Findings

- The PRC government expanded digital repression on a global scale by exporting censorship technologies to authoritarian governments, undermining human rights by enabling these governments to silence dissent.
- China's expansion of satellite communications infrastructure also raised concerns about the global spread of digital authoritarianism, as its centralized satellite internet model could enable other governments to adopt PRC-style censorship, surveillance, and information control and at the same time deepen PRC influence over global digital governance.
- During the Commission's 2025 reporting year, the Australian Strategic Policy Institute (ASPI) released a report that analyzed internal Chinese documents about the Safe Silk Road (SSR) platform, which collects information from companies operating in the Belt and Road Initiative (BRI) and expands the PRC government's surveillance and data collection practices.
- The PRC government embedded the "core values of Socialism" alongside "society's morals and ethics" into its development of artificial intelligence (AI) by mandating that a type of machine learning systems, known as large language models (LLMs), align with the policies, propaganda, and principal tenets of the Chinese Communist Party (CCP), and by enforcing censorship using data evaluation standards.
- The PRC's advancements in quantum computing and AI surveillance could pose significant threats to human rights by enabling mass censorship, undermining privacy, and amplifying CCP narratives on human rights, ultimately expanding the government's ability to monitor, manipulate, and suppress dissent.
- The operations of DeepSeek reflected how PRC authorities can use a Chinese AI startup to insert censorship, propaganda, and surveillance into emergent AI technology.

Export of Technology

The PRC government exported censorship technologies to authoritarian governments and weak democracies, undermining human rights by enabling the silencing of dissent, and expanded digital repression on a global scale. In February 2025, the National Endowment for Democracy (NED) reported that the PRC appeared to prioritize the export of surveillance technologies to "prop up" authoritarian countries and weak democracies, by assisting them in countering internal unrest and dissent while also benefiting the PRC's security and political partnerships.[1]

The Department of State previously noted that the Pakistani government "used a systematic, nationwide, content-monitoring and -filtering system" to censor information that was seen as "un-Islamic . . . or critical of the state or military forces."[2] In August 2024, the Pakistani government announced that it had designated between US$72 million and $108 million for the installation of a new web management system; a director for a think tank working on communication and information technology said that the system has content monitoring and censoring capabilities similar to the PRC's Great Firewall.[3] A Pakistani Ministry of Defense official later confirmed that Pakistan bought a firewall system from the PRC.[4] *Intelligence Online*, a publication covering the global intelligence community, reported that the Chinese and Pakistani governments collaborated for almost a year on an internet system capable of blocking foreign websites.[5] In addition, the Pakistan Telecommunications Authority approved Chinese telecommunications companies, including Huawei, to help build a "Great Digital Firewall similar to that developed in China."[6] Doublethink Lab, a civil society organization analyzing malign Chinese influence, ranked Pakistan's technology sector as number one globally for the extent of PRC influence in the country.[7]

Freedom House concluded in October 2024 that Burma (Myanmar) and China were the world's "worst environment[s] for internet freedom," noting that the Burmese military junta cracked down violently on dissent while also "building a mass censorship and surveillance regime to suppress the activities of civilian prodemocracy activists and armed resistance groups."[8] Justice for Myanmar (JFM), an activist group, reported the Burmese junta began using a web surveillance and censorship system that included technology from a Chinese company, Jizhi (Hainan) Information Technology Company Limited, also known as Geedge Networks, in May 2024.[9] JFM called for governments to impose sanctions against Geedge Networks, related companies, and Geedge's directors, including Fang Binxing, a founder of Geedge Networks and a leading pioneer in the development of the PRC's Great Firewall.[10]

China's expansion of satellite communications infrastructure also raised concerns about the global spread of digital authoritarianism, as its centralized satellite internet model could enable other governments to adopt PRC-style censorship, surveillance, and information control and at the same time deepen PRC influence over global digital governance. In August 2024, the PRC launched 18 low-Earth-orbit communication satellites, a small

portion of the total number reportedly planned.[11] By bypassing traditional internet infrastructure, which is administered by many stakeholders through multiple gateways, making it harder for any single country to control, the Chinese government could increase control over the internet to the detriment of freedom of expression.[12] An expert warned that the centralized design of satellite internet could enable other governments using Chinese satellite providers to monitor content, block sensitive topics, and shut down access during unrest, as with the Great Firewall.[13] The expert also warned that the PRC could pressure countries using these satellites to "comply with Beijing's demands, including censoring content critical of China, sharing sensitive data or suppressing domestic dissent," to the benefit of China.[14]

9TH FORUM ON CHINA-AFRICA COOPERATION

In September 2024, the 9th Forum on China-Africa Cooperation (FOCAC) took place in Beijing municipality and was "the largest diplomatic event China has hosted in recent years," according to a PRC Ministry of Foreign Affairs spokesperson.[15] According to Article 19, an international nongovernmental organization focused on freedom of expression, the PRC government used the event to promote cooperation across the continent on cybersecurity and artificial intelligence.[16] Article 19 also noted that similar cooperation initiatives had "tended to focus on the normalisation of China's model of digital governance, which favours . . . censorship and surveillance."[17] The FOCAC Beijing Action Plan (2025 to 2027) agreed to at the forum contained a new separate section on artificial intelligence (AI) alongside previous mentions of digital infrastructure and innovation, and included a statement that both sides would "jointly advance rules-making for global digital governance."[18] Article 19 raised concerns that the Action Plan would deepen cooperation in line with China's ambitions to "lead in repositioning global digital governance norms that favour its technologies and policies at the expense of rights-based models."[19]

Belt and Road Initiative

During the Commission's 2025 reporting year, the Australian Strategic Policy Institute (ASPI) released a report that analyzed internal Chinese documents about the Safe Silk Road (SSR) platform, which collects information from companies operating under the Belt and Road Initiative (BRI). The SSR is a non-public digital platform operated by the External Security Affairs Department of the PRC Ministry of Foreign Affairs (MFA).[20] Launched in 2017, the platform acts as a centralized channel to collect data from "dozens of Chinese companies" operating under the BRI abroad.[21] ASPI reported that the goal of the SSR is to expand PRC surveillance and to better understand the operating environment of Chinese interests.[22] The report notes that experts in China differ on whether to add to the traditional definition of China's interests as security of people and assets the protection of China's national image and reputation.[23] PRC central, provincial, and municipal governments made use of the SSR's information, which allows the PRC government to better analyze the safety of PRC citizens and investments.[24] Companies

submit information concerning their foreign operations and activities abroad, a country's conditions, and security incidents.[25]

The PRC government is directly involved in approving corporate users and the operation of the SSR. The MFA approves user applications, and once approved, designated users can only access the SSR while using a specifically tailored virtual private network.[26] The platform also comes in a mobile app form not available in app stores and can only be downloaded through a QR code after the PRC government approves a designated liaison within a company.[27] The MFA prohibits companies from sharing information about the SSR online, and the information is only meant for internal company use.[28]

ISOON SURVEILLANCE

The Chinese cybersecurity firm Anxun Information Technology Co. Ltd. (iS00N, or i-Soon) developed surveillance tools, targeted countries participating in the BRI, and conducted hacking on behalf of or for sale to PRC security agencies that facilitated digital transnational repression. A February 2024 leak from iS00N revealed that the company developed surveillance tools targeting government ministries and critical infrastructure in BRI partner countries.[29] The leak also demonstrated that iS00N could support PRC state surveillance by acting as a proxy to expand PRC control of cyberspace while allowing authorities to keep their distance from the operations.[30] In one example of how iS00N supported PRC surveillance, in March 2025, the U.S. Department of Justice unsealed indictments against 12 cyber actors, including iS00N executives, employees, and freelancers, for hacking operations directed by the PRC Ministry of Public Security and Ministry of State Security or undertaken by iS00N in order to sell hacked information to PRC agencies.[31] Hacking targets included several Asian foreign ministries and U.S.-based individuals critical of the Chinese Communist Party.[32]

Artificial Intelligence

AI ALIGNMENT WITH CCP IDEOLOGY

The PRC government embedded the "core values of Socialism" alongside "society's morals and ethics" into its development of AI by mandating that a type of machine learning systems, known as large language models (LLMs), align with the policies, propaganda, and principal tenets of the Chinese Communist Party (CCP), and by enforcing censorship using data evaluation standards. The PRC government passed legal provisions requiring that machine learning technology uphold "the core values of Socialism" and maintained a list of sensitive topics for training data in AI.[33] The Cyberspace Administration of China (CAC), which also has a dual-CCP role as the Office of the Central Cyberspace Affairs Commission, also required technology companies to test, review, and adjust their algorithms to ensure that LLMs produce content in line with PRC policy.[34]

PROPAGANDA, SURVEILLANCE, AND CENSORSHIP

PRC authorities used AI to monitor and analyze public sentiment on sensitive political and social issues, seeking to proactively control online discourse.[35] In March 2025, TechCrunch, a technology news

website, reported on a leaked database of 133,000 examples of content on sensitive topics that was used to train LLMs.[36] The content was related to politics, the military, and issues such as pollution, labor disputes, and fraud, that had led to protests.[37] Political satire was a priority, with "Taiwan politics" and certain portrayals of "current political figures" instantly flagged.[38] The report noted that "an LLM trained on such instructions would significantly improve the efficiency and granularity of state-led information control." A February 2025 NED report noted that instead of only searching for banned keywords, PRC authorities could rely on LLMs and multimodal foundation models to "identify the expression of sentiments" directed at the political system.[39]

Chinese LLMs aligned with "CCP values" represent a tool for amplifying CCP narratives on human rights and enhancing censorship, posing a risk to international standards of freedom of expression. One expert on technology at China Media Project reported that "most Chinese LLMs I approached interpreted 'human rights' the same way the CCP does: not rights to freedom of expression, assembly, or a fair trial, but primarily the rights to political stability and economic development."[40] He suggested that "LLMs trained on CCP values" could become a new source of international propaganda imposing the PRC's narrative of human rights.[41]

The PRC's advancements in quantum computing and AI surveillance could pose significant threats to human rights by enabling mass censorship, undermining privacy, and amplifying CCP narratives on human rights , ultimately expanding the government's ability to monitor, manipulate, and suppress dissent. The above-mentioned NED report noted that PRC authorities could use quantum computing to improve AI-powered surveillance and to circumvent encryption used by human rights defenders, journalists, and government critics to protect their communications and hide their identities.[42] The NED report also observed that AI-powered systems for data fusion and rapid analysis, known as "city brains"—the next evolution for "smart cities"—could track and visualize "pedestrians, vehicles, buildings, and police forces" on a unified map.[43] Even traffic management, if boosted by AI tools, could be a threat to human rights, for example, by clearing a path for police cars to a protest.[44]

In February 2025, OpenAI researchers reported they had banned ChatGPT accounts that likely originated in China and that had used ChatGPT's models to generate English-language social media posts criticizing Cai Xia—a critic of the CCP under Xi Jinping.[45] The banned accounts also created Spanish-language articles criticizing U.S. society and politics that were published on news websites in several Latin American countries, including some articles which were attributed to an individual allegedly linked to a Chinese company.[46]

DeepSeek

The operations of DeepSeek reflected how PRC authorities can use a Chinese AI startup to insert censorship, propaganda, and surveillance into emergent AI technology. DeepSeek has extensive ties to the PRC government, military, and state-owned entities.[47] In 2025, data analysis firm Exiger reported on numerous past or current connections between DeepSeek-affiliated researchers and PRC government-affiliated entities.[48] In addition, China Mobile, a company with direct links to the People's Liberation Army, provided DeepSeek with critical support including telecommunications infrastructure and AI servers.[49] After a meeting between PRC leader Xi Jinping and the head of DeepSeek in February 2025, PRC authorities began to adopt DeepSeek for government uses, including in public security bureaus.[50]

The Chinese cybersecurity companies TopSec and QAX announced the integration of DeepSeek to enhance their services, which the PRC government uses,[51] while another company, NetEase, said DeepSeek would improve its censorship and surveillance capabilities of texts, images, videos, and other media.[52] One researcher predicted that the PRC would likely incorporate DeepSeek and other generative AI models into its surveillance system for searching and summarizing a large amount of data, including video footage.[53]

During this reporting year, researchers and journalists noted how DeepSeek's chatbot aligned with PRC official policy, amplifying PRC propaganda and disinformation.[54] A China Media Project researcher tested DeepSeek in multiple languages, asking the model to "describe the stereotypes of Urumqi," capital of the Xinjiang Uyghur Autonomous Region (XUAR), and found uniform answers that characterized the region as having been stabilized due to "heightened security."[55] In response to a reporter asking about Uyghur scholar **Ilham Tohti,** whom a PRC court sentenced in 2014 to life in prison for "separatism," DeepSeek's chatbot responded that he was "known for spreading separatist ideas and . . . ethnic division," and that DeepSeek "firmly support[ed]" the government's actions.[56] The chatbot refused to answer questions about the violent suppression of the 1989 Tiananmen protests and gave one-sided responses consisting of either PRC official statements or answers in line with PRC propaganda when asked about U.S.-China relations, Taiwan, forced labor, and euphemisms for PRC leader Xi Jinping's name.[57] When asked about PRC violations of religious freedom, DeepSeek's chatbot displayed a "thought process" indicating that it incorporated official restrictions on discussion of "sensitive topics," including suppression of Falun Gong and detentions of Christian clergy.[58] As its technology was updated over time, DeepSeek's chatbot reportedly gave responses that were progressively more narrow and that replicated official PRC narratives, including with respect to human rights issues affecting ethnic minority groups.[59] In May 2025, computer scientists reported that DeepSeek used "possible additional censorship integration" in training its chatbot,[60] and a June 2025 paper claimed that the updated model "exhibits 'thought suppression' behavior that indicates memorization of CCP-aligned responses."[61]

Notes to Chapter 13—Technology and Human Rights

[1]Valentin Weber, "Data-Centric Authoritarianism," *International Forum for Democratic Studies, National Endowment for Democracy,* February 2025, 6–7.

[2]Bureau of Democracy, Human Rights, and Labor, U.S. Department of State, "2023 Country Reports on Human Rights Practices: Pakistan," April 2024.

[3]Adnan Aamir, "Pakistan Installs Firewall in Censorship Drive, Hitting Businesses," *Nikkei Asia,* September 4, 2024; Abid Hussain, "Pakistan Tests Secret China-like 'Firewall' to Tighten Online Surveillance," *Al Jazeera,* November 26, 2024.

[4]Adnan Aamir, "Pakistan Installs Firewall in Censorship Drive, Hitting Businesses," *Nikkei Asia,* September 4, 2024; Abid Hussain, "Pakistan Tests Secret China-like 'Firewall' to Tighten Online Surveillance," *Al Jazeera,* November 26, 2024.

[5]"China to Replicate Its 'Great Digital Firewall' in Pakistan," *Intelligence Online,* April 23, 2025; "About Us," *Intelligence Online,* accessed June 25, 2005.

[6]"China to Replicate Its 'Great Digital Firewall' in Pakistan," *Intelligence Online,* April 23, 2025.

[7]Doublethink Lab, "Pakistan," *China Index,* May 2024; "About Doublethink Lab," *Doublethink Lab,* accessed June 5, 2025.

[8]Allie Funk et al., "Freedom on the Net 2024: The Struggle for Trust Online," *Freedom House,* October 16, 2024, 2.

[9]"The Myanmar Junta's Partners in Digital Surveillance and Censorship," *Justice for Myanmar,* June 19, 2024; "Home," *Justice for Myanmar,* accessed June 9, 2025.

[10]"The Myanmar Junta's Partners in Digital Surveillance and Censorship," *Justice for Myanmar,* June 19, 2024; "Chinese Spy Tech Driving Junta Internet Crackdown: Justice For Myanmar," *Irrawaddy,* June 20, 2024.

[11]Cissy Zhou, "China Races to Outflank Elon Musk's Starlink Satellite Internet Service," *Nikkei Asia,* October 11, 2024; Mercedes Page, "China May Be Putting the Great Firewall into Orbit," *Strategist, Australian Strategic Policy Institute,* August 26, 2024.

[12]Cissy Zhou, "China Races to Outflank Elon Musk's Starlink Satellite Internet Service," *Nikkei Asia,* October 11, 2024; Mercedes Page, "China May Be Putting the Great Firewall into Orbit," *Strategist, Australian Strategic Policy Institute,* August 26, 2024.

[13]Cissy Zhou, "China Races to Outflank Elon Musk's Starlink Satellite Internet Service," *Nikkei Asia,* October 11, 2024; Mercedes Page, "China May Be Putting the Great Firewall into Orbit," *Strategist, Australian Strategic Policy Institute, August* 26, 2024.

[14]Mercedes Page, "China May Be Putting the Great Firewall into Orbit," *Strategist, Australian Strategic Policy Institute,* August 26, 2024.

[15]Ministry of Foreign Affairs, "Remarks by H.E. Ambassador LI Song at the Special Reception for the 2024 FOCAC Summit," September 12, 2024; Alfred Bulakali and Michael Caster, "China-Africa Cooperation: Beijing's Vision Raises Free Expression Concerns," *Article 19,* October 3, 2024.

[16]Alfred Bulakali and Michael Caster, "China-Africa Cooperation: Beijing's Vision Raises Free Expression Concerns," *Article 19,* October 3, 2024.

[17]Alfred Bulakali and Michael Caster, "China-Africa Cooperation: Beijing's Vision Raises Free Expression Concerns," *Article 19,* October 3, 2024; PRC Ministry of Foreign Affairs, "中非合作论坛—北京行动计划（2025-2027）" [Forum on China-Africa Cooperation—Beijing Action Plan (2025–2027)], September 5, 2024.

[18]Alfred Bulakali and Michael Caster, "China-Africa Cooperation: Beijing's Vision Raises Free Expression Concerns," *Article 19,* October 3, 2024; PRC Ministry of Foreign Affairs, "中非合作论坛—北京行动计划（2025-2027）" [Forum on China-Africa Cooperation—Beijing Action Plan (2025–2027)], September 5, 2024; PRC Ministry of Foreign Affairs, "中非合作论坛—达喀尔行动计划（2022-2024）" [Forum on China-Africa Cooperation—Dakar Action Plan (2022–2024)], December 2, 2021.

[19]Alfred Bulakali and Michael Caster, "China-Africa Cooperation: Beijing's vision raises free expression concerns," *Article 19,* October 3, 2024.

[20]Bethany Allen, Daria Impiombato, and Nathan Attrill, "Exclusive: Inside Beijing's App Collecting Information from Belt and Road Companies," *Australian Strategic Policy Institute, Strategist,* September 27, 2024.

[21]Bethany Allen, Daria Impiombato, and Nathan Attrill, "Exclusive: Inside Beijing's App Collecting Information from Belt and Road Companies," *Australian Strategic Policy Institute, Strategist,* September 27, 2024.

[22]Bethany Allen, Daria Impiombato, and Nathan Attrill, "Exclusive: Inside Beijing's App Collecting Information from Belt and Road Companies," *Australian Strategic Policy Institute, Strategist,* September 27, 2024; International Cooperation Center, "中国海外利益安全的实践类型及其战略指引" [Putting into practice and strategic guidance the security of Chinese overseas interests], September 1, 2023.

[23]Bethany Allen, Daria Impiombato, and Nathan Attrill, "Exclusive: Inside Beijing's App Collecting Information from Belt and Road Companies," *Australian Strategic Policy Institute, Strategist,* September 27, 2024; International Cooperation Center, "中国海外利益安全的实践类型及其战略指引" [Putting into practice and strategic guidance the security of Chinese overseas interests], September 1, 2023.

[24]Bethany Allen, Daria Impiombato, and Nathan Attrill, "Exclusive: Inside Beijing's App Collecting Information from Belt and Road Companies," *Australian Strategic Policy Institute, Strategist,* September 27, 2024; "北京 '境外服务宝' 启动上线" [Beijing's "Overseas Service Treasure" is launched], *China One Belt One Road Network,* August 6, 2021; "高唐县外办致我县企业的一封信," [A letter from the Gaotang County Foreign Affairs Office to our enterprises], *Gaotang County People's Government Foreign Affairs Office,* November 25, 2024; "快来下载 '平安丝路' " [Quickly download the safe "Silk Road App"], *First Kunshan,* July 8, 2021.

[25] Bethany Allen, Daria Impiombato, and Nathan Attrill, "Exclusive: Inside Beijing's App Collecting Information from Belt and Road Companies," *Australian Strategic Policy Institute, Strategist,* September 27, 2024; "北京 '境外服务宝' 启动上线" [Beijing's "Overseas Service Treasure" is launched], *China One Belt One Road Network,* August 6, 2021; "高唐县外办致我县企业的一封信," [A letter from the Gaotang County Foreign Affairs Office to our enterprises], *Gaotang County People's Government Foreign Affairs Office,* November 25, 2024; "快来下载 '平安丝路'" [Quickly download the safe "Silk Road App"], *First Kunshan,* July 8, 2021.

[26] Bethany Allen, Daria Impiombato, and Nathan Attrill, "Exclusive: Inside Beijing's App Collecting Information from Belt and Road Companies," *Australian Strategic Policy Institute, Strategist,* September 27, 2024.

[27] Bethany Allen, Daria Impiombato, and Nathan Attrill, "Exclusive: Inside Beijing's App Collecting Information from Belt and Road Companies," *Australian Strategic Policy Institute, Strategist,* September 27, 2024.

[28] Bethany Allen, Daria Impiombato, and Nathan Attrill, "Exclusive: Inside Beijing's App Collecting Information from Belt and Road Companies," *Australian Strategic Policy Institute, Strategist,* September 27, 2024.

[29] Che Chang, Lian Huang, and Athena Tong, "State Goals, Private Tools: Digital Sovereignty and Surveillance along the Belt and Road," *China Brief, Jamestown Foundation,* December 20, 2024, vol. 24, no. 24, 24–25.

[30] J. Edward Moreno, "China's Hacker Network: What to Know," *New York Times,* February 22, 2024; Che Chang, Lian Huang, and Athena Tong, "State Goals, Private Tools: Digital Sovereignty and Surveillance along the Belt and Road," *China Brief, Jamestown Foundation,* December 20, 2024, vol. 24, no. 24, 22–23, 25, 27.

[31] "Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns," *Office of Public Affairs, U.S. Department of Justice,* March 5, 2025.

[32] "Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns," *Office of Public Affairs, U.S. Department of Justice,* March 5, 2025.

[33] Cyberspace Administration of China et al., "生成式人工智能服务管理暂行办法" [Interim Measures for the Administration of Generative Artificial Intelligence Services], passed May 23, 2023, effective August 15, 2023, art. 4; "China Proposes Blacklist of Sources Used to Train Generative AI Models," *Reuters,* October 12, 2023; National Information Security Standardization Technical Committee, "生成式人工智能服务安全基本要求" [Basic security requirements for generative artificial intelligence services], October 11, 2023, 6–8; See also, e.g., Cyberspace Administration of China et al., "互联网信息服务深度合成管理规定" [Provisions on the Management of Deep Synthesis of Internet Information Services], passed November 3, 2022, effective January 10, 2023, art. 1; Cyberspace Administration of China et al., "互联网信息服务算法推荐管理规定" [Provisions on the Administration of Algorithm Recommendations for Internet Information Services], passed November 16, 2021, effective March 1, 2022, art. 1.

[34] Ryan McMorrow and Tina Hu, "China Deploys Censors to Create Socialist AI," *Financial Times,* July 17, 2024; See also Cyberspace Administration of China et al., "生成式人工智能服务管理暂行办法" [Interim Measures for the Administration of Generative Artificial Intelligence Services], passed May 23, 2023, effective August 15, 2023, art. 19.

[35] Kieran Green, Andrew Sprott, Ed Francis, et.al., "Censorship Practices of the People's Republic of China," *Center for Intelligence and Research and Analysis, Exovera,* reprinted in *U.S. Economic and Security Review Commission,* February 20, 2024, 19; See also Angela Yang, "On DeepSeek, You Can Watch AI Navigate Censorship in Real Time," *NBC,* January 30, 2025; Charles Rollett, "Leaked Data Exposes a Chinese AI Censorship Machine," *TechCrunch,* March 26, 2025; Bang Xiao, "Leaked Files Reveal How China Is Using AI to Erase the History of the Tiananmen Square Massacre," *Australian Broadcasting Corporation,* June 3, 2025.

[36] Charles Rollett, "Leaked Data Exposes a Chinese AI Censorship Machine," *TechCrunch,* March 26, 2025.

[37] Charles Rollett, "Leaked Data Exposes a Chinese AI Censorship Machine," *TechCrunch,* March 26, 2025.

[38] Charles Rollett, "Leaked Data Exposes a Chinese AI Censorship Machine," *TechCrunch,* March 26, 2025.

[39] Valentin Weber, "Data-Centric Authoritarianism," *International Forum for Democratic Studies, National Endowment for Democracy,* February 2025, 11.

[40] Alex Colville, "China_Chatbot_13," *Lingua Sinica, China Media Project,* January 16, 2025. See also Malin Oud, "The CMP Dictionary: Human Rights," *China Media Project,* May 7, 2021.

[41] Alex Colville, "China_Chatbot_13," *Lingua Sinica, China Media Project,* January 16, 2025; Alex Colville, "AI for All," *China Media Project,* December 20, 2024.

[42] Valentin Weber, "Data-Centric Authoritarianism," *International Forum for Democratic Studies, National Endowment for Democracy,* February 2025, 17, 18–19. See also Valentin Weber and Joss Wright, "(Quantum) Encryption: Europeans Need to Come Down in Favor," *German Council on Foreign Relations,* June 20, 2023; David Lauge, "U.S. and China Race to Shield Secrets from Quantum Computers," *Reuters,* December 14, 2023.

[43] Valentin Weber, "Data-Centric Authoritarianism," *International Forum for Democratic Studies, National Endowment for Democracy,* February 2025, 10–12. See also Wu Fan, "Smart Cities Deep Dive: AI-Powered Urbanization," *China Talk,* August 23, 2023; Chamila Liyanage, "Tyranny of City Brain: How China Implements Artificial Intelligence to Upgrade Its Repressive Surveillance Regime," *Journal of Illiberalism Studies,* vol. 4, no. 3, 2024.

[44] Valentin Weber, "Data-Centric Authoritarianism," *International Forum for Democratic Studies, National Endowment for Democracy,* February 2025, 12. See also Chamila Liyanage, "Tyranny of City Brain: How China Implements Artificial Intelligence to Upgrade Its Repressive Surveil-

lance Regime," *Journal of Illiberalism Studies,* vol. 4, no. 3, 2024; Ken He, "The Atlas of Urban Tech: Hangzhou City Brain," *Urban Tech Hub, Jacobs Technion-Cornell Institute at Cornell Tech,* accessed May 13, 2025.

[45] Ben Nimmo, Albert Zhang, Matthew Richard, and Matthew Hartly, "Disrupting Malicious Uses of Our Models: An Update," *OpenAI,* February 2025, 5.

[46] Ben Nimmo, Albert Zhang, Matthew Richard, and Matthew Hartly, "Disrupting Malicious Uses of Our Models: An Update," *OpenAI,* February 2025, 5, 15–17; Cade Metz, "OpenAI Uncovers Evidence of A.I.-Powered Chinese Surveillance Tool," *New York Times,* February 21, 2025.

[47] Byron Tau, "Researchers Link DeepSeek's Blockbuster Chatbot to Chinese Telecom Banned from Doing Business in US," *Associated Press,* February 5, 2025; Ally Kapassakis and Kit Conklin, "DeepSeek's Deception: How the Chinese Military and Government Funded DeepSeek's AI Research," *Exiger,* April 2025, 2, 4, 7; Alice Yam and Ha Syut, "China's DeepSeek Has Close Ties to Beijing," *Radio Free Asia,* January 28, 2025.

[48] Ally Kapassakis and Kit Conklin, "DeepSeek's Deception: How the Chinese Military and Government Funded DeepSeek's AI Research," *Exiger*, April 2025, 2; Tripp Mickle, Ana Swanson, Meaghan Tobin, and Cade Metz, "Washington Takes Aim at DeepSeek and Its American Chip Supplier, Nvidia," *New York Times,* April 16, 2025.

[49] Byron Tau, "Researchers Link DeepSeek's Blockbuster Chatbot to Chinese Telecom Banned from Doing Business in US," *Associated Press,* February 5, 2025; Bureau of Industry and Security, U.S. Department of Commerce, "Additions to the Entity List," March 28, 2025.

[50] Meaghan Tobin and Claire Fu, "From Courtrooms to Crisis Lines, Chinese Officials Embrace DeepSeek," *New York Times,* March 18, 2025. See also, e.g., "石家庄市公安局举办DeepSeek赋能公安实战应用专题培训会" [Shijiazhuang Municipal Public Security Bureau held a special training session on DeepSeek to empower public security's practical applications], *Shijiazhuang Municipal Public Security Bureau,* March 6, 2025; "「DeepSeek智启未来」永仁公安AI实训：解锁'智慧警务'新战力" [[DeepSeek Smart Future] Yongren Public Security AI Training: Unlocking the New Power of "Smart Policing"], Yongren County Public Security Bureau, March 14, 2025; "深度求索赋能警务实战丨白银市公安局举办科技赋能实战专题讲座" [In-depth exploration to empower police operations | Baiyin Municipal Public Security Bureau held a special lecture on technology empowerment], Baiyin Municipal Public Security Bureau, March 3, 2025; "A Silent, Silencing Industry: The Growing Market of Human-Powered Censorship in China," *Open Technology Fund,* March 14, 2025, 2.

[51] Fatima Tlis, "China Uses DeepSeek, Other AI models, for Surveillance and Information Attacks on US," *Voice of America,* March 4, 2025; "天融信正式接入DeepSeek！强化大模型网络安全防护势在必行" [Topsec officially connected to DeepSeek! Strengthening network security protection for large models is imperative], *TopSec*, February 6, 2025;, "奇安信安全智能体深度接入DeepSeek，在政企客户威胁研判等服务中表现卓越" [Qi'anxin Security Intelligence is Deeply Connected to DeepSeek and Performs Well in Threat Analysis and Other Services for Government and Enterprise Customers], *QAX,* February 5, 2025.

[52] Fatima Tlis, "China Uses DeepSeek, other AI models, for Surveillance and Information Attacks on US," *Voice of America,* March 4, 2025; Wenhao Ma, "Chinese Surveillance Providers Embrace DeepSeek," *Wenhao Reports,* February 28, 2025; "网易易盾接入DeepSeek，数字内容安全'智'理能力全面升级" [NetEase Yidun Integrates with DeepSeek, Comprehensively Upgrading Digital Content Security "Intelligent" Management Capabilities], *NetEase,* February 11, 2025.

[53] Valentin Weber, "Why DeepSeek Is So Dangerous," *Journal of Democracy,* March 2025.

[54] Steven Lee Myers, "DeepSeek's Answers Include Chinese Propaganda, Researchers Say," *New York Times,* January 31, 2025; "We Asked DeepSeek about Geopolitics. It Gave Us Beijing Talking Points," *Politico,* February 4, 2025; Zeyi Yang, "Here's How DeepSeek Censorship Actually Works—and How to Get Around It," *Wired,* January 31, 2025.

[55] Alex Colville, "DeepSeeking Truth," *China Media Project,* February 10, 2025.

[56] Charles Rollet (@CharlesRollet1), "DeepSeek doesn't just pretend the Tiananmen Square massacre never happened. It also 'firmly supports' imprisoning prominent Uyghur dissidents for life. 'Ilham Tohti is a person of significant notoriety in China . . . We firmly support the government's actions,'" *X,* December 26, 2024, 12:41 p.m.; Kasim Kashgar, "A Decade after Uyghur Scholar's Life Sentencing, Calls for Action Grow," *Voice of America,* September 25, 2024; "CECC Record Number: 2009-00315, Ilham Tohti," *CECC Political Prisoner Database,* accessed March 13, 2025.

[57] Kanis Leung, "DeepSeek's New AI Chatbot and ChatGPT Answer Sensitive Questions about China Differently," *Associated Press,* January 28, 2025; "We Asked DeepSeek about Geopolitics. It Gave Us Beijing Talking Points," *Politico,* February 4, 2025.

[58] Jerry An, "What DeepSeek Says about the Church in China," *Christianity Today,* January 29, 2025.

[59] Alex Colville, "China's Global AI Firewall," *China Media Project,* June 6, 2025; Kyle Wiggers, "DeepSeek's Updated R1 AI Model Is More Censored, Test Finds," *TechCrunch,* May 29, 2025.

[60] Ali Naseh et al., "R1dacted: Investigating Local Censorship in DeepSeek's R1 Language Model," *arXiv,* May 19, 2025, 1.

[61] Can Rager, Chris Wendler, Rohit Gandikota, and David Bau, "Discovering Forbidden Topics in Language Models," *arXiv* (preprint), June 11, 2025, 1.