УДК (UDC) 327:002.1 (510 : 73)
DOI: 10.26693/ahpsxxi2025.09.132

# THE INFORMATION DIMENSION OF CHINA'S FOREIGN POLICY STRATEGY TOWARD THE UNITED STATES IN THE POST-COLD WAR ERA

***Oleksandr Shevchuk,***
*e-mail: shevchukov07@gmail.com*
*ORCID: https://orcid.org/0000-0003-0335-6873*
*Petro Mohyla Black Sea National University,*
*Ukraine, 54003, Mykolaiv, 68 Desantnykiv,*

***Dmytro Konoplianyk,***
*e-mail: dmytrokonoplianyk18@gmail.com*
*ORCID: https://orcid.org/0009-0005-1973-771X*
*Mykolaiv National Agrarian University,*
*Ukraine, 54008, Mykolaiv, Georgiy Gongadze, 9*

**Abstract**

This article examines China's diverse methods of influence in the foreign policy arena, particularly concerning the United States. China employs various strategies to recruit American agents of influence to further its interests in the U.S. These include computer network operations and cyber activities conducted by Chinese citizens and supported by the government.

One of China's primary focuses is political and corporate espionage, targeting financial, defense, and technology companies, as well as research institutions in the United States. The PRC has established a legal framework that incentivizes Chinese citizens to contribute to state security efforts. Beijing utilizes multiple actors to advance its interests in the U.S. and other open democracies.

Additionally, China adopts Russian-style disinformation tactics, such as deploying social media bots to spread false narratives and amplify societal divisions, aiming to destabilize the American political system. China's economic leverage serves as an effective tool for influencing American institutions and securing favorable positions for Chinese economic entities in the U.S. market. China also actively employs soft power to compete with the United States in both geopolitical and economic spheres.

The Russian-Ukrainian war has become a significant turning point in U.S.-China relations, as evidenced by both countries' responses to Russia's aggression against Ukraine and their subsequent stances during the conflict. U.S. policy toward China suggests that Washington has adopted a containment strategy, despite official rhetoric preferring the term 'competition'.

**Keywords:** USA, China, cyberspace, foreign policy strategy, 'network state', information security, information sovereignty

# ІНФОРМАЦІЙНИЙ НАПРЯМ ЗОВНІШНЬОПОЛІТИЧНОЇ СТРАТЕГІЇ КНР ЩОДО США У ПОСТБІПОЛЯРНУ ЕПОХУ

***Олександр Шевчук,***
*e-mail: shevchukov07@gmail.com*
*ORCID: https://orcid.org/0000-0003-0335-6873*
*Чорноморський національний університет*
*імені Петра Могили,*
*Україна, 54003, Миколаїв, 68 Десантників, 10*

***Дмитро Конопляник,***
*e-mail: dmytrokonoplianyk18@gmail.com*
*ORCID: https://orcid.org/0009-0005-1973-771X*
*Миколаївський національний аграрний університет,*
*Україна, 54008, Миколаїв, Георгія Гонгадзе, 9*

**Анотація**

У статті здійснено аналіз різноманітних засобів впливу КНР на зовнішньополітичній арені загалом, і щодо США, зокрема. Використовуючи різноманітні методи, КНР вербує американських агентів впливу для реалізації китайських інтересів у США. Операції з комп’ютерними мережами, включаючи кібероперації, здійснюються як громадянами Китаю, так і за підтримки китайського уряду.

Одним з основних напрямків діяльності КНР є політичне та корпоративне шпигунство з метою доступу до мереж фінансових, оборонних і технологічних компаній та науково-дослідних установ у Сполучених Штатах Америки. Китай створив законодавче підґрунтя, яке спонукає громадян КНР робити свій внесок у сферу державної безпеки. Офіційний Пекін використовує цілу низку суб’єктів для просування своїх інтересів у США та інших відкритих демократіях.

Крім того, КНР застосовує методи дезінформації в російському стилі – спам ботів у соціальних мережах – для поширення неправдивих наративів і посилення суперечностей в американському суспільстві з метою дестабілізації американської політичної системи. Економічний тиск з боку Китаю є також ефективним інструментом кореляції позицій американських інституцій та вигідного позиціювання економічних структур КНР на американського внутрішньому ринку. Китай активно використовує м’яку силу конкуруючи із США як на геополітичній арені, так і в економічній сфері.

Зважаючи на реакцію США і КНР на агресію Росії проти України та подальше позиціювання цих держав протягом конфлікту, можна зазначити, що ця російсько-українська війна є черговою віхою в американо-китайських відносинах. Політика США щодо Китаю вказує на те, що Вашингтон розпочав стратегію стримування Китаю, хоча його офіційна риторика намагається використовувати слово «конкуренція».

**Ключові слова:** США, КНР, кіберпростір, зовнішньополітична стратегія, «мережева держава», інформаційна безпека, інформаційний суверенітет

**Постановка проблеми.** На сучасному етапі розвитку міжнародних відносин більшість країн світу розбудовують свою зовнішньополітичну стратегію, ґрунтуючись на застосуванні конструктивістської парадигми щодо наріжних каменів формування зовнішньої політики держави. Це пов’язано з тим, що на політику держав мають

суттєвий вплив недержавні актори, такі як транснаціональні компанії, засоби масової інформації (ЗМІ) й авторитетні дослідницькі центри. А процеси глобалізації, інформатизації, спонукають самі країни винаходити та застосовувати нові підходи до розв'язання своїх зовнішньополітичних завдань. Разом із стрімким соціально-економічним зростанням країн Азійсько-Тихоокеанського регіону фокус міжнародних відносин зміщається на Схід, разом з цим зростають роль і участь країн регіону у формуванні глобального порядку денного.

Кіберпростір, на відміну від інших просторів міждержавних взаємодій, є штучним віртуальним середовищем, за допомогою якого об'єднані пристрої, розташовані у різних державах, при цьому його структура може змінюватися (Ebert & Maurer, 2013: 1056). Саме кіберпростір розширив можливості впливу недержавних акторів на світову політику, що, своєю чергою, створило нові виклики для забезпечення національної безпеки країн світу (Nye, 2011: 12).

Унікальною відмінністю кіберпростору, як поля взаємодії, є те, що він виступає не лише інструментом впливу, але й сам впливає на більш традиційні простори міждержавної взаємодії. Що більше, діяльність у кіберпросторі є значно дешевше, ніж в інших політичних просторах. Це обумовлюється доступністю інформаційно-комунікаційних технологій і відтворюваністю даних, які знаходяться у кіберпросторі, що певною мірою ускладнює можливість знищення кіберзброї або елементів впливу, таких як пропагандистські вебсайти тощо (Sheldon, 2011: 111, 290). Сайт може бути заблокований або видалений, однак немає жодних гарантій, що через пару годин він не з'явиться у всесвітній мережі за новою адресою.

Розпад Радянського Союзу з одного боку, змінив полярність світу, залишивши США як глобального лідера перед викликами та загрозами регіонального та глобального характеру, а з іншого – стимулював активізацію висхідних центрів сили щодо утвердження та розширення різнорівневих сфер впливу. В цих умовах, у поєднанні із суттєвими можливостями, які надає кіберпростір, КНР цілеспрямовано нарощує свою геополітичну потужність у різних регіонах світу, конкуруючи при цьому із США.

**Аналіз попередніх досліджень і публікацій.** На сьогодні ми маємо низку наукових праць щодо інформаційних операцій КНР проти США та європейських країн. Цей напрямок є предметом уваги вітчизняних науковців, а саме: М. Копійки (Kopiyka, 2020a; Kopiyka, 2020б), О. Кучмій (Kuchmiy, 2011), Н. Вінникової (Vinnikova, 2022), С. Венідіктова (Venidiktov, 2020). Однак, практично відсутні роботи щодо висвітлення процесів перетворення Китаю на «потужну мережеву державу» як детермінанти регіональної системи міжнародних відносин у контексті жорсткої конкуренції із США.

Значний фактологічний матеріал представлений публікаціями інформаційних агентств і ЗМІ. Серед них на особливу увагу заслуговують: New York Times і The Wall Street Journal, які активно висвітлюють позиціонування КНР у регіональній і глобальній системі міжнародних відносин, особливо щодо прагнення Китаю внести корінні зміни у світовий порядок. Необхідно зазначити, що в умовах турбуленції системи міжнародних відносин, спричиненою російською агресією проти України, для КНР відкрилось своєрідне «вікно можливостей».

*Метою дослідження* є висвітлення інформаційного напряму зовнішньополітичної стратегії Китаю щодо Сполучених Штатів у постбіполярну епоху.

**Виклад основного матеріалу.** Наразі КНР має всі необхідні умови для позиціонування себе як «потужної мережевої держави» (Network State), окрім цього вона має і ресурси, й ефективну автократичну систему державних інститутів.

На сьогодні Китай має найбільшу кількість активних користувачів Інтернету в Азії: 1 010 740 000. Відразу за нею йде Індія – 833,71 млн. користувачів і Сполучені Штати – 312,32 млн. (це число перевищило прогнозовану кількість в 307,34 млн. інтернет-користувачів) (Algren, 2024).

У 2010 р. Інформаційне бюро Державної ради КНР опублікувало «Білу книгу» з основними положеннями політики КНР щодо регулювання Інтернету, де приділялася особлива увага наступним напрямам: популяризації та поширення Інтернету серед населення, підвищенню рівня доступності Інтернету, гарантування прав і свобод в інтернет-просторі, управлінні Інтернетом, забезпеченні кібербезпеки та міжнародного співробітництва у цій сфері (The Internet in China, 2010).

Слід зазначити, що вперше китайський уряд поставив питання забезпечення інформаційної та кібербезпеки в один ряд із національною безпекою країни, до обігу був введений термін «Інтернет-суверенітет». Таким чином, Китай задекларував виняткове право на регулювання своєї внутрішньої мережі, що було зроблено внаслідок посилення впливу зовнішніх акторів. Це стосувалося не лише окремих держав, таких як США, а й недержавних структур (Lewis, 2017: 19). Інтернет-суверенітет необхідний для того, щоб у процесі розвитку цифрового середовища можна було сконцентруватися на питаннях матеріального добробуту та справедливого розвитку, не зупиняючись на питаннях забезпечення безпеки, конфіденційності та боротьби за управління Інтернетом (Hong & Goodnight, 2020: 21).

З метою реалізації своєї інформаційної політики КНР почала створювати сучасну технологічну основу. У 2016 р. для забезпечення лідерства в ІТ-сфері у КНР була затверджена «Національна стратегія інформатизації та розвитку», якою передбачалося, що до 2020 р. китайські технології досягнуть світового рівня та будуть конкурентоспроможними на світовому ринку; до 2025 р. має бути побудована міжнародна мережа мобільного зв’язку, яка буде забезпечуватися передовими технологіями та програмним забезпеченням, що дозволить КНР підвищити конкурентоспроможність своєї економіки та розв’язувати питання кібербезпеки. До середини 21 ст. КНР прагнула стати «сильною мережевою державою» та мати визначальний вплив на процес інформатизації у всьому світі, спираючись на концепцію соціалізму з китайською специфікою (National Strategy for Informatization and Development of the People’s Republic of China, 2016). Таким чином, керівництво КНР спрямоване на лідерство як у сфері виробництва високотехнологічної продукції, так і у сфері створення сучасного програмного забезпечення. Ця стратегія об’єднала у собі ідеї, які були закладені у стратегічних ініціативах «Інтернет плюс» і «Роби у Китаї – 2025».

Одним з найважливіших аспектів інформаційної безпеки КНР є забезпечення зовнішньої безпеки країни. Із зростання економіки та впливу Китаю у світі з’являється все більше питань міжнародного порядку денного, де стикаються інтереси будь-якої держави та КНР. Останнім часом загострилися відносини між КНР і США. Зокрема, однією з причин їх погіршення стали саме питання кібербезпеки та захисту інтелектуальної власності. Це пов’язано і з тим, що найбільш вразливими секторами економіки для кібератак є фінансовий сектор і сфера інформаційних технологій (ІТ), водночас розвиток цих секторів підвищує рівень готовності протистояти загрозам, які виходять з кіберпростору (Makridis & Smeets, 2019: 76).

Американські дослідники стверджують, що КНР створила т. зв. «50-феневу армію» (wumaodan) – групи людей або ботів, які займаються публікацією проурядової інформації та дискредитацією користувачів, які публікують антиурядовий контент. Передбачається, що до участі у даному проекті залучаються журналісти, блогери й інші медійні особи (King, Pan & Roberts, 2017: 486).

Зважаючи на всі ризики та можливості, КНР прагне створити сприятливий для офіційного Пекіна інформаційний клімат у середині країни та протидіє впливу на нього ззовні, зокрема, ретельно фільтруються будь-які статті та висловлювання з приводу таких чутливих для Китаю питань, як Тайвань, Тибет і територіальні суперечки у Південнокитайському морі. А з початком торговельної війни із США у 2018 р. інформаційне протистояння між країнами зросло у геометричній прогресії, тому забезпечення кібербезпеки у зовнішній політиці КНР виходить на одне з чільних місць. Необхідно підкреслити, що основною причиною торговельної війни

між Пекіном і Вашингтоном були крадіжки інтелектуальної власності американських компаній китайською стороною. Разом з тим, Пекін, використовуючи сучасні інтернет-технології, намагається впливати на позиції США у глобальному світовому порядку.

Китайські аналітики з відповідною регулярністю закликають до більш мирного та справедливого глобального порядку, не надаючи чітких дефініцій того, як це має виглядати (Hart et al, 2017).

У прагненні подолати американське домінування та розширити власний геополітичний вплив, Китай вдається до різноманітних інструментів, серед яких одним з основних є інформаційні операції. У доповіді Центру стратегічних і міжнародних досліджень (CSIS) стверджується, що з 2006 р. до початку 2020-х рр. Китай виступав агресором у кіберпросторі у 108 інцидентах. У той час, коли на нього було здійснено всього 25 нападів. У свою чергу США виступали агресором лише у 9 випадках, а жертвою агресії – у 117 (Significant Cyber Incidents, 2019). Необхідно зазначити, що мова йде про загальну кількість інцидентів, а не лише ті, в яких були залучені США та КНР. Таким чином, Китай веде агресивну політику в кіберпросторі та віддає перевагу наступальним діям, про що свідчать дані американського аналітичного центру.

Використовуючи різноманітні методи, КНР, зокрема, вербувала американських агентів впливу для відстоювання китайських інтересів у США. Хоча багато з цих агентів служать Китаю мимоволі, але вони є доволі ефективними. Так, наприклад, у доповіді Конгресу США ще за 1999 р. зазначалося: «Китайський уряд продовжує домагатися впливу в Конгресі різними способами, включаючи запрошення членів Конгресу відвідати КНР, лобіюванні інтересів етнічних китайських виборців і видатних громадян США, а також залучення представників ділових кіл США для розв'язання питань, що мають спільний інтерес» (Report to Congress on Chinese Espionage…, 1999).

Вплив КНР на внутрішньополітичне середовище США з відповідною проекцією щодо зовнішньополітичного виміру має комплексний характер. Так, у своїй діяльності Китай ефективно поєднує відкриту та латентну діяльність, прагнучи мати політичний вплив в американському уряді, з метою формування сприятливого для нього зовнішньополітичного клімату. Зокрема Китай докладає зусиль для «впливу на американських вчених, журналістів, персонал аналітичних центрів, тобто тих, хто має вплив на формування основних орієнтирів громадської думки» (Terrill, 2009). Китай веде політичне та корпоративне шпигунство з метою доступу до мереж фінансових, оборонних і технологічних компаній та науково-дослідних установ у США. Так, у 2007 р. агенти китайських військових зламали аерокосмічну фірму Lockheed Martin і викрали десятки мільйонів документів, пов'язаних з найдорожчою американською системою озброєння F-35 Joint Strike Fighter. Незабаром після цього з'явився особливо схожий китайський літак J-31 (Osnos, 2020).

З початку 2010-х рр. суперництво Китаю та США в інформаційному просторі динамічно зростає, що робить відносини між країнами більш «гарячими», що своєю чергою розширює конфліктний потенціал. У 2010 р. США звинуватили Китай у зламі електронних скриньок правозахисників, що призвело до того, що до 2013 р. почалися жорсткі взаємні звинувачення з боку офіційних осіб двох держав. У березні 2013 р. президент США Б. Обама виступив зі спеціальним розпорядженням щодо процедур державних закупівель високотехнологічних рішень. За цим розпорядженням Держдепартамент США заборонив співпрацю з Китаєм у сфері закупівель IT-обладнання для організацій державного сектора (Ford, 2020).

У січні 2013 р. газета «The New York Times» повідомила, що стала жертвою спроб хакерських атак з Китаю протягом попередніх чотирьох місяців після того, як опублікувала статтю-розслідування, яка засвідчила, що родичі прем'єр-міністра Китаю Вень Цзябао накопичили статки на кілька мільярдів доларів завдяки діловим операціям. За даними газети, «атаки, схоже, є частиною ширшої кампанії

комп’ютерного шпигунства проти американських новинних медіа-компаній, які повідомляли про китайських лідерів і корпорації» (Perlroth, 2013).

Офіційний Вашингтон вважає, що Китай намагається встановити контроль над інтернет-простором з метою розширення свого «цифрового суверенітету». У травні 2013 р. на Азійському безпековому саміті в Сінгапурі тодішній міністр оборони США Ч. Гейгл заявив про те, що кількість кібератак з боку КНР на об’єкти військового та урядового призначення постійно збільшується (Hagel, 2013). Відповіддю на цю заяву стало звернення директора Центру китайсько-американських відносин у сфері оборони, створеного при Академії військових наук НВАК сфері оборони, генерал-майора Яо Юньчжу: «Вашингтон постійно нарощує військову присутність в Азійсько-Тихоокеанському регіоні, тим самим ставить під питання китайсько-американську довіру» (Beraud-Sudreau, 2020).

Згідно з дослідженням 2014 р., яке спонсорував Пентагон, Китай веде політичну війну проти Сполучених Штатів у рамках стратегії витіснення американських військових з Азії та контролю над морями поблизу її узбережжя (Freeman, 2014).

У 2017 р. Китай запровадив законодавче підґрунтя щодо внеску всього населення країни у державну безпеку. Центр стратегічних і міжнародних досліджень (CSIS) аналізуючи цей аспект, зазначив: «Цілком ймовірно, що громадяни можуть бути змушені допомагати державним суб’єктам КНР у зусиллях із втручання, ці зусилля підпадають під ширше визначення “роботи національної розвідки” та “зусиль національної розвідки”, як зазначено в Законі» (Gambill, 2021).

У доповіді Конгресу в травні 2020 р. президент США Д. Трамп висвітлив деякі аспекти загрози політичної війни: «Китайська партія-держава контролює найбільш забезпечений ресурсами набір пропагандистських інструментів у світі. Пекін передає свій наратив через державне телебачення, друковані видання, радіо та онлайн-організації, чия присутність поширюється в Сполучених Штатах і в усьому світі. Крім ЗМІ, КПК використовує цілий ряд суб’єктів для просування своїх інтересів у Сполучених Штатах та інших відкритих демократіях. Організації та агенти Об’єднаного фронту КПК спрямовані на підприємства, університети, аналітичні центри, вчених, журналістів, а також місцевих, державних і федеральних чиновників у Сполучених Штатах і в усьому світі, намагаючись вплинути на дискурс та обмежити зовнішній вплив всередині КНР. Політична війна КНР регулярно підриває діяльність Корпусу морської піхоти США та національну безпеку США в усьому світі» (Gershaneck, 2020).

Епідемія COVID-19 була використана досить ефективно керівництвом КНР з метою утвердження власного «інформаційного суверенітету». Офіційний Пекін не лише не задовольнився просуванням популяризації своєї міжнародної медичної допомоги іншим країнам під час пандемії, але й скористався можливістю, щоб значно розширити негативне висвітлення у ЗМІ реакції США на кризу та здатності Вашингтона бути лідером. Крім того, КПК інтегрувала російську тактику дезінформації у свій і без того потужний апарат інформаційної війни в Інтернеті для поширення теорій змови та дезінформації в американських соціальних мережах.

Антиамериканські меседжі просувалися кількома способами. Перший – через «офіційні» канали, такі як виступи/заяви/інтерв’ю з урядовцями КНР, надруковані у флагманських ЗМІ КНР, таких як: «Женьмінь жибао» або «Сіньхуа». Другий, через «неофіційні» канали, де існує рівень правдоподібного заперечення. Ілюстративним прикладом цього є конспірологічний пост речника МЗС КНР Чжао Ліцзяня у Twitter, в якому він звинуватив армію США у навмисному поширенні COVID в Ухані. Потім цим звинуваченням поділилися понад десяток китайських дипломатів у Twitter.

Наступними є методи дезінформації у російському стилі – спам ботів у соціальних мережах – для вставки неправдивих наративів і посилення розбрату в американському суспільстві. Pro Publica, новинна організація розслідувачів, зафіксувала зростання кількості облікових записів, які підтримують КПК, зосереджених винятково на критиці Сполучених Штатів. В їхньому звіті було

відстежено понад 10 тисяч таких облікових записів і відображено як ці підозрілі користувачі взаємодіяли один з одним, щоб просувати наративи КНР. Одна з технік передбачає використання «індивідуальних» облікових записів у соціальних мережах – облікового запису з ознаками справжнього профілю у соціальних мережах, такими як довга історія облікового запису, регулярні публікації, прямі повідомлення – для публікації «привабливого» коментаря, який потім поширюється за допомогою лайків, ретвітів і вставлених коментарів спам-акаунтами в алгоритми ігрової платформи для просування (Chan & Loftus, 2020).

Економічний тиск з боку Китаю є ефективним інструментом формування поведінки американських галузей та інституцій, а також примусу до мовчання їхніх критиків. Наприклад, у жовтні 2019 р. китайські ЗМІ піддали цензурі ігри команди NBA Houston Rockets після того, як її менеджер написав у Твіттері на підтримку продемократичних протестувальників у Гонконзі. Менеджер швидко видалив твіт, а NBA заявила, що «шкодує» про те, що менеджер образив багатьох у Китаї. Як і NBA, інші американські індустрії такі як Голлівуд, стали вразливими до китайського примусу, оскільки вони дуже сильно залежать від китайських ринків та інвестицій (Gehlen, 2022).

Окрім того, як зазначає американське видання Wall Street Journal (WSJ) Китай активно просуває серед китайського населення ідеологію «ненависті до іноземців» (серед яких американці, японці, індуси й ін.), формуючи тим самим патріотизм до власної країни, влади, мінімізуючи розпалювання будь-яких невдоволень всередині держави. Це реалізується за допомогою державних ЗМІ у школах, університетах. І як показує практика цей метод є дієвим. Чотири викладачі американського коледжу отримали ножові поранення від китайця під час прогулянки в парку у північно-китайському місті Цзіліні. МЗС Китаю заявило, що цей інцидент не вплине на «нормальний розвиток міжлюдських і культурних обмінів між Китаєм і США» (Wenxin, 2024).

**Висновки.** У подоланні американського лідерства та розширення власного впливу, Китай вдається до різноманітних заходів впливу, серед яких і кіберсфера. Використовуючи різноманітні методи, КНР вербує американських агентів впливу для відстоювання китайських інтересів у США. Операції з комп'ютерними мережами, включаючи кібероперації, здійснюються як громадянами Китаю, так і за підтримки китайського уряду. КНР активно використовує політичне та корпоративне шпигунство з метою доступу до мереж фінансових, оборонних і технологічних компаній та науково-дослідних установ США.

Ухваливши законодавчу базу, яка «стимулює» громадян робити свій внесок у державну безпеку, Пекін використовує низку суб'єктів для просування своїх інтересів у Сполучених Штатах Америки й інших відкритих демократіях. Застосовуючи методи дезінформації (спам боти у соціальних мережах для вставки неправдивих наративів) КНР цілеспрямовано посилює розбрат в американському суспільстві. Досить дієвим у цій ситуації є й китайський економічний тиск.

Сучасні тенденції засвідчують стрімке зростання КНР у контексті перетворення її на «потужну мережеву державу», що своєю чергою сприяє створенню комфортних умов для розвитку не лише національної економіки, шляхом розбудови ефективної системи регулювання Інтернету в середині країни та її захисту від зовнішнього впливу, але й її контролю інших суб'єктів міжнародного права. Варто розуміти, що перетворення Китаю у таку державу може призвести до прямого зіткнення із США, що загрожує конфліктом глобального рівня. Навряд чи єдина поки наддержава погодиться бути підконтрольною державі-челенджеру.

## References

**Algren, M.** (2024). 100+ Internet Statistics and Trends. Retrieved from https://707.su/j9Zt // **Алгрен, М.** (2024). 100+ Інтернет-статистики та тенденцій. Retrieved from https://707.su/j9Zt

**Beraud-Sudreau, L.** (2020, March 31). Assessing Chinese defence spending: proposals for new methodologies. *International Institute for Strategic Studies (IISS)*. Retrieved from https://707.su/ga7p

**Chan, E. & Loftus, P.** (2020). Chinese Communist Party Information Warfare: US–China Competition during the COVID-19 Pandemic. *Journal of Indo-Pacific Affairs*. Retrieved from https://707.su/sDVQ

**Ebert, H. & Maurer, T.** (2013). Contested Cyberspace and Rising Powers. *Third World Quarterly,* 34 (6), 1054-1074.

**Ford, C.A.** (2020, November 20). The Evolution of International Security Capacity Building. *U.S. Department of State*. Retrieved from https://707.su/jGQa

**Freeman, K.D.** (2014). China’s Three Warfares Goes Further Than Anyone Can Imagine. *Global Economic Warfare Risks & Responses*. Retrieved from https://707.su/cE4N

**Gambill, J.** (2021). China and Russia Are Waging Irregular Warfare Against the United States: It is Time for a U.S. Global Response, Led by Special Operations Command. *U.S. Naval Institute*. Retrieved from https://707.su/ZERf

**Gehlen, E.** (2022). Stop China from Winning Without Fighting. *U.S. Naval Institute*. Retrieved from https://707.su/Ix88

**Gershaneck, K.** (2020). To Win without Fighting. Defining China’s Political Warfare. *Marine Corps University*. Retrieved from https://707.su/dI6Z

**Hagel, Ch.** (2013, June 1). Speech At The Shangri-La Dialogue. *USC US-China Institute*. Retrieved from https://707.su/Z8WO

**Hart, M., Jacob, J., Rolland, N. & Stanzel, A.** (2017, October 18). Grand Designs: Does China havea ‘Grand Strategy’? *European Council on foreign relations*. Retrieved from https://707.su/yid9

**Hong, Y. & Goodnight, G.** (2020). How to Think about Cyber Sovereignty: The Case of China. *Chinese Journal of Communication,* 13 (1), 8-26.

**Jones Seth, G.** (2024, October 2). China Is Ready for War. And Thanks to a Crumbling Defense Industrial Base, America. *Foreign Affairs*. Retrieved from https://707.su/NGak

**King, G., Pan, J. & Roberts, M.** (2017). How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument. *American Political Science Review,* 111 (3), 484-501.

**Kopiyka, M.V.** (2020a). Modernization of the policy of international organizations in the field of information security. *Political life,* 1, 102-109 // **Копійка, М.В.** (2020a). Модернізація політики міжнародних організацій у сфері інформаційної безпеки. *Політичне життя,* 1, 102-109.

**Kopiyka, M.V.** (2020b). «Sharp power» in China’s information security strategy. *International relations, public communications and regional studies,* 1, 68-80 // **Копійка, М.В.** (2020b). «Гостра сила» в стратегії інформаційної безпеки Китаю. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 1, 68-80.

**Kuchmiy, O.P.** (2011). Strategy of the information economy of the People’s Republic of China. *Actual problems of international relations,* 103 (1), 85-93 // **Кучмій, О.П.** (2011). Стратегія інформаційної економіки КНР. *Актуальні проблеми міжнародних відносин,* 103 (1), 85-93.

**Lewis, D.** (2017). China’s Global Internet Ambitions: Finding Roots in ASEAN. *ICS Occasional Papers,* 14, 1-28.

**Makridis, C. & Smeets, M.** (2019). Determinants of Cyber Readiness. *Journal of Cyber Policy,* 4 (1), 72-89.

National Strategy for Informatization and Development of the People’s Republic of China (2016). *State Council of the People’s Republic of China*. Retrieved from https://707.su/DOnL

**Nye, J.S.** (2011). Jr. Nuclear Lessons for Cyber Security. *Strategic Studies Quarterly,* 5 (4), 9-20.

**Osnos, E.** (2020). The Future of America’s Contest with China. *The New Yorker*. Retrieved from https://707.su/Hz98

**Perlroth, N.** (2013). Hackers in China Attacked The Times for Last 4 Months. *The New York Times*. Retrieved from https://707.su/FzH6

Report to Congress on Chinese Espionage Activities Against the United States (1999, December 12). *FBI/CIA*. Retrieved from https://707.su/TYuv

**Sheldon, J.B.** (2011). Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly,* 5 (2), 95-112.

**Sheldon, J.B.** (2014). Geopolitics and Cyber Power: Why Geography Still Matters. *American Foreign Policy Interests,* 36 (5), 286-293.

Significant Cyber Incidents (2019). *Center for Strategic and International Studies* (*CSIS)*. Retrieved from https://707.su/J9H8

**Terrill, R.** (2009, April 30). China's Propaganda and Influence Operations, Its Intelligence Activities That Target the United States, and the Resulting Imacts on U.S. National Security. *Hearing Before the U.S-China Economic and Security Review Commission*. Retrieved from https://707.su/QZbZ

The Internet in China (2010, June). *Information Office of the State Council of the People's Republic of China*. Retrieved from https://707.su/ktXO

**Venidiktov, S.** (2020). China's media system: internal control and external autonomy. *Bulletin of the Kyiv National University of Culture and Arts. Series: Audiovisual Art and Production,* 3 (2), 229-236 // **Венідіктов, С.** (2020). Медіасистема Китаю: внутрішній контроль та зовнішня автономія. *Вісник Київського національного університету культури і мистецтв. Серія: Аудіовізуальне мистецтво і виробництво*, 3 (2), 229-236.

**Vinnikova, N.** (2022). China as a global digital empire. *Politicus*, 1, 128-130 // **Вінникова, Н.** (2022). Китай як глобальна цифрова імперія. *Політикус*, 1, 128-130.

**Wenxin, F.** (2024, October 3). China's Patriotic Rhetoric Takes a Violent. *Turn The Wall Street Journal*. Retrieved from https://707.su/5Ugg