УДК 341.1/8
DOI https://doi.org/10.32782/2524-0374/2023-11/166

КІБЕРТЕРОРИЗМ З БОКУ ДЕРЖАВ НА ПРИКЛАДІ ДІЙ КИТАЙСЬКОЇ НАРОДНОЇ РЕСПУБЛІКИ (КНР) ПРОТИ КИТАЙСЬКОЇ РЕСПУБЛІКИ (ТАЙВАНЬ). МІЖНАРОДНО-ПРАВОВИЙ АНАЛІЗ ТАКИХ ДІЙ

CYBERTERRORISM BY STATES USING THE EXAMPLE OF THE ACTIONS OF THE PEOPLE'S REPUBLIC OF CHINA (PRC) AGAINST THE REPUBLIC OF CHINA (TAIWAN). AN INTERNATIONAL LEGAL ANALYSIS OF SUCH ACTIONS

Фещуков Г.В., молодший науковий співробітник з міжнародного права
Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка

Ця наукова стаття представляє розширений аналіз феномену кібертероризму, фокусуючись на активності Китайської Народної Республіки (КНР) у контексті її агресії проти Тайваню. Основним об'єктом дослідження є міжнародно-правовий аспект таких кібератак, зокрема їх відповідність міжнародним нормам і існуючим міжнародно-правовим документам, які стосуються даного питання.

Стаття проводить комплексний аналіз різних аспектів цієї проблеми, охоплюючи правовий статус кібертерористичних дій, можливі наслідки для міжнародної безпеки та стабільності, а також різні варіанти реакції міжнародного співтовариства на подібні акти агресії. Дослідження також розглядає можливі санкції та відповідальність, які можуть бути застосовані до держав, що вчиняють кібертерористичні атаки, відповідно до існуючих норм і правил міжнародного права.

Загальна мета статті полягає в тому, щоб визначити, як міжнародне право регулює кібербезпеку та які механізми контролю та санкцій можуть бути використані для забезпечення безпеки та стабільності в кіберпросторі в контексті дій держав, таких як КНР, які використовують кібертероризм для досягнення своїх політичних цілей. На основі цього дослідження можливе виявлення ефективних способів реагування на кібертерористичні загрози та зміцнення правового фундаменту для забезпечення кібербезпеки в міжнародному вимірі.

У додатковому контексті ця наукова стаття присвячена розгляду важливого і актуального аспекту міжнародних відносин та міжнародного права. Зростаюча кількість кібератак, особливо від державних акторів, створює суттєві виклики для міжнародної громадської безпеки та стабільності. Аналізувати реакцію міжнародного співтовариства на такі кібертерористичні акти стає надзвичайно важливою задачею, яка вимагає глибокого розуміння міжнародного права та його придатності до регулювання кібербезпеки.

Підсумовуючи, ця стаття спрямована на розкриття проблеми кібертероризму через призму міжнародного права та визначення ефективних засобів та механізмів для протидії цій загрозі. Надзвичайно актуальна і спільно обговорювана, вона має на меті сприяти розвитку стратегій, спрямованих на підтримку стабільності та міжнародної безпеки в кіберпросторі, зокрема в контексті активності держав, що використовують кібертероризм для досягнення своїх політичних цілей.

Ключові слова: кібертероризм, міжнародне право, кіберпростір, кібербезпека, міжнародно-правова відповідальність, кібероперації, когнітивна війна.

This scientific article presents an expanded analysis of the phenomenon of cyberterrorism, focusing on the activities of the People's Republic of China (PRC) in the context of its aggression against Taiwan. The primary object of the study is the international legal aspect of such cyberattacks, including their compliance with international norms and existing international legal documents related to this issue.

The article conducts a comprehensive analysis of various aspects of this problem, encompassing the legal status of cyberterrorist actions, potential consequences for international security and stability, as well as various options for the international community's response to such acts of aggression. The research also examines potential sanctions and accountability that can be applied to states engaging in cyberterrorist attacks in accordance with existing norms and rules of international law.

The overall objective of the article is to determine how international law regulates cybersecurity and what mechanisms of control and sanctions can be used to ensure security and stability in cyberspace in the context of actions by states such as the PRC, which use cyberterrorism to achieve their political goals. Based on this research, it is possible to identify effective ways to respond to cyberterrorist threats and strengthen the legal foundation for ensuring cybersecurity on an international scale.

In an additional context, this scientific article is dedicated to examining an important and current aspect of international relations and international law. The increasing number of cyberattacks, especially by state actors, poses significant challenges to international public security and stability. Analyzing the response of the international community to such cyberterrorist acts becomes an exceptionally important task that requires a deep understanding of international law and its applicability to regulating cybersecurity.

In summary, this article aims to shed light on the issue of cyberterrorism through the lens of international law and to identify effective means and mechanisms to counter this threat. It is highly relevant and widely discussed, with the goal of promoting the development of strategies aimed at supporting stability and international security in cyberspace, particularly in the context of the activities of states that employ cyberterrorism to achieve their political objectives.

Key words: cyberterrorism, international law, cyberspace, cybersecurity, international legal responsibility, cyber operations, cognitive warfare.

Обираючи тему своєї статті, я не міг обійти таку проблематику як «кібертероризм», що в майбутньому може торкнутись і України, що наразі перебуває в стані війни і, безумовно, може стати «жертвою» таких дій в майбутньому. Варто зазначити, що масовані кібератаки проти Тайваню, що були організовані та сплановані владою КНР є далеко не першим прикладом кібератак як таких, що підтримуються, фінансуються, або безпосередньо проводяться однією державою проти іншої (тут варто нагадати, що Китайська Республіка є частково визнаною державою, яка, в залежності від політичної сили що приходила до влади, то позиціонувала себе як законний уряд «єдиного суверенного Китаю», то як окремою незалежною державою [1]), але є першим прикладом в світовій історії саме «кібертероризму» з боку держави. Перш ніж перейти до безпосереднього міжнародно-правового аналізу даних дій та зачепити питання можливості притягнення до міжнародно-правової відповідальності суб'єктів міжнародного права, що вчиняють такі дії, хотілось би звернути увагу на основну мету та передумови, що будуть розглянуті у вигляді таблиці поданої нижче (табл. 1).

Таблиця 1

Кібертероризм КНР проти Китайської Республіки: основна мета та передумови

Передумови	Основною передумовою виявилось те, що КНР наразі не готова до прямого збройного конфлікту з Тайванем, що отримує всебічну підтримку США, а отже КНР необхідно використовувати альтернативні методи впливу і тиску на Тайвань. Більше того, невдала агресивна війна РФ проти України лише переконала уряд КНР у правильності їх рішення та «вибору». Не дивлячись на те, що загроза прямого вторгнення на територію Тайваню не може бути повністю виключена (особливо якщо брати до уваги засекречений документ, що, як публічно заявляє розвідка США, нещодавно був підписаний Головою КНР Сі Цзіньпіном, який передбачає взяття під контроль острову Тайвань «будь-якими можливими засобами та способами» до 2027 року [2]), але така вірогідність наразі є доволі невисокою.
Мета	Основною метою є дискредитація населення Тайваню як такого в очах світової спільноти, поширення дезінформації та ІПСО всередині самого Тайваню, направлена на «єдиний можливий варіант» – об'єднання з «великою землею». Окрім цього, постійні хвилі кібератак від яких страждає Тайвань негативно впливають на економічні показники країни, а також підривають довіру місцевого населення до фінансових установ (кража особистих даних, зняття грошей з рахунків, тощо). Про постійне і масове шпигунство за різними держслужбовцями Тайваню не варто і згадувати – спроби «зламати» Твітер чи якусь чи якусь персональну сторінку такої особи стали «рутиною» роботою для хакерів з КНР [3, с. 1–29].

В період з вересня 2019 по серпень 2020 Тайвань «пережив» 1.4 млн кібератак з боку КНР, атаки були направлені на політичні, економічні та військові структури [4]. Ось лише деякі з них (табл. 2).

Таблиця 2

Кібертероризм КНР проти Китайської республіки: приклади такої «агресії»

Квітень 2022	На початку пандемії COVID-19 голова ВООЗ Тедрос Аданом Гебреїсус заявив що він став жертвою расистських висловлювань з боку тайванських «юзерів». Хоча офіційна влада Тайваню і надала офіційну позицію, заявивши, що це були «боти» з КНР, але це все одно тим чи іншим чином негативно вплинуло на імідж Тайваню в очах світової спільноти [4].
Серпень 2022	Під час візиту Спікера Палати представників США Ненсі Пелосі хакери з КНР «зламали» вивіски магазинів та інформаційні дисплеї на одній з великих залізничних станцій, критикуючи саму Пелосі та її подорож [4].
Листопад 2022	Втручання у місцеві вибори Тайваню з метою розкачування ситуації та вкидування дезінформації, що направлена проти нинішньої влади Тайваню [4].

Як і було зазначено вище, це лише деякі приклади з останніх кібератак вчинених КНР проти Тайваню. Хоч кожна кібератака і є свого роду «унікальною» та готується заздалегідь, ми можемо виділити три основні мети, які вони переслідують:

– Дискредитація населення Тайваню в очах світової спільноти Такі кібератаки направлені на цільову аудиторію, що знаходиться поза межами Тайваню, в тому числі на аудиторію, що знаходиться в самій КНР;

– Поширення дезінформації та ІПСО проти місцевого населення, основна ціль якої зневіра місцевого населення (основна теза – «Тайвань залишиться сам на сам з КНР»), просування пропаганди КНР та ідеї «єдиного Китаю»;

– Несанкціоноване отримання інформації з метою отримання економічної, політичної чи військової переваги, простими словами – кібершпигунство.

Міжнародно-правова відповідальність КНР за кібертероризм проти Тайваню

На жаль, тут необхідно зазначити дві основні тези:

– наразі не існує жодного універсального правового документа, що стосувався би кібербезпеки як такої, а також прописував би механізм моніторингу/контролю та міжнародно-правову відповідальність держав за вчинення таких дій;

– так як кібератаки КНР проти Тайваню не можна вважати такими, що перевищують «поріг застосування сили» або проводяться в рамках збройного конфлікту («військові кібероперації») [7, с. 373–393], мова про застосування міжнародного гуманітарного права також не йде.

Таким чином, можемо підтримати висліів президента Тайваню Цай Інвень про тактику ведення «когнітивної війни» проти Тайваню з боку КНР, однак це не призводить до жодних правових наслідків для КНР і, фактично, свідчить про суттєву прогалину в міжнародному праві, що пояснюється небажанням так званих «великих держав» якимось чином регулювати питання військових кібероперацій в міжнародному праві, надаючи перевагу тому, щоб все це залишалось в так званому «правовому вакуумі», таким чином уникаючи міжнародно-правових наслідків за вчинені дії, що чітко ілюструє вищеописаний приклад дій з боку КНР.

Таблиця 3

Кібертероризм КНР проти Китайської республіки: правові позиції сторін

Позиція КНР	Позиція Тайваню
Офіційна влада КНР не бере на себе відповідальність за кібератаки на Тайвань та в цілому мало коментує дану ситуацію, вдаючи вигляд, що офіційні особи/влада як така не мають жодного відношення до цього. Більше того, офіційні представники КНР неодноразово заявляли, що вони самі страждають він таких «інцидентів» [5].	Тайвань обережно оцінює такі дії. І на це є ряд своїх причин. По-перше, доволі важко довести причетність тієї чи іншої держави до кібератаки. По-друге, важко сказати чи можна вважати кібератаку тим, що перевищує «поріг застосування сили», що безпосередньо веде до правових наслідків для держави. Як зазначила президент Тайваню Цай Інвень влітку 2022 року – КНР веде «когнітивну війну» проти Тайваню [6], однак, такий термін просто відсутній в юридичній площині і наразі важко казати про якісь можливі «правові наслідки» для КНР за їх фактичний «кібертероризм» проти Тайваню.

ЛІТЕРАТУРА

1. China-Taiwan Relations Re-examined: The "1992 Consensus" and Cross-Strait Agreements. Yu-Jie Chen and Jerome A. Cohen (Published by Penn Law: Legal Scholarship Repository, 2019). URL: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1039&context=alr (date of access: 20.10.2023).

2. China 'wants to be ready to invade Taiwan by 2027' CIA director says. *Sky News Australia*. 2023. URL: https://www.news.com.au/world/asia/chinese-president-xi-jinping-has-ordered-his-military-to-be-to-invade-taiwan-in-2027-cia-director-says/news-story/06aa78c2cfcf8dfd6dc420392114dc23 (date of access: 20.10.2023).

3. Manantan, Mark Bryan. "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea." Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs 56, no. 3, 2040013 (2020): p. 1–29.

4. R. Nemoto, H. Ryugen and Y. Nakamura «China intensifies disinformation, cyberattacks on Taiwan: report». *Nikkei Asia*. 2022. URL: https://asia.nikkei.com/Politics/International-relations/Taiwan-tensions/China-intensifies-disinformation-cyberattacks-on-Taiwan-report (date of access: 20.10.2023).

5. J. Macy Yu «Chinese cyber attacks on Taiwan government becoming harder to detect: source». *Reuters*. 2018. URL: https://www.reuters.com/article/us-taiwan-china-cybersecurity-idUSKBN1JB17L (date of access: 20.10.2023).

6. Erica D. Lonergan and Grace B. Mueller «What Are the Implications of the Cyber Dimension of the China-Taiwan Crisis?» *The Council on Foreign Relations (CFR)*. 2022. URL: https://www.cfr.org/blog/what-are-implications-cyber-dimension-china-taiwan-crisis (date of access: 20.10.2023).

7. Baig, Muhamad Ali. "Conventional Military Doctrines and U.S.-China Military Engagement in the West Pacific." China Quarterly of International Strategic Studies 5, no. 3 (2019): p. 373–393.