Кам’янець-Подільський національний університет імені Івана Огієнка
Історичний факультет
Кафедра політології та філософії

Дипломна робота

бакалавра

з теми: ГІБРИДНІ ВІЙНИ ЯК НОВІТНЯ ФОРМА ГЛОБАЛЬНОГО ПРОТИСТОЯННЯ

Виконала:
студентка P1B23z групи
спеціальності 052 Політологія
заочної форми навчання
ГУМЕНЮК Ірина

Науковий керівник:
Грубі Т. В., в.о. завідувача кафедри
політології та філософії
кандидат соціологічних наук, доцент

Рецензент:

_____

Кам’янець-Подільський
2026

ЗМІСТ

ВСТУП…… 3

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ГІБРИДНИХ ВІЙН…… 7

1.1. Поняття та сутність гібридної війни у сучасній політології…… 7

1.2. Еволюція гібридних конфліктів: від класичних війн до асиметричних форм протистояння…….. 14

1.3. Структурні компоненти гібридної війни:…… 20

Висновки до розділу 1……30

РОЗДІЛ 2. МЕХАНІЗМИ РЕАЛІЗАЦІЇ ТА ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ У ГЛОБАЛЬНОМУ ВИМІРІ…… 31

2.1. Особливості та технології ведення гібридних війн (на прикладі російсько-українського конфлікту)…… 31

2.2. Міжнародний досвід протидії гібридним загрозам: інституційні та правові механізми……37

2.3. Інформаційна стійкість та когнітивна безпека суспільства в системі протидії гібридній агресії……..41

Висновки до розділу 2……50

ВИСНОВКИ…… 51

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…… 54

ВСТУП

Актуальність дослідження на початку XXI ст. традиційні форми міждержавного протистояння поступилися місцем асиметричним, комбінованим стратегіям, які отримали назву «гібридні війни». Вони об'єднують конвенційні та неконвенційні методи ведення бойових дій, кібератаки, інформаційно-психологічний вплив, економічний тиск і використання внутрішніх відносин в державі, що є об'єктом нападу.

Для України, яка з 2014 р., а після повномасштабного вторгнення 2022 р. з особливою інтенсивністю перебуває в стані гібридної війни з російською федерацією, дослідження природи, механізмів і способів протидії таким загрозам має критичне значення для національної безпеки. Український досвід уже став унікальним базисом для апробації методів стримування гібридного агресора, але водночас виявив низку системних проблем – від неузгодженості дій різних відомств до недостатньої спроможності протистояти інформаційно-психологічним операціям на рівні суспільства. Саме тому, аналіз гібридних війн як новітньої форми глобального протистояння становить безсумнівний науковий і практичний інтерес, що зумовило вибір теми дослідження: «Гібридні війни як новітня форма глобального протистояння».

Ступінь наукової розробленості проблеми. Поняття «гібридна війна» увійшло до наукового обігу на початку XXI ст. завдяки працям Ф. Гоффмана [56], однак його концептуалізація має тривалу передісторію. Теоретичні засади асиметричних форм боротьби закладали Карл фон Клаузевіц та Антуан де Жоміні, а в другій половині XX ст. проблематику нетрадиційних конфліктів розвивали Д. Галула, Мертон ван Кревельд та Е. Люттвак.

Із початком російсько-українського конфлікту 2014 р. інтерес до гібридних війн різко зріс. Серед західних авторів варто відзначити дослідження Е. Реддіна,

М. Галеотті (критика концепції «гібридної війни» та пропозиція терміну «нелінійна війна»), Л. Фрідмана [55], а також праці С. Байєра.

В українській науці фундаментальні праці з теорії та практики гібридних конфліктів належать В. Горбуліну [9; 37], І. Дерев'янко [10], О. Литвиненку [26], Г. Почепцову [31], Ю. Уздєновій [41]. Дослідження інформаційної складової гібридної агресії здійснюють М. Стрельбицький та М. Гринь [39], В. Сазонов [35], Н. Кравченко [23], О. Сальникова, І. Сівоха та А. Іващенко [36], В. Кожушко [21]. Правові аспекти протидії аналізують М. Бутенко, Б. Ворович, А. Іващенко, Д. Федянович [5], Д. Вєдєнєєв та О. Семенюк [6]. Водночас, незважаючи на значну кількість наукових праць, залишаються дискусійними питання сутності гібридної війни, недостатньо систематизовано механізми протидії на різних фазах конфлікту, а когнітивні аспекти резильєнтності суспільства в умовах тривалої гібридної агресії взагалі залишаються мало вивченими.

Метою дослідження є осмислення природи гібридних війн як новітньої форми глобального протистояння, виявлення їх структурних компонентів, механізмів реалізації та найбільш ефективних форм протидії.

Досягнення поставленої мети передбачає вирішення наступних завдань:

– систематизувати теоретико-методологічні підходи до визначення поняття «гібридна війна» та простежити еволюцію гібридних конфліктів від класичних до асиметричних форм протиборства;

– охарактеризувати структурні компоненти гібридної війни та проаналізувати сценарії їх застосування на прикладі російсько-українського конфлікту 2014-2026 рр.;

– узагальнити міжнародний досвід інституційних та правових механізмів протидії гібридним загрозам;

– визначити роль стратегічних комунікацій, медіаграмотності та суспільної резильєнтності в системі захисту від гібридної агресії.

Об'єктом дослідження є гібридні війни як форма політичного та збройного протистояння в сучасних міжнародних відносинах. **Предметом дослідження** виступають структурні компоненти, технології реалізації та стратегії протидії гібридним війнам на національному й міжнародному рівнях.

Методологічні засади дослідження базуються на комплексному міждисциплінарному підході, що поєднує інструментарій політології, конфліктології, теорії міжнародних відносин, соціології.

Діалектичний метод застосовано для аналізу гібридної війни в динаміці її розвитку та внутрішніх суперечностей. Системний метод дозволив розглядати гібридну війну як цілісну багатокомпонентну систему. Метод аналізу та синтезу використано для виокремлення структурних складових гібридної війни та їх інтеграції в узагальнену модель. Порівняльний метод дав змогу зіставити різні підходи до протидії гібридним викликам у світовій практиці. Інституційний метод застосовано для аналізу діяльності міжнародних організацій у сфері протидії гібридним загрозам. Метод кейс-стаді забезпечив поглиблене вивчення конкретних проявів гібридної війни – передусім у російсько-українському конфлікті, а також контент-аналіз та дискурс-аналіз наративів, які супроводжують гібридні операції.

Практичне значення дослідження полягає в тому, що його результати можуть бути використані для подальшого поглиблення теми в межах наукових розвідок. Матеріали дослідження, щодо механізмів ведення гібридних війн та практики протидії доцільно застосовувати в навчальному процесі при викладанні дисциплін «Гібридні війни», «Стратегічні комунікації», «Інформаційна безпека», а також для підготовки аналітичних матеріалів.

Окремі положення роботи можуть бути використані в практичній діяльності органів державної влади, що займаються питаннями інформаційної

безпеки та стратегічних комунікацій, зокрема при розробці регіональних програм медіаграмотності.

Апробація результатів дослідження. Результати дослідження були апробовані в статтях «Гібридні війни в історії міжнародних конфліктів» й опубліковані у збірнику Філософ-і-Я: наукові розвідки студентів Кам'янець-Подільського національного університету імені Івана Огієнка : наук. журнал / гол. ред. А.В. Найчук. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2025. Випуск 10 (3), «Між миром і війною: феномен гібридного протиборства в сучасних міжнародних відносинах» у збірнику Філософ-і-Я: наукові розвідки студентів Кам'янець-Подільського національного університету імені Івана Огієнка : наук. журнал / гол. ред. А.В. Найчук. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2025. Випуск 10 (4) та науковій конференція студентів і магістрантів за підсумками НДР у 2025-2026 н. р. (8-9 квітня 2026 р., м. Кам'янець-Подільський).

Структура роботи. Робота складається зі вступу, двох розділів, висновків до кожного розділу, загальних висновків, списку використаних джерел.

РОЗДІЛ 1.
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ГІБРИДНИХ ВІЙН

1.1. Поняття та сутність гібридної війни у сучасній політології

Початок XXI ст. ознаменувався глибокою трансформацією системи міжнародних відносин, що детермінувало появу якісно нових форм політичного та збройного протистояння. Холодна війна, з її відносною передбачуваністю, поступилася місцем епосі глобальної нестабільності та асиметричних загроз. У сучасному глобалізованому світі, де інформаційні та комунікаційні технології досягли безпрецедентного рівня розвитку, традиційна війна втратила монополію на досягнення геополітичних цілей. На зміну їй прийшли конфлікти нового типу, які в науковій літературі отримали назву «гібридні війни».

Як зазначає у своєму дослідженні Ю. Уздєнова, сьогодні гібридна війна дедалі частіше виступає інструментом досягнення стратегічних цілей держав, поєднуючи засоби військового, інформаційного, економічного та дипломатичного характеру [41, с. 172]. Осмислення її специфіки та природи є необхідною умовою для ефективної протидії агресору, а відсутність цього розуміння, або його фрагментарність, робить державу вразливою перед новими, нестандартними викликами [8, с. 257].

Варто наголосити на тому, що концепція «гібридної війни» не є абсолютно новим відкриттям. Спроби поєднувати звичайні військові дії з партизанськими рухами, економічним тиском або дипломатичними маніпуляціями простежуються протягом всієї історії людства. Проте, як аргументовано доводять українські дослідники, особливістю сучасного етапу є не стільки поява принципово нових інструментів, скільки зміна їхньої ролі, масштабу та ефекту від їх комплексного застосування. М. Савлюк, аналізуючи генезис російсько-української війни, констатує, що вона розпочалася задовго до активної фази у 2014 р. Цій війні, яка,

безперечно, є гібридною, багато років поспіль передували інформаційна, культурна та економічна експансії [34, с. 189]. Він звертає увагу, що ще з 90-х рр. XX ст. в Україні постійно працювали російські телеканали, які насаджували українцям прокремлівські наративи про «братні народи» та спільну історію, а російські компанії безперешкодно поглинали український бізнес. Цей комплекс агресивних дій створив сприятливе підґрунтя для подальшої збройної агресії, демонструючи довготривалий і системний характер гібридної війни [34, с. 190], яка залишатиметься своєрідним воєнним трендом у найближчі не лише роки, а й десятиліття [14, с. 56]. Саме тому важливо розрізняти ситуативні гібридні дії від довгострокової гібридної стратегії, яка передбачає багаторічну підготовку суспільної свідомості до війни.

Теоретичне осмислення феномену гібридної війни активізувалося на межі XX-XXI ст., але його історія сягає корінням у теорії «війн четвертого покоління» (Fourth Generation Warfare), які почали розроблятися ще в 1980-х рр. групою американських аналітиків на чолі з Вільямом С. Ліндом [59, с. 22]. Ця теорія виділила чотири еволюційні етапи ведення війни, де четверте покоління знаменує перехід до децентралізованих форм конфлікту, в яких держави втрачають монополію на застосування бойових сил, а межа між війною та миром стає дедалі розмитішою [59, с. 24].

Паралельно з цим науковим підходом на межі тисячоліть з’явилася ще одна концепція, яка суттєво вплинула на формування ідеї гібридності - теорія «необмеженої війни» (Unrestricted Warfare), запропонована китайськими військовими теоретиками Цяо Ляном та Ван Сянсуєм [63]. Її ключовою новацією стала позиція, що сучасне протистояння більше не обмежується виключно військовими засобами; поле бою розширюється до всього простору суспільства, включаючи фінансову, торгівельну, культурну, дипломатичну та інформаційну сфери [63, с. 43].

Формування поняття «гібридна війна» у його сучасному вигляді більшість дослідників пов’язують з працями американського військового теоретика Ф. Гоффмана, який вперше системно описав це явище у своїх роботах 2006-2007 рр. [56]. Сам термін «гібридна війна» був введений дослідником у 2006 р., та запозичений із дисертації Роберта Г. Вокера, присвяченій операціям морської піхоти США [55, с. 31]. Саме Ф. Гоффман здійснив спробу подолати прірву між традиційним розумінням регулярної та іррегулярної війни в контексті операційного середовища XXI ст. [56, с. 14]. Офіційне визнання його концепція отримала після публікації 2007 р. роботи «Conflict in the XXI st Century: The Rise of Hybrid Wars» [56].

Визначальною рисою запропонованої Ф. Гоффманом концепції стало те, що він переосмислив природу сучасних збройних конфліктів та підкреслив їх гібридний характер. Він охарактеризував гібридну війну як таку, що охоплює повний спектр різних режимів ведення війни, включаючи звичайні можливості, іррегулярну тактику та формування, терористичні акти, а також кримінальний безлад [56, с. 29]. Цей підхід кардинально відрізнявся від попередніх теорій, які часто розглядали ці форми як окремі та альтернативні одна одній. Дослідник наголошує на тому, що в умовах такого протистояння супротивник може одночасно та адаптивно використовувати звичайне озброєння, нерегулярну тактику, тероризм та злочинну поведінку для досягнення своїх політичних цілей [56, с. 31].

Осмислення природи гібридної війни неможливе без аналізу її співвідношення з суміжними поняттями, такими як асиметрична війна, кібервійна та інформаційна війна. Конструювання даного поняття має не лише теоретичне, але й надзвичайно важливе практичне значення, оскільки саме від того, як держава сприймає гібридні загрози, залежить її здатність ефективно реагувати на них. Хоча у науковому полі ці поняття часто використовуються як взаємозамінні, між ними існують фундаментальні відмінності. Найширшим за

обсягом є поняття гібридної війни, яка охоплює одночасне застосування військових, економічних, політичних, дипломатичних, інформаційних та технологічних засобів. Натомість асиметрична війна є вужчою: вона передбачає лише різницю у військовому потенціалі сторін (наприклад, протистояння регулярної армії та партизанських загонів) і не включає обов'язково невійськові інструменти. Інформаційна війна, в свою чергу, становить лише один із компонентів гібридної війни, який спрямований на маніпуляцію масовою свідомістю, дезінформацію та психологічний вплив, але не передбачає військового чи економічного тиску. Найвужчою є кібервійна - технологічна сукупність гібридних методів, обмежена діями в кіберпросторі (атаки на інфраструктуру, злам систем, викрадення даних).

Як бачимо, гібридна війна виступає своєрідним базисом, що охоплює всі ці явища, поєднуючи їх у єдину стратегію. Це є ключовим для розуміння її сутності: вона не замінює інші форми конфліктів, а синтезує їх для досягнення синергетичного ефекту [29, с. 106].

Сучасна політологія пропонує широкий спектр визначень гібридної війни, що в чергове є доказом багатовимірності цього явища. Узагальнюючи різні наукові підходи, вважаємо за доцільне виокремити три ключові підходи, що розкривають сутність досліджуваного нами феномену.

Перший, вузький (або військово-тактичний) підхід, розглядає гібридну війну як спосіб бойових дій, що поєднує на полі бою регулярні збройні формування (армію, спецпризначенців) з іррегулярними (приватні військові компанії, загони ополчення, терористичні групи). У межах цього підходу акцент робиться на синхронному застосуванні звичайної зброї та партизанської тактики в межах одного театру воєнних дій.

Другий, широкий або політологічний підхід, визначає гібридну війну не як суто військову тактику, а як комплексну стратегію, де основне навантаження переноситься на невійськові засоби впливу: інформаційно-психологічні операції,

економічний та енергетичний тиск, дипломатичну ізоляцію, кібератаки та використання внутрішніх конфліктів у країні, на яку націлена агресія.

Третій, інтегративний (або мережевий) підхід, синтезує перші два, розглядаючи гібридну війну як нову форму протистояння, у якій військові, невійськові та інформаційні компоненти діють одночасно, взаємо підсилюють одне одного та розгортаються не лише на фізичному полі бою, а й у когнітивному, кіберпросторі та гуманітарній сфері, унеможливлюючи чітке розрізнення стану війни та миру.

Погоджуємося із думкою вітчизняної дослідниці Ю. Уздєнової, що найбільш поширеним і продуктивним є політологічний підхід, який розглядає гібридну війну як сукупність заздалегідь підготовлених й оперативно реалізованих дій військового, дипломатичного, економічного, інформаційного характеру, спрямованих на досягнення стратегічних цілей. В межах цього підходу гібридна війна відрізняється від класичної тим, що всі її компоненти спрямовані на затягування конфлікту, збільшення витрат на охорону та оборону країни-жертви з метою її поступового виснаження та примусу до політичних поступок без широкомасштабних бойових дій [41, с. 176].

Окремої уваги заслуговує дискурсивний підхід до розуміння гібридної війни. Відома українська дослідниця Г. Яворська пропонує розглядати гібридну війну як складне явище з двома асиметричними модусами існування: фізичним (матеріальним) та дискурсивним. У своїх дослідженнях вона наголошує на тому, що у військовому вимірі російсько-український конфлікт є переважно локалізованим, при цьому дискурс цієї гібридної війни набув глобального масштабу [46, с. 41]. Боротьба за наративи та сенси, реалізується за допомогою дискурсивних вербально-семіотичних засобів, а конфлікт інтерпретацій використовується як різновид зброї поряд з іншими невійськовими компонентами [46, с. 42]. Цей підхід дозволяє пояснити, чому гібридна війна є настільки ефективною в умовах глобалізованого світу, де битва за свідомість та ідентичність

часто є важливішою, ніж битва за територію. Підкреслимо, що розуміння гібридної війни як дискурсивного конструкту відкриває шлях до формування та використання нових методів протидії, які передбачають не лише військову оборону, але й активну участь у міжнародному інформаційному просторі, де розгортається головне протистояння.

Осмислення природи гібридної війни неможливе без аналізу її структури. У науковій літературі виокремлюють декілька ключових елементів, що утворюють цілісну систему гібридного впливу: інформаційний, ідеологічний, психологічний, економічний, політичний, дипломатичний, військовий, технологічний та енергетичний [38, с. 63].

Інформаційний компонент передбачає цілеспрямоване створення, поширення та приховування інформації, з метою впливу на масову свідомість. Він включає дезінформацію, пропаганду, маніпуляції, а також блокування або дискредитацію незалежних джерел. Ідеологічний, в свою чергу, спрямований на нав’язування цільовій аудиторії інших цінностей, історичних наративів, політичних міфів або релігійних доктрин, що підривають національну ідентичність та легітимність державних інститутів. Психологічний підхід використовує техніки маніпуляції, емоційного тиску, провокування паніки, апатії або агресії, психологічні операції (PSYOP) для зниження волі населення до опору.

Економічний компонент охоплює санкції, торговельні обмеження, маніпуляції валютним курсом, атаки на фондовий ринок, блокування інвестицій, а також підтримку тіньового сектору та корупційних схем. Його мета - економічна дестабілізація, як наслідок, зростання безробіття, падіння рівня життя та поширення соціальної напруги. Політичний компонент як правило реалізується через підтримку політичних сил, що підтримують противника, фінансування опозиційних рухів, втручання у виборчі процеси, дискредитацію влади та розпалювання конфліктів між гілками влади або регіонами. Дипломатичний компонент полягає в ізоляції держави на міжнародній арені: блокування її

ініціатив у міжнародних організаціях, створення альтернативних дипломатичних майданчиків, а також використання «м'якої сили» для переконання союзників у доцільності нейтралітету або співпраці з агресором.

Військовий компонент у гібридному контексті не обов'язково передбачає повномасштабне вторгнення та включає застосування регулярних підрозділів без розпізнавальних знаків («зелені чоловічки»), приватних військових компаній, диверсійно-розвідувальних груп, артилерійських обстрілів території супротивника без формального оголошення війни, а також демонстративні військові навчання біля кордонів для психологічного тиску. Технологічний компонент охоплює кібератаки на критичну інфраструктуру (енергомережі, транспорт, банківську систему, зв'язок), перехоплення комунікацій, впровадження шкідливого програмного забезпечення, а також використання ШІ та deepfake для створення фальшивих відеодоказів чи зламу систем управління. Енергетичний компонент є одним із найефективніших важелів тиску: він реалізується через маніпуляцію цінами на енергоносії, обмеження або припинення постачання газу, нафти, електроенергії, атаки на енергетичну інфраструктуру (як фізичні, так і кібернетичні), а також створення енергетичної залежності через довгострокові контракти на невигідних умовах.

Кожен із цих компонентів окремо може не завдати непоправної шкоди, але в синхронному застосуванні вони детермінують потужний ефект. Саме комплексність, адаптивність та безперервність такого впливу дозволяють агресору досягати стратегічних цілей, уникаючи прямої військової конфронтації та зберігаючи для міжнародної спільноти фасад «мирних» або «обмежених» дій.

Таким чином, концептуалізація поняття гібридної війни в сучасній науці загалом і вітчизняній, зокрема, еволюціонувала від простого запозичення західних дефініцій до розробки власних комплексних теорій, що враховують специфіку російсько-української війни. Вітчизняні дослідники не лише адаптували напрацювання Ф. Гоффмана чи Дж. Мак'юена, але й розширили їх

аналізом реальних гібридних практик. Крім того, дослідили феномен суспільної стійкості: як самоорганізація громад, волонтерство та критичне мислення можуть знижувати результативність гібридних атак. Ще одним важливим напрямом стало вивчення того, як дестабілізація однієї країни впливає на сусідні через міграційні хвилі, економічні зв'язки та інформаційний простір.

1.2. Еволюція гібридних конфліктів: від класичних війн до асиметричних форм протистояння

Кожна історична епоха детермінувала свої, унікальні форми збройного насильства, які відображали рівень розвитку продуктивних сил і суспільних відносин. Як уже зазначалося нами вище, гібридна війна не є принципово новим явищем, її коріння сягає ранніх етапів історії людства [41, с. 173].

При цьому, важливо підкреслити, що хоча термінологічне оформлення гібридних війн відбулося лише на початку XXI ст., елементи гібридності простежуються у воєнних конфліктах різних епох. Вітчизняний дослідник В. Чалапко стверджує, що елементи «гібридності» були притаманні війнам у попередні сторіччя, однак у сучасному контексті вони набули якісно нових характеристик [45, с. 133].

Історичні приклади підтверджують цю тезу. У VI ст. до н. е. під час скіфо-перської війни скіфи застосовували стратегію «випаленої землі» та заманювання ворога вглиб своєї території, уникаючи генеральної битви з переважаючими силами персів [45, с. 134]. Під час греко-перських війн (499-449 рр. до н. е.) активно використовувалися методи інформаційно-психологічного впливу, зокрема дезінформація та формування вигідного образу. Наприкінці XVII ст. стратегія міждержавних конфліктів, в основі якої, по суті, закладались технології гібридних війн, розкривалась французьким ученим Г. Ноде у праці «Політичні роздуми про високу політику і майстерність державних переворотів».

У другій половині XIX ст. великий внесок у вивчення теорії та практики гібридних війн зробив видатний прусський генерал Карл фон Клаузевіц, який у своїй фундаментальній праці «Про війну» (1832 р.) представив базові підходи для підготовки до успішної війни, при цьому згадувались інструменти, які сьогодні визначаються як гібридні. Зокрема, він сформулював головний концептуальний зміст гібридного конфлікту – війна є продовженням політики, але вже іншими засобами.

Сучасні ж форми гібридних війн відрізняються цільовою спрямованістю компонентів, заходів і методів: вони розраховані на пролонгацію конфлікту, провокування гострої реакції серед населення та збільшення витрат країни-жертви на забезпечення безпеки й оборони [41, с. 176]. З огляду на це, еволюційний підхід до аналізу гібридних війн, на нашу думку, дозволяє реконструювати їх генезу і водночас відобразити структурні закономірності, що проявляються в умовах сьогодення.

Теоретичним підґрунтям для аналізу еволюції війн виступає концепція поколінь війн, розроблена У. Ліндом і Г. Тіле та опублікована 1989 р. [27]. Перше покоління війн (до 1648 р.) характеризувалося застосуванням холодної зброї та лінійної тактики, друге покоління (1648-1860-ті рр.) пов’язане із появою нарізної зброї та зростанням ролі вогневої потужності, третє покоління (1860-1918 рр.) ознаменувалося використанням кулеметів, артилерії та позиційною війною. Принципово важливо, що кожен перехід між поколіннями відображав не лише технологічний стрибок, а й зміну організаційної логіки збройного насильства: від лінії зіткнення регулярних армій до маневреної, а згодом і тотальної війни.

Класичні війни індустріальної доби, що досягли свого апогею у Першій та Другій світових війнах, були здебільшого симетричними, де протистояння вели регулярні армії держав, а лінія фронту була чітко визначеною.

Концепція четвертого покоління війн (4GW), започаткована В. Ліндом, К. Найтенгейлом, Дж. Шміттом та іншими дослідниками у 1989 р., ознаменувала

якісний розрив із попередніми етапами еволюції. Її ключовою ідеєю стало стирання відмінностей між війною та політикою, між військовими та цивільними, між фронтом і тилом [59]. Акцент змістився зі знищення живої сили противника на вплив на його політичну волю та громадську думку. Війна дедалі більше перетворювалася на боротьбу наративів, де перемога досягається не стільки на полі бою, скільки в інформаційному просторі. Саме з концепції війн четвертого покоління, на думку М. Кармазіної та І. Аблазова, виросло сучасне розуміння гібридної війни, яка зі зламу XX-XXI ст. посіла одне з центральних місць у науковому дискурсі [14, с. 54]. Вони наголошують, що гібридність залишатиметься своєрідним воєнним трендом у найближчі не лише роки, а й десятиліття, а отже, має підлягати ретельному аналізу [14, с. 56].

Водночас, концепція 4GW отримала певну критику з боку ряду науковців: так, А. Ечеварія звернув увагу на слабку ідеалізацію образу недержавного актора, а Г. Почепцов наголошував, що автор концепції не передбачив феномен «постправди» – ситуацію, для якої маніпулювання інформаційним середовищем набуває самостійного стратегічного значення [31].

У концепції війни п’ятого покоління (5GW) маніпулювання інформацією, експерименти з масовою свідомістю та зміна колективного сприйняття реальності розглядаються як ключові аспекти природи цього типу війни. На відміну від 4GW, яке руйнує межу передусім між учасниками бойових дій і некомбатантами, необмежена війна п’ятого покоління знищує кордони між полями битв і неполями битв, перетворюючи на поле бойових дій не лише всі матеріальні простори, включаючи космічний, а й простори віртуальні та ментальні. Саме в цьому контексті гібридна війна постає не як окремий феномен, а як синтетична форма, що акумулює інструментарій кількох поколінь одночасно, поєднуючи конвенційні дії з інформаційно-психологічними операціями, кібератаками та дестабілізацією через недержавних посередників [42, с. 302].

Як уже зазначалося нами вище, сучасна еволюція війн характеризується переходом від симетричного протистояння регулярних армій до дедалі більш асиметричних форм. Як зазначає І. Дерев'янко, гібридна війна – це особливий тип збройного конфлікту, в якому спостерігається зіткнення симетричних та асиметричних дій, причому асиметричність виступає важливою характеристикою багатьох сучасних збройних конфліктів, у тому числі й гібридного [10, с. 10].

Ще однією відмінністю сучасних гібридних конфліктів від класичних війн є трансформація цілей, засобів та суб'єктів. Якщо класична війна мала на меті фізичне знищення збройних сил противника та захоплення його території, то мета гібридної війни – дестабілізація політичної системи, підрив довіри до влади, руйнування національної ідентичності та примус держави-жертви діяти в інтересах агресора. Останнє реалізується за допомогою поєднання військових та невійськових засобів: кібератак, інформаційних операцій, економічного тиску, використання проксі-сил та підтримки внутрішньої опозиції. Суб'єктами гібридної війни виступають не лише регулярні збройні сили держав, але й приватні військові компанії, терористичні угруповання, бізнес-структури, транснаціональні корпорації, медіахолдинги та окремі особи. Як бачимо, війна перестала бути прерогативою державних інституцій, а стала полем діяльності різноманітних акторів. Ця трансформація нерозривно пов'язана з переходом до інформаційного суспільства, де знання та інформація стають головними ресурсами влади. В. Кожушко у своєму дослідженні слушно наголошує на тому, що сучасні гібридні протистояння кардинально змінили парадигму конфлікту, перетворивши інформаційну сферу на стратегічний театр бойових дій [21, с. 26]. Інформаційний вплив у таких конфліктах є самостійним, фундаментальним виміром, спрямованим на досягнення стратегічних цілей без використання традиційних військових засобів [21, с. 28-30]. Діпфейк-технології, боти, алгоритми ШІ стають інструментами фабрикації реальності, здатної впливати на політичну довіру та стабільність демократичних інститутів [21, с. 12].

Порівнюючи класичні та гібридні війни, можна виокремити низку критеріїв, за якими вони кардинально відрізняються:

- розмитість меж між війною та миром: гібридний конфлікт може тривати роками без офіційного оголошення війни, що ускладнює мобілізацію міжнародної підтримки для країни-жертви;
- асиметричність засобів: агресор використовує свої переваги (наприклад, монополію на інформаційному просторі або кібернетичний потенціал) проти вразливостей жертви;
- мультивекторність впливу: атака ведеться одночасно на військовому, політичному, економічному, інформаційному, соціальному та культурному фронтах;
- зміна ролі населення: цивільне населення перестає бути пасивним об'єктом захисту чи жертвою, перетворюючись на активний об'єкт інформаційно-психологічних операцій.

Важливим аспектом еволюції гібридних конфліктів є зміна ролі міжнародно-правового регулювання, адже під час гібридних війн використовуються інструменти, які традиційно не є частиною воєнних дій [29, с. 107]. Це створює серйозні виклики для міжнародного гуманітарного права, яке було розроблене для регулювання класичних симетричних конфліктів між державами.

Як слушно зазначають вітчизняні дослідники, у сучасній гібридній війні важливим, але недостатньо вивченим компонентом є так звана правова війна. російська федерація використовує внутрішнє та міжнародне право як один з основних інструментів ведення гібридної агресії проти України: інформаційні атаки, операції впливу, економічний тиск, підтримку місцевих опозиційних груп, дезінформацію та злочинну діяльність. Також застосовується приховане розміщення військ у формі без відзнак або військовослужбовців, які не входять до складу регулярних військ [5, с. 30]. Стратегічна вигода такої тактики полягає в

тому, що участь держави-агресора важко довести, а правова невизначеність затримує або розосереджує відповідні дії міжнародної спільноти.

Особливу проблему становить також і те, що гібридні інструменти спеціально розроблені для уникнення звинувачень у порушенні Статуту ООН. Економічні заходи, дезінформація та злочинна діяльність не підпадають під визначення агресії згідно зі Статтею 2(4) Статуту ООН. Водночас вони можуть являти собою форму незаконного втручання у внутрішні справи держави, що підтверджується рішенням Міжнародного суду у справі Нікарагуа (1986 р.) [5, с. 33-34].

Крім того, росія активно використовує правові аспекти в різних сферах гібридної війни: політичній (підтримка етнічного самовизначення на противагу державному суверенітету), дипломатичній (розмивання кордонів між війною і миром), соціально-культурній (використання історії для правового обґрунтування агресії), інформаційній (представлення міжнародного порядку як дискримінаційного щодо Росії), кібернетичній (протидія санкціям за втручання у вибори) тощо [5, с. 32].

З одного боку міжнародне право, зокрема Статут ООН, має достатні рамки для протидії гібридній агресії, однак на практиці відсутність чіткого визначення насильницького втручання та правові прогалини дозволяють агресору уникати відповідальності.

Отже, еволюція війн від класичних до гібридних форм є закономірним наслідком глобальних змін у технологічній, соціальній та політичній сферах. Ключові характеристики гібридних конфліктів: асиметричність, мультивекторність, розмитість межі між війною та миром, а також використання всього арсеналу засобів, включаючи військові, інформаційні, кібернетичні та економічні, визначають їх як якісно новий етап у розвитку воєнної справи. Для нашої держави, яка з 2014 р. перебуває в епіцентрі гібридної війни, розуміння цих

еволюційних змін є надзвичайно важливим для вироблення адекватних стратегій захисту національного суверенітету та територіальної цілісності.

1.3. Структурні компоненти гібридної війни: військові, інформаційні, економічні та когнітивні виміри

Гібридна війна, як комплексне багатовимірне явище, не може бути зведена до жодної зі своїх складових. Її сутність полягає не просто в наборі різних компонентів, а в їх поєднанні, коли одночасний вплив на противника за різними напрямами створює ефект, значно потужніший за суму окремих зусиль. Як зазначають дослідники, визначальними компонентами гібридних війн є військовий, інформаційний, економічний, політичний, дипломатичний, технологічний, ресурсний, енергетичний, ідеологічний та психологічний [38, с. 63]. При цьому вони наголошують на тому, що за умов якісної зміни характеру сучасних міжнародних конфліктів та розширення їх географії по-новому проявляються принципово важливі особливості гібридного протистояння: завдавання декількох зосереджених за часом і місцем невійськових ударів із неочікуваним для противника результатом і неприйнятними для жертви збитками, нав’язування ворогу протиборства у принципово новій системі координат, відсутність звичної лінії фронту та приховування політичних цілей [38, с.65].

Саме тому, врахування структурних компонентів гібридної війни є необхідною передумовою для вироблення адекватних стратегій протидії, оскільки кожен із них вимагає специфічних інструментів захисту та реагування.

Військовий компонент гібридної війни є тим виміром, який традиційно асоціюється з поняттям війни, але в гібридному контексті він набуває принципово нових форм. На відміну від класичних збройних конфліктів, де переважають симетричні зіткнення регулярних армій із чітко визначеною лінією фронту,

військова складова гібридної війни характеризується комбінуванням регулярних збройних сил, іррегулярних формувань, приватних військових компаній (ПВК), проксі-сил та спеціальних операцій. Як зазначає Ю. Уздєнова, всі компоненти, заходи та методи гібридної війни спрямовані на затягування конфлікту, детермінування відповідної реакції та збільшення витрат на охорону й оборону країни-жертви [41, с. 176]. Саме в цьому контексті особливого значення набувають такі інструменти, як приватні військові компанії та проксі-операції. Останні, є такою формою збройного конфлікту, в якій одна або декілька держав чи недержавних акторів використовують третіх осіб для досягнення власних стратегічних цілей, уникаючи прямої військової конфронтації та пов'язаної з нею відповідальності. Цей механізм є класичним прикладом асиметричного підходу, коли держава-агресор використовує формально незалежні, але фактично контрольовані нею формування для ведення бойових дій, зберігаючи при цьому можливість заперечувати свою причетність до конфлікту.

Особливу роль у військовому компоненті гібридної війни відіграють приватні військові компанії (ПВК). На думку Н. Марцінко, вони є одним із ключових інструментів гібридної війни російської федерації проти України [28]. З моменту початку агресії у 2014 р. ПВК виконували функції не лише нерегулярних військових формувань, але й економічних агентів, діяльність яких була спрямована на підрив економічної безпеки держави [28]. Особливої уваги заслуговує аналіз подій 2022-2023 рр., коли ПВК, насамперед «Вагнер», стали важливим елементом вторгнення на українську територію та водночас інструментом економічної експлуатації окупованих регіонів. Використовуючи приклади з окупованого Маріуполя, Херсонщини, Запорізької області та Мелітополя, дослідники простежують схеми демонтажу промислових об'єктів (наприклад, «Азовсталь»), вивезення зерна та сільськогосподарської техніки, захоплення підприємств та використання їх у тіньових економічних процесах. Це підтверджує тезу про те, що військовий компонент гібридної війни не існує

ізольовано, а тісно переплітається з економічним, формуючи єдиний механізм дестабілізації та експлуатації.

Проксі-війни як елемент сучасної гібридної війни заслуговують на окремий аналіз. Специфіка таких конфліктів полягає у тому, що вони є довготривалими збройними протистояннями, які ведуться всередині держави або між кількома внутрішніми акторами за фінансової, матеріальної та військової підтримки зовнішніх сил. Для країни-агресора проксі-війна має низку переваг:

– вона дозволяє досягати геополітичних цілей без прямої участі регулярної армії, що знижує ризик міжнародної ізоляції та запровадження санкцій;

– вона створює можливість для «правдоподібного заперечення» (plausible deniability) причетності до конфлікту;

– вона переносить значну частину людських і матеріальних втрат на проксі-сили, зберігаючи власний військовий потенціал.

Характеризуючи військову складову гібридної війни, варто розглянути поняття «гібридні війська» – формування, які поєднують елементи регулярної армії та нерегулярних збройних груп. Класичним прикладом є «зелені чоловічки» під час анексії Криму у 2014 р. – військовослужбовці без розпізнавальних знаків, які демонстрували високий рівень професійної підготовки, властивий регулярним підрозділам спеціального призначення, водночас використовуючи тактику та зовнішній вигляд, характерні для локальних ополченських формувань, наслідком чого є дезорієнтація противника та міжнародної спільноти, ускладнення ідентифікації агресора, як наслідок, формування відповідної адекватної реакції на акт агресії.

Сучасні технологічні досягнення кардинально змінюють обличчя військової складової гібридних конфліктів. Розвиток безпілотних літальних апаратів (БпЛА), систем ШІ, роботизованих комплексів і кібернетичних засобів

ураження створює нові можливості для ведення бойових дій з мінімальним залученням живої сили та з максимальним рівнем асиметрії. БпЛА, зокрема, стали символом сучасної гібридної війни - вони використовуються не лише для розвідки та ураження військових цілей, але й для атак на цивільну інфраструктуру, залякування населення та створення психологічного тиску. При цьому важливо підкреслити, що військовий компонент гібридної війни не обов'язково передбачає масштабне застосування збройних сил. У багатьох випадках достатньо демонстрації військової могутності, проведення навчань поблизу кордонів потенційного противника або обстрілів його території для формування фону військової загрози, який дестабілізує економіку, провокує міграційні процеси та підриває довіру до спроможності влади захистити своїх громадян.

Інформаційний компонент гібридної війни є одним із найбільш досліджуваних і водночас найбільш динамічних її вимірів. Інтерпретація цього терміну різними авторами є доволі широкою, оскільки в ній поєднуються форми та методи ведення бойових дій, використання сил і засобів військового й цивільного характеру, а також активне залучення у воєнний конфлікт соціальних груп [35, с. 337]. На відміну від класичної війни, метою якої є, як правило, захоплення території іншої держави і встановлення над нею власного суверенітету, у гібридній війні кінцевою метою є утримання держави супротивника в зоні свого геополітичного, геоекономічного та ідеологічного впливу [35, с. 338-339]. Інформаційний компонент є тим інструментом, за допомогою якого ця мета досягається. Він формує сприйняття реальності, легітимізує дії агресора, деморалізує населення противника та мобілізує власне суспільство.

Ключовим інструментом інформаційного компоненту є дезінформація, яка може бути спрямована на різні цільові аудиторії: внутрішню аудиторію країни-агресора - для консолідації суспільства навколо війни та легітимізації дій влади;

внутрішню аудиторію країни-жертви - для підриву довіри до власного уряду та збройних сил, формування панічних настроїв, розпалювання міжнаціональної та міжконфесійної ворожнечі; міжнародну аудиторію - для дискредитації країни-жертви в очах світової спільноти, формування наративу про неможливість або недоцільність її підтримки, просування власних геополітичних інтересів.

Варто наголосити на тому, що сучасна дезінформація у переважній більшості випадків не зводиться до примітивної неправди. Набагато частіше вона використовує техніки маніпуляції напівправдою, викривлення контексту, зміщення акцентів, емоційного супроводу нейтральних повідомлень. Це робить її менш помітною, але більш ефективною, оскільки аудиторія схильна довіряти інформації, яка частково збігається з її власними знаннями або уявленнями про світ.

Пропаганда в гібридній війні використовує всі доступні канали комунікації: від традиційних медіа (телебачення, радіо, друковані видання) до сучасних цифрових платформ (соціальні мережі, месенджери, блоги, відеохостинги). Технології ШІ, зокрема генеративні моделі, дозволяють створювати та поширювати контент у промислових масштабах, адаптуючи його до конкретних аудиторій, мовних груп і соціальних груп.

У сучасному інформаційному компоненті гібридної війни дедалі більшої ваги набирають технології пропаганди високої інтенсивності. Мова йде про контент «швидкого споживання», який поширюється у вигляді коротких відео, мемів, картинок з текстом тощо. Він, як правило, має потужне емоційне забарвлення (гнів, страх, захоплення, обурення), але мінімальне інформаційне навантаження. Його мета - не аргументовано переконати аудиторію, а детермінувати потрібну емоційну реакцію, яка автоматично відтворюватиме певну поведінку. Месенджери з шифруванням стали окремою проблемою для систем протидії дезінформації, оскільки модерація контенту в них є технічно неможливою або вкрай обмеженою, що дозволяє агресору поширювати найбільш

агресивні та маніпулятивні повідомлення без загрози їх блокування. Анонімність адміністраторів каналів у таких платформах дозволяє вести цілеспрямовані інформаційні кампанії, не боючись юридичної відповідальності, а використання технологій ШІ для генерації контенту та управління бот-мережами забезпечує безпрецедентні масштаби та швидкість поширення дезінформації.

Економічний компонент гібридної війни, на відміну від класичних економічних санкцій або торговельних воєн, є невід'ємною частиною комплексної стратегії з ослаблення держави-жертви зсередини. Він може використовуватися як до початку активної фази військових дій, формуючи відповідний базис для агресії, так і під час війни - для дестабілізації ситуації та підриву спроможності держави до опору.

У контексті аналізу ролі економічного компоненту в умовах українсько-російського протистояння слід зазначити, що енергетична залежність багатьох європейських країн стала вразливим чинником тиску. Як зазначають міжнародні аналітики, росія систематично використовує енергоносії як зброю, маніпулюючи енергомережами й ресурсами для впливу на глобальну політику, поєднуючи військові підходи з економічним тиском, кібератаками та дезінформацією [50]. Цей енергетичний шантаж є класичним прикладом гібридного економічного впливу, оскільки він дозволяє агресору впливати на прийняття політичних рішень іншими державами, не застосовуючи прямої сили. На енергетичних ринках, у міжнародних інституціях та двосторонніх переговорах розгортається справжня гібридна війна, де важелі дипломатії переплітаються з економічним тиском і контролем над стратегічними ресурсами.

Іншим важливим напрямом економічного компонента є санкційний тиск. Країни-агресори намагаються запроваджувати односторонні або багатосторонні економічні обмеження проти своїх опонентів, а також долати санкції, введені проти них міжнародною спільнотою. Створення так званих «тіньових флотів», використання третіх країн для обходу торговельних обмежень, маніпуляції з

валютним курсом, використання криптовалют для фінансування протиправної діяльності, а також намагання зруйнувати глобальні ланцюги постачань - усе це є складовими економічного виміру гібридної війни.

Так, діяльність ряду приватних військових компаній не обмежується лише забезпеченням воєнних операцій, а має виражений економічний характер: вони беруть участь у перерозподілі власності, охороні логістичних шляхів та контролі над стратегічними галузями економіки на окупованих територіях [28], що є ознакою поєднання економічного компонента з військовим, коли військові формування стають не лише інструментом захоплення території, але й засобом економічної експлуатації, розграбування природних ресурсів та промислового потенціалу. Така економічна експлуатація окупованих територій переслідує подвійну мету: по-перше, вона забезпечує ресурсами саму війну; по-друге, вона системно підриває економічну базу країни-жертви, знищуючи її промисловий потенціал на довгі роки вперед.

Важливою складовою економічного компонента є також підрив довіри до фінансово-банківської системи держави-жертви. Це може досягатися через поширення чуток про банкрутство банків, девальвацію національної валюти, замороження депозитів, а також через створення паніки на фінансових ринках за допомогою кібератак на біржі, банки та платіжні системи. Одночасно з цим країна-агресор може проводити політику економічної ізоляції держави-жертви, заохочуючи своїх сателітів і треті країни розривати з нею торговельні відносини, блокувати транзит, вводити мита та обмеження. У російсько-українському контексті така політика включала, зокрема, спроби заблокувати український експорт через Чорне море, знищити аграрну інфраструктуру, перешкоджати міжнародним фінансовим транзакціям та інвестиціям в українську економіку.

Когнітивний вимір гібридної війни є найбільш складним, найменш дослідженим, але, можливо, найважливішим серед усіх її структурних компонентів. Когнітивна війна - це цілеспрямований вплив на мислення й

поведінку цивільних і військових за допомогою інформаційних, психологічних та технологічних інструментів [61]. У звіті Головного наукового радника НАТО за 2025 р. когнітивну війну визначено як системну боротьбу за контроль над процесами мислення, у якій інформація є лише одним з елементів, а не кінцевою метою. Ключове відмежування когнітивної війни від інформаційної полягає в тому, що у фокусі впливу перебувають когнітивні процеси - увага, пам’ять, емоції, логіка інтерпретації та механізми ухвалення рішень, а не сама інформація як така. Ряд досліджень підтверджують це: у стані інформаційного перевантаження людина втрачає до 30-40% здатності до критичного аналізу, що означає, що ключовим стає не зміст повідомлень, а їх кількість, ритм і емоційне забарвлення [61].

Для розуміння сутності когнітивної війни важливою є концепція Г. Яворської, яка виокремлює два асиметричні вектори існування війни: фізичний і дискурсивний. На думку дослідниці, у військовому (матеріальному) вимірі російсько-український конфлікт має локалізований характер, тоді як його дискурсивна складова набуває глобального масштабу [46, с. 41]. Це свідчить про те, що сучасне протистояння виходить далеко за межі поля бою та переноситься у сферу смислів, інтерпретацій і суспільного сприйняття.

Інтерпретаційна складова гібридної війни формує її когнітивний вимір. Вона реалізується через систему вербально-семіотичних засобів, за допомогою яких здійснюється вплив на свідомість аудиторії, конструюються потрібні наративи та моделі сприйняття реальності. Конфлікт інтерпретацій стає невід’ємним елементом гібридної війни та використовується як специфічний різновид зброї поряд з іншими невійськовими інструментами впливу [46, с. 43].

Небезпека такого впливу полягає в тому, що він спрямований не лише на зміну окремих поглядів чи переконань, а й на трансформацію самих механізмів мислення, через які людина сприймає інформацію, формує оцінки та ухвалює рішення. Саме тому когнітивна війна є не просто складовою інформаційного

протиборства, а його якісно вищим рівнем. Її головна мета - контроль над процесами осмислення реальності, формуванням суспільних реакцій, установок і поведінкових моделей.

Основним об'єктом впливу в когнітивній війні є не окремі особи, а когнітивні системи - спільні знання, вірування, цінності, наративи та способи мислення соціальних груп, мета яких не просто переконати, а «перезавантажити» світогляд цільової аудиторії таким чином, щоб вона почала сприймати агресора як миротворця, жертву - як агресора, брехню - як те, що відповідає дійсності.

НАТО прив'язує когнітивну війну до циклу OODA (Observe-Orient-Decide-Act), демонструючи, що ключовим об'єктом ураження є швидкість і якість ухвалення рішень [61]. Противник не обов'язково намагається змінити фінальне рішення, йому достатньо зламати перші два етапи циклу (спостереження та орієнтацію), щоб вони стали запізнілими та суперечливими.

Російська федерація активно застосовує саме такий підхід. Як зазначає М. Балабан, перед повномасштабним вторгненням росія заповнювала інформаційний простір різними, часто несумісними поясненнями подій, не намагаючись довести одну «правду», а запускаючи одразу кілька версій: що нападу не буде, що це провокація України, що йдеться про внутрішній конфлікт або що Захід усе перебільшує [2]. Мета такої інформаційної агресії було створення інформаційної невизначеності, у якій будь-яке рішення стає складним та вразливим до маніпуляцій.

В мовах сучасного українського російського протистояння противник веде когнітивну війну одночасно проти армії й цивільного населення: військових намагаються деморалізувати фейками про масові капітуляції та «катастрофічні втрати», цивільних - панікою, зневірою і переконанням у неминучості поразки [2].

Отже, визначальною характеристикою когнітивної війни є її багатовимірність та інтегративність: фізичний і дискурсивний вектори діють

одночасно, причому кожен із них може використовуватися як самостійно, так і в різних комбінаціях, що потребує комплексного підходу до розробки дієвих заходів протидії [46, с. 45].

Аналіз структурних компонентів гібридної війни дає підстави для кількох важливих висновків:

– жоден із її компонентів не функціонує ізольовано, оскільки всі вони є взаємопов'язаними та взаємозумовленими. Військовий тиск супроводжується інформаційними кампаніями, економічний вплив підсилюється когнітивними операціями, а інформаційні атаки, своєю чергою, створюють умови для досягнення військових і політичних цілей;

– сучасні гібридні війни характеризуються високим рівнем гнучкості та адаптивності. Агресор здатний оперативно змінювати інструменти впливу, переорієнтовуючи ресурси між військовим, інформаційним, економічним і когнітивним компонентами залежно від конкретної ситуації та ефективності застосованих засобів;

– найбільш уразливими в умовах такого протистояння є держави, які не готові здійснювати комплексну протидію гібридним загрозам. Обмеження виключно військовими засобами без належної уваги до інформаційного, економічного чи когнітивного вимірів суттєво послаблює їх здатність ефективно реагувати на сучасні форми агресії.

Український досвід протидії російській агресії засвідчує, що ефективна відповідь на гібридну війну можлива лише за умови формування інтегрованої системи національної безпеки, яка охоплює всі ключові компоненти гібридного протистояння та забезпечує їх координацію на стратегічному рівні.

Таким чином, структурний аналіз гібридної війни демонструє, що вона є не сукупністю окремих дій, а цілісною системою комплексного впливу, у межах якої військові, інформаційні, економічні та когнітивні компоненти взаємодіють і

підсилюють один одного. Їх поєднання створює синергетичний ефект, значно потужніший за результати застосування кожного інструменту окремо. За таких умов ефективна стратегія протидії не може обмежуватися лише військовими заходами, а повинна охоплювати всі сфери суспільного життя - від оборони та економіки до інформаційної політики, освіти й розвитку суспільної стійкості.

Висновки до розділу 1

Гібридна війна є специфічною формою сучасних конфліктів, у межах якої поєднуються військові та невійськові засоби впливу для досягнення політичних і стратегічних цілей. У сучасному науковому дискурсі відсутнє єдине універсальне визначення цього феномену, однак більшість підходів акцентують увагу на комплексному застосуванні військових, інформаційних, економічних, кібернетичних і когнітивних інструментів.

Хоча окремі елементи гібридних методів ведення боротьби простежувалися і в попередні історичні періоди, розвиток інформаційних технологій, цифрових комунікацій і кіберпростору суттєво трансформував характер сучасних конфліктів. Це виявляється, по-перше, у розширенні спектра інструментів впливу, по-друге, у стиранні меж між війною та миром, а по-третє, в активному використанні інформаційно-психологічних операцій, кібератак, проксі-структур і невійськових механізмів тиску.

Ефективна протидія гібридним загрозам потребує комплексного підходу, який охоплює не лише оборонну сферу, а й інформаційну безпеку, економічну стійкість, розвиток медіаграмотності та формування когнітивної резильєнтності суспільства.

РОЗДІЛ 2
МЕХАНІЗМИ РЕАЛІЗАЦІЇ ТА ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ У ГЛОБАЛЬНОМУ ВИМІРІ

2.1. Особливості та технології ведення гібридних війн (на прикладі російсько-українського конфлікту)

Гібридна війна, яку російська федерація розгорнула проти України з 2014 р., стала викликом не лише для національної безпеки України, але й для всієї системи євроатлантичної безпеки. Як уже зазначалося нами у першому розділі дослідження, на відміну від класичних збройних конфліктів, гібридна війна передбачає синхронне або асинхронне застосування військових, дипломатичних, інформаційних, економічних, кібернетичних та психологічних інструментів, спрямованих на дестабілізацію держави-жертви зсередини. Вона є заздалегідь підготовленою сукупністю дій, де невійськові засоби переважають за значущістю над класичними збройними методами, а головним об'єктом впливу стає свідомість людей та стійкість державних інститутів [41, с. 174]. За більш ніж десять років протистояння Україна зіткнулася з усіма можливими складовими гібридної агресії: політичним тиском, енергетичним шантажем, інформаційно-психологічними операціями, кібератаками, використанням недержавних збройних формувань та проксі-сил, а з лютого 2022 р. – відкритим військовим вторгненням. Серед цих інструментів пріоритетне місце посідає інформаційно-психологічна складова, яка, як слушно зауважує Н. Кравченко, розгорталася задовго до військової фази, починаючи з 2000-х рр. росія системно формувала антиукраїнський дискурс, спрямований на девальвацію української державності, дискредитацію національної мови та культури, а також ревізію історичної пам'яті [23, с. 107]. Механізмами цього впливу стали: стратегія «керованої нестабільності», підтримка проросійських політичних сил, створення інформаційних бульбашок через контрольовані медіа та соціальні мережі. При

цьому ряд дослідників вказують на парадоксальний характер гібридної війни: агресор використовує інститути демократії – свободу слова, вибори, громадські організації – як зброю проти демократичної держави [48, с. 106]. Особливого значення у цьому контексті набуває маніпулювання соціальними мережами (Twitter, Facebook, Telegram), де фейкові акаунти, боти та тролі імітують автентичну громадську думку, провокують соціальні розколи та впливають на політичні рішення. Реалізація цих технологій підпорядковувалася стратегічній меті – формуванню в Україні стану «керованого хаосу», покликаному унеможливити ефективне державне управління ще до початку збройної фази конфлікту [24, с. 65].

Поглибленням інформаційної складової стала когнітивна війна – якісно новий рівень впливу на мислення, цінності та поведінкові моделі суспільства. Вона є сукупністю дій, спрямованих на зміну системи сприйняття реальності цільовою аудиторією, шляхом маніпулювання інформаційними потоками, створення стійких когнітивних упереджень та руйнування критичного мислення [42, с. 303]. На відміну від традиційної пропаганди, яка впливає на думки, когнітивна війна атакує самі механізми пізнання: увагу, пам’ять, здатність до аналізу. У російській стратегії когнітивний вимір є фундаментом, на якому будуються всі інші види агресії – збройна, економічна, політична, оскільки дезорієнтоване, розколоте суспільство не здатне чинити системний опір [39, с. 52]. Особливу небезпеку становить прихований характер когнітивного впливу: він реалізується через масову культуру, освітні продукти, розважальний контент і навіть наукові дискурси, що робить його важко ідентифікованим і майже неврегульованим чинним законодавством.

У контексті російсько-українського протистояння когнітивна війна найбільш яскраво проявилася у таких технологіях, як нав’язування наративу про «громадянську війну», штучне посилення регіональних відмінностей,

використання історичних міфів (наприклад, про «єдиний народ») та систематичні інформаційні провокації.

У цьому ж контексті кібероперації стали інтегральною технологічною складовою гібридної війни. Ю. Калайда аналізує їх як ключовий елемент українсько-російської кібервійни, яка триває безперервно з 2014 р. та значно посилилася після повномасштабного вторгнення у лютому 2022 р. [15, с. 84]. Характерною особливістю цих технологій є інтеграція кібероперацій з кінетичними діями. До прикладу, атака на енергосистему України в грудні 2015 р. (перший в історії випадок відключення електроенергії в результаті кібератаки) супроводжувалася інформаційною кампанією та телефонними дзвінками з погрозами диспетчерам. М. Досон зі співавторами на основі відомостей Глобальної бази даних тероризму (GTD) демонструють, що російські кібероперації функціонують не як самостійний вид терористичної діяльності, а як стратегічний інструмент у координації з конвенційними військовими діями [52, с. 30]. Показовим у цьому контексті є також вірус NotPetya (2017 р.), який завдав збитків на мільярди доларів по всьому світу, але був замаскований під шкідливе ПЗ типу «вимагач»; wiper-атаки напередодні повномасштабного вторгнення 2022 р.; а також постійні спроби зламу енергетичних, транспортних та телекомунікаційних мереж. Водночас, не зважаючи на очевидний деструктивний потенціал цих дій, у науковій літературі фіксуємо позиції, що попри значну кількість кіберінцидентів, немає достатніх доказів того, що кібероперації Росії суттєво вплинули на перебіг бойових дій, забезпечили тактичні переваги на полі бою або мали стратегічну цінність [53, с. 105]. Частково можемо погодитися із цією позицією, адже кібероперації схильні продукувати нелінійні, слабко передбачувані ефекти, тому вони є швидше доповненням до конвенційного впливу, інструментом розвідки та засобом створення «інформаційного шуму», аніж самостійним визначальним фактором.

Енергетичний та економічний тиск є ще однією класичною технологією гібридної війни, яку росія застосовувала проти України. Р. Фордонський аналізує поняття «гібридної зброї» на прикладі використання росією експорту енергоносіїв як інструменту політичного тиску не лише на Україну, але й на європейських членів Контактної групи [54]. Ще в 2014-2015 рр. вона неодноразово припиняла постачання газу до України, вимагаючи перегляду цін та політичних поступок; паралельно будувався газопровід «Північний потік-2», що мав позбавити нашу державу транзитної ролі та посилити енергетичну залежність Європи. Після початку повномасштабного вторгнення атаки на критичну енергетичну інфраструктуру (електростанції, підстанції, газосховища) стали систематичними й цілеспрямованими, набувши характеру воєнного злочину. Крім того, росія блокувала українські порти, перешкоджаючи експорту зерна, що спричинило продовольчу кризу в багатьох країнах світу. Такі дії є класичним прикладом «енергетичної зброї» в гібридному конфлікті, де економічні важелі використовуються для досягнення військових та політичних цілей.

Однак не менш значущим фактором, що визначає сучасний перебіг війни, стало активне впровадження новітніх технологій, зокрема систем штучного інтелекту ШІ. Більшість дослідників називають цей конфлікт «технологічною війною», оскільки застосування ШІ, передових безпілотних систем, супутникової розвідки та алгоритмів машинного навчання вже змінює характер бойових дій та геополітичний ландшафт. ШІ використовується для аналізу супутникових знімків, визначення цілей, логістичного планування, а також для ведення інформаційно-психологічних операцій. Генерація дипфейків (наприклад, фальшивих відеозвернень президента В. Зеленського чи глав держав), автоматизоване створення тисяч коментарів у соціальних мережах, персоналізована дезінформація на основі аналізу поведінки користувачів – усе це стало реальністю. Алгоритмічна війна, тобто використання рекомендаційних алгоритмів платформ (YouTube, TikTok, Telegram) для створення інформаційних

бульбашок, дозволяє утримувати різні аудиторії в ізольованих когнітивних просторах, де кожна група отримує власну версію подій. Це робить традиційні методи спростування дезінформації майже неефективними, оскільки люди фізично не стикаються з альтернативними точками зору. На противагу цьому пасивному стану сприйняття, Україна активно використовує ШІ для реалізації оборонних завдань: системи розпізнавання цілей, аналізу даних з безпілотників, автоматизованого управління вогнем. Таким чином виникає ситуація «технологічного протистояння», де перевага належить тій стороні, яка швидше впроваджує інновації та ефективніше захищає свої алгоритми від злому та маніпуляцій.

Важливим інструментом російської гібридної стратегії на початковому етапі конфлікту стали проксі-операції та приватні військові компанії. У науковому дискурсі проксі-операції визначаються як форма опосередкованої участі держави-агресора у збройному конлфікті шляхом залучення недержавних акторів (збройних формувань, найманців, приватних військових компаній) для досягнення військових чи політичних цілей на території іншої держави із запереченням власної прямої участі [19, с. 47]. Саме така модель була реалізована росією у 2014-2015 рр.: так звані «зелені чоловічки» в Криму та проросійські бойовики на Донбасі, які позиціонувалися як місцеві ополченці, однак фактично були кадровими військовими рф без розпізнавальних знаків. Згодом активізувалася діяльність ПВК «Вагнер», яка брала участь у бойових діях у Сирії, Лівії, країнах Африки, а також на початковому етапі російсько-української війни. Використання найманців дозволяло кремлю проводити військові операції без формального оголошення війни, мінімізуючи ризик втрат серед регулярної армії та зберігаючи фасад заперечності.

Основними критеріями ефективності проксі-операцій виступають рівень дестабілізації регіону, ступінь контролю над окупованою територією, масштаб жертв серед цивільного населення та здатність агресора уникати міжнародної

юридичної відповідальності [19, с. 51]. Після переходу росії до відкритого військового вторгнення у 2022 р. проксі-стратегії не зникли повністю, а трансформувалися: на окупованих територіях діють підконтрольні збройні формування, а в складі російських військ з'явилися підрозділи, укомплектовані ув'язненими («шторм-зет»), а також найманцями з Непалу, Сомалі, Сербії та інших країн.

Характерною особливістю російсько-української гібридної війни є також використання міграційних та гуманітарних важелів як інструменту збройної агресії. Уже в 2014-2015 рр. росія застосовувала практики так званих «гуманітарних конвоїв», які фактично використовувалися для постачання підтримки проросійським збройним формуванням; паралельно блокувався доступ міжнародних гуманітарних організацій до окупованих територій, а місцеве населення примусово залучалося до процедури отримання російських паспортів. Після повномасштабного вторгнення 2022 р. росія розпочала систематичне руйнування цивільної інфраструктури, що спричинило вимушене переміщення мільйонів осіб. Згодом це стало ще одним із інструментів гібридного впливу, зокрема дестабілізації приймаючих країн – через поширення прокремлівської пропаганди серед українських біженців у Європі, створення підконтрольних росії громадських організацій за кордоном та інші форми гібридного впливу

Цей багатовимірний характер гібридної агресії безпосередньо підводить до її найважливішої особливості – взаємодії складових. Жоден із елементів окремо не завдає вирішального впливу, але їх комбінація, підсилена часовою та просторовою координацією, створює ефект «гібридного удару», який перевищує суму окремих складових [18, с. 88]. Наприклад, перед атакою на енергооб'єкти запускається хвиля дезінформації про «зраду» чиновників, паралельно проводяться кібератаки на системи оповіщення, а після удару – кампанія з дискредитації рятувальних служб. Така синхронізація робить оборону вкрай

складною, оскільки вимагає одночасної роботи різних відомств, які часто не мають спільних протоколів реагування. Крім того, гібридна війна характеризується розмитими часовими рамками, і ймовірно, триватиме ще досить довго після припинення активних бойових дій у вигляді інформаційних, кібер- та дипломатичних операцій.

Отже, російсько-український конфлікт демонструє еволюцію гібридної війни від окремих «сірих» операцій (2014-2021 рр.) до комплексної багатовимірної агресії (2022-2026 рр.), в якій усі компоненти – інформаційний, когнітивний, кібернетичний, енергетичний, технологічний та проксі здійснюють відчутний вплив. Сучасні технології, зокрема ШІ, дипфейки, алгоритмічні маніпуляції, перетворюють гібридну війну на інструмент тотального контролю над суспільною свідомістю, що вимагає вироблення принципово нових підходів, що забезпечать формування належного рівня стійкості суспільства.

2.2. Міжнародний досвід протидії гібридним загрозам: інституційні та правові механізми

Активізація гібридних загроз у глобальному безпековому середовищі, найбільш показовим прикладом яких стала російсько-українська війна, зумовила необхідність вироблення системної та скоординованої відповіді з боку міжнародних інституцій. Дж. Ахмадлі зазначає, що з початку української кризи на всіх самітах НАТО однією з головних тем стала розробка спільної стратегії протидії гібридним загрозам; у цьому контексті були зроблені серйозні кроки щодо формування правової бази та визначення практичних кроків [1, с. 67].

Незважаючи на значний обсяг теоретичних напрацювань у дослідженні феномену гібридної війни, практичні механізми протидії їй на міждержавному й наднаціональному рівнях тривалий час залишалися фрагментованими. Як засвідчують результати досліджень [12, с. 20], в основі моделювання сценаріїв

протидії гібридній війні лежить розуміння того, що класичні військові підходи в такому конфлікті забезпечують лише частковий, а не комплексний захист. Саме це зумовило еволюцію інституційних підходів НАТО та ЄС, які дедалі більше акцентують увагу на інструментах раннього попередження, соціальної стійкості, когнітивної безпеки та поступового реагування. Починаючи з ІІ пол. XXI ст. проблеми неконвенційних загроз та гібридної конфліктності увійшли до категорії пріоритетних у воєнно-політичних та оборонно-безпекових документах цих інституцій [6, с. 57].

Спільною організаційною платформою співробітництва НАТО і ЄС стала Міжвідомча комісія з боротьби з гібридними загрозами. Складовою євроатлантичної системи підготовки до попередження й відвернення цих загроз визначено комплексні навчання у рамках співробітництва НАТО і ЄС, які відбуваються із використанням аналітичної продукції відповідних дослідницьких центрів із вивчення проблематики гібридної конфліктності [6, с. 57].

Одним із ключових напрямів діяльності міжнародних інституцій у сфері протидії гібридним загрозам є вдосконалення систем раннього виявлення, аналізу та обміну розвідувальною інформацією. Як засвідчує досвід ЄС, без належного рівня ситуаційної обізнаності неможливо адекватно оцінити природу та масштаб гібридної атаки, що часто має прихований характер [29, с. 113]. У відповідь на цей виклик у 2016 р. в рамках Європейської служби зовнішніх дій (EEAS) було створено Гібридний координаційний осередок (EU Hybrid Fusion Cell).

До дієвих механізмів протидії гібридним загрозам в ЄС належать інституційні ініціативи, санкційна політика, а також конкретні заходи щодо інформаційної, енергетичної та кібербезпеки, зокрема діяльність Європейського центру передового досвіду з протидії гібридним загрозам, зменшення ресурсної залежності країн внаслідок диверсифікації постачання, заснування Європейського агентства з кібербезпеки та кампанії протидії дезінформації [17, с. 178].

Протидія гібридним загрозам вимагає застосування різних підходів до їх запобігання та зміцнення стійкості. Це, своєю чергою, зумовило розробку Моделі комплексної екосистеми стійкості ЄС (2023 р.), структура якої охоплює такі складові (сфери діяльності), простори (громадський, управління та послуг) та рівні (локальний, національний, міжнародний) [17, с. 180].

Ефективність міжнародної протидії гібридним загрозам значною мірою залежить не лише від інституційної будови, а й від здатності оперативно реагувати на кризові ситуації на місцях, що вимагає відповідних правових механізмів і процедур. Одним із найбільш перспективних інструментів у цьому контексті стало створення Гібридних груп швидкого реагування для координації зусиль, зміцнення взаємодії між державними органами та приватним і публічним секторами, впровадження заходів для забезпечення кібербезпеки та захисту критичної інфраструктури, міжнародної співпраці [44, с. 359].

Важливим напрямом міжнародної діяльності, який поки що перебуває в стадії активного становлення, є протидія дезінформації та зміцнення інформаційної стійкості [21, с. 14]. Так, у рамках ЄС з 2015 р. діє проєкт EUvsDisinfo – флагманська ініціатива Європейської служби зовнішніх дій, спрямована на виявлення, аналіз та підвищення обізнаності про дезінформацію, з особливим акцентом на наративи та тактики кремля. Ця інституція стала основою для формування розгалуженої системи протидії маніпулюванню інформацією, у межах якої стратегічні комунікації визначаються як базисний елемент боротьби з дезінформацією, причому пріоритетним завданням визнається не лише викриття фейкових новинних каналів, але й притягнення їх авторів до відповідальності [35, с. 340].

Наочною ілюстрацією ефективності міжнародних механізмів протидії гібридним загрозам є досвід країн Балтії, які внаслідок свого географічного положення та історичного контексту опинилися на передовій гібридної агресії. Литва, Латвія та Естонія сформували спільні механізми координації протидії

гібридним загрозам, інвестуючи у розвиток спроможностей місцевого рівня через навчання, підвищення обізнаності населення та залучення громадянського суспільства до заходів стійкості.

Окрім того, країни Балтії демонструють ефективність підходу, заснованого на зменшенні критичних залежностей: 8 лютого 2025 р. вони досягли повної незалежності від російської електроенергії та газу, завершивши синхронізацію з європейською енергомережею.

Окремої уваги заслуговує діяльність Європейського центру передового досвіду з протидії гібридним загрозам (Hybrid CoE), створеного у 2017 р. в Гельсінкі. Основною його місією є вдосконалення спроможностей країн-учасниць у сфері протидії гібридним загрозам шляхом проведення прикладних досліджень, навчань та обміну найкращими практиками.

Водночас, попри значні досягнення у формуванні інституційних механізмів, залишається низка суттєвих проблем. Зокрема, існує диспропорція між швидкою еволюцією природи гібридних загроз та консервативною вертикально-ієрархічною моделлю управління [33, с. 71]. Агресор зазвичай діє не прямолінійно, а через розгалужену мережу осередків, використовуючи прогалини між повноваженнями різних відомств, а також між державними структурами та приватними операторами критичної інфраструктури [33, с. 73]. Чинна нормативна база не дає змоги ефективно координувати дії різних відомств і обмінюватися даними в реальному часі. Через це розвідувальна інформація постійно запізнюється і не перетворюється на своєчасні превентивні заходи [33, с. 75]. Одним із варіантів виходу із цієї ситуації є створення Об’єднаного аналітичного центру гібридних загроз (ОАЦГЗ), структури, яка здатна забезпечити ефективну координацію та швидке реагування [33, с. 80].

Проте ефективність навіть найкращих інституційних рішень залежить від того, наскільки вони враховують реальний стан справ у країні. Саме тому проблема адаптації міжнародного досвіду до українських реалій є особливо

актуальною. Корисним буде також комплексний підхід у державному реагуванні, що включає посилення міжвідомчої координації, розвиток публічно-приватного партнерства та підвищення рівня цифрової, медійної грамотності населення.

Підкреслимо, що аналіз інституційних та правових механізмів запобігання гібридній агресії дає змогу виокремити як досягнення, так і проблеми, що потребують подальшого вирішення. Найбільш вагомим досягненням є формування комплексної та багаторівневої системи реагування – від створення аналітичних структур і механізмів швидкого сповіщення до формування оперативних груп реагування та цільових санкцій. Важливо, що ці інструменти не дублюють, а взаємодоповнюють один одного, утворюючи своєрідну екосистему протидії.

Водночас ключовим викликом залишається неузгодженість підходів між різними міжнародними акторами, особливо між НАТО та ЄС, а також між самими державами-членами. Залишаються також недостатньо вирішеними питання щодо ефективного обміну розвідувальною інформацією в реальному часі та забезпечення узгодженості у системі стратегічних комунікацій.

Отже, міжнародний досвід протидії гібридним загрозам демонструє поступовий рух у напрямі створення цілісної системи інституційно-правового реагування, яка базується на трьох ключових принципах: удосконалення аналітичних спроможностей, розвиток інструментів оперативного реагування та зміцнення суспільної стійкості з акцентом на когнітивну безпеку.

2.3. Інформаційна стійкість та когнітивна безпека суспільства в системі протидії гібридній агресії

Сучасна гібридна війна, яку росія розгорнула проти України, має яскраво виражений інформаційно-когнітивний вимір. На відміну від класичних збройних конфліктів, де головним об’єктом нападу є військова інфраструктура та особовий

склад, у гібридній війні пріоритетною ціллю стає свідомість населення, система цінностей, історична пам’ять та національна ідентичність. Саме тому категорії інформаційної стійкості (information resilience) та когнітивної безпеки (cognitive security) набувають стратегічного значення в системі національної безпеки. Як слушно зауважує Т. Кобець, когнітивна безпека – це здатність суспільства зберігати цілісність світосприйняття, критичне мислення та довіру до власних інституцій в умовах систематичного інформаційно-психологічного тиску [20, с. 4]. Водночас інформаційна стійкість є комплексною властивістю соціальної системи, що включає здатність розпізнавати дезінформацію та маніпуляції, спроможність протистояти панічним настроям і зберігати соціальну згуртованість, а також уміння швидко відновлювати комунікаційні мережі та довіру до джерел інформації після кризових подій.

У західній академічній традиції це поняття часто ототожнюється з «соціальною стійкістю», яка, за визначенням Європейської Комісії, є спроможністю суспільства протистояти дестабілізаційним зусиллям ззовні та зсередини, зберігаючи демократичні інститути та громадянські свободи [65, с. 171]. В контексті когнітивної безпеки соціальна резильєнтність не є пасивним захистом, а активною стратегією, яка передбачає постійне навчання та адаптацію до викликів й загроз [65, с. 173].

Нами зафіксовано у попередньому розділі дослідження, що особливістю російсько-української війни стало те, що агресор застосував усі відомі технології когнітивного впливу – від класичної пропаганди та «фейкових новин» до використання ШІ для генерації дипфейків та автоматизованих бот-атак. Це сформувало запит на появу нових аналітичних інструментів, здатних працювати не лише з фактами, але й із упередженнями та установками, що формуються на рівні масової свідомості. П. Лисянський пропонує новий інструмент аналізу цих процесів – смислову розвідку, тобто системну діяльність з виявлення, аналізу, інтерпретації та прогнозування смислових структур і ціннісних кодів, що

формують суспільну свідомість [25, с. 5]. На відміну від традиційної розвідки, яка оперує фактами (що? де? коли?), смислова розвідка працює з глибинними шарами - архетипами, національними наративами, емоційними реакціями. Дослідник обґрунтовує трирівневу модель такої розвідки:

- аналітичний рівень (виявлення смислових сигналів – нових наративів, метафор, символів, які впроваджуються в інформаційний простір);
- прогностичний рівень (моделювання сценаріїв поширення цих смислів та їх впливу на суспільну свідомість);
- проєктний рівень (створення позитивних контр-кодів і нових смислів, що зміцнюють національну ідентичність) [25, с. 8].

Практичне впровадження таких моделей у вітчизняну практику відбувалося поетапно:

- перший етап (2014-2021 рр.) – реактивна фаза, спричинена початком гібридної агресії. У цей період дії України були здебільшого ситуативними, спрямованими на блокування російських пропагандистських каналів та спростування найбільш грубих фейків [20, с. 11];
- другий етап (2022-2023 рр.) – фаза адаптації до повномасштабної війни, було створено Координаційний штаб з питань кібербезпеки при РНБО, запроваджено єдиний телемарафон та розгорнуто мережу центрів протидії дезінформації;
- третій етап (2024 р. – до сьогодні) – фаза інституційної розбудови та захисту, яка передбачає створення постійно діючих аналітичних структур, впровадження систем моніторингу на основі ШІ та уніфікацію законодавства з нормами ЄС у сфері протидії дезінформації [20, с. 12].

У відповідь на це російська федерація вибудувала власну концепцію когнітивної війни. Її застосування проти України базується на кількох фундаментальних принципах:

– принцип безперервності – інформаційний вплив не припиняється навіть у періоди відносного затишшя, створюючи ефект «білого шуму», до якого суспільство звикає і перестає критично оцінювати [58, с. 63];

– принцип асиметричності – агресор використовує слабкі місця демократичних суспільств, такі як свобода слова, відкритість кордонів для інформаційних потоків, незалежність судів та ЗМІ, перетворюючи їх на інструменти дестабілізації;

– принцип емоційного зараження – акцент робиться не на раціональні аргументи, а на сильні негативні емоції: страх, гнів, обурення, безнадію [49, с. 2].

У зв'язку з цим традиційні підходи до забезпечення національної безпеки, що акцентують увагу на військовій силі, економічному потенціалі та дипломатії, є недостатніми без розвитку критичного мислення як ключової компетентності громадян. Як засвідчують емпіричні дані, особи, які пройшли навчання з медіаграмотності, у 2,5 рази рідше поширюють недостовірну інформацію та втричі частіше звертаються до офіційних джерел у кризових ситуаціях [58, с. 71].

Технологіями когнітивної війни під час російсько-українського протистояння стали дипфейки, інформаційні бульбашки, війна ботів, дезінформація, експлуатація воєнних злочинів тощо. Так, дипфейки, згенеровані ШІ відео- та аудіоматеріали, найчастіше використовувалися для імітації висловлювань публічних осіб. Найбільш резонансним прикладом став фейк про «виїзд» Президента України на початку березня 2022 р., який було швидко спростовано завдяки оперативним діям Центру стратегічних комунікацій [25, с. 14]. Інформаційні бульбашки систематично формували для соціальних груп різні версії реальності через персоналізовані стрічки новин у соціальних мережах, Telegram, TikTok та YouTube підсилювали це контентами, що викликають емоційну реакцію та паніку [64, с. 3]. Війна ботів реалізувалася через автоматизовані акаунти, які генерували тисячі коментарів за хвилину, імітуючи так звану «народну думку»: за даними аналітичних центрів, у перші місяці

повномасштабного вторгнення до 40% україномовних коментарів у соціальних мережах щодо війни генерувалися ботофермами, розташованими на території росії [20, с. 18]. Дезінформація щодо допомоги ЄС поширювала наративи про те, що західна військова допомога не доходить до лінії фронту, розкрадається або спрямована проти самих українців; метою таких дій був підрив довіри до міжнародних партнерів і формування відчуття «зради» [65, с. 177]. Експлуатація воєнних злочинів виявилася у використанні реальних трагедій (Буча, Маріуполь, Краматорськ) для зворотного звинувачення України через наративи «самообстрілів» та «інсценування» – техніка, відома як «газлайтинг» (gaslighting), тобто спонукання жертви сумніватися у власному сприйнятті реальності [49, с. 4].

Як бачимо, у гібридній війні, де лінія фронту проходить через інформаційний простір, критичне мислення населення є тим ресурсом, який визначає ефективність усієї системи національної безпеки. Без сформованої когнітивної стійкості громадян навіть найдосконаліші механізми кіберзахисту, стратегічних комунікацій та інституційної координації залишаються недостатніми. Одним з найбільш ефективних довгострокових механізмів підвищення інформаційної стійкості є системне навчання критичного мислення. Дослідження, проведені в Україні в 2023-2025 рр., зафіксували, що навіть короткострокові тренінги (від 8 до 16 год.) підвищують здатність громадян розпізнавати маніпуляції в середньому на 35-40% [58, с. 73].

Найбільш ефективними виявилися програми, що поєднують теоретичні знання про технології пропаганди з практичними вправами на аналіз реальних кейсів. Важливу роль у цьому процесі відіграють громадські організації та волонтерські ініціативи. В Україні діють такі проєкти, як «Без брехні», «По той бік новин», «VoxCheck», «StopFake», які не лише викривають фейки, але й проводять навчання для вчителів, бібліотекарів, держслужбовців та військових.

За оцінками, станом на 2026 р. понад 2 млн українців пройшли різні форми навчання медіаграмотності [20, с. 22].

Паралельно з цим ініційовано процеси інституціоналізації медіаосвіти на державному рівні. У 2023 р. КМ України затвердив Концепцію впровадження медіаграмотності в освітній процес, яка передбачає інтеграцію відповідних тем у шкільні програми з історії, української мови, громадянської освіти та інформатики. Окремим напрямом є підготовка тренерів-викладачів з медіаграмотності для ВВНЗ, оскільки військовослужбовці є однією з головних цілей ворожих інформаційних атак [20, с. 23].

Невід'ємною частиною інформаційної стійкості є кіберстійкість (cyber resilience) – здатність держави, організацій та громадян протистояти кібератакам, мінімізувати їх наслідки та швидко відновлювати порушені функції. Р. Раду слушно зазначає, що когнітивна війна все частіше ведеться через кібератаки, які мають не лише технічний, але й психологічний ефект [64, с. 2]. Наприклад, злам державних сайтів та публікація фейкових повідомлень (як це сталося з сайтом Міністерства оборони України у січні 2022 р.) спрямовані не стільки на технічну шкоду, скільки на підрив довіри до офіційних джерел та створення паніки. Авторка пропонує трикомпонентну модель кіберстійкості в контексті когнітивної безпеки:

- технічний компонент (захист інфраструктури, резервування, шифрування, системи виявлення вторгнень);
- людський компонент (навчання персоналу розпізнавати фішингові атаки, соціальну інженерію та дотримуватися правил цифрової гігієни);
- комунікаційний компонент (швидке та прозоре інформування громадян про кіберінциденти з метою запобігання поширенню чуток та дезінформації) [64, с. 4].

Лише інтеграція всіх трьох компонентів дозволяє створити дієву систему кіберстійкості. Український досвід демонструє, що найбільш вразливими до

кібератак є енергетичний сектор, транспорт та державні реєстри. Атаки на ці об’єкти мають потужний когнітивний ефект, оскільки створюють відчуття безпорадності та незахищеності перед «невидимим ворогом». Саме тому одним з пріоритетів державної політики стало створення «кіберполігонів» – навчальних майданчиків, де фахівці відпрацьовують дії у відповідь на змодельовані кібератаки [64, с. 5].

Однак технічний захист інформаційного простору є лише однією стороною проблеми. На рівні безпосередньої комунікації з населенням постає інший виклик: традиційні комунікаційні кампанії, побудовані на раціональних аргументах та фактах, часто програють в інформаційному просторі емоційно зарядженій пропаганді. Інструментом, який дозволить мінімізувати ці впливи, є концепція емоційно обґрунтованих стратегічних комунікацій (Emotionally Based Strategic Communications – EBSC), яка використовує досягнення когнітивної нейронауки та ШІ для створення повідомлень, що резонують з емоційним станом цільової аудиторії [49, с. 3]. Зазначена методологія базується на трьох принципах:

- перший – емоційне калібрування: за допомогою аналізу великих даних (пости в соціальних мережах, коментарі, пошукові запити) визначається домінуючий емоційний стан аудиторії (страх, гнів, надія, втома);
- другий – конгруентність: комунікаційне повідомлення має відповідати цьому стану – не заперечувати емоцію, а визнавати її та пропонувати конструктивний вихід. Наприклад, замість фрази «не бійтеся» слід використовувати «ваш страх зрозумілий, ось що ви можете зробити, щоб почуватися безпечніше»;
- третій – емоційна контратака: ворожа дезінформація, що викликає негативні емоції, нейтралізується не спростуванням, а перемиканням емоційного фокусу на позитивні дії та спільні цінності [49, с. 5].

Прикладом успішного застосування описаного підходу є кампанія під час першої зими повномасштабної війни (2022-2023 рр.), коли російська федерація

систематично атакувала енергетичну інфраструктуру України. Ворожа дезінформація спекулювала на страху людей залишитися без світла та тепла. Українська комунікаційна кампанія «Пункти незламності» не просто інформувала про місця розташування пунктів, але й створювала емоційний наратив: «Ми - незламні. Ми зігріваємо одне одного». Це перетворило об'єктивну проблему на символ єдності та спротиву [49, с. 6].

Забезпечення інформаційної стійкості неможливе без створення відповідних інституційних механізмів. В Україні цю функцію виконують: Центр протидії дезінформації при РНБО України (створений у 2021 р.) - аналітичний орган, який виявляє, моніторить та спростовує фейки, веде базу дезінформації, готує аналітичні звіти для державних органів; Координаційний штаб з питань кібербезпеки (забезпечує оперативне реагування на кібератаки, координацію між СБУ, Держспецзв'язку, Міноборони та приватними компаніями); СтратКом ЗСУ (підрозділ, відповідальний за інформаційну підтримку військових операцій, швидке спростування ворожих наративів та комунікацію з цивільним населенням на деокупованих територіях).

На міжнародному рівні важливу роль відіграють структури ЄС та НАТО. У 2015 році створено Групу стратегічних комунікацій Східного партнерства (East StratCom Task Force), яка систематично викриває прокремлівську дезінформацію та публікує щотижневі дайджести (EUvsDisinfo). У 2017 р. засновано Європейський центр передового досвіду з протидії гібридним загрозам (Hybrid CoE) у Гельсінкі, який об'єднує експертів країн для розробки методик та проведення навчань [65, с. 179].

Важливим кроком у цьому напрямку стало прийняття ЄС Акту про цифрові послуги та Акту про цифрові ринки, які зобов'язують великі технологічні платформи (Facebook, Twitter, YouTube, TikTok) активно боротися з дезінформацією, маркувати контент, згенерований ШІ, та забезпечувати

прозорість алгоритмів. Україна розпочала процес гармонізації власного законодавства з цими актами в рамках євроінтеграційного процесу [20, с. 26].

Незважаючи на значний прогрес, сфера когнітивної безпеки України стикається з низкою викликів:

- кадровий дефіцит: брак фахівців, які одночасно володіють навичками аналізу даних, когнітивною психологією, медіаграмотністю та розумінням російської пропагандистської машини;
- технологічне відставання: росія інвестує значні кошти у розвиток ШІ для генерації дипфейків та автоматизації бот-атак, тоді як Україна більше використовує ручну аналітику та волонтерські ініціативи;
- законодавчі прогалини: баланс між необхідністю блокувати дезінформацію та свободою слова залишається складним питанням, особливо в контексті європейської інтеграції, де вимоги до захисту прав людини є надзвичайно високими [20, с. 28].

З метою оптимізації означених проблем, у перспективі реалізація наступних проєктів:

- створення Національної системи когнітивної безпеки як окремого напряму державної політики з відповідним фінансуванням та кадровим забезпеченням;
- впровадження обов'язкових курсів медіаграмотності в усіх закладах освіти, від шкіл до університетів та курсів підвищення кваліфікації держслужбовців;
- розвиток публічно-приватного партнерства з технологічними компаніями для отримання доступу до даних про бот-мережі та дезінформаційні кампанії;
- поглиблення співпраці з Hybrid CoE та НАТО StratCom CoE для обміну досвідом та участі у спільних навчаннях [20, с. 29-30].

Отже, інформаційна стійкість та когнітивна безпека суспільства є ключовими складовими системи протидії гібридній агресії, реалізація яких є можливою на основі трьох компонентів: розвитку критичного мислення та медіаграмотності населення, що формує «когнітивний імунітет» суспільства; інституційному забезпеченні, що передбачає створення спеціалізованих аналітичних центрів, систем моніторингу та механізмів швидкого реагування, а також міжнародної координації й адаптації найкращих практик ЄС та НАТО, зокрема у сферах кіберстійкості та комунікацій.

Висновки до розділу 2

Узагальнення механізмів реалізації гібридних загроз на прикладі російсько-українського конфлікту дає змогу стверджувати, що сучасна гібридна війна набула характеру тотального впливу на всі сфери життєдіяльності суспільства - від критичної інфраструктури до індивідуальної свідомості. Характерною особливістю цього феномену є не стільки окрема потужність кожного інструменту, скільки їх здатність взаємопідсилювати один одного.

Аналіз міжнародного досвіду демонструє, що НАТО та ЄС пройшли шлях від фрагментарного реагування на окремі гібридні інциденти до формування багаторівневої інституційної структури, яка охоплює стратегічні комунікації, раннє попередження, санкційну політику та захист критичної інфраструктури.

Встановлено, що інформаційна стійкість та когнітивна безпека виступають не додатковими, а базисними чинниками національної безпеки в умовах гібридної війни. Розвиток критичного мислення населення, системне навчання медіаграмотності та формування «когнітивного імунітету» є довгостроковими стратегічними інвестиціями, які дозволять мінімізувати ефективність ворожих інформаційно-психологічних операцій.

ВИСНОВКИ

У сучасній науковій літературі гібридну війну розглядають як системне утворення, де військові, інформаційні, економічні, кібернетичні, технологічні та когнітивні компоненти перебувають у тісному зв’язку та посилюють один одного. Результат такого поєднання є ефективним інструментом впливу, що відрізняє гібридну війну від класичних збройних конфліктів, де переважають симетричні дії регулярних армій із чітко визначеною лінією фронту. Традиційні механізми реагування в таких умовах виявляються малоефективними, оскільки основні події розгортаються в інформаційному, когнітивному та дипломатичному просторах, а не на полі бою.

Теоретичний базис дослідження гібридних війн сформували концепції «війн четвертого покоління» В. Лінда, теорія «необмеженої війни» Цяо Ляна та Ван Сянсуя, а також праці Ф. Гоффмана, який описав даний феномен як поєднання звичайних, іррегулярних, терористичних і кримінальних засобів.

У сучасному науковому дискурсі виокремлюють три основні підходи до розуміння гібридної війни: вузький (військово-тактичний), широкий (політологічний) та інтегративний (мережевий). Найбільш продуктивним є політологічний підхід, який трактує гібридну війну як комплексну стратегію, спрямовану на виснаження країни-жертви без широкомасштабних бойових дій. Важливими в межах нашого дослідження є дискурсивний підхід Г. Яворської, який розглядає гібридну війну як боротьбу наративів у глобальному інформаційному просторі, а також структурний аналіз, що виокремлює інформаційний, ідеологічний, психологічний, економічний, політичний, дипломатичний, військовий, технологічний та енергетичний компоненти гібридного впливу.

Аналіз еволюції природи збройних конфліктів продемонстрував, що гібридні методи ведення протистояння не є винаходом XXI ст., однак саме в

сучасну добу вони набули системного та домінуючого характеру. Концепція поколінь війн дає змогу простежити цю трансформацію: від лінійних тактик першого покоління до децентралізованих мережевих структур четвертого та інформаційно-когнітивних впливів п’ятого.

Ключовими ознаками сучасних гібридних конфліктів виступають розмитість межі між війною та миром, асиметричність засобів, мультивекторність впливу (одночасне застосування військових, політичних, економічних, інформаційних та когнітивних інструментів) та зміна ролі населення, яке з пасивного об’єкту захисту перетворюється на активну ціль інформаційно-психологічних операцій.

Російсько-український конфлікт, який став емпіричним базисом дослідження, демонструє трансформацію гібридної війни від окремих «сірих» операцій із використанням проксі-сил та інформаційного впливу на початковому етапі до тотальної багатовимірної агресії, що поєднує повномасштабне військове вторгнення із застосуванням технологій когнітивного впливу, кібератак, енергетичного терору та інформаційних маніпуляцій.

Вивчення міжнародного досвіду дозволяє констатувати, що інституційна структура НАТО та ЄС у сфері протидії гібридним загрозам досягла значного рівня розвитку, однак її практична ефективність обмежується кількома факторами. По-перше, вертикальна модель управління є недостатньо гнучкою для реагування на гібридні загрози. По-друге, міждержавна координація ускладнюється через відсутність спільних операційних протоколів, що призводить до ситуативних, а не системних рішень. По-третє, часовий розрив між отриманням розвідувальних даних та їх трансформацією в конкретні заходи залишається критичною перешкодою для переходу до активних моделей захисту.

Технологічний вимір гібридної війни також зазнав кардинальних змін у зв’язку із впровадженням систем ШІ. Останній використовується агресором не лише для автоматизації традиційних форм впливу (генерація дипфейків,

керування бот-мережами), а й для створення принципово нових можливостей – алгоритмічної війни, персоналізованої дезінформації на основі аналізу поведінки користувачів, автоматизованого визначення найбільш вразливих сегментів аудиторії.

У сфері когнітивної безпеки України існують три системні виклики: брак фахівців із міждисциплінарними знаннями на межі аналізу даних, когнітивної психології та медіаграмотності; технологічне відставання від агресора, який масово застосовує ШІ для генерації дипфейків та автоматизації бот-атак, а також законодавча невизначеність щодо меж блокування дезінформації. Подолання цих викликів вимагає зміни статусу когнітивної безпеки: вона має стати окремим пріоритетним напрямом державної політики з відповідним ресурсним забезпеченням.

Перспективні напрями подальших наукових досліджень вбачаємо у вивченні можливостей застосування ШІ для прогнозування поширення дезінформації та автоматизації процесів її виявлення; аналізі ефективності різних моделей інституційної координації в сфері когнітивної безпеки. Окремої уваги потребує дослідження впливів інформаційно-психологічних операцій на масову свідомість та дієвих інструментів захисту від фейкового інформаційного контенту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ахмадлі Дж. Огляд боротьби НАТО і ЄС проти гібридних загроз. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2022. Вип. 2(54). С. 66-72. DOI: https://doi.org/10.20535/2308-5053.2022.2(54).264384

2. Балабан М. Когнітивна війна: чому український досвід випереджає доктрини НАТО. *Українська правда*. 2026. 17 січня. URL: https://www.pravda.com.ua/columns/2026/01/17/8016485/ (дата звернення: 13.05.2026).

3. Бідзіля Ю. М. Державна політика інформаційної безпеки в умовах гібридних загроз. *Український політико-правовий дискурс*, (17). 2025. https://doi.org/10.5281/zenodo.17757320

4. Буряченко О. Гібридна війна як нова форма глобального протистояння. *Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління*. 2024. Вип. 2(74). С. 24-31. DOI: https://doi.org/10.32689/2523-4625-2024-2(74)-3.

5. Бутенко М. П., Ворович Б. О., Іващенко А. М., Федянович Д. Л. Міжнародно-правові аспекти протидії гібридній війні. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2020. № 1. С. 30-34.

6. Вєдєнєєв Д. В., Семенюк О. Г. Система державних установ з розробки теорії протидії гібридним загрозам у країнах ЄС і НАТО. *Юридичний науковий електронний журнал*. 2022. № 6. С. 56-60. DOI: https://doi.org/10.32782/2524-0374/2022-6/11

7. Воєнні аспекти протидії гібридний агресії: досвід України : монографія / за заг. ред. А. М. Сиротенка. Київ : НУОУ, 2020. 612 с.

8. Габчак В. «Гібридна війна»: поняття та сутність. *Вісник Прикарпатського університету. Політологі*я. 2018. Вип. 12. С. 257-262.

9. Горбулін В. П. (ред.). Світова гібридна війна: український фронт: монографія. Київ : НІСД, 2017. 494 с.

10. Дерев'янко І. П. Гібридна війна як різновид асиметричних дій. *Міжнародні відносини: теоретико-практичні аспекти*. 2023. Вип. 11. С. 6-16. DOI: https://doi.org/10.31866/2616-745X.11.2023.278396.

11. Додонов Р. О. (ред.). Гібридна війна: in verbo et in praxi : монографія. Вінниця: ТОВ «Нілан-ЛТД», 2017. 412 с. URL: https://jmonographs.donnu.edu.ua/article/view/3781 (дата звернення: 13.05.2026).

12. ІващенкоА. М., Семененко В. М., Полякова О. В. Особливості воєнних аспектів сценаріїв протидії гібридній війні. *Збірник наукових праць Центру воєнно-стратегічних досліджень університету оборони України Національного імені Черняховського*. Київ, 2019. № 1 (65). С. 19-24.

13. Іжутова І. В. Українські стратегічні комунікації та російсько-українська війна. *Наукові інновації та передові технології*. 2023. № 2(22). С. 46-51. DOI: https://doi.org/10.33099/2618-1614-2023-22-2-46-51

14. Кармазіна М. С., Аблазов І. В. Концепт «гібридна війна»: аналіз наукового дискурсу. *Наукові записки Національного університету «Острозька академія»*. Серія «Політологія». 2025. Вип. 1. С. 54-62.

15. Калайда Ю. П. Гібридні кібератаки в умовах українсько-російської кібервійни. *Інформація і право*. 2025. № 4(55). С. 82-94. DOI: https://doi.org/10.37750/2616-6798.2025.4(55).346481

16. Каприця Р. О. Комунікативні стратегії політичних еліт України в умовах гібридної війни: типологія та моделі реалізації. *Політичне життя*. 2026. (Травень). С.141-148. DOI: https://doi.org/10.31558/2519-2949.2026.2.15.

17. Карпенко О. Європейський досвід протидії гібридним загрозам для економічного відродження України. *International Economic Policy*. 2024. № 41. С. 176-186. DOI: https://doi.org/10.33111/iep.2024.41.12

18. Кириченко А. В., Іваненко С. М., Ремез В. В. Гібридна війна як новий вимір сучасних конфліктів. *Вісник Національного університету оборони України. 2025*. Т. 86, № 4. С. 85-95. DOI: https://doi.org/10.33099/2617-6858-2025-86-4-85-95.

19. Коваль В. В. Проксі-операції у контексті російсько-української війни: природа, принципи та показники ефективності. *Воєнно-технічний збірник*. 2024. Вип. 1. С. 46-58.

20. Кобець Т. Когнітивна безпека та суспільна стійкість: протидія інформаційному тиску в умовах гібридної війни. *Вісник Прикарпатського університету. Політологія.* 2026. Вип. 23. С. 3-31. DOI: https://doi.org/10.32782/2312-1815/2026-23-10

21. Кожушко В. В. Інформаційна війна в гібридних конфліктах: від пропаганди до кібервпливу. *Наукові праці Державного науково-дослідного інституту МВС України.* 2025. № 1. С. 12-30. DOI: https://doi.org/10.5281/zenodo.16658818.

22. Королюк Т. О., Чворун К. Г. Стратегічні комунікації у безпековій політиці: досвід України, країн ЄС та НАТО. *Стратегія економічного розвитку України*. Вип. 53(2023). С. 50-56. DOI: https://doi.org/10.33111/sedu.2023.53.050.063

23. Кравченко Н. Інформаційна складова як ключовий аспект гібридної війни. *Acta de Historia & Politica: Saeculum XXI* . 2022. 04 (жовтень). С. 106-118. DOI: https://doi.org/10.26693/ahpsxxi2022.04.106.

24. Лисецький Ю. М., Старовойтенко О. О., Семенюк Ю. В., Павленко Д. Г. Гібридні війни. Компоненти та особливості. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія:*

Публічне управління та адміністрування. 2021. Т. 32 (71), № 5. С. 63-68. DOI: https://doi.org/10.32838/TNU-2663-6468/2021.5/11.

25. Лисянський П. Л. Смислова розвідка (Cemint) як нова парадигма когнітивної безпеки України. *Політичні дослідження*. 2025. № 2. С. 4-22. DOI: https://doi.org/10.5281/zenodo.17498614

26. Литвиненко О. «Гібридна» війна Росії – виклик і загроза для Європи. *Дзеркало тижня*. 2016. 16 груд. URL: https://zn.ua/ukr/internal/gibridna-viyna-rosiyi-viklik-i-zagroza-dlya-yevropi-_.html (дата звернення: 13.05.2026).

27. Лойшин А. Аналіз поколінь війн згідно з концепціями технологічного та хвильового розвитку суспільства. *Social Development and Security*. 2022. Vol. 12, No. 2. P. 3-16. DOI: https://doi.org/10.33445/sds.2022.12.2.1.

28. Марцінко Н. Гібридна діяльність приватних військових компаній та її економічний вплив на Україну в умовах російсько-української війни. *Вісник Національної академії сухопутних військ*. 2026. Вип. 1. DOI: https://doi.org/10.5281/zenodo.18757653.

29. Павленко Ж. О., Антонов А. О. «Гібридна війна»: аналіз визначень поняття. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: філософія, філософія права, політологія, соціологія*. 2022. № 2(53). С. 106-119. DOI: https://doi.org/10.21564/2663-5704.53.258155.

30. Пирожков С. І. Національна стійкість України: стратегія забезпечення. *Український географічний журнал*. 2022. № 2(118). С. 3-11. DOI: https://doi.org/10.15407/ugz2022.02.003

31. Почепцов Г. Г. Гібридна війна: інформаційна складова. *Media Sapiens*. 2015. 25 жовт. URL: https://ms.detector.media/trends/1411978127/gibridna (дата звернення: 13.05.2026).

32. Присяжнюк С. В. Функціонал гуманітарної політики як чинника протидії інформаційній агресії. *Політичне життя*. 2024. № 3. С. 61-67. DOI: https://doi.org/10.31558/2519-2949.2024.3.7

33. Романенко Є. О., Сокоринський Ю. В., Жора, В. В. Аналіз диспропорції між динамікою гібридних (допорогових) загроз та чинною моделлю управління сектором безпеки і оборони України. *Military strategy and technology*, 2026. Вип.1(4). С.71-82. DOI: https://doi.org/10.63978/3083-6476.2026.1.4.06

34. Савлюк М. Гібридна війна в Україні: сучасні підходи. *Вісник Прикарпатського університету. Політологія*. 2024. Вип. 17. С. 187-196. DOI: https://doi.org/10.32782/2312-1815/2024-17-23.

35. Сазонов В. Інформаційний складник гібридної війни. *Вісник Львівського університету.* Серія філософсько-політологічні студії. 2025. Вип. 62. С. 336-344. DOI: https://doi.org/10.30970/PPS.2025.62.40.

36. Сальникова, О., Сівоха І., Іващенко А. Стратегічні комунікації в сучасній гібридній війні. *Соціальний розвиток і безпека* . 2019. Вип. 9 (5). С. 133-142. DOI: https://doi.org/10.33445/sds.2019.9.5.9

37. Світова гібридна війна: український фронт : монографія / за заг. ред. В.П. Горбуліна. Київ : НІСД, 2017. 496 с.

38. Старовойтенко О. О., Лисецький Ю. М., Семенюк Ю. В., Павленко Д. Г. Гібридні війни. Компоненти та особливості. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. Серія: Публічне управління та адміністрування. 2021. Т. 32 (71), № 5. С. 63-68. DOI: https://doi.org/10.32838/TNU-2663-6468/2021.5/11.

39. Стрельбицький М., Гринь М. Когнітивна війна Росії проти України. *Наукові праці Міжрегіональної Академії управління персоналом*. Юридичні науки, 2023. Вип.1 (64). С. 46-52. DOI: https://doi.org/10.32689/2522-4603.2023.1.7

40. Тригуб О. П., Місяць М. Феномен гібридної війни в українській та зарубіжній політології. *Наукові праці. Політологія*. 2019. Вип. 312. Т. 324. С. 66-71. URL: http://politics.chdu.edu.ua/article/view/200683 (дата звернення: 13.05.2026).

41. Уздєнова Ю. М. Гібридна війна: сутність, складові та ключові поняття. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. Серія: Публічне управління та адміністрування. 2024. Т. 35 (74). № 4. С. 172-178. DOI: https://doi.org/10.32782/TNU-2663-6468/2024.4/26.

42. Шемаєв В.М., Срьоміна Л.В. Когнітивна війна як складова сучасної гібридної війни. *Юридичний науковий електронний журнал*. 2024. № 7 С. 302-305. DOI: https://doi.org/10.32782/2524-0374/2024-7/73

43. Хорішко Л. С. Досвід реалізації стратегічних комунікацій у діяльності НАТО та ЄС: інституційний аспект. *Регіональні студії*. 2021. № 26. С. 54-59. DOI: https://doi.org/10.32782/2663-6170/2021.26.11

44. Хмиров І., Хряпинський А., Алієва П., Копотун І., Свобода І. Міжнародний досвід розвинених країн у державному управлінні протидією гібридним загрозам. *Revista Jurídica Portucalense* , 2024. Вип. 36. С. 359-380. DOI: https://doi.org/10.34625/issn.2183-2705(36)2024.ic-16

45. Чалапко В. В. Гібридна війна як сучасна форма насильства. *Вісник Національного юридичного університету імені Ярослава Мудрого*. Серія: філософія, філософія права, політологія, соціологія. 2021. № 1(48). С. 133-145. DOI: https://doi.org/10.21564/2075-7190.48.224421.

46. Яворська Г. М. Гібридна війна як дискурсивний конструкт. *Стратегічні пріоритети. Серія: Політика*. 2016. № 4(41). С. 41-48. URL: https://ippi.org.ua/sites/default/files/yavorskaya.pdf (дата звернення: 13.05.2026).

47. Anagnostakis D. Hybrid Threats: A European Response. In: Springer Optimization and Its Applications. 2023. Vol. 205. P. 425-441. DOI: https://doi.org/10.1007/978-3-031-39542-0_21

48. Andriyevskyy T. G. Цілі російсько-української гібридної війни. Політичне життя. Вип. 2 (Лип 2018). С. 103-108. DOI: https://doi.org/10.31558/2519-2949.2018.2.17.

49. Ćosić K., Popović S., Wiederhold B. Emotionally based strategic communications as a new tool in defensive cognitive warfare. Frontiers in Psychology. 2026. Vol. 17. DOI: 10.3389/fpsyg.2026.1751406

50. Daily Sabah. From pipelines to power games: Russia's energy chessboard in a hybrid war. 2025. April 4. URL: https://www.dailysabah.com/ (дата звернення: 13.05.2026).

51. Danylenko S., Zagorodsky A. Cross-sectoral resilience: lessons from Ukrainian local communities' response to hybrid threats. Social Sciences & Humanities Open. 2025. Vol. 12. DOI: https://doi.org/10.1016/j.ssaho.2025.102037

52. Dawson M., Harrell T., Moore S. Cyber Operations and Hybrid Conflict In Ukraine: Evidence From The Global Terrorism Database And State Linked Cyber Campaigns. Land Forces Academy Review. 2026. Vol. 31, No. 1. P. 27-37. DOI: https://doi.org/10.2478/raft-2026-0003

53. Firdini F., Panggabean J., Anwar S. The Role of Russian Cyber Operations in The Russian-Ukraine War in Achieving Russia's Strategic Objectives. Jurnal Perencanaan Pembangunan. 2024. Vol. 8, No. 1. P. 98-112. DOI: https://doi.org/10.36574/jpp.v8i1.470

54. Fordoński R. Notion of hybrid weapon in hybrid conflict – legal assessment of Russian Federation's use of energy weapon against European allies of Ukraine. Studia Prawnoustrojowe. 2025. No. 67. DOI: https://doi.org/10.31648/sp.10827

55. Fridman O. Russian «Hybrid Warfare»: Resurgence and Politicization. Oxford University Press, 2018. 250 p. DOI: https://doi.org/10.1093/oso/9780190877378.001.0001

56. Hoffman F. G. Conflict in the XXI st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies, 2007. 72 p.

57. Jacuch A. Countering Hybrid Threats: Resilience in the EU and NATO's Strategies. The Copernicus Journal of Political Studies. 2020. No. 1. P. 9-24. DOI: https://doi.org/10.12775/CJPS.2020.001

58. Kurylo V., Vovk S., Bader A., Karaman O. Armed Violence as a Challenge to National Security: Critical Thinking Perspectives. Connections: The Quarterly Journal. 2024. Vol. 23, No. 1. P. 59-78. DOI: https://doi.org/10.11610/Connections.23.1.02

59. Lind W. S., Nightengale K., Schmitt J. F., Sutton J. W., Wilson G. I. The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette. 1989. Vol. 73, No. 10. P. 22-26.

60. Mârzac E. Strategic Communication as a Tool for Countering Hybrid Threats: A Focus on National Resilience and Public Trust. Studia Securitatis. 2024. Vol. XVIII, No. 2. P. 55-67.

61. NATO. Cognitive Warfare: A New Frontier of Modern Conflict. Report of the Chief Scientific Advisor. Brussels: NATO Science and Technology Organization, 2025.

62. Oxford Bibliographies. Hybrid Warfare. Last reviewed: 22 September 2021. DOI: 10.1093/obo/9780199743292-0260

63. Qiao Liang, Wang Xiangsui. Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House, 1999. 256 p.

64. Radu R. Building Cyber Resilience to Face the Challenges of Cognitive Warfare. European Conference on Cyber Warfare and Security. 2025. Vol. 24, No. 1. DOI: https://doi.org/10.34190/eccws.24.1.3520

65. Siewier M. A. Resilience as a Strategic Pillar of Cognitive Security. Humanities and Social Sciences. 2025. Vol. 32, No. 4. P. 169-183. DOI: https://doi.org/10.7862/rz.2025.hss.50

66. Wither J. K. Making Sense of Hybrid Warfare. Connections: The Quarterly Journal. 2016. Vol. 15, No. 2. P. 73-87. DOI: https://doi.org/10.11610/Connections.15.2.06.