

Beijing's Vision for Global Cyberspace Governance

By Thomas Shrimpton
OE Watch Commentary

China identifies the Internet and cyberspace as a critical domain for ensuring national security, economic and social stability, and ultimately, the legitimacy of the Chinese Communist Party (CCP). Recently, Beijing presented its vision for international cooperation in cyberspace via a white paper from the State Council Information Office. The white paper reflects Beijing's tightening grip on information flows and fundamental freedoms, its growing concerns over Western digital advantages in its operational environment, and its expanding efforts to export digital authoritarianism to the developing world.

For Beijing to realize its global superpower aspirations and compete with the United States as a cyber superpower, it must present a vision for an equitable and inclusive global community. The 2022 white paper lays out Beijing's vision for such a community through "extensive consultation, joint contribution and shared benefits in global governance, and promot[ion of] a multilateral, democratic, and transparent international internet governance system." The document further highlights Beijing's achievements in internet development (e.g. expansion of its internet penetration, digital economy, and tech sector) and cyberspace governance (e.g. the Cybersecurity Law, Data Security Law, Personal Information Protection Law, and Cybersecurity Review Measures)¹ while advocating for the rights of all countries to formulate their own national cybersecurity strategies. However, these seemingly liberal themes are trumped by Beijing's emphasis on cyber sovereignty as its core guiding principle in international cyberspace governance.

Cyber sovereignty is the notion that individual countries should maintain the exclusive right to govern their own territory's cyberspace, superseding any supposed rights for the mutual interest of a future shared community in cyberspace. As such, reliance on the principle

of cyber sovereignty serves to justify the CCP's long-term strategic control over information flows available to Chinese internet users and to facilitate Beijing's digital security apparatus' ability to enforce social stability to buttress CCP legitimacy.

Problems with the internet such as unbalanced development, unsound regulation, and unreasonable order are becoming more prominent. Cyber-hegemonism poses a new threat to world peace and development.

Simultaneously, China looks to promote this version of internet governance abroad. This conception of cyberspace governance diverges from the principles of an "open, free, global, interoperable, reliable, and secure Internet" advocated for by the United States and 61 partner nation signatories of the "Declaration for the Future of the Internet."² Indeed, Beijing's white paper presents China's achievements and vision of shared internet development and cyberspace governance in stark contrast to its vision of Western "cyber hegemonism," the idea that "certain countries are exploiting the internet and information technology as a tool to seek hegemony, interfere in other countries internal affairs, and engage in large-scale cyber theft and surveillance." Despite the liberal rhetoric framing a "community with a shared future in cyberspace," the more Beijing can affiliate cyber sovereignty with equitable and inclusive participation in cyberspace governance to developing countries, the wider its brand of digital authoritarianism will spread.

Continued: Beijing's Vision for Global Cyberspace Governance

Source: “携手构建网络空间命运共同体 (Jointly Build a Community with a Shared Future in Cyberspace),” *State Council Information Office*, 7 November 2022. <http://www.scio.gov.cn/zfbps/32832/Document/1732898/1732898.htm> (Chinese) http://english.scio.gov.cn/whitepapers/2022-11/07/content_78505694.htm (English).

Problems with the internet such as unbalanced development, unsound regulation, and unreasonable order are becoming more prominent. Cyber-hegemonism poses a new threat to world peace and development.

Certain countries are exploiting the internet and information technology as a tool to seek hegemony, interfere in other countries' internal affairs, and engage in large-scale cyber theft and surveillance, raising the risk of conflict in cyberspace.

Some countries attempt to decouple with others, and create schism and confrontation in cyberspace. The increasingly complex cybersecurity situation calls for more just, reasonable and effective cyberspace governance. Global threats and challenges in cyberspace necessitate strong global responses.

All countries have the right to formulate public policies, laws, and regulations on cyberspace in the context of their national conditions and international experience. No country should seek cyber hegemony; use the internet to interfere in other countries' internal affairs; engage in, incite, or support cyber activities that endanger other countries' national security, or infringe on other countries' key information infrastructure.

Notes:

[1] For more on the PRC's evolving cyberspace and data governance legislation see: “China's Evolving Data Governance Regime,” U.S.-China Economic and Security Review Commission, 26 July 2022. https://www.uscc.gov/sites/default/files/2022-07/Chinas_Evolving_Data_Governance_Regime.pdf

[2] For more on the Biden administration's articulation of the United States' vision for cyberspace governance see: “A Declaration for the Future of the Internet,” *The White House*, 28 April 2022. https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf