isu-conference.com

ISU

INTERNATIONAL SCIENTIFIC UNITY

COLLECTION OF SCIENTIFIC PAPERS

ISSUE №36

4TH INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

MODERN SCIENCE, ECONOMY AND DIGITAL INNOVATION

SEPTEMBER 10-12, 2025
BUCHAREST, ROMANIA

INTERNATIONAL SCIENTIFIC UNITY

4th International Scientific and Practical Conference
«Modern Science, Economy and Digital Innovation»

Collection of Scientific Papers

September 10-12, 2025
Bucharest, Romania

UDC 001(08)

Modern Science, Economy and Digital Innovation: Collection of Scientific Papers with Proceedings of the 4th International Scientific and Practical Conference. International Scientific Unity. September 10-12, 2025. Bucharest, Romania. 130 p.

ISBN 979-8-89704-986-8 (series)
DOI 10.70286/ISU-10.09.2025

The conference is included in the Academic Research Index ReserchBib International catalog of scientific conferences.

The collection of scientific papers presents the materials of the participants of the 4th International Scientific and Practical Conference "Modern Science, Economy and Digital Innovation" (September 10-12, 2025. Bucharest, Romania).

ISBN 979-8-89704-986-8 (series)

ISU
INTERNATIONAL SCIENTIFIC UNITY

Official site: https://isu-conference.com/

SECTION: INTERNATIONAL RELATIONS

DOI 10.70286/isu-10.09.2025.002

THE FEATURES OF THE PRC'S POLICY IN THE FIELD OF CYBER DIPLOMACY

Nepochatov Danylo
First-year Ph.D. student
Kuz Oleh
Doctor of Philosophy, Professor
Department of International Relations and Political Philosophy
Simon Kuznets Kharkiv National University of Economics, Ukraine

The approaches of democratic and authoritarian regimes to employing cyber diplomacy as a tool of cybersecurity differ significantly. The People's Republic of China, as an authoritarian state, views cyber diplomacy as a means of advancing the concept of digital sovereignty — a framework that legitimizes increased state control over the information space, both domestically and globally.

Cyberdiplomacy represents a manifestation of the new era in international relations, in which digital instruments function simultaneously as both means and ends, while political power increasingly derives from the capacity to operate, negotiate, and contest within cyberspace.

Two central institutions play a decisive role in shaping China's cyber policy: the Cyberspace Administration of China (CAC), established in 2011 under the State Council, and the Central Cyberspace Affairs Commission (CCAC), created in 2018 as a body directly subordinate to the Central Committee of the Communist Party of China. Both institutions are responsible for coordinating digital policy, including internet regulation, content oversight, and control over the use of digital technologies [1].

China's cyber policy is grounded in a regulatory framework that began to take shape in 2016 with the adoption of the Cybersecurity Law. This law was the first to grant formal legal status to the concept of cyber sovereignty, establishing key provisions such as mandatory data localization, compulsory security assessments for network operators, and the obligation for companies to cooperate closely with state authorities.

In 2021, the legal framework was significantly expanded with the enactment of the Data Security Law and the Personal Information Protection Law, both of which strengthened the state's capacity to control data flows and regulate the activities of technology companies [2].

On the international stage, China has been actively promoting an alternative model of global internet governance, distinct from Western approaches to cyberspace regulation. In addition to participating in United Nations processes, Beijing advances

its vision through groupings such as BRICS and the Shanghai Cooperation Organization (SCO), as well as through new institutional platforms like the World Internet Conference (WIC), which was established as an international organization in 2022 to foster digital cooperation and governance partnerships [3].

The ideological foundation of China's external cyber policy is articulated in its White Paper titled "Jointly Building a Community with a Shared Future in Cyberspace", first released in 2015 and updated most recently in 2022. The document outlines a governance model based on cyber sovereignty, asserting that the state has the legitimate authority to determine the rules governing its national segment of the internet. From this standpoint, national governments—not private corporations or transnational technical bodies—should bear primary responsibility for balancing the interests of citizens, businesses, and international partners in the digital domain.

An important role in China's international cyber positioning is played by the Shanghai Cooperation Organization (SCO). In 2009, the SCO member states signed an intergovernmental agreement in Yekaterinburg on cooperation in the field of international information security. The document defines "information security" in a broader sense than is typical in Western discourse: it considers not only interference with information systems as a threat, but also the content of information itself, particularly when it is deemed to endanger political stability or societal moral values. This interpretation is frequently criticized by democratic states, which view such a stance as a potential threat to freedom of expression and human rights [4].

Since 2014, China has hosted the World Internet Conference (WIC), which was formally established as a permanent international organization in 2022. Its declared objective is to build a "community with a shared future in cyberspace" — a concept that reflects China's ambition to develop an alternative vision of global digital governance distinct from Western models.

The WIC functions as a diplomatic platform for advancing China's model of cyber sovereignty, showcasing technological achievements by Chinese firms, and creating the appearance of international endorsement for its approach to internet regulation.

At the 2023 conference, China introduced the idea of "digital civilization", which envisions digital technologies serving the common good of all humanity and contributing to the formation of a global digital community. This narrative aligns closely with official policy documents — particularly the White Paper titled "Jointly Building a Community with a Shared Future in Cyberspace" — which emphasizes the role of the nation-state as the primary actor in managing its own internet space [3].

In September 2011, China, together with Russia and supported by Tajikistan and Uzbekistan, submitted a joint letter to the United Nations General Assembly proposing the development of an International Code of Conduct for Information Security. The document aimed to launch a global discussion, under the auspices of the UN, on the establishment of rules for responsible state behavior in cyberspace. The initiative reflected an attempt to formalize an alternative conception of cybersecurity, grounded in sovereignty and state oversight of information flows, on the international legal level [5].

The analysis above suggests that he proposed International Code of Conduct for Information Security reflected the collective vision of SCO member states regarding the principles of internet governance. At the core of this approach lies the notion of non-interference in the internal affairs of states within cyberspace and the recognition of cyber sovereignty as a cornerstone of political stability. In contrast, the dominant view in Western discourse prioritizes freedom of expression and access to information, which is why the SCO's proposed model is often seen as a threat to internet openness and fundamental rights.

This deep normative divide between authoritarian and democratic regimes has become a source of persistent tension surrounding China and Russia's initiatives within the UN framework. In essence, SCO states advocate for the creation of a separate international legal architecture that would regulate the digital domain based on principles of information control justified by national security considerations.

In this context, the cyber diplomacy of the People's Republic of China emerges not merely as an instrument of foreign policy, but as a deliberate projection of its domestic model of digital governance onto the global stage. At the heart of this strategy lies the principle of cyber sovereignty, which grants the state primacy in regulating the information environment — both within its borders and through international norms.

This approach treats the internet not as an open arena for exchange and pluralism, but as a sensitive domain intricately linked to national security, regime stability, and sovereign oversight. Through the creation of specialized platforms (such as the World Internet Conference), active engagement in multilateral forums (including the UN, SCO, and BRICS), and the development of an extensive legal framework (including the Cybersecurity Law, Data Security Law, and Personal Information Protection Law), China is shaping an alternative model of global digital governance — one that directly challenges liberal democratic conceptions of cyberspace as a space for free speech and decentralized participation.

References

1. Overview of Cybersecurity Landscape for Industrie 4.0. 2021. 10 p. URL: https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/China/policy-landscape-overview-cybersecurity.pdf?__blob=publicationFile&v=1 (date of access: 01.09.2025).
2. Personal Information Protection Law of the People's Republic of China : Public Law of 01.11.2021. URL: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (date of access: 02.09.2025).
3. Shanghai Cooperation Organisation. CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. URL: https://ccdcoe.org/organisations/sco/ (date of access: 03.09.2025).
4. Cary D. Community watch: China's vision for the future of the internet. 2023. 14 p. URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-

internet/#:~:text=Jointly%20Building%20a%20Community%20with,that%20the%20state%20decides%20the (date of access: 03.09.2025).
5. Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General : Letter of 13.01.2015 no. A/69/723. URL: https://digitallibrary.un.org/record/786846?ln=en&v=pdf (date of access: 02.09.2025).