

МІЖНАРОДНЕ ПРАВО

КУШНІР В. В.,
аспірант кафедри морського
та міжнародного права
(Міжнародний гуманітарний
університет)

УДК 341.3

DOI <https://doi.org/10.32842/2078-3736/2025.3.2.29>

ПОНЯТТЯ ІНФОРМАЦІЙНОЇ ВІЙНИ В МІЖНАРОДНОМУ ПРАВІ

Стаття присвячена аналізу підходів та концепцій до змісту поняття «інформаційна війна».

Позначено, що сьогоденні міжнародно-правові проблеми ускладнюють зусилля міжнародної спільноти щодо здійснення відповідей на певні атаки інформаційної війни. Принципи міжнародного права регулюють певні моменти, безумовно, які застосовуватимуться до інформаційної війни, та позначають юридичні обмеження щодо вчинення агресивних дій. Однак зміст положення норм Статуту ООН не містить прямої вказівки на інформаційні атаки. Такі атаки потрібно виявити та довести, що вони є актом агресії.

Підкреслено, що фундаментальний принцип міжнародного права сьогодні потрібно розширено тлумачити, щоб застосовувати його до інформаційної війни. Так, має бути встановлено зв'язок інформаційних атак з порушенням принципу незастосування сили чи погрози силою. Так само незрозуміло яким чином міжнародне гуманітарне право покликане стримувати інформаційні атаки.

Позначено, що неоднозначний стан міжнародного права щодо інформаційної війни може надавати країнам можливість вчиняти інформаційні атаки безкарно. Прикладом в цьому випадку є збройний конфлікт в Україні.

Підкреслено, що доречно укласти угоди щодо захисту критично важливих інформаційних систем, або заборонити атаки на певні системи чи об'єкти, або створити міжнародні режими захисту для окремих систем. Так, інформаційна війна може бути відповідною сферою для укладання угод щодо контролю над озброєнням.

Зроблено акцент на думках зарубіжних та українських вчених, які надають своє бачення в розумінні того, що таке інформаційна війна і, яким чином вона пов'язана з пропагандою та впливом на свідомість населення, які дії можна прирівняти до актів інформаційної агресії.

Позначено, що інформаційні технології швидко розвиваються та змінюють спосіб комунікації в міжнародній спільноті. Поточна база міжнародного права може бути ефективно застосована до інформаційних операцій і війни, якщо запровадити системну співпрацю та ефективний контроль над інформаційними системами.

Зроблено висновок, що інформаційна війна – це певні наступальні інформаційні операції чи атаки, які використовуються під час кризи чи конфлікту для досягнення або просування конкретних цілей проти конкретного противника.

Ключові слова: інформаційна війна, Статут ООН, збройний конфлікт, пропаганда, інформаційна атака, інформаційні технології, принципи міжнародного права.



Kushnir V. V. The concept of information warfare in international law

The article is devoted to the analysis of approaches and concepts to the content of the concept of “information war”.

It is noted that today’s international legal problems complicate the efforts of the international community to respond to certain attacks of information warfare. The principles of international law regulate certain points, of course, which will be applied to information warfare, and indicate legal restrictions on committing aggressive actions. However, the content of the provisions of the UN Charter does not contain a direct indication of information attacks. Such attacks must be identified and proven to be an act of aggression.

It is emphasized that the fundamental principle of international law today needs to be broadly interpreted in order to apply it to information warfare. Yes, the connection between information attacks and the violation of the principle of non-use of force or the threat of force must be established. It is also unclear how international humanitarian law is designed to deter information attacks.

It is noted that the ambiguous state of international law regarding information warfare may give countries the opportunity to carry out information attacks with impunity. An example in this case is the armed conflict in Ukraine.

It is emphasized that it is appropriate to conclude agreements on the protection of critical information systems, or to prohibit attacks on certain systems or objects, or to create international protection regimes for individual systems. Yes, information warfare may be an appropriate area for arms control agreements.

It is noted that information technologies are rapidly developing and changing the way of communication in the international community. The current framework of international law can be effectively applied to information operations and warfare if systematic cooperation and effective control over information systems are implemented.

It is concluded that information warfare is certain offensive information operations or attacks that are used during a crisis or conflict to achieve or advance specific goals against a specific adversary.

Key words: *information war, UN Charter, armed conflict, propaganda, information attack, information technologies, principles of international law.*

Вступ. Розвиток концепції поняття «інформаційна війна» представляє собою актуальне питання міжнародного права. Сьогоднішні міжнародно-правові проблеми ускладнюють зусилля міжнародної спільноти щодо здійснення відповідей на певні атаки інформаційної війни, зокрема ті, що використовують комп’ютери, телекомунікації або мережі для атак на інформаційні системи противника.

Сучасні міжнародні відносини все частіше супроводжуються використанням інформаційних технологій як інструментів впливу, дестабілізації та досягнення політичних цілей. У зв’язку з цим виникає потреба в науковому аналізі явища інформаційної війни, яке дедалі більше загрожує міжнародному миру, безпеці та суверенітету держав. Міжнародне право традиційно регулює збройні конфлікти, кібероперації, пропаганду війни та втручання у внутрішні справи держав, проте поняття «інформаційна війна» досі не має чіткого та усталеного визначення в міжнародно-правових документах. Це ускладнює розробку ефективних правових механізмів протидії інформаційній агресії, захисту інформаційного суверенітету та притягнення до відповідальності за відповідні дії.

Принципи міжнародного права регулюють певні моменти, безумовно, які застосовуватимуться до інформаційної війни, та позначають юридичні обмеження щодо вчинення агресивних дій. Тим не менш, новизна окремих методів інформаційної війни може вивести їх з-під застосування встановлених правових категорій. Крім того, здатність інформаційних сигналів поширюватися міжнародними мережами та впливати на системи управління



у віддалених країнах суперечить давньому принципу – національного територіального суверенітету.

Постановка завдання. Метою статті є всебічне дослідження поняття інформаційної війни в контексті міжнародного права, зокрема виявлення прогалин у нормативному регулюванні цього явища, аналіз існуючих правових підходів до визначення та кваліфікації інформаційної агресії, а також формулювання пропозицій щодо удосконалення міжнародно-правового механізму протидії інформаційним загрозам.

Результати дослідження. Термін «інформаційна війна» з'явився в середині 1970-х років. Його запропонував вчений-фізик Томас Рон, який не тільки першим зрозумів, але і науково обґрунтував те, що саме інформація є найслабшою ланкою будь-якої армії [1, с. 300].

Які ж проблемні моменти в міжнародному праві сьогодні виникають щодо змісту та сутності поняття «інформаційна війна».

По-перше, має бути встановлено зв'язок інформаційних атак з порушенням принципу незастосування сили чи погрози силою. Треба встановити зв'язок між такою атакою та наслідками, особливо якщо вони не є смертельними або фізично руйнівними.

Таким чином, такі напади можуть бути легальними формами примусу навіть у мирний час, і використання звичайних збройних сил може бути невідповідною відповіддю на такі напади. Відповідно до Статуту ООН таку відповідь дійсно можна вважати вже актом агресії, а не самозахистом. З іншого боку, жодне положення міжнародного права не заважає країнам вживати дії проти інших держав, таких як ембарго, які завдають великих труднощів цим державам та їх населенню.

Як позначають І. Жаровська, Н. Ортинська: «Стаття 51 Статуту ООН визначає, що цей документ «жодним чином не зачіпає невід'ємного права на індивідуальну або колективну самооборону, якщо відбудеться збройний напад на Члена Організації, доти, поки Рада Безпеки не вдасться до заходів, необхідних для підтримки міжнародного миру й безпеки». Отож принципи міжнародного права вказують чітко про збройний напад на територію, тому немає чіткої прив'язки до можливості застосування даної норми широко» [2, с. 59].

По-друге, так само незрозуміло, чи є частина шкоди, яку можуть завдати атаки інформаційної війни, як-от порушення урядових або приватних баз даних і систем, шкодою, яку покликане стримувати міжнародне гуманітарне право.

Як позначає І. В. Феценко: «Міжнародне право не має притаманних йому «силових» механізмів і структур примусу, тому виконання його вимог складає особливу проблему. Зважаючи на відсутність потужних важелів виконання приписів міжнародного гуманітарного права (суд, поліція, армія) ефективність його регулятивної функції залежить від дійсної імплементації та функціонування механізму реалізації» [3, с. 101].

Нарешті, там, де атаки можуть бути здійснені через міжнародні мережі, держави/державам може знадобитися звернутись за допомогою до іншої країни чи міжнародної організації у виявленні та реагуванні на тих, хто здійснив інформаційну атаку.

Неоднозначний стан міжнародного права щодо інформаційної війни може надавати країнам можливість вчиняти інформаційні атаки безкарно. І навпаки, це може дозволити супротивникам атакувати країну-агресора та їх інформаційні системи. Прикладом в цьому випадку є збройний конфлікт в Україні.

Яскравим прикладом інформаційної війни може стати міждержавний конфлікт між Україною та Росією, в якому використовується політична та соціологічна пропаганда, комплекс заходів, постійно здійснюваних урядовими та неурядовими організаціями Росії та України в інформаційному просторі України, Росії, інших країн та міжнародних організацій, спрямованих на отримання стратегічно-політичних переваг шляхом деморалізації або введення в оману противника та протидії заходам іншої сторони у глобальному протистоянні Росії і України, а також протистоянні Росії та «Західного світу» [4].

Анексія Криму, військовий конфлікт на Сході нашої держави – це наслідок цілеспрямованого впливу інформаційної війни, тому питання правового регулювання вказаної проблеми є особливо актуальним. Вказане підтверджує той факт, що Спеціальна європейська



група по боротьбі з фальшивими прокремлівськими повідомленнями повідомила про більш ніж 5 тисяч випадків російської дезінформації з 2015 року, з них близько 2 тис стосувалися України [2, с. 58].

Тим не менш, ми можемо обговорити кілька міжнародно-правових підходів, які можуть використовувати держави для захисту своїх інформаційних систем та мереж або уточнення своїх наступальних, оборонних і інших варіантів відповіді.

По-перше, міжнародна спільнота могла б вже сьогодні використовувати до інформаційної атаки такі поняття, як «сила» або «збройний напад», які стосуються інформаційної війни; такі визначення можуть допомогти визначити, коли такі атаки можуть бути здійснені та як країни можуть на них відповісти.

По-друге, на рівні ООН чи інших міжнародних організацій потрібно організувати платформа для обговорення та дискусії щодо міжнародного співробітництва проти атак інформаційної війни, заохочуючи співпрацю у розслідуванні та переслідуванні відповідальних за атаки, зокрема терористів та інших злочинців.

По-третє, доречно укласти угоди щодо захисту критично важливих інформаційних систем, або заборонити атаки на певні системи чи об'єкти, або створити міжнародні режими захисту для окремих систем.

По-четверте, деякі припускають, що інформаційна війна може бути відповідною сферою для укладання угод щодо контролю над озброєнням. Однак кілька факторів, у тому числі новизна багатьох технологій і методів інформаційної війни, широке розповсюдження, малий розмір і переважно цивільний характер багатьох інформаційних технологій, а також небезпека того, що контроль над озброєннями не поширюватиметься на недержавних акторів, таких як терористи, все свідчить про те, що прагнення до контролю над озброєнням було б у кращому випадку передчасним, особливо у зв'язку з переважно над нелетальними технологіями. Незважаючи на очевидну привабливість вжиття правових заходів для захисту інформаційних систем, міжнародно-правова регламентація може бути достатньо повільно здійснена, щоб встигнути за технологічними змінами, і, отже, втрачає в деякому сенсі свою актуальність.

Оскільки всесвітній розвиток інформаційних технологій, включаючи комп'ютери, телекомунікації та мережі, змінює спосіб ведення бізнесу, урядування та освіти, він вимагає змін до розуміння підходів для регулювання інформаційної сфери. Інформаційні технології поширюються практично на всю військову зброю, засоби зв'язку і системи командування та управління, а також цивільні системи, які підтримують сучасні економіки та їхні військові зусилля. Як позначають Лоуренс Т. Грінберг, Сеймур Е. Гудмен, Кевін Дж. Су Ху деякі з нових способів ведення інформаційних атак було названо «інформаційною війною», яка в широкому сенсі визначається як «будь-яка дія, спрямована на заперечення, використання, пошкодження або знищення інформації супротивника та його функцій; захист себе від цих дій і використання власних військових інформаційних функцій» [5, р. 1]. Таким чином, інформаційна війна включає як нові методи, такі як комп'ютерне втручання та збій і телекомунікаційний спуфінг, так і старі, такі як хитрощі, маскування та фізичні атаки на спостережні пости та лінії зв'язку.

Дехто припускає, що інформаційна війна може започаткувати еру здебільшого безкровного конфлікту; битва відбуватиметься в «кіберпросторі», оскільки «інформаційні війни» зможуть вивести з ладу важливі ворожі системи командування та управління або цивільну інфраструктуру з невеликими, якщо взагалі будуть, жертвами. Інші науковці прогнозують майбутні конфлікти, у яких кровопролиття лише посилюється завдяки покращенню та розширенню комунікацій [6, р. 22]. Треті – припускають, що інформаційні технології можуть сприяти розвитку нових форм соціальної організації разом із новими формами конфлікту [7, р. 275].

Незалежно від того, що розвиток і розповсюдження інформаційних технологій означають для майбутнього війни, очевидно, що деякі з нових форм атак, створених інформаційними технологіями, можуть якісно відрізнятися від попередніх форм атак. Використання таких засобів, як комп'ютерне вторгнення та комп'ютерні віруси, наприклад, може вивести війну



з фізичного, кінетичного світу та перенести її в нематеріальний, електронний. Ці нові форми атак, деякі з яких можуть здатися продуктом наукової фантастики, варіюються вздовж континуумів, починаючи від тих, які не мають фізичного впливу на ворога, до таких, які можуть спричинити серйозні руйнування або загибель людей, від тих, які не мають фізичного втручання за межами національних кордонів до тих, що вимагають традиційних військових вторгнень, і від тих, що вражають суто цивільні цілі, до тих, які вражають суто військові. Атаки можуть здійснюватися на відстані, через радіохвилі або інтернет, без фізичного вторгнення за межами ворожих кордонів. Збитки можуть варіюватися від загибелі військових чи цивільних через збої в системі, до відмови в обслуговуванні важливих військових чи державних систем під час кризи, до економічних труднощів або просто незручностей для цивільного населення, яке залежить від інформаційних систем у своєму повсякденному житті.

Я. Малик позначає, що «інформаційна війна – це форма ведення інформаційного протистояння між різними суб'єктами, наприклад, державами, неурядовими, економічними та іншими структурами, яка передбачає проведення комплексу з нанесення шкоди інформаційній сфері конкуруючої сторони і захисту власної інформаційної сфери, конкуруючої сторони і захисту власної інформаційної безпеки» [8].

Наведемо деякі приклади інформаційних атак, які впливають на розуміння поняття «інформаційна війна». «Інфоблокада» може дозволити певній кількості інформації не потрапляти до певної країни чи не виходити за її межі. Також інфраструктура командування та контролю в країні може бути порушена, а окремі військові підрозділи не зможуть спілкуватися між собою або з центральним командуванням. Інший приклад – фондові або товарні біржі, електромережі та муніципальні системи управління рухом, системи управління повітряним рухом або навігації можуть бути піддані маніпуляціям або збоєм, що супроводжується економічними чи суспільними порушеннями, фізичним знищенням або людськими жертвами.

В.С. Яковчук, Б.І. Малець, Ю.О. Борзов розуміють що інформаційна війна – складова частина ідеологічної боротьби, елементом якої є пропаганда. Пропаганда є механізмом холодної війни, потреба в якій надала суттєвий поштовх розробці теорії комунікації, бо виникла велика кількість суто прикладних завдань у галузі комунікації [9].

І. Жаровська, Н. Ортинська підкреслюють, що «особливістю інформаційної війни є не тільки те, що вплив здійснюється з використанням новітніх засобів, а й те, що це невідконтрольний ресурс, який дуже слабо піддається правовій регламентації, тому активно застосовує неправдиву, перекручену інформацію як засіб маніпуляції свідомістю» [2, с. 60].

І.І. Проноза в цьому ж аспекті надає визначення інформаційній війні: «Так, в рамках психологічної парадигми інформаційна війна розуміється як латентний вплив інформації на індивідуальну, групову і масову свідомість за допомогою методів пропаганди, дезінформації, маніпулювання з метою формування нових поглядів на соціально-політичну організацію суспільства через зміну ціннісних орієнтацій і базових установок особистості» [10, с. 78].

В період ведення інформаційної війни для широкомасштабної експансії ворог може маніпулювати свідомістю і загрожувати національній безпеці України. Тому необхідна адекватна інформаційна протидія як з боку нашої країни, так і міжнародної спільноти.

П. Шевчук з цього приводу пропонує здійснення конкретних кроків, які з метою покращать стан вітчизняної інформаційної політики та національної безпеки загалом, зменшать інформаційно-психологічний вплив російської федерації та захистять інформаційне поле нашої держави [11].

Висновки. Отже, інформаційні технології швидко розвиваються та змінюють спосіб комунікації в міжнародній спільноті. Інформаційні технології у сфері міжнародного права, це ще один інструмент в розвитку військових технологій, який не змінив основних фундаментальних принципів права та ведення війни в нашій нинішній парадигмі міжнародного права. Поточна база міжнародного права може бути ефективно застосована до інформаційних операцій і війни. Це досягається шляхом використання оперативного контролю. Такий підхід передбачає поступові, еволюційні зміни та перегляд сучасної системи міжнародних відносин з метою адаптації до мінливого інформаційного середовища.



Інформаційна війна як явище набуває дедалі більшої актуальності в сучасних міжнародних відносинах, порушуючи фундаментальні принципи суверенітету, невтручання та миру. Водночас міжнародне право залишається недостатньо адаптованим до викликів, що пов'язані з масштабними та системними інформаційними впливами, особливо в умовах цифровізації та глобалізації. Незважаючи на наявність низки міжнародно-правових актів, що торкаються окремих аспектів інформаційної діяльності – таких як заборона пропаганди війни, кібербезпека, права людини в інформаційному просторі – уніфікованого та загально-визнаного поняття «інформаційної війни» міжнародне право поки що не містить.

У результаті проведеного аналізу встановлено, що інформаційна війна має багатовимірний характер і може включати елементи дезінформації, кібератак, психологічного впливу, пропаганди та втручання у внутрішні справи держав. Це вимагає формування нового підходу до правової кваліфікації відповідних дій, а також розробки міжнародно-правового інструментарію, який би встановлював чіткі межі відповідальності та засоби захисту від інформаційної агресії.

Таким чином, подальший розвиток міжнародного права має передбачати як доктринальне осмислення інформаційної війни, так і нормативну кодифікацію цього явища через прийняття відповідних багатосторонніх угод або оновлення вже існуючих міжнародних документів у сфері безпеки, гуманітарного права та прав людини.

Отже, наступальні інформаційні операції чи атаки, які використовуються під час кризи чи конфлікту для досягнення або просування конкретних цілей проти конкретного противника, називаються інформаційною війною.

Список використаних джерел:

1. Короход Я.Д. Інформаційно-психологічні війни – зброя XXI. *Актуальні проблеми політики*. 2013. Вип. 50. С. 299–307.
2. Жаровська І., Ортинська Н. Інформаційна війна як сучасне глобалізаційне явище. *Вісник Національного університету «Львівська політехніка»*. Серія: «Юридичні науки». 2020. Т. 7. № 2. С. 56–61.
3. Фещенко І.В. Інформаційна війна як органічна складова сучасного збройно-політичного конфлікту. *Філософія та політологія в контексті сучасної культури*. 2021 Т. 13. № 1. С. 96–103.
4. Російсько-українська інформаційна війна. URL: <https://uk.wikipedia.org/wiki> (дата звернення: 10.05.2025).
5. Greenberg Lawrence T., Goodman Seymour E., Soo Hoo Kevin J. *Information Warfare and International Law*. National Defense University Press, 1998. 53 p.
6. Dunlap Jr. Charles J. How We Lost the High-Tech War of 2007: A Warning for the Future, *The Weekly Standard*. 1996. January 29. P. 22–28.
7. Arquilla John, Ronfeldt David. The Advent of Netwar. *In Athena's Camp: Preparing for Conflict in the Information Age*. 1997. P. 275–294.
8. Малик Я.Й. Інформаційна війна і Україна. *Демократичне врядування*. 2015. Вип. 15. URL: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3 (дата звернення: 10.05.2025).
9. Яковчук В.С., Малець Б.І., Борзов Ю.О. Інформаційні війни в сучасному світі. *Захист інформації в інформаційно-комунікаційних системах*: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих вчених, курсантів та студентів. Львів, ЛДУ БЖД, 2020. URL: <https://sci.ldubgd.edu.ua:8080/jspui/handle/123456789/7424> (дата звернення: 10.05.2025).
10. Проноза І.І. Інформаційна війна: сутність та особливості прояву. *Актуальні проблеми політики*. 2018. Вип. 61. С. 76–84.
11. Шевчук П. Інформаційно-психологічна війна Росії проти України: як їй протидіяти. *Демократичне врядування*. 2014. Вип. 13. URL: http://nbuv.gov.ua/UJRN/DeVr_2014_13_11 (дата звернення: 10.05.2025).

