ФІЛОСОФІЯ ТА ПОЛІТОЛОГІЯ В КОНТЕКСТІ СУЧАСНОЇ КУЛЬТУРИ
ISSN 2663-0265 (print) ISSN 2663-0273 (online)
Journal home page: https://fip.dp.ua/index.php/FIP

МІЖНАРОДНІ ВІДНОСИНИ

Данило Олександрович НЕПОЧАТОВ
Аспірант кафедри міжнародних відносин і політичної філософії,
Харківський національний економічний університет імені Семена Кузнеця,
пр. Науки, 9А, Харків, 61166, Україна

Danylo NEPOCHATOV
PhD Student at the Department of International Relations and Political Philosophy,
S.Kuznets KhNUE,
9A Nauky Ave., Kharkiv,
61166, Ukraine

E-mail: danylo.nepochatov@hneu.net, ORCID: https://orcid.org/0009-0006-5819-5842

УДК 327+341(510)

КІБЕРДИПЛОМАТІЯ КИТАЮ ЯК ІНСТРУМЕНТ РЕВІЗІЇ ГЛОБАЛЬНОГО ЦИФРОВОГО ПРОСТОРУ: ПОЛІТИКО-ПРАВОВИЙ АНАЛІЗ

Received 18 March 2026; revised 21 April 2026; accepted 10 May 2026
DOI: 10.15421/352624 дата публікації: 30.05.2026

Анотація

Стаття досліджує взаємозв'язок між внутрішньою технічною, інституційною та нормативною архітектурою кіберпростору КНР і зовнішньополітичною стратегією Пекіна у сфері глобального управління інтернетом. Метою статті є з'ясувати, яким чином внутрішня технічна, інституційна та нормативна основа китайського інтернету формує і живить зовнішньополітичну стратегію КНР у сфері глобального управління кіберпростором. Предметом дослідження є механізми взаємодії між внутрішньою архітектурою кіберпростору КНР та зовнішньополітичною кібердипломатичною стратегією Пекіна. Дослідження застосовує системний та історико-генетичний підходи, порівняльний аналіз міжнародно-правових документів і концептуальний інструментарій теорії сек'юритизації Копенгагенської школи. Наукова новизна полягає у доведенні того, що внутрішня цифрова інфраструктура КНР функціонує як середовище апробації норм і моделей, які Пекін згодом просуває на міжнародній арені. Дослідження встановлює, що еволюція китайської інтернет-політики від «Тимчасових положень» 1996 року до тріади кіберзаконів 2017-2021 років формує правовий каркас доктрини кіберсуверенітету. Виявлено, що концептуальний перехід від «інформаційного суверенітету» до «кіберсуверенітету» відображає зміну стратегічної позиції Пекіна – від оборонної ізоляції до наступального формування глобального нормативного порядку. Проаналізовано багаторівневу кібердипломатичну стратегію КНР на майданчиках ООН, ШОС, ITU та Всесвітньої інтернет-конференції, а також інфраструктурний вимір через ініціативу «Цифровий шовковий шлях». Результати дослідження мають практичне значення для формування позиції України в міжнародних дискусіях щодо управління кіберпростором, зокрема в контексті протидії просуванню авторитарних моделей цифрового регулювання державами – союзниками КНР.

Ключові слова: КНР, кіберпростір, кіберсуверенітет, кібердипломатія, Великий файрвол, глобальне управління інтернетом.

CHINA'S CYBER DIPLOMACY AS AN INSTRUMENT FOR REVISING THE GLOBAL DIGITAL SPACE: A POLITICAL AND LEGAL ANALYSIS

Abstract

The article examines the relationship between the internal technical, institutional, and normative architecture of China's cyberspace and Beijing's foreign policy strategy in global internet governance. The article aims to examine how the internal technical, institutional, and normative foundations of the Chinese internet shape and sustain Beijing's foreign policy strategy in global cyberspace governance. The subject of the study is the interaction mechanisms between the internal architecture of China's cyberspace and Beijing's foreign policy cyberdiplomacy strategy. The study applies a systemic and historical-genetic approach, comparative analysis of international legal documents, and the conceptual framework of the Copenhagen School securitization theory. The scientific novelty lies in demonstrating that China's internal digital infrastructure functions as an environment for testing norms and governance models that Beijing subsequently promotes on the international stage. The study establishes that the evolution of Chinese internet policy from the 1996 Interim Regulations to

the triad of cyber laws enacted between 2017 and 2021 constructs the legal foundation of the cybersovereignty doctrine. The research reveals that the conceptual shift from "information sovereignty" to "cybersovereignty" reflects Beijing's strategic transition from defensive isolation toward an assertive effort to shape the global normative order in cyberspace. The study traces China's multilevel cyberdiplomacy across UN negotiation formats [GGE and OEWG), the Shanghai Cooperation Organisation, the International Telecommunication Union, and the World Internet Conference, and identifies the Digital Silk Road as the infrastructure dimension of this strategy. The findings carry practical significance for Ukraine in developing a clear position within international cyberspace governance discussions, particularly in countering the promotion of authoritarian digital regulation models by states aligned with China.

Keywords: ***PRC, cyberspace, cyber sovereignty, cyber diplomacy, Great Firewall, global internet governance.***

Постановка проблеми.

Сьогодні кіберпростір є одним із важливих арен протиборства між державами. За умов прискореної цифровізації суспільств питання про те, хто і на яких засадах контролює інтернет, набуває не лише технічного, а й глибоко геополітичного значення, адже підходи регулювання цифрової сфери демократій та авторитарних країн відрізняються. Урядам держав з різними політичними режимами важливо визначати не лише технічні стандарти, а й політичні, які конструюють «правильний» інтернет. Саме у нормативній конкуренції Китайська Народна Республіка посідає унікальне місце: держава, що збудувала найбільш розвинену у світі систему суверенного інтернету, водночас перетворилася на найбільш послідовного і впливового актора, який прагне поширити ці принципи на рівень міжнародних норм.

Виходячи із зазначеного, **метою** статті є з'ясувати, яким чином внутрішня технічна, інституційна та нормативна архітектура кіберпростору КНР формує зовнішньополітичну стратегію Пекіна у сфері глобального управління інтернетом та дослідити концепцію кіберсуверенітету як спосіб втілення внутрішню цифрову політику Китаю та його кібердипломатичну активність на міжнародній арені. Для реалізації мети дослідження було проаналізовано еволюцію законодавчого та інституційного забезпечення китайського кіберпростору від першого підключення до інтернету до ухвалення тріади кіберзаконів 2017-2021 років; розкрито концептуальну трансформацію від поняття «інформаційного суверенітету» до доктрини «кіберсуверенітету»; проаналізовано багаторівневу кібердипломатичну стратегію КНР на ключових міжнародних майданчиках – ООН, ШОС, МСЕ та WIC; простежено логіку взаємозв'язку між внутрішньою цензурною практикою та зовнішньополітичним просуванням альтернативної моделі управління глобальним інтернетом.

Актуальність теми визначається низкою ключових подій 2020-2026 років: накладення санкцій Сполученими Штатами Америки на виробників китайського телекомунікаційного обладнання та напівпровідників; ухваленням Конвенції ООН про кіберзлочинність – довгострокового дипломатичного проєкту Пекіна і Москви; приєднання до країн BRICS Індонезії, що надає його основним членам Росії та Китаю залучення в орбіту впливу великого та динамічного гравця південноазійського ринку. Ці події наочно демонструють, що Захід поступово втрачає свій вплив у різних куточках світу. Натомість КНР через різні інституції та власну економічну привабливість залучає все більше країн. Це дозволяє Пекіну пропонувати урядам країн власний погляд на технологічну та політичну архітектуру кіберпростору.

Методологія дослідження ґрунтується на поєднанні системного та історико-генетичного підходів, порівняльного аналізу міжнародно-правових документів, концептуального аналізу політичних доктрин та інструментарію конструктивістської теорії міжнародних відносин. Системний підхід дозволив розглянути кіберпростір КНР як цілісну архітектуру взаємопов'язаних технічних, інституційних та нормативних елементів. Історико-генетичний метод забезпечив простеження еволюції китайської інтернет-політики від законодавчих актів 1996–1997 років до сучасних кібердипломатичних ініціатив. Порівняльний аналіз застосовувався для зіставлення китайської моделі кіберсуверенітету із західною концепцією мультистейкхолдеризму, а також для оцінки нормативних позицій держав у рамках переговорних форматів ООН. Концептуальний аналіз первинних джерел – законодавчих актів, стратегічних документів, офіційних позиційних документів КНР – дозволив реконструювати внутрішню логіку китайського підходу до управління кіберпростором. Теорія сек'юритизації Копенгагенської школи слугувала

аналітичною рамкою для інтерпретації переведення кіберпростору до категорії питань національної безпеки за лідерства Сі Цзіньпіна. Сукупність цих методів дозволила розкрити механізм конвертації внутрішньої цифрової практики КНР у зовнішньополітичний ресурс кібердипломатії.

Аналіз останніх досліджень і публікацій. Технічну та політичну логіку Великого файрволу детально розкрито у дослідженнях Ґарі Кінга, Дженніфер Пан і Марґарет Робертс. У статті ««Як цензура в Китаї дозволяє критику уряду, але пригнічує колективне вираження поглядів» [King et al. 2013] вони встановили, що цензура блокує насамперед контент, здатний мобілізувати колективні дії, а не просту критику влади. Робертс розширила цей аналіз у монографії «Цензура: відволікання та перенаправлення всередині Великого китайського файрволу» [Wasserstrom, 2018], виокремивши три механізми цензурного впливу: страх, тертя та затоплення [fear, friction, flooding]. Технічні аспекти – IP-блокування, DNS-фільтрацію та глибоку перевірку пакетів [DPI] – систематизовано у роботі Чандела [Chandel et al. 2019]. Академічну інтерпретацію концепції кіберсуверенітету запропонували Рогір Кременс [Creemers, 2024], а Тім Стівенс застерігає від уявлення про монолітність китайської позиції [Stevens 2026].

Метою статті є дослідити особливості кіберпростору КНР крізь призму кібердипломатії – розгляд того, як внутрішня технічна, інституційна і нормативна основа китайського інтернету формує і живить зовнішньополітичну стратегію Пекіна у сфері глобального управління кіберпростором.

Виклад основного матеріалу.

Перший контакт Китаю з глобальним інтернетом відбувся 14 вересня 1987 року, коли дослідники Пекінського інституту комп'ютерних технологій та застосунків надіслали електронний лист до Університету Карлсруе зі словами «Через Велику стіну ми можемо досягти кожного куточка світу» [Jiang 2025]. Справжнє комерційне підключення відбулося у 1994р., однак вже 1996-го Державна рада ухвалила «Тимчасові положення КНР про управління міжнародним підключенням комп'ютерних інформаційних мереж» – перший законодавчий акт у сфері інтернет-цензури [Creemers 1996]. Суть документу полягає у закріпленні на законодавчому рівні принципу, за яким глобальний інтернет не є відкритим простором вільного доступу для громадян, а розглядається як зовнішнє середовище. Доступ до цього середовища має здійснюватися виключно через суворо контрольовані державою цифрові «пункти пропуску». Саме цей документ заклав правові основи для впровадження комплексної системи інтернет-цензури «Золотого щита» (система внутрішнього нагляду) та «Великого китайського файрволу» (зовнішній кіберкордон).

У 1997 р. Міністерство громадської безпеки оприлюднило документ «Заходи з управління та захисту безпеки міжнародних з'єднань комп'ютерних інформаційних мереж», який фактично заборонив дев'ять категорій онлайн-контенту [Creemers 1997]. Ці два документи засвідчують: КНР від початку розглядала інтернет як середовище, що потребує суверенного управління та контролю. Центральним проєктом цього етапу стало будівництво «Золотого щита», розпочате 1998 р. Міністерством громадської безпеки і впроваджене у 2003 р. Його цензурний підпроєкт – «Великий файрвол» (GFW) – запрацював у листопаді 2003 р. Технологічна інфраструктура проєкту частково будувалася з використанням апаратного забезпечення Cisco Systems, що згодом стало предметом критики у Конгресі США [Tang, Huhe 2016]. Фактично GFW поєднав ідеологічний контроль із економічним протекціонізмом: блокуючи Google, Facebook і YouTube, він водночас створив захищений інкубатор для власних технологічних гігантів – Baidu, Alibaba і Tencent. Фізична мережева архітектура будувалася таким чином, щоб централізувати весь міжнародний трафік через обмежену кількість контрольованих шлюзів – подібно до «митниці на цифровому кордоні», де держава могла інспектувати і фільтрувати потоки інформації.

Перший великий етап розвитку (1994-2013) китайського кіберпростору правильніше характеризувати крізь призму парадигми «інформатизації»: Політбюро Комуністичної партії Китаю в жовтні 2000 року на 5-му пленумі ЦК КПК 15-го скликання підняла проблему цифровізації на найвищий стратегічний рівень. Тодішній лідер КНР Цзян Цземінь у рамках занепокоєння КПК цифровізацією висунув у підсумковій доповіді 2002 року фундаментальну формулу, яка визначила політику на десятиліття: «Інформатизація має стимулювати індустріалізацію, а індустріалізація – сприяти інформатизації» [Jiang 2002]. Саме за цей період були створені національні технологічні гіганти званої трійки BAT [Baidu, Alibaba, Tencent], які заповнили вакуум, утворений першими діями «Великого файрволу». Справжнім вибухом поширення інтернету серед китайського населення відбулось в КНР за лідерства Ху Цзіньтао у

2003-2013 роках. За даними звітів Китайського інформаційного центру мережі Інтернет (CNNIC) у цей період кількість інтернет-користувачів зросла з 80 до понад 600 млн [*Statistical Report on Internet Development in China* 2013]. У цей же час відбувся перехід до так званої епохи Web 2.0, характеристика якої є генерація приватними користувачами контенту. До того ж, зростання аудиторії користувачів інтернету у 8 разів змусило владу вдатися до витонченіших методів цензурування інтернету як впровадження алгоритмічної цензури, глибокого аналізу пакетів (DPI) та систем деанонімізації.

З початком президенства Сі Цзіньпіна у 2012 році настав другий етап трансформації китайського інтернету. Дослідники німецького інституту вивчення КНР Катя Дрінгхаузен і Джон Лі, стверджують, що одним з каталізаторів трансформації підходів адміністрації Сі Цзіньпіна до управління інтернетом стали події, пов'язані з викриттям колишнього працівника ЦРУ та Агентства національної безпеки Едварда Сноудена [Drinhausen Lee 2021]. Викриття Сноудена стали для Пекіна шоком, оскільки продемонстрували, що американські спецслужби мали доступ до магістральних маршрутизаторів Китаю, серверів університетів та телекомунікаційних компаній. Уряд КНР відреагував на це викриття державною кампанією «De-IOE» – поступове витіснення з державного та банківського секторів Китаю американських технологічних гігантів: серверів IBM, баз даних Oracle та систем зберігання даних EMC на користь національних аналогів як Alibaba, Huawei (2021).

Другим важливим нововведенням в управлінні кіберпростором епохи Сі Цзіньпіна стало заснування у 2014 році так звану керівну групу Центральну комісію з кіберпростору та інформатизації (ССАС), яка у 2018 році під час масштабної інституційної реформи була офіційно реорганізовано в Центральну комісію з питань кіберпростору, що закріпило його постійний статус на вершині партійної ієрархії. Безпрецедентним кроком стало те, що комісію особисто очолив Генеральний секретар ЦК КПК Сі Цзіньпін. За оцінкою нідерландського дослідника Рогіра Кременса [Creemers 2024] та американського дослідника Сеґала [Segal 2016], це перевело питання кіберпростору з категорії технологічного чи економічного адміністрування у вимір вищої національної безпеки. Фактично задачею ССАС є формування політичної волі партії. На думку Кременса персональне головування Сі Цзіньпіна в ССАС є класичним прикладом «секьюритизації» – переведення проблеми кіберпростору до категорії екзистенційних загроз через словесні конструкти, які цьому сприяють [Creemers 2024]. Якщо раніше інтернет-регулювання розглядалося як технічно-економічне адміністрування, то після 2014 р. воно набуло статусу питання національної безпеки. Безпосереднє регулювання кіберпростору здійснює Адміністрації кіберпростору Китаю (САС). Цей орган був заснований у 2011 році, однак реальних повноважень набув лише у 2014 році, коли китайський уряд наділив САС ексклюзивними правами на регулювання всього інтернет-контенту. САС стала єдиним виконавчим апаратом (канцелярією) нової партійної групи. Фактично ці два органи – САС та ССАС створюють дворівневу централізовану архітектуру управління де головним є Центральна комісія з питань кіберпростору (ССАС), а її виконавчим органом – Адміністрація кіберпростору Китаю (САС) [Horsley 2022].

Законодавчий розвиток в КНР поняття кібersуверенітету бере свій початок з 2016 року, коли Адміністрація кіберпростору Китаю (САС) оприлюднила Національну стратегію безпеки кіберпростору [National Cyberspace Security Strategy 2016]. Для Пекіна це був перший подібний документ з регулювання кіберпростору. У стратегії кіберсуверенітет визначений як перший принцип державної кіберполітики. Фактично Китай підірвав усталений Європою та США підхід до управління інтернетом за незалежної участі зацікавлений організацій та корпорацій. Проголошення кіберсуверенітету як державної доктрини отримало законодавче підкріплення через ухвалення тріади ключових правових актів. Закон про кібербезпеку [Cybersecurity Law of the People's Republic of China 2017] запровадив обов'язкову реєстрацію під реальним іменем, вимогу локалізації даних для операторів критичної інформаційної інфраструктури та механізм огляду безпеки технологічної продукції. Закон про безпеку даних [Data Security Law of People's Republic of China 2021] запровадив національну систему класифікації даних з екстериторіальним застосуванням. Закон про захист персональних даних закріпив принцип згоди та обмеження транскордонної передачі даних [Personal Information Protection Law of the People's Republic of China 2021]. У сукупності ці три документи формують правовий каркас, які перетворюють концептуальні заяви про кіберсуверенітет на виконавчі механізми, що регулюють весь процес цифрової діяльності.

У академічних колах КНР ідеї необхідності

контролю над інтернетом розпочався з 1998 року. Доктринальним ядром цієї системи є концепція кіберсуверенітету, теоретиком якої вважають китайського науковця Гун Веньсяна. Веньсян у статті 1998 року «Міжнародна комунікація в інформаційну епоху: нові проблеми міжнародних відносин» запропонував ряд концепцій та визначень, які фактично характеризують сучасну китайську політику у кіберпросторі. Автор запроваджує концепт «інформаційного суверенітету» (попередника кіберсуверенітету) – право держави контролювати поширення інформації, наприклад, право видавати закони і керувати новинами та пресою. Веньсян стверджує, що спроби Заходу порушити інформаційний простір не є боротьба за свободу слова, а пряме порушення державного суверенітету, що є схожим на порушення повітряного чи морського простору. До того ж, на думку Веньсяна, ідея вільного потоку інформації в інтернеті, якої дотримуються західні країни неможлива, адже розвинені країни [20% населення] контролюють 80% світового інформаційного потоку [Wenxiang 1998]. Відповідно, «глобалізація» мережі в західному розумінні призводить до нерівноправного, «пасивного обміну», коли сильні держави нав'язують свої цінності слабкішим. Канадаська дослідниця Ваншу Конг та нідерландський дослідник Йоннас Тумфарт доповнюють цей аналіз постколоніальним виміром: концепція інформаційного суверенітету виникла як реакція Пекіна на американську цифрову гегемонію – що безпосередньо перегукується з аргументами Гун Веньсяна про нерівномірний розподіл інформаційних потоків [Cong, Thumfart 2022].

Можемо констатувати, що інформаційний суверенітет був оборонною реакцією епохи традиційних медіа [спробою закрити країну від чужих ідей], то кіберсуверенітет – це наступальна, всеосяжна стратегія епохи великих даних та когнітивних війн. Остаточно закріпив поняття кіберсуверенітету Сі Цзіньпін на Другій Всесвітній конференції з інтернету в Учжені в 2015 році: «Ми повинні поважати право кожної країни самостійно обирати свій шлях розвитку інтернету, модель управління мережею, публічну політику в інтернеті, а також право на рівноправну участь у міжнародному управлінні кіберпростором» [Jinping 2015]. Бачення слів Сі дістало системне відображення у Білій книзі уряду КНР «Спільне будівництво спільноти зі спільною долею в кіберпросторі», уперше оприлюдненій у 2015р. та оновленій у наступні роки, зокрема у 2022 р. Документ формує концептуальну основу китайського підходу до цифрової політики та репрезентує бачення КНР щодо альтернативної моделі глобального управління інтернетом. У центрі цього підходу перебуває теза про те, що держава має пріоритетне право визначати правила функціонування власного національного сегмента мережі, оскільки це розглядається як складова державного суверенітету [White Paper 2022]. Таким чином, Пекін постійно підкреслює, що всі держави повинні мати рівне право голосу у виробленні міжнародних норм і стандартів у цифровій сфері. За такої логіки саме державні інституції, а не приватні корпорації чи технічні міжнародні структури, наділяються головною відповідальністю за узгодження інтересів суспільства, бізнесу та зовнішніх акторів.

Внутрішня політика КНР формує кібердипломатичну активність Пекіна на міжнародній арені. Китай перетворив внутрішню потребу в цензурі та контролі на глобальну дипломатичну доктрину, протиставляючи західній моделі відкритого інтернету ідею державного мультилатералізму, де кожна держава має абсолютне право на ізоляцію та управління своїм національним сегментом мережі.

Закріпленням прагнень КНР вибудувати альтернативну Заходу модель управління кіберпростором відобразилась в Міжнародній стратегії співробітництва в кіберпросторі 2017-го року. Стратегія пропонує наступні підходи: принцип суверенітету як перший і головний стовп зовнішньої політики Китаю в цифровій сфері; необхідність посилення ролі ООН у глобальному управлінні інтернетом, а не недержавні актори як пропонує західна модель; держави зобов'язані не порушувати суверенітет інших, не вчиняти актів ворожості за допомогою ІКТ та не втручатися у внутрішні справи через цифрові мережі [International Strategy of Cooperation on Cyberspace 2017].

Наступним кроком відстоювання КНР альтернативної Заходу моделі інтернету відобразилось у документі, поданому у 2021 році в комітет роззброєння ООН «Погляди КНР на застосування принципів суверенітету у кіберпросторі», повторюється та посилюється твердження вищезазначеної стратегії 2017 року. У документі державний суверенітет у кіберпросторі визначається як юридично обов'язковим принципом згідно з міжнародним правом; держави, незалежно від розміру чи багатства, мають право на рівноправну участь у міжнародних кіберспрвах; деталізується право через три види юрисдикції: законодавчу (право

видавати закони для захисту безпеки), адміністративну (право керувати ресурсами) та судову. Важливим визначенням у цьому документі є класифікація кіберпростору на рівні, над якими держава має здійснювати суверенітет: фізичний рівень: юрисдикція над інфраструктурою та базовими послугами на своїй території; логічний рівень: незалежне встановлення технічних стандартів та протоколів зі збереженням інтероперабельності інтернету; прикладний рівень: право регулювати поширення онлайн-контенту та обмежувати інформацію, що шкодить суспільним інтересам або національній безпеці; соціальний рівень: юрисдикція над користувачами та платформами для формування відповідного соціального середовища [China's Views on the Application of the Principle of Sovereignty in Cyberspace 2021]. До того ж, КНР намається піддати сумніву західну модель мультистейкхолдеризму управління інтернетом, де рішення ухвалюють не центральні уряди країн, а організації та корпорації. Натомість просуває модель мультилатералізму, де управління здійснюється виключно на міжурядовому рівні, а ООН є центральним і єдиним легітимним майданчиком для розробки правил.

Для КНР пошук союзників у просуванні власного порядку денного та протистоянні з Заходом здійснюється через різні міжнародні майданчики. Одним з таких майданчиків є Організація Об'єднаних Націй, яка стала для Китаю головною ареною кібердипломатичної діяльності та просування ідей регулювання кіберпростору. Для втілення задумів КНР розгорнула масштабну дипломатичну боротьбу, яка відстоює нові правила, які б дозволили державам легально контролювати інформаційні потоки та цензурувати контент. Західні країни, як ми зазначали вище, історично вважають, що на інтернет автоматично поширюється чинне міжнародне право, а керувати ним мають усі зацікавлені сторони. Ця нормативна битва розгорнулася у трьох ключових переговорних форматах.

Спочатку головні дискусії велися у вузькому форматі Групи урядових експертів ООН. На ранніх етапах група працювала успішно і навіть ухвалила 11 добровільних правил поведінки країн в інтернеті. Однак у 2016-2017 роках процес зазнав краху: Китай навідріз відмовилися визнавати, що на кіберпростір поширюється міжнародне гуманітарне право і право на самооборону. Пекін аргументував це тим, що такі норми нібито «легалізують війну в інтернеті». Проте реальна стратегічна логіка Китаю була іншою: він не хотів визнавати кібератаки зброєю, щоб уникнути юридичної відповідальності за власні масштабні хакерські операції [Soesanto 2017].

Зрозумівши обмеженість експертного формату GGE, у 2018 році Росія за підтримки Китаю ініціювала створення Відкритої робочої групи [OEWG], яка передбачала участь для всіх 193 держав-членів ООН. Це дозволило заглушити голоси заходу серед інших країн, яким дуже сподобалася китайська ідея державного контролю над інтернетом. У липні 2025 року група завершила роботу черговою перемогою Китаю: було створено постійний глобальний механізм ООН з кіберпитан [Pytlak 2025]. Це дозволить Пекіну і надалі використовувати свою перевагу в кількості голосів, блокуючи західні ініціативи. Стратегічним тріумфом китайської кібердипломатії стало ухвалення нової Конвенції ООН про кіберзлочинність [прийнята наприкінці 2024 року, відкрита для підписання у жовтні 2025-го]. Документ, який починався як російська ініціатива, був підтриманий Пекіном як альтернатива західній Будапештській конвенції [United Nations Convention against Cybercrime 2024].

Фактичним напрацювання ідей китайського управління інтернетом та їх апробація для міжнародної арени стала Шанхайська організація співробітництва (ШОС), де вперше було сформульовано підхід до міжнародної інформаційної безпеки, близький до сучасного розуміння кіберсуверенітету. Важливим документом у цьому контексті є «Угода про співробітництво у забезпеченні міжнародної інформаційної безпеки», яка закріпила широке трактування інформаційної безпеки, включаючи загрози не лише технічному функціонуванню інформаційних систем, а й соціально-економічній та суспільно-політичній стабільності держави [SCO 2009]. У межах такого підходу загроза пов'язується не лише з кібератаками на інфраструктуру, а й із поширенням інформаційного контенту, який може розглядатися як дестабілізуючий. Саме цим підхід ШОС відрізняється від більш вузького, переважно технічного розуміння кібербезпеки, характерного для демократичних держав. У цьому сенсі ШОС відіграла важливу роль у просуванні та розробці альтернативного нормативного бачення інформаційної безпеки на рівні ООН, ідеї яких відобразились у зазначених вище «Міжнародному кодексі поведінки у сфері інформаційної безпеки», поданому до Генасамблеї у 2011 році [UN 2011] та оновленому у 2015р. [UN 2015]. Даніель Флонк стверджує, шо роль ШОС у поширенні норм

авторитарного управління інтернетом. Фактично, на думку Флонк, Китай і Росія застосовують «стратегію послідовності»: спочатку консолідують нормативну позицію у регіональних форматах ШОС і ШОС+, а потім просувають її на рівень ООН. При цьому контроль над контентом подається не як готовий стандарт, а як «норма, що формується». Це знижує опір з боку інших держав і полегшує поступове прийняття [Flonk 2021]. Дослідники Citizen Lab [Університет Торонто] стверджують, що Кодекс поведінки 2011 і 2015 років суттєво розширює концепцію суверенітету ШОС на цифровий простір і викликає серйозні питання у сфері прав людини [McKune 2015].

Іншим важливим майданчиком для КНР є міжнародний союз електрозв'язку [ITU], де китайський уряд намагається перетворити доктрину кіберсуверенітету на технічні стандарти. За дослідженням італійського дослідника Джанлуїджі Негро, Китай системно нарощував вплив в ITU з 2015 по 2022 рр., коли посаду Генерального секретаря займав Чжао Хоулінь – перший громадянин КНР на чолі цієї організації [Negro 2020]. Протягом цього часу Huawei подала тисячі стандартизаційних пропозицій, зокрема щодо 5G та систем розпізнавання облич на базі ШІ. Найбільш резонансною стала ініціатива «New IP»: у 2019-2020 роках Huawei подали до сектору стандартизації МСЕ – ITU-T проєкт заміни базового протоколу TCP/IP новою архітектурою. Розслідувачі Financial Times попереджали про вбудовану функцію «вимкнення» [shut-up command], що могла б легалізувати відключення окремих користувачів або цілих сегментів мережі на рівні протоколу [Murgia, Gross 2020]. ITU-T відхилив пропозицію у грудні 2020 р., однак сам цей епізод наочно демонструє: Китай прагне поширити принципи кіберсуверенітету не лише на рівні дипломатичних декларацій, а й на рівні фізичної та логічної архітектури глобального інтернету – тобто здійснює «суверенізацію» знизу, через стандарти, паралельно з «суверенізацією» зверху, через міжнародне право.

Якщо попередні міжнародні майданчики як ООН або ШОС вимагають компромісів та дипломатичності, то вже згадана вище Всесвітня інтернет-конференція [WIC] також відома як Учженський саміт була започаткована Пекіном у 2014 році як домашня арена монопольного формування порядку денного китайської кібердипломатії.

WIC виконує три стратегічні функції:

1. Інституційна альтернатива західним форматам.

2. Вітрина, де Китай щорічно демонструє світові свою візію управління інтернетом.

3. Експорт китайської моделі на Глобальний Південь, адже на саміт в Учжень масово запрошують представників країн Африки, Азії та Латинської Америки.

Дипломатична активність КНР на майданчиках ООН і просування її підходів через Всесвітню інтернет-конференцію (WIC) супроводжувалися практичними інструментами їх реалізації. Одним із таких інструментів стала ініціатива «Цифровий шовковий шлях» [Digital Silk Road, DSR], започаткована у 2015 р. як технологічний компонент ширшого проєкту «Один пояс, один шлях». Якщо в офіційних документах, адресованих ООН, зокрема в Позиційному документі 2021р. [China's Positions on International Rules-Making in Cyberspace 2021] Китай обґрунтовує право держави здійснювати контроль над фізичною інфраструктурою кіберпростору, то DSR створює практичні умови для реалізації такого підходу, зокрема в країнах Глобального Півдня, де пролягає його маршрут. Через інвестиції у прокладання підводних кабелів, розвиток мереж 5G за участю китайських техногігантів Huawei і ZTE, а також будівництво дата-центрів Китай не лише розширює свою технологічну присутність, а й поширює власне бачення державного управління цифровим середовищем.

Особливе значення в цьому контексті мають рішення, що експортуються в межах DSR під назвою «Безпечне місто» (Safe City). Разом із телекомунікаційною інфраструктурою держави-отримувачі отримують системи відеоспостереження, технології розпізнавання обличчя і засоби моніторингу та фільтрації трафіку. Це посилює спроможність урядів контролювати національний інформаційний простір і розширює їхні можливості у сфері цифрового нагляду [Brookings 2020]. Водночас таке технологічне співробітництво формує довготривалу залежність від китайських рішень, стандартів і постачальників. У політичному вимірі це має і зовнішньополітичні наслідки. Країни, залучені до проєктів DSR, нерідко виявляються більш схильними підтримувати китайські підходи в міжнародних дискусіях щодо управління кіберпростором, зокрема на майданчиках Відкритої робочої групи ООН (OEWG) та Міжнародного союзу електрозв'язку (МСЕ). У такий спосіб технологічна співпраця стає не лише економічним, а й дипломатичним ресурсом китайської кібердипломатії.

Висновки.

По-перше, кіберпростір КНР є не стільки технічним середовищем, скільки інституційно сконструйованим політичним простором. Від перших законодавчих актів 1996-1997 років до тріади кіберзаконів 2017-2021 років Пекін послідовно вибудовував правовий каркас, що перетворює глобальну мережу на керований національний ресурс. Ця система не є реакцією на зовнішні загрози – вона є проактивною архітектурою суверенного цифрового простору, спроєктованою з моменту першого підключення до інтернету.

По-друге, еволюція концептуальної основи від «інформаційного суверенітету» до «кіберсуверенітету» відображає якісний стрибок у стратегічному мисленні Пекіна. Якщо перша концепція була оборонною – захист від чужих ідей та інформаційних потоків – то друга є наступальною: це всеосяжна стратегія, що претендує на формування глобального нормативного порядку в цифровій сфері. Цей перехід збігся зі зміною лідерства та переведенням кіберпростору до категорії питань найвищої національної безпеки.

По-третє, кібердипломатична стратегія КНР характеризується багаторівневістю та взаємодоповнюваністю інструментів. Нормативний вимір реалізується через ООН (GGE, OEWG), де Китай блокує небажані прецеденти та просуває власні резолюції; організаційний – через ШОС як регіональний полігон апробації норм та WIC як власну інституційну платформу; технічний – через ITU та ініціативу «New IP», що намагається вбудувати принципи суверенітету безпосередньо в архітектуру протоколів; інфраструктурний – через «Цифровий шовковий шлях», що створює технологічну залежність і конвертує її в дипломатичну підтримку. Сукупність цих інструментів утворює цілісну стратегію «суверенізації» кіберпростору одночасно знизу (через стандарти та інфраструктуру) і згори (через міжнародне право).

По-четверте, ключовою суперечністю китайського підходу залишається напруга між проголошеним принципом рівноправного мультилатералізму та фактичною асиметрією впливу. Пекін послідовно критикує «цифрову гегемонію» Заходу, водночас самостійно формуючи власні міжнародні організації, просуваючи єдиний технологічний стандарт через Huawei та ZTE і використовуючи економічні стимули DSR для консолідації коаліції підтримки серед країн Глобального Півдня. Таким чином, китайська модель пропонує не відмову від гегемонії, а зміну.

Бібліографічні посилання / References

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

Bentley, D. (2020). Cyber espionage and international law. *International Affairs*, 96(2), 527-528. DOI: https://doi.org/10.1093/ia/iiaa042

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

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

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

China's Views on the Application of the Principle of Sovereignty in Cyberspace. (2021). *UNDP.* URL: https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf

Cong, W., Thumfart, J. (2022). A Chinese Precursor to the Digital Sovereignty Debate: Digital Anti-Colonialism and Authoritarianism from the Post-Cold War Era to the Tunis Agenda. Global Studies Quarterly, 2(4), ksac059. DOI: иhttps://doi.org/10.1093/isagsq/ksac059

Creemers, R. (1996). Provisional Management Regulations for the International Connection of Computer Information Networks of the People's Republic of China. *DigiChina.* URL: https://surl.li/bzlfjy

Creemers, R. (1997). Computer Information Network International Interconnection Security Protection Management Rules. DigiChina. URL: https://digichina.stanford.edu/work/computer-information-network-international-interconnection-security-protection-management-rules/

Creemers, R. (2024). The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy. *Journal of Contemporary China*, 33(146), 173-188. DOI: https://doi.org/10.1080/10670564.2023.2196508

Cybersecurity Law of the People's Republic of China. (2017). URL: https://chinacopyrightandmedia.wordpress.com/2016/11/07/cybersecurity-law-of-the-peoples-republic-of-china/

Data Security Law of People's Republic of China. (2021). URL: https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/

Dealing with demand for China's global surveillance exports. (2020). URL: https://www.brookings.edu/articles/dealing-with-demand-for-chinas-global-surveillance-exports/

Drinhausen, K., Lee, J. (2021, June 15). The CCP in 2021: Smart governance, cyber sovereignty and tech supremacy. *MERICS.* URL: https://merics.org/en/ccp-2021-smart-governance-cyber-sovereignty-and-tech-supremacy

Flonk, D. (2021). Emerging illiberal norms: Russia and China as promoters of internet content control. *International Affairs,* 97(6), 1925-1944. DOI: https://doi.org/10.1093/ia/iiab146

Horsley, J.P. (2022). *Behind the Facade of China's Cyber Super-Regulator.* URL: https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/

International Strategy of Cooperation on Cyberspace. (2017). *Ministry of Foreign Affairs of the People's Republic of China.* URL: https://www.mfa.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202406/t20240606_11405181.html

Jiang, M. (2025). Chinese internet policies: Historical reflections and new research directions. *Communication and the Public,* 10(3), 162-167. DOI: https://doi.org/10.1177/20570473251316590

Jiang, Z. (2002). *Build a Well-off Society in an All-Round Way and Create a New Situation in Building Socialism with Chinese Characteristics.* Report to the 16th National Congress of the Communist Party of China.

Jinping, X. (2015). Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World. I*nternet Conference_Ministry of Foreign Affairs of the People's Republic of China.* URL: https://www.mfa.gov.cn/eng/xw/zyjh/202405/t20240530_11341037.html

Jointly Build a Community with a Shared Future in Cyberspace. (2022). (*White Paper*). *The State Council Information Office of the People's Republic of China.* URL: http://english.scio.gov.cn/whitepapers/2022-11/07/content_78505694.htm

King, G., Pan, J., Roberts, M. E. (2013). How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review,* 107(2), 326-343. DOI: https://doi.org/10.1017/S0003055413000014

Legacy. (2021, September 23). The 'De-IOE' in China. DU Economics Society. URL: https://www.dueconsoc.org.uk/single-post/2017/11/05/the-de-ioe-in-china

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. (2015). *UN.* URL: https://docs.un.org/en/a/69/723

Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. (2011). *UN.* URL: https://docs.un.org/en/a/66/359

McKune, S. (2015). Analysis of International Code of Conduct. *The Citizen Lab.* URL: https://citizenlab.ca/research/international-code-of-conduct/

Murgia, M., Gross, A. (2020, March 27). China and Huawei propose reinvention of the internet. *Financial Times.* URL: https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2?syn-25a6b1a6=1

National Cyberspace Security Strategy. (2016). *Cyberspace Administration of China.* URL: https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

Negro, G. (2020). A history of Chinese global Internet governance and its relations with ITU and ICANN. *Chinese Journal of Communication,* 13(1), 104-121. DOI: https://doi.org/10.1080/17544750.2019.1650789

Personal Information Protection Law of the People's Republic of China. (2021). URL: https://surl.li/winziy

Pytlak, A. (2025, August 4). Cyber Diplomacy 2.0: From Process to Impact. *Stimson Center.* URL: https://www.stimson.org/2025/cyber-diplomacy-2-0-from-process-to-impact/

Segal, A. M. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age* (First edition). PublicAffairs.

Soesanto, F. D., Stefan. (2017, August 15). The UN GGE is dead: Time to fall forward – European Council on Foreign Relations. *ECFR.* URL: https://ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance/

Statistical Report on Internet Development in China. (2013).

Stevens, T. (2026). *Cyber Risk: Managing Uncertainty in a Digital World.* Bristol University Press.

Tang, M., Huhe, N. (2016). The Variant Effect of Decentralization on Trust in National and Local Governments in Asia. *Political Studies,* 64(1), 216-34. DOI: https://doi.org/10.1111/1467-9248.12177

United Nations Convention against Cybercrime. (2024). (Resolution). *UN.* DOI: https://docs.un.org/en/A/RES/79/243

Wasserstrom, J.N. (2018). Review: Censored: Distraction and Diversion inside China's Great Firewall Margaret E. Roberts Princeton and Oxford: Princeton University Press. *The China Quarterly,* 236, 1206-1208. DOI:https://doi.org/10.1017/S0305741018001431

Wenxiang, G. (1998). International Communication in the Information Age: New Problems Faced by International Relations. *International Politics Studies*, (2), 41-48.