УДК (UDC) 32.019.51 : 004.056 (510)
DOI: 10.26693/ahpsxxi2023.si.105

INFORMATION WARS AND CYBERWARFARE IN CHINA

Oleksandra Rura,
e-mail: aleksandrarura@gmail.com
ORCID: https://orcid.org/0009-0006-1839-2411
Petro Mohyla Black Sea National University,
Ukraine, 54003, Mykolaiv, 68 Desantnykiv, 10

Nataliia Shynkaruk,
e-mail: natalisch1003@gmail.com
ORCID: https://orcid.org/0000-0002-4488-6240
National University of Life and Environmental Sciences of Ukraine,
Ukraine, 03041, Kyiv, Geroiv Oborony str., 15

Abstract

The article discusses the specifics of China's conduct in information and cyber warfare. Chinese official media promote Russian narratives regarding aggression against Ukraine. While not officially supporting Russia in the war, China conducts disinformation attacks on social media, taking into account the blocking of Russian media resources. China's cooperation with Russia in information warfare aims to create a positive image of Putin and his regime in the war, as well as to discredit the collective West and Ukraine among the Chinese population and foreign consumers of new media. In the military dimension, China's interest in information warfare began after the US victory in the First Gulf War (1990-1991). The success of the US was the result of information technologies and the total dominance they could provide on the battlefield. From this moment, the People's Liberation Army of China (PLA) started to invest significantly in developing its concepts of information warfare. China's strategic influence operations increasingly target the European Union, especially Central and Eastern European countries.

Taiwan is the biggest victim of the People's Republic of China in carrying out information warfare. Taiwan is highly vulnerable to Chinese cyber aggression. China's doctrine calls for extensive use of cyber tools in preparing for, executing, and dealing with the consequences of military actions against the island. These operations are ongoing and will gain popularity and aggression as tensions escalate in the Taiwan Strait, including possible attacks. The Russian-Ukrainian war presented a golden opportunity for China to launch cyber-attacks against Taiwan, aiming to demoralize the Taiwanese and incline them towards voluntary reunification with mainland China. The Russian invasion of Ukraine was meant to serve as an example of the unwillingness and inability of the US to support its allies during armed conflicts. For Europe and the US, the attack on the island was supposed to serve as a distraction from Russian military crimes in Ukraine and act as a deterrent against a new war.

Keywords: information warfare, cyber warfare, cyber-attack, China, Taiwan, EU, USA

ІНФОРМАЦІЙНІ ВІЙНИ І КІБЕРВІЙНИ КНР

Олександра Рура,
e-mail: aleksandrarura@gmail.com
ORCID: https://orcid.org/0009-0006-1839-2411
Чорноморський національний університет імені Петра Могили,
Україна, 54003, м. Миколаїв, вул. 68 Десантників, 10

Наталія Шинкарук,
e-mail: natalisch1003@gmail.com
ORCID: https://orcid.org/0000-0002-4488-6240
Національний університет біоресурсів і природокористування України,
Україна, 03041, м. Київ, Героїв оборони, 15

Анотація

У статті розкрито особливості ведення інформаційних та кібервійн КНР. Китайські офіційні ЗМІ просувають російські наративни стосовно агресії проти України. Офіційно не підтримуючи бік РФ у війні, КНР проводить дезінформаційні атаки у соціальних мережах, враховуючи блокування російських медіа ресурсів. Співпраця Китаю із Росією у інформаційній війні спрямована на формування позитивного образу Путіна і його режиму у війні, а також дискредитація колективного Заходу та України серед китайського населення, а також іноземних споживачів нових медіа.

У військовому вимірі інтерес Китаю до інформаційної війни почався після перемоги США у війні в Перській затоці (1990-1991 рр.). Успіх США став результатом інформаційних технологій і тотального домінування, яке вони змогли забезпечити у бойовому просторі. З цього моменту НВАК почала серйозно інвестувати і розробляти власні концепції інформаційної війни. Операції стратегічного впливу Китаю все частіше націлені на Європейський Союз, особливо на країни Центрально-Східної Європи. Найбільшою жертвою Китайської народної республіки у здійсненні інформаційної війни є Тайвань. Тайвань катастрофічно вразливий до китайської кібератресії. Китайська доктрина закликає до широкого використання кіберзасобів при підготовці, виконанні і ліквідації наслідків військових дій проти острова. Ці операції вже тривають і будуть набувати популярності та посилення агресії в міру ескалації напруженості в Тайванській протоці, включаючи можливі напади. Російсько-українська війна стала гарною нагодою для здійснення кібератак КНР проти Тайваню, що покликана деморалізувати тайванців та схилити їх до добровільного об'єднання з материковим Китаєм. Російське вторгнення в Україну мало стати прикладом небажання та неспроможності США підтримати своїх союзників під час збройних конфліктів. Для Європи та США інформаційна атака на острів мала стати відволікаючим фактором від російських військових злочинів в Україні, а також актом залякуванням новою війною.

Ключові слова: інформаційна війна, кібервійна, кібератака, КНР, Тайвань, ЄС, США

Постановка проблеми. Китай продемонстрував свій намір стати провідним міжнародним гравцем у сфері інформаційної та кібернетичної війни. Інформаційна війна включає дії, що застосовуються для досягнення інформаційної переваги шляхом впливу на інформацію супротивника, інформаційні процеси, інформаційні системи та комп'ютерні мережі, позбавляючи супротивника здатності робити те ж саме. За останні два десятиліття Китайська Народна Республіка скористалася

глобальним зв'язком епохи Інтернету, як жодна інша нація. Китай, який колись вважався кібердержавою «другого рівня», агресивно й послідовно розбудовував свою національну кіберпрограму до того моменту, поки не став вважатися коли одним із провідних кібергравців у світі. Тому, актуальність даної тематики не викликає ніяких сумнівів і важливості дослідження даного напряму.

Аналіз попередніх досліджень та публікацій. Інформаційні та кібервійни КНР є предметом аналізу багатьох зарубіжних дослідників, тому сьогодні ми маємо низку наукових праць, які висвітлюють ключові аспекти даної тематики. Першопрохідцями у даному випадку були саме науковці США. Серед таких варто виокремити роботу Д. Вентре (Ventre, 2010), в якій висвітлено питання стратегії Китаю у веденні інформаційної війни. Ґрунтовними є й напрацювання Б. Фармера (Farmer, 2022), який розкриває особливості кібератак Китаю на Тайвань, Г. Вінгера (Winger, 2020), що аналізує інформаційні атаки КНР на Філіппіни. Також слід відзначити праці Дж. Гудмана (Goodman, 2021), С. Мартіна (Martin, 2021), А. Бастлана (Bastlan, 2022) та інших, які висвітлюють питання застосування КНР дизінформаційні та пропагандистські технології технологій у ведені такого роду воєн.

Серед вітчизняних науковців варто виокремити праці Г. Калінічевої (Kalinicheva, 2023), О. Запорожець (Zaporozhets, 2023) та Д. Дубова (Dubov, 2014), які розкривають загальні аспекти кібервійни, ролі Інтернет-тролінгу та забезпечення безпеки в кіберпросторі.

Метою дослідження є аналіз інформаційних та кібервійн КНР як на регіональній системі міжнародних відносин, так і глобальній.

Методи та прийоми дослідження. Методологічним підґрунтям дослідження стали принципи наукового пізнання – історизму, об'єктивності, системності, багатофакторності та детермінізму. Для досягнення поставленої мети авторами був використаний комплекс загальнонаукових (аналіз і синтез, збір, обробка та аналіз матеріалів з даної тематики, метод узагальнення) і спеціальних методів (історичний, метод порівняльного аналізу) дослідження. Використання цих методів та принципів дозволили розкрити особливості інформаційних атака КНР у період з кінця XX – XXI ст.

Виклад основного матеріалу. Підхід Китаю до інформаційної війни і кібервійни має два основних виміри: військовий і цивільний, обидва розвиваються з теоретичних і практичних міркувань.

У цивільному просторі Китайська інформаційна війна в основному присвячена управлінню силовими відносинами із зовнішнім світом, але це може бути застосовано і в рамках його кордонів: перевага в інформації та кіберпросторі є питанням сили в Китаї. В останні роки технічний прогрес зіграв свою роль. Соціальні мережі (Twitter, Facebook) стали новими акторами та інструментами на національній та міжнародній політичній арені. У серпні 2009 р. стаття, опублікована на веб-сайті Central European News китайською мовою (Cenews), описала Twitter та інші соціальні мережі як нову зброю, що використовується для культурної підривної діяльності та політичного проникнення в країну (Ventre, 2010).

Китай залучає мільйони громадян для моніторингу інтернету та масового впливу на громадську думку в Інтернеті. Ці новобранці відомі як «50-центова армія» – названа так через повідомлення про те, що їм платили 0,5 юаня за посаду. Ця «клавіатурна армія» вже давно активна в китайських соціальних мережах. Її метою був агресивний захист іміджу Китаю за кордоном. Під час твітів англійською мовою повідомлення спрямовані на західну аудиторію, подібно до ферм тролів у Росії, які сіють розбрат. Нічого не підозрюючому читачеві вони можуть здатися патріотичними громадянами, які діють незалежно, але часто вони виконують вказівки китайської влади (Goodman, 2021). Вони посилюють прокитайські наративи, подібні до тих, які просувають представники китайської держави та державні ЗМІ. Значна частина контенту, яким ділиться мережа, зосереджена на

США і, зокрема, на суперечливих питаннях, таких як закони про зброю та расова політика (Martin, 2021).

У військовому вимірі інтерес Китаю до інформаційної війни почався після перемоги США у війні в Перській затоці (1990-1991 рр.). Успіх США став результатом інформаційних технологій і тотального домінування, яке вони змогли забезпечити у бойовому просторі. З цього моменту НВАК почала серйозно інвестувати і розробляти власні концепції інформаційної війни і те, що вони означають для Китаю (Ventre, 2010).

У 2003 р. Центральна військова комісія (ЦВК) затвердила керівну концептуальну парасольку інформаційних операцій для Народно-визвольної армії Китаю (НВАК) – «Три війни». Концепція базується на трьох взаємодоповнюючих стратегіях: 1) скоординоване використання стратегічних психологічних операцій; 2) відкрите та приховане маніпулювання засобами масової інформації; 3) правова війна, спрямована на маніпулювання стратегіями, оборонною політикою та сприйняттям цільової аудиторії за кордоном (Raska, 2015).

Якщо маніпулювання ЗМІ Китаю впливає на формування і контролювання іноземними поглядами через пресу та є елементом війни громадської думки, то психологічна війна спрямована на міжнародні центри прийняття рішень. Юридична війна прагне сформувати правовий контекст для дій Китаю (Wibawa, 2019).

Операції стратегічного впливу Китаю все частіше націлені на Європейський Союз, особливо на країни Центрально-Східної Європи, які входять до формули регіонального співробітництва Китаю «16+1». Пекін розглядає регіон як важливий плацдарм для своєї подальшої економічної експансії в Європі. Згідно з щорічною доповіддю контррозвідки БМР в Чеській Республіці за 2014 рік, адміністрація Китаю і його спецслужби роблять акцент на отриманні впливу на чеські політичні і державні структури та на зборі політичної розвідувальної інформації за активної участі окремих чеських еліт, включаючи політиків і державних чиновників (Raska, 2015).

У доповіді від 24 квітня 2020 р. Комуністична партія Китаю (КПК) успішно змусила Європейський Союз пом'якшити критику щодо КНР, у якій документуються операції з дезінформації, пов'язані з пандемією COVID-19.

Основна мета, що стимулює дезінформаційну кампанію КПК, полягає в тому, щоб просувати спекуляції про те, що COVID-19 виник за межами Китаю. Наприклад, китайські державні ЗМІ неправдиво стверджували, що COVID-19 виник у Південній Кореї та Італії. МВС Німеччини виявило, що китайські дипломати закликали Берлін позитивно повідомляти про зусилля Пекіна з реагування на COVID-19. Однак, відповідь німецького уряду була негативною. Тим не менш, Берлін не критикував публічно Пекін за його операції з дезінформації.

Через призму збільшення гуманітарної та медичної допомоги в усьому світі, Пекін поширює та підтверджує не лише свій імідж щедрого благодійника, але й сприяє розвитку залежних відносин з іноземними урядами. Як наслідок країни світу готові опосередковано формувати повідомлення щодо Китаю та його причетності до поширення COVID-19. Зокрема, як згадувалося вище, Європейський Союз відклав, а потім пом'якшив свій звіт про дезінформаційні операції Китаю, після того, як Пекін попередив, що цей звіт негативно вплине на їх співпрацю з ЄС. Розуміючи усі наслідки висвітлення правдивого звіту, представники прийняли рішення про його пом'якшення, боячись втратити майбутню медичної допомоги від Китаю (На, 2020).

Варто зауважити, що Філіппіни, як союзник США і їх стратегічний партер Індійсько-Тихоокеанському регіоні, стали ідеальною мішенню для реалізації КНР своїх можливостей в операціях іноземного впливу. Китай використав Facebook (яким активно користуються філіппінці) для здійснення своєї маніпулятивної політики щодо цієї країни. Так, з березня 2018 р., Китай почав впроваджувати в життя операцію Naval Gazing, головною метою якої стало створення низки облікових записів, сторінок і груп у Facebook, які рекламували діяльність філіппінських

політиків, що симпатизують Китаю, а також однозначно агітували за те, щоб Філіппіни переорієнтувалися на співпрацю з КНР (Winger, 2020).

Іншою країною, проти якої у 2017 р. (Доклам) було організовано три китайські інформаційні війни, стала Індія. Війна в ЗМІ велася з метою перешкодити Індії продовжувати свої дії в Бутані та применшити претензії Бутану. Китайські ЗМІ та численні міністерства зробили заяви на численних публічних форумах щодо неправдивих заяв індійського уряду щодо Бутану. Наступною була психологічна війна, головною метою якої стало поширення інформації про міністра закордонних справ Індії, якого звинуватили в брехні щодо зміни позиції Китаю до індійського штату Сіккім і, у свою чергу, «звільнить» Сіккім від індійського контролю. Третя юридична війна включала заяви Китаю про те, що Бутан прийняв китайські претензії на Доклам і що конвенція 1890 р. повинна дотримуватися, ігноруючи конвенцію 1914 р. (Bagchi, 2020).

Найбільшою жертвою Китайської народної республіки у здійсненні інформаційної війни є Тайвань, який мага вразливий до китайської кіберагресії. Китайська доктрина закликає до широкого використання кіберзасобів при підготовці, виконанні і ліквідації наслідків військових дій проти острова. Ці операції вже тривають і будуть набувати популярності та агресії в міру ескалації напруженості в Тайванській протоці, включаючи можливі напади.

Критично важлива інфраструктура, урядові послуги та ключові військові можливості острова вже зазнають від 20 до 40 мільйонів кібератак щомісяця, причому переважна більшість з них надходить з Китаю (Taking Taiwan Through Cyber, N.d).

Повномасштабне вторгнення Росії на територію України 24 лютого 2023 р. дало поштовх Китаю до посилення своєї ролі у світовому інформаційному просторі. Пекін формально не схвалював агресію РФ, але й не засуджував її. Китайські офіційні представники ніколи не використовують терміни як «вторгнення» та «війна». Як і Москва, офіційний Пекін просуває наратив про відповідальність колективного Заходу за війну, оскільки розширення НАТО змусило Росію терміново вжити відповідних заходів безпеки.

Підконтрольні державі ЗМІ Китаю у своєму висвітленні війни суворо дотримувалися офіційної лінії уряду. Китайські ЗМІ зайняли проросійську позицію у своїх звітах про війну.

У той час як ЗМІ КНР час від часу показували зображення зруйнованих українських міст і страждань мирного населення, здебільшого їхні звіти про війну були копією російських пропагандистських наративів, і це часто містило пряме репостування офіційних заяв представників російського уряду.

Оскільки китайські та російські державні засоби масової інформації витратили останні кілька років на те, щоб поступово нарощувати співпрацю один з одним (підписуючи численні угоди про публікацію взаємно схвалених матеріалів і віддзеркалюючи офіційні медіа-наративи один одного) їхнє аналогічне висвітлення війни в Україні триває довгий час (Düben, 2022).

Для населення КНР урядові ЗМІ створили альтернативну реальність. Згідно із національним мовником CCTV так звана «спеціальна військова операція» продиктована США, а також Сполучені Штати, можливо, фінансують програму біологічної зброї в Україні, а президент Росії Владімір Путін є жертвою, яка виступає за Росію, що опинилася в облозі.

Аналіз публікацій китайських користувачів у популярних соцмережах, здійснений службою новин CNN, показав, що найбільш поширені пости про події в Україні у більшості є проросійськими або ж містять інформацію, взяту з російських інтернет-джерел. Немає офіційних підтверджень стосовно належності цих дописів скоординованій пропагандистській кампанії між двома країнами, але це узгоджується з існуючою тенденцією, в якій російські та китайські ЗМІ посилюють свої часто взаємозамінні тези з таких питань, як поводження з російськими

дисидентами, гонконгські продемократичні протести. витоки пандемії COVID-19 або передбачувана роль Америки в розпалюванні «кольорових революцій» проти авторитарних режимів.

Таке взаємне підкріплення також вилилося в широкі закордонні та англомовні пропагандистські операції, які обидві країни створили для просування своїх поглядів у всьому світі – шлях, який став більш важливим, оскільки російські державні ЗМІ були заборонені в ефірі та в Інтернеті в деяких країнах Заходу (McCarthy, 2022).

Згідно із дослідженням некомерційної організації Центр протидії цифровій ненависті (CCDH), компанія Facebook (Meta) не перешкоджає поширенню дезінформації, змови та пропаганди. Дослідження виявило дописи, що містять «екстремальну» дезінформацію, пов'язану з Україною, на сторінках Facebook CGTN, Global Times, Xinhua News і T-House, чотирьох ЗМІ, які Facebook раніше позначали як китайські державні ЗМІ (Majid, 2022).

Зважаючи на визнання компанії Meta екстремістською організацією та заборону її діяльності на території РФ, активізування пропагандистської діяльності китайської армії ботів у цих соціальних мережах, ознаменує початок чергової інформаційної боротьби проти Західного світу.

У Європейському Союзі підтримувані Кремлем ЗМІ RT і Sputnik були офіційно заборонені. А такі компанії, як Meta, материнська компанія Facebook та Instagram, YouTube втрутилися, щоб заблокувати їхній контент. Але на китайських каналах, таких як CGTN і Global Times, російські публікації наявні і активно друкуються. Публікації з цих акаунтів свідчать про те, що Україна та США ніби мають пронацистські нахили, повторюють російську дезінформацію про лабораторії і цитують Росію, яка заперечує, що планує повалити чинний уряд у своїй так званій «спеціальній військовій операції» в Україні (McCarthy, 2022).

Низка пов'язаних з китайським урядом ЗМІ та проросійських акаунтів у соціальних мережах поширюють прокремлівські настрої в китайському інтернеті, неправильно перекладаючи або маніпулюючи міжнародними новинами про війну в Україні. 21 квітня 2022 р. стаття, опублікована The Guardian, розповіла, як мирні жителі, які загинули під час російської окупації українського міста Буча, були вбиті крихітними металевими стрілами, які називаються флешетами, від снарядів такого типу, випущених російською артилерією. Однак South Review, офіційне державне ЗМІ та дочірнє підприємство Комуністичної партії Китаю, що належить газетній групі Guangzhou Daily, неправильно переклало статтю, стверджуючи, що снаряди були випущені українськими силами. Дебати про російське вторгнення дійсно існують у Китаї, але в соціальних мережах, за якими ретельно стежать, погляди, подібні до тих, що існують у західних ЗМІ, часто стикаються з цензурою. Антизахідні коментатори подій дотримуються лінії Кремля, звинувачуючи НАТО і США в тому, що вони називають «спеціальними військовими діями» (Tondo, 2022).

Не тільки загравранням із російськими наративами відзначився Китай за останній рік. Поки весь світ зосередився на підтримці українського уряду у боротьбі з агресором, виникла небезпека вторгнення КНР в Тайвань.

16 квітня 2022 р. президент Тайваню Цай Інвень назвала інформаційний напад на Тайвань «тактикою когнітивної війни». Для тайванців це давня проблема. Хоча загроза вторгнення є досить серйозною. Пекін давно прагне підірвати тайванську демократію і переконати острів добровільно або напівдобровільно вибрати об'єднання з материком. Якщо це неможливо, Китай докладе усіх зусиль аби роз'єднати Тайвань із середини аби він став легкою мішенню для китайського вторгнення і повернення цієї території.

Офіційне видання Народно-визвольної армії Китаю (НВАК) від 17 березня 2022 р. окреслює її пріоритет інформаційної війни, описуючи її як центральну роль над звичайною військовою силою. Він постулює, що війна еволюціонує від механізованих боїв до інформаційних нападів, заявляючи, що війна інформаційної ери залежить головним чином від інформації, щоб підкорити ворога. Офіційний

документ НВАК описує тактику в загальних рисах як позбавлення противника інформаційної переваги при одночасному зміцненні його власних інформаційних можливостей шляхом побудови інформаційної бойової системи. Документ не ідентифікує конкретного ворога, але Тайвань є вічною мішенню. У документі стверджується, що інформаційна війна як система призначена для боротьби з ворогом з переважаючою механізованою військовою міццю, ймовірно, натякаючи на Сполучені Штати та їх західних союзників (Bastlan, 2022).

У серпні 2022 р. Китай не лише привернув увагу світу своїми масштабними військовими навчаннями біля Тайваню, але зорганізував наступ на Тайвань у цифровій сфері. У соціальних мережах з'явилися сфабриковані історії про намір Китаю евакуювати своїх громадян з Тайваню після того як ракети були націлені на місцевий аеропорт через приїзд спікера Палати представників США Ненсі Пелосі на острів. А на зламаних цифрових вивісках у магазинах 7-Eleven по всьому Тайваню з'явилися повідомлення: «Розпалювач війни Пелосі, забирайся з Тайваню!». На залізничній станції в південному портовому місті Гаосюн цифрові знаки були замінені на «Пелосі стара відьма».

Саме з цим візитом американської спікери зросли як спроби хакерства, так і поширення дезінформації на популярних платформах соціальних мереж Facebook, YouTube та LINE, популярний на Тайвані додаток для обміну миттєвими повідомленнями.

Фейкові новини в соціальних мережах – це спосіб для Китаю прокласти шлях для їх можливої операції. Вони спрямовані на деморалізацію громадської думки, що тим самим полегшить КНР захопити Тайвань. Це та технологія, яку яка застосовувалася Росією щодо української громадськості перед початком повномасштабного вторгнення.

Більшість неправдивої опублікованої інформації в таких додатках, як LINE, виглядає так, ніби продукується звичайними громадянами, виглядають як звичайні громадяни Китаю, а не урядовими шпигунами. Вони працюють над зміцненням довіри з тайванським народом у своїх групах чату, спочатку публікуючи нешкідливу інформацію, таку як знижки в супермаркеті або заходи в місцевому храмі (Farmer, 2022).

Хоча щоденні напади на Тайвань абстрактні, одним із найбільш загрозливих сценаріїв для Тайваню є фізичний напад на ключову інформаційну лінію. Китай може розірвати підводний інтернет-кабель, який в даний час є єдиним джерелом доступу до Інтернету на острові. Кабель з'єднує Тайвань з материком, створюючи залежність від материка. Якщо цей кабель буде перерізано, більшість пристроїв зв'язку Тайваню вимкнуться і запобігатимуть будь-яким інтелектуальним системам озброєння та військовій координації на острові, фактично зробивши майже всі системи оборони непрацездатними. Але Китай має побоювання, що в найближчі 10 років власна інформаційна бойова система Тайваню може кинути виклик китайській, особливо з огляду на загрозу того, що Тайвань поділиться розвідданими зі Сполученими Штатами Америки.

Політична інформаційна війна Пекіна проти свого сусіда значною мірою провалилася. Настрої незалежності зростають з кожним роком. Це означає, що початкова мета, мирне – принаймні на поверхні – возз'єднання, виглядає все більш малоймовірним. Пекін все ще проводить кампанію за це, частково тому, що його власна риторика вдома залежить від ідеї, що тайванці є ошуканими співвітчизниками, яким можна показати світло. Китай випромінює це світло частково через процвітаючу індустрію контент-ферм Тайваню. Деякі з цих компаній мають міцні зв'язки з материком.

Дезінформаційні кампанії Китаю, спрямовані на те, щоб применшити або стерти російське вторгнення та військові злочини в Україні, стікають кров'ю на Тайвань через ці ЗМІ. Дослідження дезінформації навіть виявило зв'язки з традиційними ЗМІ. Два з чотирьох основних тайванських новинних агентств мали

значні фінансові зв'язки з материком. Один з них отримував платежі за написання статей про конкретні аспекти кризи проток (Bastlan, 2022).

Дезінформація – не єдиний фронт кібервійни Китаю. Кібератаки також можуть проявлятися у формі збоїв і спроб злому - як великомасштабних спроб інфраструктури, так і нападів на цифрові цілі меншого рівня, включаючи відмову в доступі або спотворенні урядових веб-сайтів (Farmer, 2022).

Китай неодноразово заперечував здійснення кібератак проти Тайваню та інших країн. У заяві CNN Business Міністерство закордонних справ назвало звинувачення острова «безпідставними і чисто зловмисними». Управління у справах Тайваню Китаю також розкритикувало тайванську владу за використання кібератак для обмовляння материка як «звичного трюку» та зміщення уваги громадськості від недавнього спалаху COVID-19 на острові.

«Ми наполегливо закликаємо Сполучені Штати та їхніх союзників припинити лити брудну воду на Китай з питань кібербезпеки», – заявив представник Міністерства закордонних справ Китаю Чжао Ліцзянь. «Китай рішуче виступає проти кібератак будь-якого роду, не кажучи вже про те, щоб заохочувати, підтримувати або потурати їм» (Cheung, 2021).

Висновки. Інформаційні війни та кібервійни, які проводить Китайська Народна Республіка, стають все більш важливими аспектами сучасної геополітичної боротьби. КНР визнає значення інформаційної влади та використовує різноманітні засоби для досягнення своїх політичних та військових цілей. Інформаційні війни включають розповсюдження дезінформації, маніпулювання громадською думкою та психологічні операції для зміни уявлень та переконань громадян в інших країнах. Китай використовує свої державні ЗМІ для просування власних ідеологій та переконань за межами своїх кордонів. Також він веде кібератаки, що означає зловживання комп'ютерними системами та мережами для завдання шкоди іншим країнам або організаціям. У кібервійнах, КНР використовує різноманітні методи, включаючи хакерські атаки, кібершпигунство, а також здатність заволодіти та контролювати інформаційні системи інших країн. Ці атаки можуть бути спрямовані на військові, економічні або політичні цілі.

Співпраця Китаю із Росією у інформаційній війні спрямована на формування позитивного образу Путіна і його режиму у війні, а також дискредитація колективного Заходу та України серед китайського населення, а також іноземних споживачів нових медіа.

В свою чергу російсько-українська війна стала гарною нагодою для здійснення Китаєм кібератак проти Тайваню, що покликана деморалізувати тайванців та схилити їх до добровільного об'єднання з материковим Китаєм. Російське вторгнення в Україну мало стати прикладом небажання та неспроможності США підтримати своїх союзників під час збройних конфліктів. Для Європи та США інформаційна атака на острів мала стати відволікаючим фактором від російських військових злочинів в Україні, а також актом залякуванням новою війною.

REFERENCES

Bagchi, I. (2020). Doklam standoff: China playing out its 'Three Warfares' strategy against India. *The Times of India*. Retrieved from https://cutt.ly/pwWatLex

Bastlan, A.A. (2022). China Is Stepping Up Its Information War on Taiwan. *Foreign policy*. Retrieved from https://cutt.ly/SwWauSLU

Cheung, E. & Ripley, W. (2021). How Taiwan is trying to defend against a cyber 'World War III'. *CNN busness*. Retrieved from https://cutt.ly/qwWaiqlG

Düben, B.A. (2022). What Putin's War in Ukraine Means for the Future of China-Russia Relations. *LSE IDEAS*, 6-7 Retrieved from https://cutt.ly/bwWayi8e

Dubov, D. (2014). *Cyber space as a new dimension geopolitical rivalry*. Kyiv: NIST // **Дубов, Д.** (2014). *Кберпростір як новий вимір геополітичного суперництва*. Київ: НІСТ.

Farmer, B.M. (2022). China's cyber assault on Taiwan. *CBS news*. Retrieved from https://cutt.ly/dwWauNJ8

Goodman, J. (2021). The disinformation tactics used by China. *BBC news*. Retrieved from https://cutt.ly/gwWaevFi

Ha, M. & Cho, A. (2020). China's Coronavirus Disinformation Campaigns Are Integral to Its Global Information Warfare Strategy. *FDD*. Retrieved from https://cutt.ly/ewWatphB

Kalinicheva, H. (2023). Use of informational and psychological weapons in the conditions of the Russian-Ukrainian war. *Acta de Historia & Politica: Saeculum XXI, 6,* 53-65. DOI: https://doi.org/10.26693/ahpsxxi2023.06.053 // **Калінічева, Г.** (2023). Використання інформаційно-психологічної зброї в умовах російсько-української війни. *Acta de Historia & Politica: Saeculum XXI*, 6, *53-65*. DOI: https://doi.org/10.26693/ahpsxxi2023.06.053

Martin, S. (2021). How a fake network pushes pro-China propaganda. *BBC news*. Retrieved from https://cutt.ly/TwWaeO5x

Majid, A. (2022). How Chinese state media outlets use Facebook to promote pro-Russia misinformation. *PressGazette*. 2022 Retrieved from https://cutt.ly/ZwWayGu9

McCarthy, S. (2022). China's promotion of Russian disinformation indicates where its loyalties lie. *CNN World*. Retrieved from https://cutt.ly/nwWaym2w

Raska, M. (2015). China and the 'Three Warfares'. *The Diplomat*. Retrieved from https://cutt.ly/iwWaeB8u

Taking Taiwan Through Cyber (N.d) *Defending Taiwan*. *American Enterprise Institute* Retrieved from https://cutt.ly/fwWat37k

Tondo, L. & Ni, V. (2022). China's pro-Russia propaganda exposed by online activists. *The Gardian*. 2022 Retrieved from https://cutt.ly/TwWausV9

Ventre, D. (2010). China's Strategy for Information Warfare: A Focus on Energy. *Jornal of Energy Security*. Retrieved from https://cutt.ly/xwWaefMl

Wibawa, T. (2019). China's national security and the 'three warfares': How Beijing decides who or what to target. *ABC news*. Retrieved from https://cutt.ly/ewWarikZ

Winger, G. (2020). China's Disinformation Campaign in the Philippines. *The Diplomat*. Retrieved from https://cutt.ly/qwWatbbr

Zaporozhets, O. (2023). Internet Trolling As Information Warfare Tool. *Acta de Historia & Politica: Saeculum XXI*, 6, 66-74. DOI: https://doi.org/10.26693/ahpsxxi2023.06.066 // **Запорожець, О.** (2023). Інтернет-тролінг я к інструмент інформаційної війни. *Acta de Historia & Politica: Saeculum XXI,* 6, 66-74. DOI: https://doi.org/10.26693/ahpsxxi2023.06.066