

ГІБРИДНА ВІЙНА ЯК НОВИЙ ВИМІР СУЧАСНИХ КОНФЛІКТІВ

Кириченко А. В. доктор філософії (PhD),
старший викладач кафедри внутрішніх комунікацій
Національного університету оборони України
<https://orcid.org/0000-0002-1333-5980>

Іваненко С. М. доктор філософії (PhD),
старий викладач кафедри воєнної історії України
Національного університету оборони України
<https://orcid.org/0000-0001-6382-040X>

Ремез В. В. доктор філософії (PhD),
старший викладач кафедри територіальної оборони
Національного університету оборони України
<https://orcid.org/0000-0002-2561-1081>

Гібридна війна є новим типом військово-політичного конфлікту, що поєднує військові та невійськові методи впливу, зокрема інформаційно-психологічні, кібернетичні, економічні та політичні інструменти. У статті проаналізовано концептуальні підходи до гібридної війни, її механізми та наслідки для України, зокрема через призму теоретичних досліджень західних і вітчизняних науковців.

Ключові слова: гібридна війна; інформаційно-психологічна війна; дезінформація; кібератаки; економічний тиск; політичні маніпуляції; міжнародна безпека; стратегічна комунікація.

Вступ. Сьогодні гібридна війна стає одним із найактуальніших викликів для національної безпеки багатьох держав. Особливого значення ця проблема набуває і перед нашою країною після порушення росією умов Будапештського меморандуму та анексії значної частини території. Відкрита військова агресія супроводжувалася потужним інформаційно-психологічним впливом, метою якого є формування сприятливого суспільного середовища для поширення ідеології так званого “руського мира”. За більш ніж одинадцять років протистояння Україна зіткнулася з усіма можливими інструментами гібридної війни, що включають як невійськові (політичні, економічні, гуманітарні, кібернетичні, інформаційно-психологічні), так і військові методи (кризове врегулювання, стратегічне розгортання, військова інтервенція тощо). Саме поєднання різноформатних заходів, спрямованих на підрив суверенітету й незалежності держави, визначає сутність гібридної війни. Аналізуючи особливості гібридної війни, необхідно розглянути її основні складові, методи ведення та наслідки для України й світу загалом. Дослідження цього явища має ключове значення для розробки ефективних механізмів протидії сучасним викликам та загрозам у сфері національної безпеки.

Теоретичне підґрунтя. Гібридна війна як новий тип військово-політичного конфлікту стає предметом дослідження як зарубіжних, так і вітчизняних науковців. Важливий внесок у вивчення цього явища зробили такі зарубіжні дослідники, як Ф. Гофман, М. Макфейт, Е. Луттвак, Дж. Най, Л. Фрідман, М. Галеотті, Т. Рідер, які аналізували стратегії та тактики гібридної війни, механізми інформаційного впливу та дезінформації. Серед українських науковців, які зробили значний внесок у дослідження гібридної війни, варто виділити праці В.Алещенка, Т. Андрієвського, О. Барановського, П. Гай-Нижника, В. Горбуліна, В. Головченка, М. Дорошка, О. Їжака, Ю. Когута, Є. Магда, Б. Парахонського, Г. Перепелиці, Г. Почепцова, І. Рущенка, Ю. Узденової, Г. Яворської, які розглядали політичні, військові, інформаційні та економічні аспекти гібридної агресії.

Отже, дослідження гібридної війни, її механізмів та наслідків є надзвичайно важливим для розуміння сучасних військово-політичних конфліктів та розробки ефективних заходів протидії.

Методи дослідження. У науковому дослідженні було застосовано комплекс теоретичних та емпіричних методів, що дозволили здійснити всебічний аналіз проблеми гібридної війни. *Теоретичні*

методи включали аналіз, синтез, абстрагування, узагальнення, індукцію та дедукцію, що сприяло формуванню загального уявлення про сутність, складові та механізми ведення гібридної війни. Для глибшого розуміння проблеми використовувався *порівняльний метод*, який дав змогу зіставити підходи до ведення гібридної війни у різних країнах та оцінити ефективність заходів протидії. *Системний підхід* дозволив розглянути гібридну війну як багатокомпонентне явище, що поєднує військові, політичні, економічні, інформаційні та кібернетичні аспекти. Для аналізу інформаційно-психологічного впливу та пропаганди застосовувався *контент-аналіз*, який дав змогу виокремити основні наративи, що використовуються в медійному просторі. *Статистичний метод* використовувався для збору та обробки кількісних даних, що стосуються інформаційних атак, економічного тиску та інших форм гібридної агресії. Крім того, було залучено *метод експертного оцінювання*, що передбачав аналіз поглядів фахівців у сфері безпеки, оборони, політології та міжнародних відносин для визначення ефективних стратегій протидії гібридним загрозам. Застосування сукупності цих методів дозволило здійснити комплексний аналіз досліджуваної проблеми, систематизувати наявні наукові підходи та розробити обґрунтовані висновки.

Результати і обговорення. У сучасних реаліях війна змінює свої прояви, набуваючи гібридного характеру. Водночас, на думку експертів, така еволюція збройних конфліктів не є принципово новим явищем у світовій історії, адже подібні підходи до ведення війни застосовувалися протягом століть, хоча й відрізнялися масштабами та формами. При цьому можна спостерігати суттєві зміни у методах і формах гібридних війн, однак їхня основна природа та першопричини конфліктів між державами залишаються незмінними. Беручи до уваги думку видатного китайського стратега і мислителя *Сунь-Цзи (VI–V ст. до н.е.)*, який у своєму відомому трактаті “Мистецтво війни” акцентував увагу на тому, що вершина військового мистецтва – це здобуття перемоги над ворогом без бою, можна стверджувати, що концепція

гібридної війни має глибоке історичне підґрунтя. Використання непрямих методів боротьби, включно з інформаційним, економічним та політичним впливом, було характерним для стратегічного мистецтва ще в давнину. Отже, хоча форми та засоби ведення таких конфліктів зазнають змін відповідно до розвитку технологій і суспільних умов, їхня сутність, що полягає в досягненні перемоги без відкритого військового зіткнення, залишається незмінною й у сучасному світі.

Досвід воєн в Афганістані та Іраку демонструє, що навіть за значної різниці у військових спроможностях конфлікти залишаються вкрай витратними. Це спричиняє зниження прагнення до відкритих збройних зіткнень і стимулює використання гібридної війни як інструменту досягнення стратегічних цілей із мінімальними втратами. Як зазначав Карл фон Клаузевіц, “війна – це не більше ніж продовження політики іншими засобами”, однак сучасні гібридні війни значно розширюють спектр цих засобів. У результаті матриця “політика-війна” ускладнюється, а динаміка збройних конфліктів постійно змінюється (*Гібридна війна – нові загрози*, 2021).

Розглядаючи сутність гібридної війни, слід зазначити, що американський військовий аналітик і колишній офіцер морської піхоти США Френк Гофман (2007) є одним із провідних дослідників цього явища, яке набуло особливого значення у глобальній безпеці після закінчення Холодної війни. У 2007 році він сформулював концепцію “гібридних загроз” та “гібридної війни”, яка описує сучасні конфлікти, що поєднують традиційні військові дії з асиметричними та нетрадиційними методами. Його теорія широко використовується у військовій стратегії США, НАТО, а також у аналізі сучасних збройних конфліктів, зокрема агресії росії проти України. Основні положення концепції Гофмана щодо гібридної війни можна сформулювати так: 1) Поєднання різних методів війни. Гібридна війна включає комбінацію традиційних (регулярні армії), нерегулярних (партизанська тактика, повстанці), терористичних і кримінальних методів ведення бойових дій. 2) Роль інформаційних

та кібератак. Військові дії супроводжуються масованими кампаніями з дезінформації, пропаганди та маніпуляцій через ЗМІ та соціальні мережі, спрямованими на дестабілізацію суспільства. 3) Залучення недержавних акторів. Військові конфлікти можуть вестися за участі проксі-груп, бойовиків, спецслужб, хакерів та організованих злочинних угруповань. 4) Розмитість меж між війною і миром. Гібридна війна не починається раптово, а розгортається поступово через економічний тиск, інформаційні атаки, диверсії та підтримку внутрішньої опозиції.

Гофман аналізує події у Лівані, зокрема дії “Хезболли” у 2006 році, які стали одним із ранніх прикладів гібридної війни. Згодом його концепція знайшла застосування у поясненні російської агресії в Україні (Крим, Донбас). Науковець наголошує, що гібридна війна не має офіційного оголошення, що значно ускладнює ідентифікацію агресора та правову реакцію на загрози. Її основою є інформаційні маніпуляції, спрямовані на дискредитацію противника, зокрема через звинувачення у радикалізмі чи екстремізмі (наприклад, риторика росії щодо України: “фашисти”, “бандерівці”). Головна мета гібридної війни — не стільки захоплення територій, скільки створення хаосу та системна дестабілізація країни-жертви шляхом провокацій. Дослідження Гофмана в цьому напрямку суттєво вплинули на формування сучасних військових доктрин та стратегій, особливо в контексті протидії гібридним загрозам (*Assessing Baltic Sea Regional Maritime Security*, 2017; Hoffman F., 2007; *Future Warfare*, 2005).

У свої працях Монтгомері Макфейт (2018) детально розглядає аспекти, як недержавні актори та нерегулярні сили використовують нетрадиційні методи ведення війни, такі як інформаційні операції, пропаганда та психологічний вплив. Ці елементи є ключовими компонентами гібридної війни, де поєднуються військові та невійськові засоби для досягнення стратегічних цілей.

Едвард Луттвак (2016) наголошує, що війни майбутнього включають не лише відкриті збройні зіткнення, а й економічний тиск, інформаційні кампанії, дипломатичний вплив та кібероперації. Він описує

поєднання традиційних і нетрадиційних методів ведення бойових дій, що є однією з основ гібридної війни. Його ідея полягає в тому, що успішна військова стратегія має діяти за парадоксальними принципами — наприклад, чим сильніше тисне держава-агресор, тим потужніший може бути опір. На його думку, це пояснює, чому російська гібридна агресія проти України викликала ефект, протилежний очікуваному: Україна зміцнила свою обороноздатність, отримала міжнародну підтримку та посилила національну ідентичність. Аналізуючи актуальні механізми запобігання війнам і гібридним загрозам, Луттвак підкреслює важливість економічних санкцій, розвідки, інформаційної війни та спеціальних операцій як ключових інструментів сучасної боротьби.

За концепцією “м’якої сили” (*soft power*), яку розробив Джозеф Най (2005, 2011), можна зрозуміти нетрадиційні методи впливу у воєнних конфліктах. Він звертає увагу на здатність держав досягати своїх цілей не через примус чи військову силу, а через культуру, політичні цінності та дипломатію. На думку автора, російська гібридна агресія широко використовує м’яку силу для впливу на інші країни через пропаганду, інформаційні війни, дипломатію та економічні важелі. Водночас Най вводить поняття “розумної сили” (*smart power*), яка поєднує м’яку силу (культуру, інформаційний вплив) із жорсткою силою (економічний тиск, військова агресія). Це є суттю гібридної війни, яка у XXI столітті є настільки ж ефективною, як і військові кампанії. У російсько-українській війні ворог застосовує пропаганду, дезінформацію, енергетичний шантаж та військову загрозу одночасно.

Лоуренс Фрідман (2022) підкреслює, що гібридні війни характеризуються розмиттям меж між миром і війною, а також активним використанням пропаганди та дезінформації для досягнення стратегічних цілей. Він зазначає, що путін розпочав війну, ґрунтуючись на наративі, вибудованому з потужних символів, глибоко вкорінених образів, історичних міфів і хибних тверджень про Україну, які легко спростовуються при першій же перевірці. Це є масштабний обман, але насамперед самообман, адже саме путін

створив цей наратив і був найбільш переконаний у його правдивій силі.

Дослідження Марка Галеотті (2016, 2017) допомагають краще зрозуміти природу гібридних загроз та розробити ефективні стратегії протидії таким викликам у сучасному світі. У своїх працях він аналізує стратегії та тактики, які росія використовує для досягнення своїх геополітичних цілей, поєднуючи військові, інформаційні, економічні та політичні засоби впливу. Галеотті підкреслює, що сучасна війна виходить за межі традиційних бойових дій і включає широкий спектр інструментів, таких як пропаганда, дезінформація, кібератаки та економічний тиск. У таких війнах перевага на боці невійськових форм боротьби, що проявляється у відповідному співвідношенні 4:1 на користь непрямих методів впливу. На думку Галеотті, гібридна війна займає нижчу сходинку порівняно з традиційною війною, яка, попри свою складність і високі витрати, дає більш відчутні результати. Водночас гібридні методи мають певні переваги, оскільки вони є простішими, менш затратними та дозволяють ефективно поширювати дезінформацію без необхідності відкритого застосування військової сили. Науковець зазначає, що російські спецслужби розглядають війну в значно ширшому контексті, аніж просто збройне протистояння, і активно використовують невійськові методи для досягнення своїх стратегічних цілей. У сучасних умовах, пов'язаних з анексією Криму та повномасштабним вторгненням в Україну, Галеотті аналізує, як росія застосовує комплексний підхід, поєднуючи військову силу з інформаційно-психологічними операціями, політичним впливом та іншими невійськовими методами для дестабілізації ситуації та досягнення своїх інтересів. В цьому контексті гібридна війна стає своєрідним тестом для перевірки стійкості держави. Такий підхід поступово наближає агресора до перемоги без відкритого збройного зіткнення, ослаблюючи супротивника зсередини та створюючи сприятливі умови для подальшого контролю.

У дослідженні гібридних війн Томас Рід (2021) зазначає, що хакерські атаки, маніпуляція інформацією та цифрові

кампанії мають суттєвий вплив на геополітичну ситуацію. На його думку, пропаганда та кібератаки в XXI столітті стали ключовими компонентами сучасних воєн, доповнюючи традиційні методи агресії.

Колектив авторів навчального посібника “Гібридна війна” росії проти України: інформаційний вимір наголошує, що у ході гібридних конфліктів на території пострадянського простору керівництво росії ставить перед собою низку завдань, які в сукупності є частиною проєкту створення так званого “русского мира”. Головною метою російської федерації є встановлення маріонеткових проросійських режимів, які сприятимуть реалізації зовнішньополітичного курсу кремля та самостійно контролюватимуть ситуацію всередині своєї країни. Це так званий перехідний етап, необхідний для повного підпорядкування пострадянських країн впливу росії. Такий вид агресії називають гібридною війною, що розглядається як сучасний метод здійснення агресивної політики. До її основних елементів автори відносять: 1) пропаганду, що базується на брехні, маніпуляції та підміні понять; 2) заперечення початкової фази війни та факту участі російської федерації в ній; 3) спотворення української історії та звинувачення України у власних злочинах; 4) торговельно-економічний тиск та енергетичну блокаду; 5) терор та залякування громадян України; 6) кібератаки та дестабілізацію критичної інфраструктури. Пропаганда росії поступово зміцнює ідеологічне підґрунтя для агресії, систематично впливаючи на суспільну свідомість. Особливу роль у цьому відіграє інформаційно-психологічна кампанія, спрямована на підлив патріотичних настроїв українців та формування сумнівів щодо власної історії й національної ідентичності. Для цього використовуються маніпулятивні наративи про “спільне минуле”, концепція “старшого брата”, романтизація СРСР, а також дискредитація українських героїв і боротьби за незалежність. Перекручуючи історичні події, росія намагається виправдати свою агресію та нав'язати Україні вигідну їй інтерпретацію реальності (Агаєв, Н.А. Герасименко, М.В., Дикун, В.Г. & Стасюк, В.В., 2020).

На думку фахівців Національного інституту стратегічних досліджень, гібридна війна не є поверненням до формату холодної війни, а є її еволюційною заміною, що призводить до складних багатовимірних конфліктів на світовій арені. Поняття гібридної війни найбільшою мірою відповідає стратегії російської федерації, яка системно поєднує військові, економічні, інформаційні, дипломатичні засоби, кібератаки та ядерний шантаж для досягнення геополітичних цілей, часто незрозумілих міжнародній спільноті. Ця стратегія застосовується не лише в Україні, але й у різних регіонах світу, зокрема у Європі, на Близькому Сході та в Африці, де росія використовує військові проксі-сили, енергетичний тиск та інформаційні маніпуляції для дестабілізації та розширення власного впливу. Країна-агресорка у своєму нинішньому вигляді становить загрозу як для всього світу, так і для самої себе (*Світова гібридна війна*, 2025).

Академік Національної академії наук України В. Горбулін (2017) пропонує цікаві концептуальні підходи до розуміння феномену гібридної війни. Він зазначає, що хоча окремі її елементи не є новими та використовувалися в минулому, їхня унікальність полягає в гнучкості, узгодженості, взаємозв'язку та зростаючій ролі інформаційного чинника. З часом інформаційний компонент набуває самостійності, а його впливовість може перевищувати вагу безпосередньо військових засобів. В. Горбулін також акцентує увагу на модернізації термінології для опису конфліктів нового типу, зокрема акцентує увагу поняття “*змішана війна*”, “*нерегулярна війна*”, “*неконвенційна війна*”. Поняття гібридної війни є синонімом нетрадиційного міждержавного протистояння та водночас окремою категорією, що відображає новітні форми конфліктності (протидії) між державами. Станом на сьогодні терміни “гібридна війна” (“*hybrid warfare*”) та “гібридна загроза” (“*hybrid warfare threats*”) офіційно закріплені в термінології західної військово-політичної стратегії.

Розглядаючи російсько-українську гібридну війну Рушенко І. (2015) зазначає, що цей конфлікт виходить за межі традиційного військового протистояння та

включає інформаційні, економічні, соціально-психологічні та культурні аспекти впливу. Він підкреслює, що ключову роль у веденні гібридної війни відіграють інформаційні технології, які використовуються для маніпуляції громадською думкою, підриву довіри до державних інституцій та створення розколу в суспільстві. На думку Руценка, російська стратегія в цьому конфлікті спирається на активне використання пропаганди, дезінформації, фальсифікації історичних подій та експлуатацію суспільних протиріч, що сприяє формуванню вигідних для агресора наративів. Він також наголошує, що важливою складовою гібридної війни є соціально-психологічний тиск, який включає залякування, терор та використання агентів впливу.

Згідно з дослідженням В. Алещенка (2016), технології “гібридної війни”, зокрема її інформаційно-психологічна складова, стали ключовим інструментом політики рф щодо України, спрямованим на дестабілізацію держави та підлив суспільної єдності. На думку вченого, це вимагає глибокого перегляду підходів до національної безпеки, зокрема посилення стратегічних комунікацій, інформаційного захисту та ефективної протидії ворожим операціям на тимчасово окупованих територіях. На думку ученого, у сучасній війні перемагає той, хто контролює суспільні настрої, тому інформаційно-психологічні операції мають стати не просто інструментом, а центральним елементом державної політики безпеки. Всі аспекти діяльності Збройних Сил України повинні включати ефективні інформаційні заходи для нейтралізації загроз.

Так, М. Савлюк (2024) у своїх дослідженнях наголошує, що людство безперервно розвивається в усіх сферах, зокрема у військовій, де гібридна війна набуває дедалі ширших масштабів. Аналіз генезису російсько-українського конфлікту свідчить, що його витoki сягають значно раніше 2014 року, оскільки росія вела інформаційну, культурну та економічну експансію задовго до відкритої агресії. Попри заборону російських соцмереж і телеканалів після 2017 року, з початком повномасштабної війни в 2022 році інформаційна агресія рф лише посилилася,

зокрема через діяльність ботоферм, які завдають ударів по соціально та політично чутливих питаннях, провокують внутрішньодержавні конфлікти та підривають довіру до влади. Протягом останніх років росія значно активізувала диверсійну та підривну діяльність проти європейських союзників України, а у 2024 році перейшла до жорстокіших дій, включаючи вбивства та атаки на критичну інфраструктуру

Водночас дослідження Лейденського університету показує, що кількість російських диверсій у Європі зростає з 6 у 2022 році до 44 у 2024 році, охоплюючи військові бази, комунікаційні системи та операції впливу на політиків. Експерти попереджають, що Москва дедалі частіше вдається до державного тероризму, використовуючи саботаж, кібератаки та змови, що створює загрозу стабільності Європи. У майбутньому росія не планує застосовувати ядерну зброю, оскільки це може викликати зворотну реакцію союзників України. Натомість вона зосереджується на моральному придушенні жителів Європи та послабленні їхньої підтримки України (Григор'єв В., 2025).

Згідно з результатами всеукраїнського опитування, проведеного Київським міжнародним інститутом соціології в період з 14 лютого по 4 березня 2025 року, було виявлено, що 87% українців вважають, що росія не зупиниться на вже окупованих територіях, а її головною метою є або геноцид українців (28%), або повне знищення української державності (38%). Опитування також показує, що навіть у найбільш вразливих регіонах України більшість населення не сприймає наратив про обмеженість російських територіальних амбіцій, оскільки на Заході та в Центрі від 68 до 70% респондентів, а на Півдні та Сході 62% і 46% відповідно, вважають, що росія прагне знищити українську націю. Загалом соціологічні дані демонструють низький рівень довіри українців до будь-яких заяв Кремля про припинення експансії, оскільки лише 4% респондентів вірять, що росія обмежиться вже окупованими територіями (*Яку мету Росія зараз ставить перед собою у війні проти України*, 2025).

Дослідник Арсалан Білал (2024) зазначає, що росія активно використовує

гібридну війну як стратегічний інструмент для підриву західних держав, комбінуючи військові та невійськові засоби, такі як дезінформація, втручання у вибори, кібератаки та підтримка недержавних акторів. Вона прагне компенсувати свою військову та економічну слабкість через синхронізоване використання політичних маніпуляцій, енергетичного шантажу та прихованих операцій із впливу на демократичні процеси. Незважаючи на певні успіхи у дестабілізації Заходу, росія не змогла завадити демократичним державам формувати глобальний політичний, економічний та культурний порядок. Тому Захід повинен розробити згуртовану та стратегічно продуману відповідь на агресивну гібридну тактику Москви, щоб ефективно протистояти її впливу.

Гібридна війна має дві ключові особливості. По-перше, межа між миром і війною є розмитою, що ускладнює визначення початку збройного конфлікту, адже замість відкритої агресії використовуються інструменти дезінформації та співпраця з недержавними суб'єктами. Це дозволяє агресору досягати стратегічних цілей із меншими ризиками та витратами, водночас завдаючи суттєвої шкоди державі-мішені. По-друге, гібридна війна характеризується високим рівнем невизначеності, що ускладнює як ідентифікацію самої атаки, так і визначення її ініціатора. Завдяки цій невизначеності країна-агресор може уникати відповідальності, що суттєво ускладнює протидію гібридним загрозам (*Гібридна війна – нові загрози*, 2021).

Аксель Гагельстам наголошує на необхідності спільної протидії гібридним загрозам, які постійно змінюються, включаючи методи від дезінформації до військової сили. Заходи протидії повинні бути адаптивними та випереджати загрози, що вимагає тісної співпраці між НАТО, ЄС та національними органами безпеки. Ключовим є зміцнення стійкості суспільства та захист критичної інфраструктури, оскільки атака на одну країну може мати глобальні наслідки. Після появи “зелених чоловічків” у Криму в 2014 році гібридні загрози стали пріоритетом НАТО, що призвело до розробки Об'єднаної структури протидії гібридним загрозам у 2016 році.

Важливими результатами стали створення групи зі збирання даних у Розвідувальному центрі ЄС та Європейського центру передового досвіду в Гельсінкі (*Співпраця заради протидії гібридним загрозам*, 2018).

Аналізуючи порушену проблематику, необхідно звернути увагу на статистичні дані, що відображають масштаби військової агресії та інформаційного впливу з огляду гібридної війни проти України. За даними видання *Janes Defence Weekly*, на початок конфлікту на Сході України проти українських сил оборони діяли: 14 400 військовослужбовців регулярної російської армії та 29 300 озброєних сепаратистів. Таким чином, загальна чисельність ворожих сил на Донбасі становила 43 700 осіб. Крім того, у Криму було розміщено 29 800 російських військових, а вздовж українсько-російського кордону – ще 55 800. Загалом, сили, що безпосередньо загрожували Україні, налічували близько 129 300 осіб (*Україні протистойть 130 тисяч озброєних людей у гібридній війні*, 2015). Водночас дослідження, проведене у 2022 році, аналізувало поширення проросійської пропаганди у соціальних мережах під час вторгнення в Україну. Було зібрано 349 455 повідомлень у *Twitter* з проросійським змістом, які отримали приблизно 251 000 ретвітів та охопили близько 14,4 мільйона користувачів. Важливо відзначити, що 20,28% поширювачів цих повідомлень були класифіковані як боти, більшість з яких створено на початку вторгнення (*Анексія Криму та світова “гібридна війна”*, 2017; *Russian propaganda on social media during the 2022 invasion of Ukraine*, 2023). Інше дослідження вивчало розповсюдження пропаганди та дезінформації на платформах *Facebook* та *Twitter* у перші місяці конфлікту. Результати показали, що лише 8-15% публікацій, які містили посилання на російську пропаганду або ненадійні джерела, були видалені модераторами платформ, що свідчить про вразливість соціальних мереж до поширення дезінформації під час кризових ситуацій (*У 2024 році кількість кібератак на Україну зросла на 70%*, 2024)

На початку широкомасштабного вторгнення, починаючи з 2020 року, кількість інформаційних атак, економічного тиску та інших форм агресії стрімко

зростала. Узагальнені дані щодо кібератак на Україну свідчать про їхнє поступове збільшення: у 2020 році зафіксовано 800 атак, у 2021 – 1 400, у 2022 – 2 541, у 2023 – 4 315, а у 2024 – 4 315 кібератак. Ця статистика демонструє стійку тенденцію до зростання кіберагресії проти України, що вказує на посилення інформаційної складової гібридної війни (*Кількість кібератак на рік на критичну інфраструктуру України зросла з 800 до 4500*, 2024).

В умовах російсько-української війни ворог систематично здійснює інформаційно-психологічний вплив як на громадянське суспільство України та міжнародну спільноту, так і на військовослужбовців Сил оборони України. Одним із ключових інструментів поширення його ідеологічних наративів є медіа (від лат. *medium* – посередник). У межах інформаційної війни противник активно використовує різні засоби масової комунікації, зокрема телебачення, радіо, друковані видання (газети, журнали, книги), інтернет-ресурси та соціальні мережі (*Facebook*, *Instagram*, *Twitter*, *TikTok*). Отже, розв'язана російською федерацією гібридна війна вкотре підкреслює важливість усвідомлення проблеми психологічної підтримки особового складу військових частин (підрозділів) та необхідності захисту від негативного інформаційно-психологічного впливу ворога, який є одним із ключових інструментів його агресії.

Висновок. Гібридна війна як форма сучасного конфлікту є багатовимірним явищем, що охоплює як традиційні військові дії, так і невійськові методи впливу, включаючи інформаційні атаки, економічний тиск та політичні маніпуляції. Вона спрямована на підрив суверенітету держави шляхом комплексного використання дезінформації, кібератак та дипломатичного впливу. Україна протягом одинадцяти років протистояння російській агресії зіткнулася з усіма складовими гібридної війни, що змусило адаптувати національну систему безпеки до нових викликів. Інформаційна війна, що супроводжує бойові дії, відіграє вирішальну роль у формуванні суспільної думки та міжнародної підтримки, що є ключовим фактором у протидії агресору. Досвід

України у боротьбі з гібридною війною підкреслює необхідність розробки ефективних стратегій протидії таким загрозам на глобальному рівні. Це вимагає посилення міжнародної співпраці,

зміцнення кібербезпеки, вдосконалення інформаційної політики та розвитку механізмів стратегічної комунікації для запобігання дестабілізації держав через гібридні методи впливу.

Список використаних джерел

1. Агаєв, Н.А. Герасименко, М.В., Дикун, В.Г. & Стасюк, В.В. (2020) *“Гібридна війна” росії проти України: інформаційний вимір: навч. посіб.* Київ, ТОВ “7БЦ”.
2. Алещенко, В.І. (2016) Феноменологія “гібридної війни” та її особливості у виконанні російської федерації: інформаційно-психологічний аспект. Вісн. Київ. нац. ун-ту імені Тараса Шевченка. *Військово-спеціальні науки*. Вип. 1. С. 6 – 11.
3. *Анексія Криму та світова “гібридна війна”*. (2017) Крим реалії: веб-сайт. Вилучено з https://ua.krymr.com/a/28527438.html?utm_source=chatgpt.com
4. Білал, А. (2024) *Гібридна війна росії проти Заходу*. Думки, аналіз і обговорення питань безпеки. NATO Review: веб-сайт. Вилучено з <https://www.nato.int/docu/review/uk/articles/2024/04/26/index.html>
5. Галеотті, М. (2017) *Російська розвідка веде політичну війну*. Погляд: веб-сайт. Вилучено з <https://independentview.net/2017/06/02/mark-haleotty-rossyjskaya-razvedka/>
6. *Гібридна війна – нові загрози, складність і “довіра” як антидот*. (2021) Думки, аналіз і обговорення питань безпеки. NATO Review: веб-сайт. Вилучено з <https://www.nato.int/docu/review/uk/articles/2021/11/30/gbridna-vjna-nov-zagrozi-skladnst-dovra-yak-antidot/index.html>
7. Горбулін, В.П. (ред.) (2017) *Світова гібридна війна: український фронт: монографія*. Київ: НІСД.
8. Григор’єв В. (2025) *Як далеко може зайти рф у гібридній війні проти Європи: у Foreign Policy дізналися деталі*. Інформаційне агентство УНІАН: веб-сайт. Вилучено з <https://www.unian.ua/world/gibridna-viyna-yak-daleko-mozhe-zayti-rosiya-v-yevropi-12880026.html>
9. *Кількість кібератак на рік на критичну інфраструктуру України зросла з 800 до 4500: СБУ назвала організаторів*. (2024) Мінфін: веб-сайт. https://minfin.com.ua/ua/2024/05/07/126427603/?utm_source=chatgpt.com
10. *Породження війни з безсилля миру: смислова логіка війни*. (2022) Національний інститут досліджень: веб-сайт. Вилучено з https://niss.gov.ua/news/statti/porodzhennya-viyny-z-bezsylyya-myr-smyslova-lohika-viyny?utm_source=chatgpt.com
11. Рушенко, І.П. (2015) *російсько-українська гібридна війна: погляд соціолога: монографія*. Харків: ФОП Павленко О.Г.
12. Савлюк, М. (2024) *Гібридна війна в Україні: сучасні підходи*. Вісник Прикарпатського університету. Серія: Політологія. Випуск 17, 2024. С. 187 – 197. DOI 10.32782/2312-1815/2024-17-23
13. *Співпраця заради протидії гібридним загрозам* (2018) NATO Review: веб-сайт. Вилучено з <https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi-protid-gbridnim-zagrozam/index.html>
14. *Україні протистойть 130 тисяч озброєних людей у гібридній війні*. (2015) Радіо Свобода: веб-сайт. Вилучено з https://www.radiosvoboda.org/a/26884092.html?utm_source=chatgpt.com
15. *У 2024 році кількість кібератак на Україну зросла на 70%*. (2024) Інститут масової інформації: веб-сайт. Вилучено з https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931?utm_source=chatgpt.com
16. *Яку мету росія зараз ставить перед собою у війні проти України*. (2025) Прес-релізи та звіти. Київський міжнародний інститут соціології: веб-сайт. Вилучено з <https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1505&page=1>
17. *Assessing Baltic Sea Regional Maritime Security*. (2017) Foreign Policy Research Institute: website. Removed from <https://www.fpri.org/article/2017/06/assessing-baltic-sea-regional-maritime-security/>
18. Freedman, L. (2022) *Absolute Ends with Limited Means: Putin’s Self-Deception*. Comment is Freed. Removed from <https://samf.substack.com/p/absolute-ends-with-limited-means?/>
19. *Future Warfare: The Rise of Hybrid Wars*. (2005) U.S. Naval Institute: website. Removed from <http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf>
20. Galeotti, M. (2016) *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right*. Military History (Books).
21. Hoffman, F. (2007) *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies.
22. Luttwak, E. (2016) *Coup d'État: A Practical Handbook, Revised Edition*. Harvard University Press.

23. Montgomery, McFate. (2018) *Military Anthropology: Soldiers, Scholars and Subjects at the Margins of Empire* Oxford University Press.
24. Nye, J. (2005) *Soft Power: The Means To Success In World Politics*. PublicAffairs.
25. Nye, J. (2011) *The Future of Power*. PublicAffairs.
26. Rid, T. (2021) *Active Measures: The Secret History of Disinformation and Political Warfare*. Profile Books.
27. *Russian propaganda on social media during the 2022 invasion of Ukraine*. (2023) Springer Open: website. Removed from <https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-023-00414-5>

References

1. Aghaev, N.A., Herasymenko, M.V., Dykun, V.G. & Stasiuk, V.V. (2020) Russia's "hybrid war" against Ukraine: the information dimension: study guide. [Russia's "hybrid war" against Ukraine: the information dimension]. Kyiv, LLC "7Bts". (in Ukraine)
2. Aleshchenko, V.I. (2016) Phenomenology of "hybrid war" and its features in the performance of the Russian Federation: informational and psychological aspect. [Fenomenolohiya "hibrydnoyi viyny" ta yiyi osoblyvosti u vykonanni rosiys'koyi federatsiyi: informatsiyno-psykholohichnyy aspekt]. Visn. Kyiv. National Taras Shevchenko University. Military and Special Sciences. Issue 1. Pp. 6 – 11. (in Ukraine)
3. The annexation of Crimea and the global "hybrid war". (2017) [The annexation of Crimea and the global "hybrid war"]. Crimea realities: website. URL: https://ua.krymr.com/a/28527438.html?utm_source=chatgpt.com (in Ukraine)
4. Bilal, A. (2024) Russia's Hybrid War Against the West. [Hibrydna viyna rosiyi proty Zakhodu]. Opinion, Analysis and Discussion on Security Issues. NATO Review: website. Retrieved from <https://www.nato.int/docu/review/uk/articles/2024/04/26/index.html> (in England)
5. Galeotti M. Russian intelligence is waging a political war. [Mark Haleotti: Rosiys'ka rozvidka vede politychnu viynu]. (2017) View: website. URL: <https://independentview.net/2017/06/02/mark-haleotti-rossyjskaya-razvedka/> (in Ukraine)
6. Hybrid Warfare – New Threats, Complexity and "Trust" as an Antidote. (2021) [Hibrydna viyna – novi zahrozy, skladnist' i "dovira" yak protyotruta]. Opinion, Analysis and Discussion on Security Issues. NATO Review: website. Retrieved from <https://www.nato.int/docu/review/uk/articles/2021/11/30/gbridna-vjna-nov-zagrozi-skladnst-dovra-yak-antidot/index.html> (in England)
7. Gorbulin, V.P. (ed.) (2017) *World Hybrid War: Ukrainian Front* [Svitova hibrydna viyna: ukrayins'kyy front]; monograph. Kyiv: NISD (in Ukraine)
8. Grigoriev V. (2025) How far can the Russian Federation go in a hybrid war against Europe [Yak daleko mozhe zayty rf u hibrydnyy viyni proty Yevropy]: Foreign Policy learned the details. UNIAN News Agency: website. Retrieved from <https://www.unian.ua/world/gibridna-viyna-yak-daleko-mozhe-zayti-rosiya-v-yevropi-12880026.html> (in Ukraine)
9. The number of cyberattacks per year on Ukraine's critical infrastructure has increased from 800 to 4500: the SBU has named the organizers. [Kil'kist' kiberatak na rik na krytychnu infrastrukturu Ukrayiny zrosla z 800 do 4500: SBU nazvala orhanizatoriv]. (2024) Ministry of Finance: website. Retrieved from https://minfin.com.ua/ua/2024/05/07/126427603/?utm_source=chatgpt.com (in Ukraine)
10. The birth of war from the impotence of peace: the semantic logic of war (2022). [Porodzhennya viyny z bezsyllya myru: smyslova lohika viyny]. National Research Institute: website. Retrieved from https://niss.gov.ua/news/statti/porodzhennya-viyny-z-bezsyllya-myr-smyslova-lohika-viyny?utm_source=chatgpt.com (in Ukraine)
11. Rushenko, I.P. (2015) Russian-Ukrainian hybrid war: a sociologist's view. [Rosiys'ko-ukrayins'ka hibrydna viyna: pohlyad sotsioloha]; monograph. Kharkiv: FOP Pavlenko O.G. (in Ukraine)
12. Savlyuk, M. (2024) Hybrid War in Ukraine: Modern Approaches. [Hibrydna viyna v Ukrayini: suchasni pidkhody] Bulletin of the Precarpathian University. Series: Political Science. Issue 17, 2024. Pp. 187 – 197. DOI 10.32782/2312-1815/2024-17-23 (in Ukraine)
13. Cooperation to Counter Hybrid Threats. [Spivpratsya za rady protydiyi hybrydnym zahrozam] (2018) NATO Review: website. Retrieved from <https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi-protid-gbridnim-zagrozm/index.html> (in England)
14. Ukraine is opposed by 130 thousand armed people in a hybrid war. (2015) [Ukrayini protystoyit' 130 tysyach ozbroynykh lyudey u hibrydnyy viyni]. Radio Liberty: website. Retrieved from https://www.radiosvoboda.org/a/26884092.html?utm_source=chatgpt.com (in Ukraine)
15. In 2024, the number of cyberattacks on Ukraine increased by 70%. (2024) [U 2024 rotsi kil'kist' kiberatak na Ukrayinu zrosla na 70%]. Institute of Mass Information: website. Retrieved from https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931?utm_source=chatgpt.com (in Ukraine)

16. What goal does Russia now set for itself in the war against Ukraine? (2025) [Yaku metu rosiya zaraz stavyt' pered soboyu u viyni proty Ukrayiny]. Press releases and reports. Kyiv International Institute of Sociology: website. Retrieved from <https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1505&page=1> (in Ukraine)
17. *Assessing Baltic Sea Regional Maritime Security*. (2017) Foreign Policy Research Institute: website. Removed from <https://www.fpri.org/article/2017/06/assessing-baltic-sea-regional-maritime-security/>
18. Freedman, L. (2022) *Absolute Ends with Limited Means: Putin's Self-Deception*. Comment is Freed. Removed from <https://samf.substack.com/p/absolute-ends-with-limited-means?/>
19. *Future Warfare: The Rise of Hybrid Wars*. (2005) U.S. Naval Institute: website. Removed from <http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf>
20. Galeotti, M. (2016) *Hybrid War or Gibrinaya Voina? Getting Russia's non-linear military challenge right*. Military History (Books).
21. Hoffman, F. (2007) *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies.
22. Luttwak, E. (2016) *Coup d'État: A Practical Handbook, Revised Edition*. Harvard University Press.
23. Montgomery, McFate. (2018) *Military Anthropology: Soldiers, Scholars and Subjects at the Margins of Empire* Oxford University Press.
24. Nye, J. (2005) *Soft Power: The Means To Success In World Politics*. PublicAffairs.
25. Nye, J. (2011) *The Future of Power*. PublicAffairs.
26. Rid, T. (2021) *Active Measures: The Secret History of Disinformation and Political Warfare*. Profile Books.
27. *Russian propaganda on social media during the 2022 invasion of Ukraine*. (2023) Springer Open: website. Removed from <https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-023-00414-5>

Summary

HYBRID WARFARE AS A NEW DIMENSION OF MODERN CONFLICTS

Kyrychenko A. doctor of philosophy (PhD),
senior teacher of the Internal Communications
Chair of the National Defence University of Ukraine
Ivanenko S. doctor of philosophy (PhD), senior teacher
of the Internal Department of Military History of Ukraine,
National Defense University of Ukraine
Remez V. doctor of philosophy (PhD), senior teacher
of the Department of Territorial Defense,
National Defense University of Ukraine

Introduction. Today, the hybrid warfare is becoming one of the most pressing challenges for the national security of many states. This problem is of particular importance for our country after Russia violated the terms of the Budapest Memorandum and annexed a significant part of its territory. Open military aggression was accompanied by a powerful informational and psychological influence, the purpose of which was to form a favorable social environment for the spread of the ideology of the so-called "Russian world". Over more than eleven years of confrontation, Ukraine has faced all possible instruments of hybrid warfare, including both non-military (political, economic, humanitarian, cyber, informational and psychological) and military methods (crisis management, strategic deployment, military intervention, etc.). It is the combination of various measures aimed at undermining the sovereignty and independence of the state that defines the essence of hybrid warfare. Analyzing the features of hybrid warfare, it is necessary to consider its main components, methods of conduct, and consequences for Ukraine and the world as a whole. Researching this phenomenon is a key of importance for developing effective mechanisms to counter modern challenges and threats in the field of national security.

Theoretical background. Theoretical background. Hybrid war as a new type of military-political conflict is becoming a subject of research by both foreign and domestic scholars. An important contribution to the study of this phenomenon was made by such foreign researchers as F. Hoffman, M. McFate, E. Luttwak, J. Nye, L. Freedman, M. Galeotti, T. Rieder, who analyzed the strategies and tactics of hybrid war, the mechanisms of information influence and disinformation. Among Ukrainian scientists who have made a significant contribution to the study of hybrid warfare, it is worth highlighting the works of V. Aleshchenko, T. Andriievskiy, O. Baranovskiy, P. Hai-Nyzhnyk, V. Horbulin, V. Holovchenko, M. Doroshko, O. Yizhak, Yu. Kohut, Ye. Mahda, B. Parakhonskyi, H. Perepelytsia, H. Pocheptsov, I. Rushchenko, Yu. Uzdenova, H. Yavorska, who considered the political, military, informational and economic aspects of hybrid aggression.

Therefore, the study of hybrid warfare, its mechanisms and consequences is extremely important for understanding modern military-political conflicts and developing effective countermeasures.

Research methods. The scientific research applied a complex of theoretical and empirical methods that allowed for a comprehensive analysis of the problem of hybrid warfare. Theoretical methods included analysis, synthesis, abstraction, generalization, induction, and deduction, which contributed to the formation of a general idea of the essence, components, and mechanisms of conducting hybrid warfare. For a deeper understanding of the problem, a comparative method was used, which made it possible to compare approaches to conducting hybrid warfare in different countries and assess the effectiveness of countermeasures. The systemic approach allowed us to consider hybrid warfare as a multi-component phenomenon that combines military, political, economic, informational and cyber aspects. Content analysis was used to analyze informational and psychological influence and propaganda, which allowed us to identify the main narratives used in the media space. Statistical methods were used to collect and process quantitative data related to information attacks, economic pressure, and other forms of hybrid aggression. In addition, an expert assessment method was used, which involved analyzing the views of specialists in the fields of security, defense, political science, and international relations to determine effective strategies for countering hybrid threats. The use of a combination of these methods allowed for a comprehensive analysis of the problem under study, systematization of existing scientific approaches, and development of substantiated conclusions.

Conclusion. Hybrid warfare as a form of modern conflict is a multidimensional phenomenon that encompasses both traditional military actions and non-military methods of influence, including information attacks, economic pressure, and political manipulation. It aims to undermine state sovereignty through the integrated use of disinformation, cyberattacks, and diplomatic influence. During the eleven years of resistance to Russian aggression, Ukraine has faced all the components of hybrid warfare, which has forced it to adapt its national security system to new challenges. The information war that accompanies hostilities plays a crucial role in shaping public opinion and international support, which is a key factor in countering the aggressor. Ukraine's experience in combating hybrid warfare highlights the need to develop effective strategies to counter such threats at the global level. This requires increased international cooperation, strengthening cybersecurity, improving information policy, and developing strategic communication mechanisms to prevent the destabilization of states through hybrid methods of influence.

Keywords: hybrid warfare; information and psychological warfare; disinformation; cyberattacks; economic pressure; political manipulation; international security; strategic communication.

Концептуалізація – Кириченко А.В.

Ресурси – Іваненко С.М.

Формальний аналіз – Ремез В.В.

Автори заявляють про відсутність конфлікту інтересів.

The authors declare that they have no conflict of interest.

Дата надходження рукопису/Date of receipt of the manuscript: 24.03.25.

Дата прийняття рукопису/Date of acceptance of the manuscript: 28.05.25.

© 2025. This work is under an open license CC BY-NC 4.0.