eoss-conf.com

ISSUE
№103

EUROPEAN OPEN
SCIENCE SPACE

COLLECTION OF SCIENTIFIC PAPERS

6TH INTERNATIONAL
SCIENTIFIC
AND PRACTICAL
CONFERENCE

INNOVATIONS IN SCIENCE: FROM THEORETICAL FOUNDATIONS TO PRACTICAL IMPACT

AUGUST 31 – SEPTEMBER 2, 2026
ANTWERP, BELGIUM

EUROPEAN OPEN SCIENCE SPACE

Proceedings of the 6th International Scientific and Practical Conference

"Innovations in Science: From Theoretical Foundations to Practical Impact"

August 31 – September 2, 2026

Antwerp, Belgium

Collection of Scientific Papers

Belgium, 2026

UDC 01.1

Collection of Scientific Papers with the Proceedings of the 6th International Scientific and Practical Conference «Innovations in Science: From Theoretical Foundations to Practical Impact» (August 31 – September 2, 2026, Antwerp, Belgium). European Open Science Space. 2026.

ISBN 979-8-89704-968-4 (series)
DOI 10.70286/EOSS-31.08.2026

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

The conference is registered in the database of scientific and technical events of UkrISTEI to be held on the territory of Ukraine (Certificate No.557 dated 28.07.2026).

The materials of the collection are presented in the author's edition and printed in the original language. The authors of the published materials bear full responsibility for the authenticity of the given facts, proper names, geographical names, quotations, economic and statistical data, industry terminology, and other information.

ISBN 979-8-89704-968-4

EUROPEAN OPEN SCIENCE SPACE

DOI 10.70286/EOSS-31.08.2026.009.162-166

ДВОРІВНЕВА СУВЕРЕНІЗАЦІЯ КІБЕРПРОСТОРУ: МЕХАНІЗМ ЕКСПОРТУ КИТАЙСЬКОЇ РЕГУЛЯТОРНОЇ МОДЕЛІ У ГЛОБАЛЬНЕ УПРАВЛІННЯ ІНТЕРНЕТОМ

Непочатов Данило Олександрович
аспірант, викладач
Кафедра міжнародних відносин і політичної філософії
Харківський національний економічний
університет імені Семена Кузнеця
м. Харків, Україна

Анотація. У тезах досліджено механізм експорту китайської регуляторної моделі управління кіберпростором через поєднання правового, інституційного, технічного та інфраструктурного вимірів. Обґрунтовано, що КНР просуває концепцію кіберсуверенітету не лише як доктрину внутрішнього контролю, а як інструмент трансформації глобального управління інтернетом. Особливу увагу приділено взаємодії низхідного нормативно-правового вектора та висхідного інфраструктурно-стандартизаційного вектора, які взаємно підсилюють легітимність китайської моделі на міжнародному рівні.

Ключові слова: КНР, кіберсуверенітет, кібердипломатія, глобальне управління інтернетом, технічна стандартизація, «Цифровий шовковий шлях».

Вступ. Актуальність дослідження зумовлена посиленням конкуренції між різними моделями глобального управління інтернетом, у межах якої китайська концепція кіберсуверенітету дедалі активніше пропонується як альтернатива відкритій мультистейкхолдерній моделі. В умовах зростання ролі цифрової інфраструктури, технічних стандартів і міжнародно-правових норм аналіз механізмів поширення цієї моделі є важливим для розуміння сучасних трансформацій кібердипломатії та цифрової геополітики.

Мета та задачі дослідження. Метою дослідження є визначення механізму, за допомогою якого КНР експортує власну регуляторну модель кіберпростору в систему глобального управління інтернетом. Для досягнення цієї мети поставлено такі задачі: простежити еволюцію внутрішньої китайської політики кіберрегулювання; з’ясувати концептуальні відмінності між інформаційним суверенітетом і кіберсуверенітетом; проаналізувати правові та інституційні інструменти просування китайської моделі на міжнародному рівні; охарактеризувати роль технічної стандартизації та цифрової інфраструктури у формуванні залежностей держав-реципієнтів; визначити практичні імплікації цього процесу для України.

Результати дослідження та їх обговорення. Проведений аналіз дає підстави розглядати китайську стратегію суверенізації кіберпростору як дворівневий процес, у якому нормативно-правове оформлення та інфраструктурно-технічне втілення функціонують як взаємопов'язані елементи єдиного механізму.

Полеміку навколо глобального управління інтернетом прийнято зводити до протистояння двох нормативних моделей – мультистейкхолдерної, за якої правила виробляються за участю технічної спільноти, бізнесу та громадянського суспільства, і міжурядової, де єдиним легітимним суб'єктом нормотворчості визнається держава. Така оптика фіксує результат розбіжності, проте залишає поза увагою питання про те, у який спосіб альтернативна модель набуває міжнародної ваги. Пропонована теза полягає в тому, що Пекін оперує не в одному, а у двох регістрах одночасно: низхідному – через міжнародно-правову аргументацію та резолюційну активність, і висхідному – через технічні стандарти, протоколи й фізичну інфраструктуру. Ці вектори не паралельні, а взаємно легітимують один одного: інфраструктурна присутність створює коаліцію держав, готових підтримати нормативну позицію, а нормативні документи, своєю чергою, легалізують уже сформовані технологічні залежності.

Внутрішній контур як полігон нормотворення. Регуляторна траєкторія КНР демонструє послідовність, нетипову для реактивної політики. «Тимчасові положення про управління міжнародним підключенням комп'ютерних інформаційних мереж» (1996) зафіксували принципову настанову: глобальна мережа трактується не як простір вільного доступу, а як зовнішнє середовище, контакт із яким опосередковується державними «пунктами пропуску». Наступного року Міністерство громадської безпеки визначило перелік заборонених категорій онлайн-контенту, а з 1998 р. розпочалося будівництво «Золотого щита», зовнішній контур якого – Великий китайський файрвол почав функціонувати у листопаді 2003 р. Показово, що фільтрація від початку виконувала подвійну функцію: обмежуючи доступ до Google, Facebook і YouTube, вона одночасно формувала протекціоністську нішу для національних платформ.

Другий етап пов'язаний із приходом Сі Цзіньпіна та реакцією на викриття Едварда Сноудена, які продемонстрували вразливість китайської магістральної інфраструктури. Створення у 2014 р. Центральної керівної групи (з 2018 р. – Центральної комісії) з питань кіберпростору під особистим головуванням генерального секретаря ЦК КПК, а також наділення Адміністрації кіберпростору Китаю виключними регуляторними повноваженнями завершили переведення цифрової сфери з режиму технічного адміністрування у режим найвищої національної безпеки. Тріада законодавчих актів — про кібербезпеку (2017), про безпеку даних (2021) та про захист персональної інформації (2021) – перетворила декларативний принцип на систему виконавчих механізмів із виразним екстериторіальним потенціалом. Ключовим для подальшого аналізу є не хронологія як така, а її функція: кожен інструмент попередньо апробується на

аудиторії, що перевищує мільярд користувачів, і лише згодом пропонується зовнішнім партнерам як перевірене практикою рішення.

Концептуальна еволюція. Категоріальний апарат китайського підходу сформувався ще до появи самої доктрини. Гун Веньсян у 1998 р. увів поняття інформаційного суверенітету, прирівнявши несанкціоноване проникнення в національний інформаційний простір до порушення повітряного або морського кордону, та вказав на структурну асиметрію глобальних інформаційних потоків. Ця конструкція мала оборонний характер – вона захищала внутрішнє середовище від зовнішнього впливу. Натомість кіберсуверенітет, остаточно артикульований Сі Цзіньпіном на Всесвітній інтернет-конференції в Учжені (2015) та розгорнутий у Білій книзі про «спільноту зі спільною долею в кіберпросторі», є конструкцією наступальною: вона претендує не на автономію окремого сегмента, а на переформатування самих правил глобального порядку. Перехід від захисту кордону до проєктування архітектури — саме той зсув, що уможливлює експорт моделі.

Низхідний вектор: право. Нормативна складова реалізується передусім на майданчиках ООН. Формат Групи урядових експертів вичерпав себе у 2016–2017 рр., коли Пекін відмовився визнати автоматичну застосовність міжнародного гуманітарного права та права на самооборону до кіберпростору; за офіційною аргументацією про «легалізацію війни в мережі» проглядається прагматичний розрахунок — уникнути правової кваліфікації власних операцій. Ініційована Росією за підтримки КНР Відкрита робоча група (2018) змінила саму механіку переговорів, перенісши їх у середовище, де чисельна перевага держав Глобального Півдня має вирішальне значення; завершення її роботи у липні 2025 р. створенням постійного механізму ООН з кіберпитань закріпило цю перевагу інституційно. Ухвалення Конвенції ООН про кіберзлочинність (2024, відкрита для підписання у жовтні 2025 р.) як альтернативи Будапештській конвенції завершило цикл. Регіональним полігоном попередньої обкатки норм слугувала ШОС, чия угода 2009 р. закріпила розширене трактування інформаційної безпеки, що охоплює не лише технічні загрози, а й соціально-політичну стабільність.

Висхідний вектор: стандарти та інфраструктура. Паралельно доктрина втілюється у технічному шарі. Період головування Чжао Хоуліня в Міжнародному союзі електрозв'язку (2015–2022) супроводжувався тисячами стандартизаційних пропозицій китайських компаній. Найпоказовішим епізодом стала ініціатива «New IP» (2019–2020) – проєкт заміни архітектури TCP/IP, що передбачав можливість відключення окремих користувачів або сегментів на рівні протоколу. Відхилення пропозиції ITU-T у грудні 2020 р. не скасовує її діагностичного значення: ідеться про спробу вбудувати принцип керованості безпосередньо в логічну архітектуру мережі. Інфраструктурним продовженням є «Цифровий шовковий шлях» (з 2015 р.) та експорт рішень класу Safe City, які постачаються в комплекті з телекомунікаційним обладнанням і формують у

країнах-реципієнтах тривалу технологічну залежність, що конвертується у передбачувану дипломатичну підтримку.

Внутрішня суперечність моделі. Риторика рівноправного мультилатералізму співіснує з практикою вибудовування асиметричних відносин: критикуючи «цифрову гегемонію» Заходу, Пекін формує власні інституційні майданчики, просуває єдиний технологічний стандарт через національних постачальників і використовує економічні стимули для консолідації коаліції підтримки. Отже, пропонується не демонтаж ієрархії в управлінні кіберпростором, а заміщення її центру. Ця суперечність є водночас і найвразливішим місцем моделі: держави-реципієнти, які приймають аргумент про рівність суверенітетів, з часом стикаються з обмеженням власної технологічної автономії – залежністю від закритих стандартів, постачальницьких ланцюгів і сервісного обслуговування. Артикуляція саме цього розриву між обіцянкою та наслідком видається продуктивнішою лінією контраргументації, ніж апеляція до універсальних цінностей.

Практичні імплікації для України. По-перше, оцінюючи ініціативи в межах ООН, доцільно враховувати не лише їх текстуальний зміст, а й інфраструктурний контекст голосування держав-учасниць. По-друге, участь у технічній стандартизації (ITU-T, IETF) має розглядатися як самостійний напрям зовнішньої політики, а не як суто інженерна діяльність. По-третє, під час повоєнної відбудови цифрової інфраструктури вибір постачальників доцільно оцінювати з урахуванням довгострокових нормативних наслідків. По-четверте, аргументація на захист відкритої моделі виграє від переорієнтації з ціннісної риторики на демонстрацію практичних витрат фрагментації мережі – саме такий регістр є сприйнятливим для держав, що визначаються з позицією.

Висновки. Таким чином, ефективність китайської кібердипломатії пояснюється не окремими дипломатичними успіхами, а узгодженістю двох різнорівневих вимірів дії. Суверенізація «згори» без інфраструктурної опори залишалася б декларацією, а суверенізація «знизу» без правового оформлення – комерційною експансією. Їх поєднання становить механізм експорту китайської регуляторної моделі, що потребує адекватної аналітичної та політичної відповіді. Для України це означає необхідність уважного поєднання кібердипломатії, участі у технічній стандартизації та стратегічного контролю за вибором цифрових постачальників у процесі післявоєнної відбудови.

Список використаних джерел

1. Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization. (2009). SCO. URL: https://eng.sectsco.org/files/207508/207508
2. Bentley, D. (2020). Cyber espionage and international law. International Affairs, 96(2), 527-528. DOI: https://doi.org/10.1093/ia/iiaa042
3. Chandel, S., Jingji, Z., Yunnan, Y., Jingyao, S., Zhipeng, Z. (2019). The Golden Shield Project of China: A Decade Later-An in-Depth Study of the Great Firewall.

International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 111-119. DOI: https://doi.org/10.1109/CyberC.2019.00027
4. Chen, X., Gao, X. (2024). Norm diffusion in cyber governance: China as an emerging norm entrepreneur? International Affairs, 100(6), 2419-2440. DOI: https://doi.org/10.1093/ia/iiae237
5. China's Positions on International Rules-making in Cyberspace. (2021). UN. URL: https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-ENG.pdf

Proceedings of the 6th International Scientific
and Practical Conference
"Innovations in Science: From Theoretical Foundations to Practical Impact"
August 31 – September 2, 2026
Antwerp, Belgium

Contact details of the organizing committee:
European Open Science Space
E-mail: info@eoss-conf.com
URL: https://www.eoss-conf.com/

EUROPEAN OPEN
SCIENCE SPACE