Поправка Марія Олександрівна

Трансформація гібридних загроз у цифровому суспільстві

УДК 327.56:004.056.5:355.02
DOI https://doi.org/10.24195/2414-9616.2026-1.23

Поправка Марія Олександрівна
аспірант кафедри політології
Одеського національного університету
імені І. І. Мечникова
Французький бульвар, 24/26,
Одеса, Україна
ORCID: 0009-0003-6151-8540

Статтю присвячено аналізу трансформації гібридної війни в умовах цифрового суспільства та визначенню її ключових інструментів, спрямованих на досягнення когнітивної домінації. Гібридна війна – скоординоване поєднання військових, кібернетичних, економічних та інформаційно-психологічних засобів – перетворилася на основний механізм зовнішньополітичного тиску, що дозволяє державі-агресору підривати суверенітет без формального оголошення війни, діючи у «сірій зоні» між миром і збройним конфліктом. Проаналізовано три основні моделі гібридного впливу, що застосовуються Росією проти України: кібернетичний, інформаційно-психологічний та економічний виміри. Кіберпростір став повноцінним театром бойових дій: кібератаки паралізують критичну інфраструктуру – енергетику, фінанси, комунікації, – являючи собою прямий акт державного впливу. Якісно новим виміром інформаційної війни стало масове поширення deepfake-технологій, що генерують гіперреалістичні фальшиві аудіовізуальні матеріали. Це не просто маніпуляція фактами, а фабрикація самої реальності – пряма атака на політичну довіру та стійкість демократичних інституцій. Алгоритми соціальних платформ посилюють цей ефект, замикаючи аудиторію у «медіа-бульбашках» і підвищуючи її сприйнятливість до цілеспрямованої дезінформації. Окремо досліджено правову «сіру зону»: показано, що чинне законодавство України не містить прямого визначення гібридної війни, а міжнародне право досі позбавлене механізмів для кваліфікації масштабних кібератак і deepfake-кампаній як актів агресії. Обґрунтовано три стратегічні імперативи протидії: розробка державної політики медіаграмотності як основи когнітивного імунітету суспільства; формування комплексної національної стратегії кіберстійкості; ухвалення міжнародних доктрин, що дозволяють кваліфікувати масштабні кібератаки та дезінформаційні кампанії як акти агресії з передбаченими зовнішньополітичними наслідками.

Ключові слова: *гібридна війна, інформаційна війна, когнітивна домінація, deepfake, кіберпростір, кібератаки, дезінформація, медіаграмотність, кіберстійкість, інформаційно-психологічні засоби, політична довіра, стратегія національної безпеки.*

Вступ. Цифрова трансформація суспільства радикально змінила природу воєнних конфліктів. Гібридна війна вийшла за межі класичної воєнної парадигми і стала головним інструментом зовнішньополітичного тиску: вона дозволяє підривати суверенітет держав асиметричними методами, не вдаючись до повномасштабної агресії. Кіберпростір перетворився на ключове поле битви, де атаки на енергетику чи комунікації замінюють артилерійські удари. Цей виклик потребує адекватних концептуальних відповідей, зокрема розробки механізмів захисту національного інформаційного простору [6]. Окремою загрозою є алгоритмічна архітектура соціальних платформ, яка замикає суспільство у «медіа-бульбашках» [5] і робить його вразливим до цілеспрямованих маніпуляцій.

Сучасна наукова дискусія довкола природи гібридних загроз активно розвивається – насамперед у контексті російської агресії. Роботи С.Стецюка, О.Вознюка, В.Кожушка, С.Дерев'янка, А. Пехник та А. Бахметьєва формують концептуальну основу для розуміння цього феномену.

А. Пехник і А. Бахметьєв визначають гібридну війну як форму конфлікту, що одночасно задіює традиційні й нетрадиційні засоби впливу – інформаційні, психологічні, економічні – з метою дестабілізації політичної системи противника [4]. О. Вознюк акцентує на багаторівневій структурі російської інформаційної війни: маніпуляції в соціальних мережах, продукування деструктивних наративів і планомірна дискредитація державних інституцій. В. Кожушко зазначає, що гібридні конфлікти перетворили інформаційний простір на критично важливий театр бойових дій, а deepfake-технології стали центральним проявом цієї трансформації – вони замінили маніпуляцію інформацією на пряму фабрикацію реальності.

Попри значний науковий доробок, низка аспектів потребує подальшого дослідження. Вплив deepfake на інститут політичної довіри залишається недостатньо вивченим у стратегічному вимірі. Виявлення й блокування гіперреалістичного deepfake-контенту в закритих мережевих середовищах досі не має ефективного технологічного рішення. Прогалини у глобальній протидії: О. Вознюк справедливо вказує, що вплив російської інформаційної війни на міжнародні інформаційні процеси залишається недостатньо дослідженим, що послаблює спроможність України протидіяти цим загрозам на міжнародному рівні. Правова кваліфікація «сірої зони»: чинне законодавство України не дає прямого визначення гібридної війни, а міжнародне право не має механізмів для кваліфікації масштабних кібератак і deepfake-кампаній як актів агресії.

Мета та завдання статті – проаналізувати гібридну війну в умовах цифрової трансформації на прикладі агресії рф, систематизувати сучасні інструменти когнітивної домінації (зокрема

deepfake-технології) та обґрунтувати стратегічні заходи для зміцнення національної стійкості й протидії гібридним загрозам.

Методи. Методологічну основу дослідження становить комплексний підхід, що базується на поєднанні загальнонаукових та спеціальних методів, що дозволило проаналізувати феномен гібридної війни у його динаміці:

- Системний метод застосовано для розгляду гібридної війни як цілісної системи скоординованих засобів (військових, економічних, кібернетичних), що взаємодіють для досягнення єдиної стратегічної мети – когнітивної домінації.

- Метод термінологічного аналізу використано для уточнення дефініцій «сіра зона», «когнітивна домінація» та «кіберстійкість» в умовах сучасного цифрового суспільства.

- Метод кейс-стаді дозволив проаналізувати конкретні приклади застосування deepfake-технологій та масштабних кібератак як інструментів підриву політичної довіри в демократичних країнах.

- Компаративний (порівняльний) метод використано для зіставлення традиційних форм інформаційно-психологічного впливу з новітніми інструментами фабрикації реальності в соціальних медіа.

- Метод моделювання та прогнозування застосовано для розробки стратегічних імперативів протидії гібридним загрозам, зокрема формування моделі «когнітивного імунітету» суспільства через політику медіаграмотності.

- Інституційний аналіз залучено для обґрунтування необхідності змін у міжнародних доктринах та національному законодавстві щодо кваліфікації кібератак як актів агресії.

Результати. Складність ідентифікації гібридних загроз зумовлює необхідність ретельного аналізу наукових підходів до визначення змісту та інструментарію сучасних конфліктів. Оскільки цифровізація суспільства трансформувала класичну пропаганду в складні технологічні операції, виникає потреба у систематизації поглядів провідних дослідників на природу інформаційної та гібридної війни. Це дозволяє не лише окреслити межі сірої зони, а й виявити конкретні механізми впливу на державні інституції та суспільну свідомість. Розглядаючи результати аналізу сучасного наукового дискурсу, ми спостерігаємо зміщення фокуса від суто мілітарних аспектів до вивчення когнітивних і технологічних складників агресії. Зокрема, в українському науковому просторі сформувалося кілька ключових концепцій, що пояснюють природу цього феномену.

О. Вознюк характеризує російську інформаційну війну як багаторівневе явище, що охоплює маніпуляції громадською думкою через соціальні мережі, створення деструктивних наративів, дискредитацію державних інституцій і втручання в міжнародний інформаційний простір. Дослідник наголошує, що саме ці аспекти «недостатньо вивчені з погляду їхнього впливу на глобальні інформаційні процеси, що створює прогалини у спроможності України ефективно протидіяти таким загрозам» [1].

А. Пехник і А. Бахметьєв визначають гібридну війну як «форму конфлікту, в якій застосовуються як традиційні військові засоби, так і нетрадиційні інструменти впливу, включаючи інформаційні, психологічні, економічні, дипломатичні й технологічні засоби. Її головною метою є дестабілізація політичної системи супротивника без повномасштабного застосування армії» [5].

У межах цього дослідження під гібридною війною розуміється скоординоване застосування комплексу інструментів: військових (нерегулярні формування), політичних, економічних, кібернетичних та інформаційно-психологічних (дезінформація) – задля досягнення геополітичних цілей.

Чинне законодавство України не містить прямого визначення «гібридної війни». Частково це поняття розкривалося у скасованій «Воєнній доктрині України» (2015), де гібридна війна трактувалася як асиметричне застосування воєнної сили незаконними формуваннями поряд із комплексним використанням військових і невійськових інструментів (економічних, політичних, інформаційно-психологічних). Після скасування Доктрини у 2021 році «Стратегія воєнної безпеки України» підтвердила, що головним безпековим викликом залишається «розв'язана російською федерацією гібридна війна». Вона описується як поєднання прихованого застосування регулярних військ, незаконних збройних формувань та терористичних організацій; пропаганди, саботажу, терору, диверсій; навмисного завдання шкоди громадянам, юридичним особам та об'єктам державної власності в Україні.

Чинна Стратегія інформаційної безпеки України (Указ Президента від 28.12.2021 № 685/2021) розглядає гібридну війну в контексті загроз та підкреслює, що інформаційна політика й технології, які застосовує РФ проти України, загрожують не лише їй, але й іншим демократичним державам. Механізми інформаційного втручання РФ активно адаптуються до локальних контекстів і регуляторних середовищ різних країн.

Попри аналітичну цінність Стратегії 2021 року, після початку повномасштабної агресії у лютому 2022 року термін «гібридна війна» фактично зникає з офіційного законодавчого дискурсу, хоча посилання на загрози гібридного характеру зберігаються.

Схожа термінологія присутня у воєнних доктринах інших держав. Національна оборонна стратегія США (2022) кваліфікує Росію як «гостру загрозу» для США та НАТО, характеризує її агресію проти України як «жорстоку й неспровоковану» і декларує зобов'язання посилити стійкість східного флангу Євроатлантичного простору, зокрема до гібридних і кібернетичних дій. Воєнна доктрина РФ (2014) прямо не вживає поняття «гібридна війна», проте

описує всі її ключові ознаки, прикриваючись риторикою «спеціальної військової операції» з метою «демілітаризації та денацифікації України».

Незважаючи на очевидну загрозу суверенітету й територіальній цілісності України, юридична кваліфікація подій як «війна» не закріплена у жодному нормативному акті з 2014 року. Водночас у суспільній свідомості й політичному дискурсі визначення «російсько-українська війна» є домінуючим і поступово утверджується у міжнародній риториці.

Інформаційна складова посідає ключове місце у сучасних конфліктах. Інформаційна безпека України – це стан захищеності державного суверенітету, територіальної цілісності та конституційних прав громадян, що забезпечується системою протидії: скоординованому поширенню недостовірної інформації, деструктивній пропаганді, інформаційним операціям, несанкціонованому поширенню та порушенню цілісності інформації з обмеженим доступом.

В. Кожушко наголошує, що «гібридні конфлікти кардинально змінили парадигму війни, перетворивши інформаційний простір на критично важливий театр бойових дій». Він зазначає, що «центральним відкриттям цієї трансформації є поява та стрімке поширення deepfake-технологій, які якісно змінюють природу дезінформації, перетворюючи маніпуляцію інформацією на справжню фабрикацію реальності» [3].

О. Вознюк виокремлює дезінформацію як найактивніший інструмент впливу: вона «поширювалася через різні канали – від традиційних ЗМІ до соціальних мереж» і «часто поєднувалася з кібернетичними атаками, спрямованими на порушення роботи урядових інституцій, руйнування довіри до українських ЗМІ та створення хаосу в суспільстві» [1].

До основних інструментів інформаційного впливу в умовах гібридної війни можна віднести такі:

– Дезінформація та deepfake: соціальні мережі й месенджери слугують каналами миттєвого поширення фальшивого контенту, спрямованого на маніпуляцію громадською думкою та підрив довіри до держави.

– Контроль даних та ідентичностей: аналіз великих даних (Big Data) дозволяє створювати персоналізовані повідомлення, що посилюють соціальні розколи й поляризацію суспільства.

– Економічна гібридизація: криптовалюти та кіберінструменти використовуються для економічного тиску – кіберздирництва, підриву фінансових систем, обходу санкційних режимів.

Гібридна війна дозволяє агресору досягати геополітичних цілей, уникаючи прямої відповідальності. Серед ключових механізмів: втручання у виборчі процеси, фінансування дестабілізуючих груп, постійний інформаційний та економічний тиск для нав'язування вигідних рішень. Усе це відбувається в «сірій зоні» – просторі між миром і війною, де класичні механізми міжнародного права виявляються малоефективними. Як зазначає Т. Рід, дезінформаційні кампанії є не новим явищем, а відточеним інструментом державної стратегії, що у цифрову епоху набув безпрецедентного масштабу та швидкості поширення завдяки соціальним мережам і автоматизованим ботам [7].

В. Кожушко акцентує, що «deepfake-контент, генеруючи гіперреалістичні сфабриковані матеріали, створює безпрецедентну загрозу інституту політичної довіри та стабільності демократичних систем». Досвід агресії РФ проти України демонструє, як ці технології використовуються для деморалізації, дезорієнтації й делегітимізації влади. «Швидкість та масштабованість поширення такого контенту в цифрову епоху значно посилюють його деструктивний потенціал», – констатує дослідник [3].

Український досвід з 2014 року є показовим кейсом застосування гібридної стратегії: кібератаки на енергосистеми, масована дезінформація, використання нерегулярних формувань.

Головними вразливостями держав перед гібридними загрозами є висока залежність критичної інфраструктури від цифрових технологій і низький рівень медіаграмотності населення. Обидва чинники взаємопов'язані: технічна вразливість і когнітивна неготовність суспільства разом формують ефективний плацдарм для агресора. Н. Янкович, аналізуючи досвід України та країн Центрально-Східної Європи, переконливо доводить, що медіаграмотність є першим і найважливішим кроком до перемоги в інформаційній війні, а демократії залишаються вразливими до дезінформації доти, доки не зміцнять стійкість власних суспільних інститутів [8].

Системна відповідь передбачає три виміри: комплексна національна стратегія кіберзахисту та підвищення медіаграмотності; міжнародна співпраця для ідентифікації суб'єктів гібридної агресії та притягнення їх до відповідальності; розробка доктрин, що дозволяють кваліфікувати масштабні кібератаки й дезінформаційні кампанії як акти агресії з відповідними наслідками у міжнародному праві.

С. Дерев'янко слушно зауважує, що «гібридні війни стали реальністю нашого часу й, на думку політиків і науковців, визначатимуть безпекове середовище майбутнього. Інформаційна війна, яку інтенсивно веде РФ проти України, стала суттєвим компонентом гібридного протистояння. Втягнутими до неї виявилися фактично всі громадяни держави – свідомо чи ні. Право на інформацію є одним із фундаментальних прав людини, і його реалізація несе в собі одночасно значний комунікативний і маніпулятивний потенціал» [2].

Висновки. На початку третього десятиліття XXI століття гібридна війна остаточно затвердилася як провідна форма міждержавного протистояння. Це не стихійне явище – а скоординована державна стратегія, спрямована на досягнення геополітичних

цілей через системний підрив суверенітету. Росія веде «війну третього покоління», де метою є не лише фізична, але й когнітивна домінація – маніпуляція колективною свідомістю.

Інформаційна війна є не допоміжним, а фундаментальним виміром цього конфлікту. Кібератаки паралізують критичну інфраструктуру – енергетику, фінанси – і створюють стан функціональної нестабільності. Deepfake-технології знаменують якісний стрибок: агресор отримав можливість не просто спотворювати факти, а фабрикувати переконливу альтернативну реальність. Це пряма атака на довіру до інституцій і легітимність демократичних систем. Приц цьому, як правильно зазначають А. Пехник і А. Бахметьєв, необхідно «враховувати специфіку українського контексту, в якому суспільство веде не лише збройну боротьбу, але й війну за смисли» [4].

Ефективна протидія виходить за межі суто військової відповіді і потребує реалізації трьох невідкладних заходів: розробка державної політики підвищення медіаграмотності – суспільство з розвиненим критичним мисленням є найефективнішим захистом від дезінформації та deepfake; створення комплексної стратегії кіберстійкості, здатної захистити критичну інфраструктуру як основну мішень гібридної агресії; ухвалення міжнародних доктрин, що дозволяють кваліфікувати масштабні кібератаки й дезінформаційні кампанії як акти агресії з передбаченими зовнішньополітичними наслідками.

Гібридна війна трансформувалася в домінуючу форму міждержавного протистояння, де метою РФ є когнітивна домінація – маніпуляція колективною свідомістю. Deepfake-технології є ключовим інструментом цієї «війни третього покоління». Український досвід обнажає правові суперечності «сірої зони»: суспільне сприйняття подій як «війни» і їх формальна юридична кваліфікація досі не збігаються, що ускладнює інституційне реагування. Стратегічна безпека України та інших демократій залежить від розвитку когнітивного імунітету й комплексної стратегії кіберстійкості для протидії фабрикації реальності.

Перспективи подальших досліджень: вивчення швидкості та масштабованості поширення deepfake-контенту і розробка ефективних технологічних інструментів його ідентифікації та блокування; формування міжнародної доктрини кваліфікації кібер- та інформаційних операцій як актів агресії; поглиблений аналіз впливу алгоритмів соціальних мереж на поляризацію суспільства в умовах гібридної війни.

ЛІТЕРАТУРА:

1. Вознюк О. Інформаційна війська як інструмент міжнародної політики (досвід для України). *Історико-політичні проблеми сучасного світу*. 2024. № 50. С. 9–19. https://doi.org/10.31861/mhpi2024.50.9-19

2. Дерев'янко С. Гібридна війна: інформаційно-безпековий вимір. *Вісник Прикарпатського університету. Серія: Політологія* . 2024. Вип. 18. https://doi.org/10.32782/2312-1815/2024-18-11

3. Кожушко В. Інформаційна війна в гібридних конфліктах: від пропаганди до кібервпливу. *Український політико-правовий дискурс.* 2025. https://doi.org/10.5281/zenodo.16658818

4. Пехник А., Бахметьєв А. Політична журналістика як гравець гібридної війни: виклики для українських медіа. *Філософія та політологія в контексті сучасної культури.* 2025. Т. 17, № 1. С. 147–152. https://doi.org/10.15421/352519

5. Пехник А., Бахметьєв А. Конструкція політичної реальності в умовах інформаційної війни: когнітивна дилема журналіста. *Епістемологічні дослідження у філософії, соціальних і політичних науках.* 2025. Т. 8, № 1. С. 263–268. https://doi.org/10.15421/342532

6. Стецюк С. Маніпулятивні технології під час гібридної війни в Україні та їх вплив на громадську думку. *Вісник Львівського університету. Серія: Журналістика*. 2018. Вип. 43. С. 153–161.

7. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. New York Farrar, Straus and Giroux. 2020. 528 p

8. Jankowicz N. How to Lose the Information War: Russia, Fake News, and the Future of Conflict. London : I.B. Tauris. 2020. 296 c.

REFERENCES:

1. Vozniuk, O. (2024). Informatsiina viina yak instrument mizhnarodnoi polityky (dosvid dlia Ukrainy) [Information war as an instrument of international politics (experience for Ukraine)]. Istoryko-politychni problemy suchasnoho svitu. Chernivtsi: Chernivetskyi natsionalnyi universytet, no. 50, pp. 9–19. https://doi.org/10.31861/mhpi2024.50.9-19 [in Ukrainian].

2. Derevianko, S. (2024). Hibrydna viina: informatsiino-bezpekovyi vymir [Hybrid war: the information and security dimension]. Visnyk Prykarpatskoho universytetu. Seriia: Politolohiia. Ivano-Frankivsk: Prykarpat. nats. un-t, iss. 18. https://doi.org/10.32782/2312-1815/2024-18-11 [in Ukrainian].

3. Kozhushko, V. (2025). Informatsiina viina v hibrydnykh konfliktakh: vid propahandy do kibervplyvu [Information war in hybrid conflicts: from propaganda to cyber influence]. Ukrainskyi polityko-pravovyi dyskurs. https://doi.org/10.5281/zenodo.16658818 [in Ukrainian].

4. Pekhnyk, A., & Bakhmetyev, A. (2025). Politychna zhurnalistyka yak aktor hibrydnoi viiny: vyklyky dlia ukrainskykh media [Political journalism as an actor of hybrid war: challenges for Ukrainian media]. Filosofiia ta politolohiia v konteksti suchasnoi kultury. Dnipro: DNU, vol. 17, no. 1, pp. 147–152. https://doi.org/10.15421/352519 [in Ukrainian].

5. Pekhnyk, A., & Bakhmetyev, A. (2025). Konstruktsiia politychnoi realnosti v umovakh informatsiinoi viiny: kohnityvna dylema zhurnalista [Construction of politi-

cal reality in the context of information war: the journalist's cognitive dilemma]. Epistemolohichni doslidzhennia v filosofii, sotsialnykh i politychnykh naukakh. Dnipro: DNU, vol. 8, no. 1, pp. 263–268. https://doi.org/10.15421/342532 [in Ukrainian].

6. Stetsiuk, S. (2018). Manipuliatyvni tekhnolohii pid chas hibrydnoi viiny v Ukraini ta yikh vplyv na hromadsku dumku [Manipulative technologies during the hybrid war in Ukraine and their influence on public opinion]. Visnyk Lvivskoho universytetu. Seriia: Zhurnalistyka. Lviv: LNU im. Ivana Franka, iss. 43, pp. 153–161 [in Ukrainian].

7. Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux. 528 p.

8. Jankowicz, N. (2020). How to Lose the Information War: Russia, Fake News, and the Future of Conflict. London: I.B. Tauris. 296 p.

Transformation of hybrid threats in the digital society

Popravka Mariia Oleksandrivna

Postgraduate Student at the Department of Political Science
Odesa I. I. Mechnikov National University
Frantsuzkyi Blvd Blvd, 24/26,
Odesa, Ukraine
ORCID: 0009-0003-6151-8540

This article analyses the transformation of hybrid warfare in the context of global digital transformation and identifies its key instruments aimed at achieving cognitive domination. Hybrid warfare – defined as the coordinated application of military, cyber, economic, and information-psychological means – has become the primary mechanism of foreign policy coercion, enabling the aggressor state to undermine sovereignty without a formal declaration of war by operating within the "grey zone" between peace and armed conflict. Three principal models of hybrid influence employed by Russia against Ukraine are examined: the cyber, information-psychological, and economic dimensions. Cyberspace has been transformed into a full-fledged theatre of operations, with cyberattacks paralysing critical infrastructure – energy, finance, and communications – and thereby constituting a direct act of state coercion. The rapid proliferation of deepfake technologies represents a qualitatively new dimension of information warfare: by generating hyper-realistic fabricated audiovisual materials, they do not merely manipulate facts but fabricate reality itself, launching a direct attack on political trust and the resilience of democratic institutions. The algorithmic architecture of social media platforms amplifies this effect by confining audiences within "media bubbles" and heightening their susceptibility to targeted disinformation. The article separately examines the legal "grey zone", demonstrating that Ukrainian legislation contains no direct definition of hybrid warfare, while international law remains devoid of mechanisms to qualify large-scale cyberattacks and deepfake campaigns as acts of aggression. Three strategic imperatives of counteraction are substantiated: the development of a state media literacy policy as the foundation of society's cognitive immunity; the formation of a comprehensive national cyber resilience strategy; and the adoption of international doctrines enabling the qualification of large-scale cyberattacks and disinformation campaigns as acts of aggression with corresponding consequences under international law.

Key words: *Hybrid warfare, information warfare, cognitive domination, Deepfake, cyberspace, cyberattacks, disinformation, media literacy, cyber resilience, information-psychological means, political trust, national security strategy.*

Дата першого надходження статті до видання: 18.02.2026
Дата прийняття статті до друку після рецензування: 24.03.2026
Дата публікації (оприлюднення) статті: 27.04.2026