refers to the use of AI-based tools such as ChatGPT, Claude, and Perplexity to generate text, images, voices, and videos from simple prompts. In 2022, China introduced the term "Deep Synthesis", an alternative term for Deepfake, and simultaneously announced a regulatory framework to govern its use. Deep synthesis regulation includes popular applications of generative AI, including text, image, voice, and video. Recent research demonstrated new forms of Large Language Model (LLM) emerging from many new forms of risk, such as inference risks, personal and emotional bias. As the LLM itself had a potential threat of spreading disinformation, the 2023 generative AI regulation required users to ensure accuracy, objectivity, and diversity yet embody CCP value on their training data. The regulation instructs the generative AI from generating content relating to sex or race and also requires training data adhering to intellectual property rights ^[24]. This framework places significant pressure on tech companies, requiring extensive compliance efforts to remain competitive in the rapid AI market.

Data, the foundation of the AI triad is also another essential focus for China's governance framework. For instance, feeding a huge amount of surveillance data into a training dataset will bias the algorithm. Those who control models can nudge individuals to make certain choices that favor their end goal. Such applications are often used to find target customers from big tech companies, but they are now also considered threatening by the CCP due to the fact that many giant tech companies like Alibaba and ByteDance now have more data than the government ^[25]. Those giant tech actions created tension between them and the CCP. In response, the CCP cracked down on

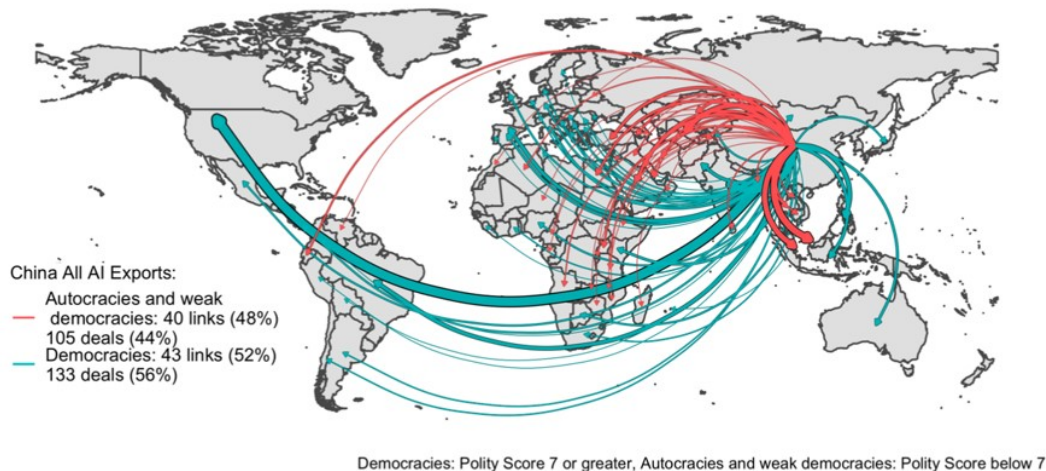
some prominent domestic names such as Alibaba and Ant Group ^[26]. The latest move of the CAC included ordering Chinese big tech companies 3 months to fix recommendation algorithms ^[27] that create “echo chambers”. The new rule insists that tech companies must allow users to decline personalization recommendations ^[28]. It also includes concrete criteria for online content, requiring social media platforms to intervene in the list of content. Contents that are marked qualified should reflect Socialist core values ^[29]. These measures illustrate the CCP’s effort to centralize data control, mitigate the influence of private tech giants, and ensure that AI technologies align with its ideological and political objectives.

Geopolitical Implications of China’s Digital Authoritarianism

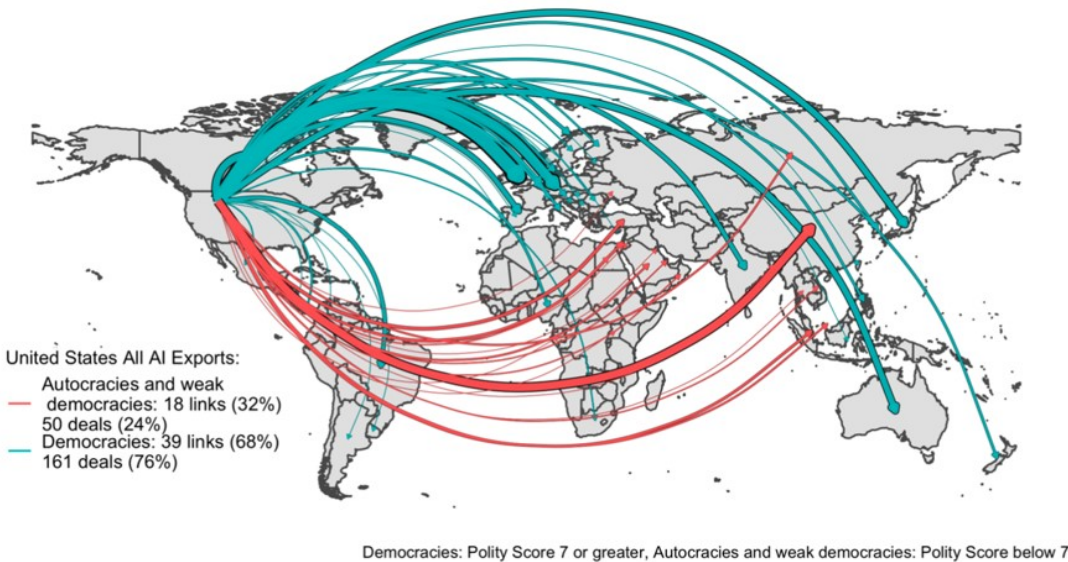
China’s digital authoritarianism has significant global implications. More than half of the world’s one billion surveillance cameras, with approximately 700 million cameras, are from China ^[30]. Snooping gradually becomes a brownfield in China, where surveillance start-ups export their practice with roughly twice as much as the US ^[31].

Surveillance AI exports from China and the US by regime type ^[32]

Panel A: China

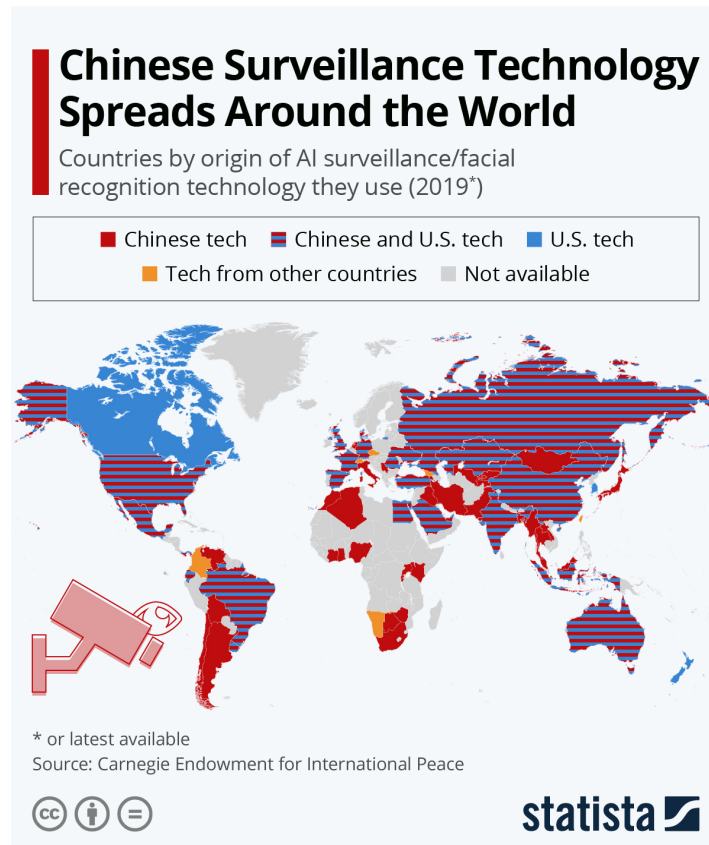


Panel B: United States



Numerous studies reveal that facial recognition technology in China has much autocratic bias [\[33\]](#), suggesting that China specifically exports to autocratic regimes or weak democracies. Notably, these governments are more likely to import these surveillance technologies when experiencing domestic unrest. China integrated monitoring practices by using surveillance tools such as facial recognition, biometric data tracking, iris scanning, and mandatory DNA sampling [\[34\]](#). In moments of unrest, AI firms create a vicious and mutually reinforcing cycle of oppression.

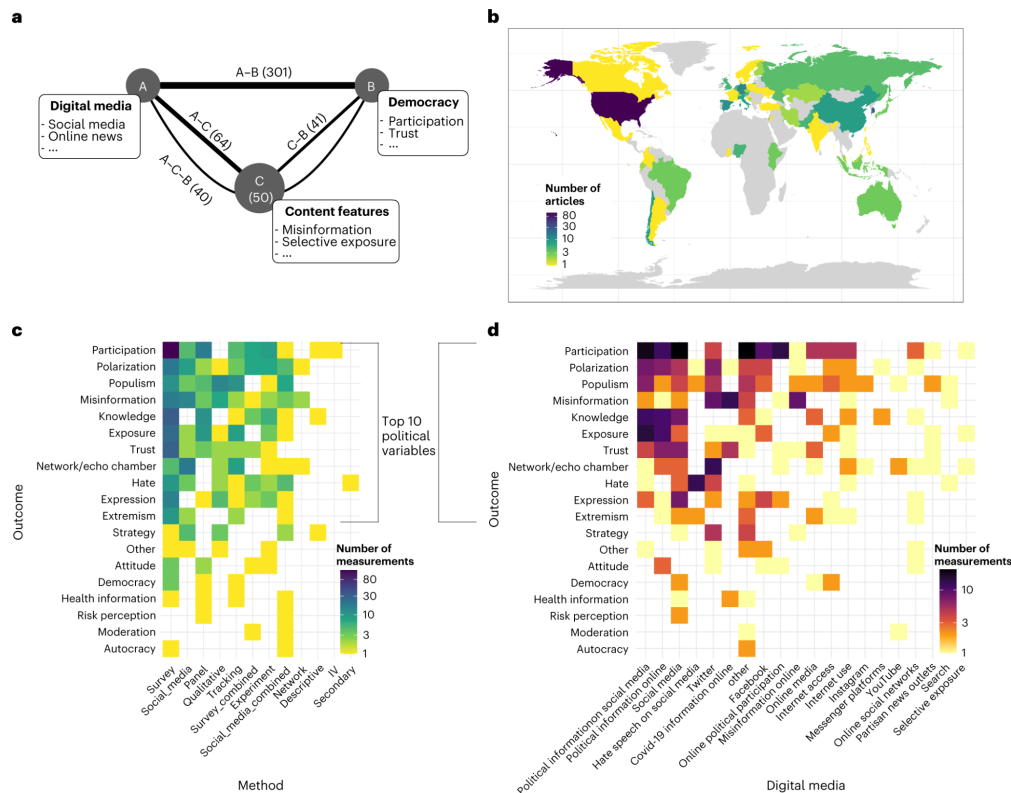
Specifically, China exports its digital authoritarian model to many like-minded autocratic regimes such as Zimbabwe, Iran, Saudi Arabia, Sudan, Syria, Egypt and so on [\[35\]](#). These developing countries are more likely to import these technologies under the facade of security and maintain public order. Some prominent controlling tools, including FRT, AI, and IoT technology [\[36\]](#) have even been reported in democratic countries like Turkey [\[37\]](#).



Countries that imported China surveillance camera, Statista 2020.^[38]

Beyond surveillance systems, China also uses AI technology to expand its control via social media and online news. CAC issued “Provisions on the Management of Internet Post Comments Services” in 2017.^[39] where article 24 stated that users are required to verify their identity if they want to register to any Internet forum. If a user refuses to do so, the platform must prohibit him from its services. Any attempts to help online users evade the block content, once detected, would be sentenced. An Uyghur university student was sentenced to 13 years for using a virtual private network (VPN)^[40]. One of the most extreme measures occurred in Xinjiang, where the government shut down the internet for ten months during periods of unrest^[41].

At least 47 governments are reported to be rigorously adopting China’s tactics^[42]. For instance, Vietnam is mandating that as of December 25, 2024, only accounts verified by phone numbers can share or post content on social media^[43]. Zimbabwe citizens also experienced multiple times of the internet cracking down, and social media such as Facebook or WhatsApp also being blocked to suppress the protest^[44]. Such measures reflect China’s pattern of digital authoritarianism.

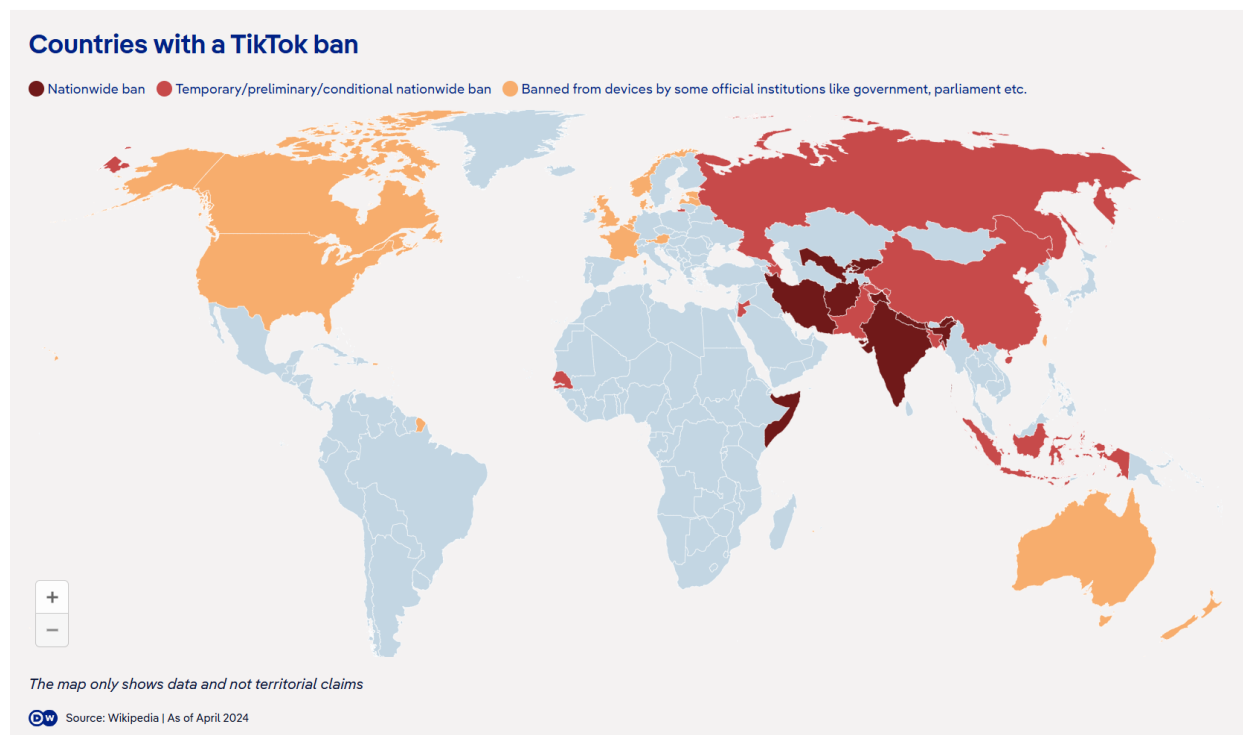


"A systematic review of worldwide causal and correlational evidence on digital media and democracy," by Lorenz-Spreen, P., Oswald, L., Lewandowsky, S., & Hertwig, R., 2022, *Nature Human Behaviour*, 6, 1460–1472. Copyright 2022 by Springer Nature.^[45]

Countering China's Digital Authoritarianism

De-risking China's authoritarian AI would be challenging. Even though China has the second lowest manufacturing cost in the world ^[46], various punitive measures are still implemented to address human rights violations and curb the spread of authoritarianism. For instance, in 2022, the US Department of Commerce introduced new restrictions on China's access to advanced AI chips to curb its ability to develop AI-empower weapons of mass destruction and surveillance technology. ^[47] In response, China invests in domestic AI chip development that aims to reduce the long-term impact of these restrictions. Similarly, In 2023, European regulators also hit TikTok with a \$368 million fine for violating children's privacy by collecting data about children under 13 ^[48]. The Information Commissioner's Office (ICO) also issued a \$15.7 million fine to TikTok for misusing children's data. ^[49] TikTok has also been receiving backlash on a global scale for infringement on personal privacy. Many countries have reported that TikTok will be permanently banned from their

realm. But they do not directly curb China's export of surveillance AI to authoritarian states.



List of countries that banned TikTok^[50]

International bodies have made significant efforts to limit the risk of digital authoritarianism, with multilateral initiatives to create safeguards against the misuse of advanced technology. The Australian Strategic Policy Institute introduced a new three-step-process framework that includes auditing, red teaming, and regulation to mitigate the risk of AI-enabled products and services ^[51]. A 2023 Fact Sheet from President Biden was issued alongside an Executive Order to establish a new standard for AI safety, protect citizen privacy, and advance equity and civil rights ^[52]. This new law aims to ensure that the government uses AI responsibly and effectively while advancing American leadership on the global stage.

Global AI governance frameworks like the General Data Protection Regulation (GDPR) and the Organization for Economic Cooperation and Development AI Principles (OECD AI) also exemplify multilateral cooperation to counter digital authoritarianism. These frameworks uphold democratic values such as transparency, accountability, fairness, and privacy while also upholding human rights and ethical standards in the digital age ^[53]. Furthermore, three global tech leaders, Google DeepMind ^[54], OpenAI ^[55], and Anthropic ^[56] have also published their if-then frameworks to anticipate the potential risks of AI ^[57]. For example, if a “red line” is crossed, then a corresponding governmental action might be triggered. Similarly, if a surveillance show is biased by disproportionately targeting specific groups, then the government must stop using that tool. In

short, countering China's digital authoritarianism requires pervasive efforts from international policymakers, companies, and individuals.

Conclusion

All in all, Realism reminds a reality where states prioritize their sovereignty and enhance relative power. China's digital authoritarianism exemplifies the Realist's international relations perspective by exporting China's governance model to reshape the international influence landscape. China's strategic use of AI demonstrates the competitive nature of states since technological capabilities increasingly dictate power dynamics. As explored in this paper, AI entrenched in authoritarian regimes creates a resilient infrastructure because digital authoritarianism is more challenging to dismantle than traditional authoritarian regimes. Such development brings the Owerllian state closer to reality. International bodies must coalesce around the transparent, accountable development and adoption of explainable and responsible AI to mitigate these trajectories. As AI-power authoritarianism grows, international cooperation must rethink how to counter not just China's AI policies but also the global spread of digital autocracy.

References

1. Statista. (2024). Number of internet users worldwide from 2010 to 2024. Retrieved from <https://www.statista.com>
2. Pew Research Center. (2022). Digital technologies and their impact on democracy. Retrieved from <https://www.pewresearch.org>
3. The White House. (2023). The authoritarian counterrevolution and AI. Retrieved from <https://www.whitehouse.gov>
4. IDC. (2024). Worldwide spending on artificial intelligence is forecast to reach \$154 billion in 2023. Retrieved from <https://www.idc.com/getdoc.jsp?containerId=prUS52530724>
5. Pew Research Center. (2022, December 6). Social media seen as mostly good for democracy across many nations, but U.S. is a major outlier. Retrieved from <https://www.pewresearch.org/global/2022/12/06/social-media-seen-as-mostly-good-for-democracy-across-many-nations-but-u-s-is-a-major-outlier/>
6. World Population Review. (n.d.). What countries have authoritarian governments? Retrieved from <https://worldpopulationreview.com/country-rankings/what-countries-have-authoritarian-government>
7. The White House. (2023, March 29). Fact sheet: Advancing technology for democracy at home and abroad. Retrieved from <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/29/fact-sheet-advancing-technology-for-democracy-at-home-and-abroad/>
8. Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models", (Washington DC: Brookings Institute, 2019).
9. Scharre (2023, May 4). Center for a New American Security (CNAS). The dangers of the global spread of China's digital authoritarianism. Retrieved from <https://www.cnas.org/publications/congressional-testimony/the-dangers-of-the-global-spread-of-chinas-digital-authoritarianism>
10. Goldman Sachs. (2024, August 5). Will the \$1 trillion of generative AI investment pay off? Retrieved from <https://www.goldmansachs.com/insights/articles/will-the-1-trillion-of-generative-ai-investment-pay-off>
11. Morgenthau, H. J. (1948). Politics among nations: The struggle for power and peace. New York: Alfred A. Knopf.
12. Morgenthau, H. J. (1948). Politics among nations: The struggle for power and peace. New York: Alfred A. Knopf.
13. Jervis, R. (1998). Realism in the study of world politics. *International Organization*, 52(4), 971-991.
<https://doi.org/10.1162/002081898550725>
14. Sheehan, M. (2023, July 10). China's AI regulations and how they get made. Carnegie Endowment for International Peace. Retrieved from <https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made?lang=en>
15. Cyberspace Administration of China (CAC). (2022, January 4). Algorithms. Retrieved from https://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm
16. Cyberspace Administration of China (CAC). (2022, December 11). Deep synthesis. Retrieved from https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm
17. Cyberspace Administration of China (CAC). (2023, April 11). Overview of draft measures on generative AI. Retrieved from https://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm
18. Nover, S. (2024, August 27). China spends big on AI. GZERO Media. Retrieved from <https://www.gzeromedia.com/gzero-ai/china-spends-big-on-ai>
19. Wu, Y. (2023, July 27). How to interpret China's first effort to regulate generative AI measures. China Briefing. <https://www.china-briefing.com/news/how-to-interpret-chinas-first-effort-to-regulate-generative-ai-measures/>
20. Binns, R. (2023, November 6). Websites banned in China. Verified by A. Reeves. *The Independent*. Retrieved from <https://www.independent.co.uk/advisor/vpn/websites-banned-in-china#:~:text=With%20the%20aim%20of%20suppressing,than%208%2C000%20websites%20to%20date>
21. People's Daily. (2017, September 18). Strengthening ideological work in the new era. Retrieved from <http://opinion.people.com.cn/n1/2017/0918/c1003-29540709.html>

22. Cyberspace Administration of China (CAC). (n.d.). National internet information service platform. Retrieved from <https://beian.cac.gov.cn/#/index>
23. Sheehan, M., & Du, S. (2022, December 9). What China's algorithm registry reveals about AI governance. Carnegie Endowment for International Peace. Retrieved from <https://carnegieendowment.org/posts/2022/12/what-chinas-algorithm-registry-reveals-about-ai-governance?lang=en>
24. Toner, H., Haluza, Z., Luo, Y., Dan, X., Sheehan, M., Huang, S., Chen, K., Creemers, R., Triolo, P., & Meinhardt, C. (2023, April 19). How will China's generative AI regulations shape the future? A DigiChina forum. DigiChina, Stanford University. Retrieved from <https://digichina.stanford.edu/work/how-will-chinas-generative-ai-regulations-shape-the-future-a-digichina-forum/>
25. Liang, A. (2022, August 16). China's tech giants rush to show AI can align with Communist Party values. BBC News. Retrieved from <https://www.bbc.com/news/business-62544950>
26. Zhang, L. (2023, July 15). Timeline: China's 32-month Big Tech crackdown that killed the world's largest IPO and wiped out trillions in value. South China Morning Post. Retrieved from <https://www.scmp.com/tech/big-tech/article/3227753/timeline-chinas-32-month-big-tech-crackdown-killed-worlds-largest-ipo-and-wiped-out-trillions-value>
27. Wong, H. (2024, November 24). China sets deadline for Big Tech to clear algorithm issues, close echo chambers. South China Morning Post. Retrieved from <https://www.scmp.com/news/china/politics/article/3287929/china-sets-deadline-big-tech-clear-algorithm-issue-s-close-echo-chambers>
28. Qu, T. (2022, March 1). China's algorithm law takes effect to curb Big Tech's sway on public opinion. South China Morning Post. Retrieved from <https://www.scmp.com/tech/policy/article/3168816/chinas-algorithm-law-takes-effect-curb-big-techs-sway-public-opinion?module=inline&pgtype=article>
29. Huang, S., Toner, H., Haluza, Z., Creemers, R., & Webster, G. (2023, April 12). Translation: Measures for the management of generative artificial intelligence services (draft for comment), April 2023. DigiChina, Stanford University. Retrieved from <https://digichina.stanford.edu/work/translation-measures-for-the-management-of-generative-artificial-intelligence-services-draft-for-comment-april-2023/>
30. Statista. (n.d.). Number of surveillance cameras in major cities in China in 2022. Retrieved from <https://www.statista.com/statistics/1456936/china-number-of-surveillance-cameras-by-city/>
31. Beraja, M., Yang, D. Y., & Yuchtman, N. (2024, July 24). China's AI surveillance technology and autocratization. Project Syndicate. Retrieved from <https://www.project-syndicate.org/commentary/china-exports-ai-surveillance-technology-associated-with-autocratization-by-martin-beraja-et-al-2024-07>
32. Beraja, M., Kao, A., Yang, D., & Yuchtman, N. (2023, September 10). How the surveillance state is exported through trade in AI. VoxDev. Retrieved from <https://voxdev.org/topic/trade/how-surveillance-state-exported-through-trade-ai>
33. Martin Beraja, Andrew Kao, David Y Yang, Noam Yuchtman, AI-tocracy, *The Quarterly Journal of Economics*, Volume 138, Issue 3, August 2023, Pages 1349–1402, <https://doi.org/10.1093/qje/qjad012>
34. Feldstein, S. (2022, October 27). China's high-tech surveillance drives oppression of Uyghurs. *The Bulletin of the Atomic Scientists*. Retrieved from <https://thebulletin.org/2022/10/chinas-high-tech-surveillance-drives-oppression-of-uyghurs/>
35. Gallagher, R. (2019). Export laws: China is selling on surveillance technology to the rest of the world. *Index on Censorship*, 48(3), 35-37. <https://doi.org/10.1177/0306422019876445>

36. Yayboke, E., & Brannen, S. (2020, October 15). *Promote and build: A strategic approach to digital authoritarianism*. Center for Strategic and International Studies (CSIS). Retrieved from <https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism>
37. Yücel, A. (2024). Hybrid digital authoritarianism in Turkey: the 'Censorship Law' and AI-generated disinformation strategy. *Turkish Studies*, 1–27. <https://doi.org/10.1080/14683849.2024.2392816>
38. Buchholz, K. (2020, August 18). *Origin of AI surveillance technology by country*. Statista. Retrieved from <https://www.statista.com/chart/20221/origin-of-ai-surveillance-technology-by-country/>
39. China Law Translate. (2017, August 29). *Provisions on the management of internet post comments services*. Retrieved from <https://www.chinalawtranslate.com/en/provisions-on-the-management-of-internet-post-comments-services/>
40. RFA Uyghur. (2023, June 8). Uyghur student sentenced for sharing religious content on WeChat. Radio Free Asia. Retrieved from <https://www.rfa.org/english/news/uyghur/student-sentenced-06082023154805.html>
41. Reuters. (2010, May 14). China allows internet access in Xinjiang 10 months after riots. Retrieved from <https://www.reuters.com/article/technology/china-allows-internet-access-in-xinjiang-10-months-after-riots-idUSTRE64DOMB/>
42. Funk, A., Shahbaz, A., & Vesteinsson, K. (2023). *Repressive power of artificial intelligence*. Freedom House. Retrieved from <https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence>
43. [42] Chinhphu.vn. (2024, November 25). *Từ 25/12 xác thực tài khoản mạng xã hội bằng số điện thoại di động*. Retrieved from <https://xaydungchinhhsach.chinhphu.vn/tu-25-12-xac-thuc-tai-khoan-mang-xa-hoi-bang-so-dien-thoai-di-dong-119241112163033918.htm>
44. BBC News. (2019, January 18). Zimbabwe's Mnangagwa promises investigation into crackdown. Retrieved from <https://www.bbc.co.uk/news/world-africa-46917259>
45. Lorenz-Spreen, P., Oswald, L., Lewandowsky, S., & Hertwig, R. (2022). A systematic review of worldwide causal and correlational evidence on digital media and democracy. *Nature Human Behaviour*, 6(11), 1460–1472. <https://doi.org/10.1038/s41562-022-01460-1>
46. U.S. News & World Report. (n.d.). *Best countries for cheap manufacturing costs*. Retrieved from <https://www.usnews.com/news/best-countries/rankings/cheap-manufacturing-costs>
47. Knight, W., & Matsakis, L. (2024, November 27). *Memory restrictions in China: The fight for advanced chips*. Wired. Retrieved from <https://www.wired.com/story/memory-restrictions-china-advanced-chips/>
48. Chan, K. (2023, September 15). *TikTok faces fine over data privacy concerns in Europe*. Associated Press. Retrieved from <https://apnews.com/article/tiktok-data-privacy-europe-regulation-fine-8ebacba7646ef872fb8e85a1bcb93876>
49. Information Commissioner's Office (ICO). (2023, April 4). *ICO fines TikTok £12.7 million for misusing children's data*. Retrieved from <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/>
50. Walter, J. D. (2024, April 26). *Which countries have banned TikTok?* DW. Retrieved from <https://www.dw.com/en/which-countries-have-banned-tiktok/a-68930678#:~:text=China%27s%20neighbor%2C%20India%2C%20was%20among,that%20it%20shares%20with%20China.>
51. Gilding, S. (2023, July). *De-risking authoritarian AI*. Australian Strategic Policy Institute (ASPI). Retrieved from <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-07/De-risking%20authoritarian%20AI.pdf?VersionId=zJYnuXNnkbViSO1YCflscWYLaOlXMrSq>
52. The White House. (2023, October 30). *Fact sheet: President Biden issues executive order on safe, secure, and trustworthy artificial intelligence*. Retrieved from <https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/>

53. Organisation for Economic Co-operation and Development (OECD). (2019, May 22; amended 2024, May 3). *OECD principles on artificial intelligence* (OECD/LEGAL/0449). Retrieved from <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
54. Dragan, A., King, H., & Dafoe, A. (2024, May 7). *Introducing the frontier safety framework*. DeepMind. Retrieved from <https://deepmind.google/discover/blog/introducing-the-frontier-safety-framework/>
55. OpenAI. (n.d.). *Safety and alignment at OpenAI*. Retrieved from <https://openai.com/safety/>
56. Anthropic. (2023, September 19). *Anthropic's responsible scaling policy*. Retrieved from <https://www.anthropic.com/news/anthropics-responsible-scaling-policy>
57. Karnofsky, H. (2024, September 13). *If-then commitments for AI risk reduction*. Carnegie Endowment for International Peace. Retrieved from <https://carnegieendowment.org/research/2024/09/if-then-commitments-for-ai-risk-reduction?lang=en>