УДК 355.02:327.7(477)

Орлов Олександр Валентинович
доктор наук з державного управління, професор,
професор кафедри публічної політики
ННІ «Інститут державного управління»
Харківського національного університету імені В.Н. Каразіна
Orlov Oleksandr
Doctor of Science in Public Administration, Professor,
Professor of the Department of Public Policy
Education and Research Institute of Public Administration
V.N. Karazin Kharkiv National University
ORCID: 0000-0001-8995-7383

Дворянов Віктор Петрович
аспірант кафедри публічної політики
ННІ «Інститут державного управління»
Харківського національного університету імені В.Н. Каразіна
Dvorianov Viktor
Post-Graduate Student of the Department of Public Policy
Education and Research Institute of Public Administration
V.N. Karazin Kharkiv National University
ORCID: 0000-0002-6705-6549

DOI: 10.25313/2617-572X-2026-2-11981

ТРАНСФОРМАЦІЯ СУЧАСНИХ ЗБРОЙНИХ КОНФЛІКТІВ У КОНТЕКСТІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ ТА ДЕРЖАВНІ МЕХАНІЗМИ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

TRANSFORMATION OF MODERN ARMED CONFLICTS IN THE CONTEXT OF THE RUSSIAN-UKRAINIAN WAR AND STATE MECHANISMS FOR COUNTERING HYBRID THREATS

Анотація. *Вступ. Стаття присвячена комплексному аналізу трансформації сучасних збройних конфліктів та відповідної державної протидії. Детально досліджено специфіку гібридних операцій у російсько-українській війні та систематизовано типологію застосованих загроз, що дозволяє перейти від абстрактних теоретичних конструктів до емпіричного аналізу конкретних проявів гібридної війни. Це, у свою чергу, створює підґрунтя для аналізу національних та міжнародних механізмів протидії гібридним загрозам, оцінки їх ефективності та виявлення системних недоліків. Завершальним етапом дослідження є розробка рекомендацій щодо вдосконалення державної політики України у сфері протидії гібридним загрозам, що забезпечує практичну орієнтованість наукового пошуку. Дослідження може бути використане для удосконалення систем національної безпеки та підвищення стійкості держави до війн нового типу.*

Мета. Метою дослідження є аналіз трансформації сучасних збройних конфліктів через призму російсько-української війни та визначення ефективних державних механізмів протидії гібридним загрозам у контексті національної безпеки.

Матеріали і методи. Матеріалами дослідження є: 1) нормативна база з питань національної безпеки та оборони України; 2) праці вітчизняних та зарубіжних авторів, що провадять свої науково-практичні дослідження у царині глобалізації та національної безпеки.

У дослідженні використано комплекс загальнонаукових і спеціальних методів: системний аналіз (для вивчення структури гібридних загроз), компаративний метод (для порівняння підходів різних держав до протидії гібридним загрозам), метод case study (аналіз конкретних прикладів гібридних операцій у російсько-українській війні), контент-аналіз (дослідження нормативно-правових актів та стратегічних документів).

Результати. У науковій статті визначено ключові характеристики трансформації сучасних збройних конфліктів, систематизовано типологію гібридних загроз у російсько-українській війні, проаналізовано національні та міжнародні механізми протидії, сформульовано рекомендації щодо вдосконалення державної політики у сфері протидії гібридним загрозам.

Перспективи. Подальші наукові дослідження мають бути спрямовані на підвищення ефективності державних механізмів протидії гібридним загрозам у контексті національної безпеки.

Ключові слова: *гібридна війна, збройний конфлікт, національна безпека, інформаційні операції, кібербезпека, стратегічні комунікації, когнітивна війна, російсько-українська війна.*

Summary. *Introduction. The article is devoted to a comprehensive analysis of the transformation of modern armed conflicts and the corresponding state response. The specifics of hybrid operations in the Russian-Ukrainian war have been studied in detail and the typology of applied threats has been systematized, which allows us to move from abstract theoretical constructs to an empirical analysis of concrete manifestations of hybrid war. This, in turn, creates the basis for the analysis of national and international mechanisms for countering hybrid threats, assessing their effectiveness and identifying systemic flaws. The final stage of the research is the development of recommendations for improving the state policy of Ukraine in the field of countering hybrid threats, which ensures a practical orientation of scientific research. The research can be used to improve national security systems and increase the state's resistance to new types of wars.*

Purpose. The purpose of the study is to analyze the transformation of modern armed conflicts through the prism of the Russian-Ukrainian war and to determine effective state mechanisms for countering hybrid threats in the context of national security.

Materials and methods. The research materials are: 1) regulatory framework on national security and defense of Ukraine; 2) works of domestic and foreign authors conducting scientific and practical research in the field of globalization and national security.

The research uses a set of general scientific and special methods: system analysis (to study the structure of hybrid threats), comparative method (to compare the approaches of different states to countering hybrid threats), case study method (analysis of specific examples of hybrid operations in the Russian-Ukrainian war), content analysis (study of legal acts and strategic documents).

Results. The scientific article identifies the key characteristics of the transformation of modern armed conflicts, systematizes the typology of hybrid threats in the Russian-Ukrainian war, analyzes national and international countermeasures, and formulates recommendations for improving state policy in the field of countering hybrid threats.

Discussion. Further research should be aimed at increasing the effectiveness of state mechanisms for countering hybrid threats in the context of national security.

Key words: *hybrid warfare, armed conflict, national security, information operations, cyber security, strategic communications, cognitive warfare, Russian-Ukrainian war.*

Постановка проблеми. Сучасний етап розвитку міжнародних відносин характеризується фундаментальною трансформацією природи збройних конфліктів. Класична модель міждержавної війни, що базувалася на протистоянні регулярних збройних сил на чітко визначеному фронті, поступається місцем гібридним формам конфліктів, де військові дії поєднуються з кібератаками, інформаційно-психологічними операціями, економічним тиском та дипломатичними маніпуляціями (Hoffman, 2007; Gerasimov, 2013) [7]. Ця трансформація не є лише зміною тактики ведення бойових дій, а відображає глибинні зміни у самій онтології війни, що вимагає переосмислення традиційних підходів до забезпечення національної безпеки.

Російсько-українська війна, що розпочалася у 2014 році анексією Криму та військовою агресією на Донбасі, а 24 лютого 2022 року переросла у повномасштабне вторгнення, стала найяскравішим прикладом застосування гібридних стратегій у XXI столітті. За оцінками експертів NATO Strategic Communications Centre of Excellence [14], російська агресія проти України демонструє безпрецедентне поєднання конвенційних військових операцій з масованими кампаніями дезінформації, кібератаками на критичну інфраструктуру та економічним шантажем (Pynnöniemi & Rácz, 2016). Звідси випливає, що цей конфлікт являє собою унікальну можливість для емпіричного дослідження механізмів гібридної війни та ефективності різних стратегій протидії.

Масштаби інформаційної агресії вражають своєю інтенсивністю. За даними Центру протидії дезінформації при РНБО України, у період з лютого по грудень 2022 року було зафіксовано понад 50,000 дезінформаційних повідомлень, спрямованих проти України у глобальному інформаційному просторі (Центр протидії дезінформації, 2023). Водночас, кібератаки на українську критичну інфраструктуру, зокрема енергетичний сектор, банківську систему

// ISSN 2617-572X //

та державні інформаційні ресурси, досягли рівня, який CERT-UA класифікує як «системну загрозу національній безпеці» (CERT-UA, 2023). З наведених даних випливає, що інформаційний та кібернетичний виміри конфлікту стали рівноправними компонентами війни, а не допоміжними інструментами.

Ця ситуація актуалізує необхідність комплексного наукового аналізу трансформації сучасних збройних конфліктів та розробки ефективних державних механізмів протидії гібридним загрозам. Більше того, багаторічний досвід протистояння російській агресії дає можливість не лише теоретично осмислити феномен гібридної війни, а й емпірично верифікувати ефективність різних стратегій протидії, що й становить предмет цього дослідження.

Аналіз останніх досліджень і публікацій. Теоретичні аспекти гібридної війни досліджувалися у працях зарубіжних науковців: Ф. Гоффмана (F. Hoffman, 2007, 2009) [8], який запропонував концептуальне визначення гібридної війни; Дж. Маккуена (J. McCuen, 2008) [12], що проаналізував гібридні конфлікти через призму асиметричних стратегій; Р. Глена (R. Glenn et al., 2009) [6], який досліджував досвід гібридних операцій Хезболли; П. Мансура (P. Mansoor, 2012), що вивчав еволюцію гібридної війни від Давида і Голіафа до сучасності.

Російську специфіку гібридної агресії аналізували М. Гейл (M. Galeotti, 2016, 2019) [4], К. Гілс (K. Giles, 2016) [5], М. Монаґен (A. Monaghan, 2016) [13], які досліджували так звану «доктрину Герасимова» та російські підходи до невійськових засобів досягнення стратегічних цілей.

Серед українських дослідників значний внесок у розробку проблематики зробили: Горбулін В. П. (2017) [9], який проаналізував «світову гібридну війну»; Магда Є. В. (2015) [11], що досліджував гібридну агресію Росії проти України; Власюк О. С. та Кононенко С. В. (2020) [17], які вивчали актуальні проблеми та напрями забезпечення національної безпеки України; Ліпкан В. А. (2019) [10], що розробляв теоретичні засади національної безпеки в умовах гібридної війни.

Водночас, динамічний характер російсько-української війни, поява нових форм гібридних загроз (зокрема, когнітивна війна, використання AI-генерованого контенту, автономні системи дезінформації) та еволюція механізмів протидії вимагають постійного оновлення наукових досліджень у цій сфері.

Метою статті є комплексний аналіз трансформації сучасних збройних конфліктів у контексті російсько-української війни та визначення ефективних державних механізмів протидії гібридним загрозам.

Досягнення поставленої мети передбачає послідовне вирішення взаємопов'язаних дослідницьких завдань. Насамперед, необхідно визначити теоретико-методологічні засади дослідження гібридних конфліктів та систематизувати підходи до їх концептуалізації, що дозволить сформувати понятійний апарат дослідження. На цій основі стає можливим проаналізувати ключові характеристики трансформації сучасних збройних конфліктів порівняно з класичними формами міждержавних війн, виявляючи парадигмальні зміни у природі воєнного протиборства.

Звідси випливає необхідність детального дослідження специфіки гібридних операцій у російсько-українській війні та систематизації типології застосованих загроз, що дозволить перейти від абстрактних теоретичних конструктів до емпіричного аналізу конкретних проявів гібридної війни. Це, у свою чергу, створює підґрунтя для аналізу національних та міжнародних механізмів протидії гібридним загрозам, оцінки їх ефективності та виявлення системних недоліків. Завершальним етапом дослідження є розробка рекомендацій щодо вдосконалення державної політики України у сфері протидії гібридним загрозам, що забезпечує практичну орієнтованість наукового пошуку.

Об'єкт дослідження: процеси трансформації сучасних збройних конфліктів у контексті гібридної війни.

Предмет дослідження: державні механізми протидії гібридним загрозам у контексті російсько-української війни.

Матеріали і методи. Матеріалами дослідження є: 1) нормативна база з питань національної безпеки та оборони України; 2) праці вітчизняних та зарубіжних авторів, що провадять свої науково-практичні дослідження у царині глобалізації та національної безпеки.

У дослідженні використано комплекс загальнонаукових і спеціальних методів: системний аналіз (для вивчення структури гібридних загроз), компаративний метод (для порівняння підходів різних держав до протидії гібридним загрозам), метод case study (аналіз конкретних прикладів гібридних операцій у російсько-українській війні), контент-аналіз (дослідження нормативно-правових актів та стратегічних документів).

Виклад основного матеріалу. Термін «гібридна війна» увійшов до наукового та політичного дискурсу у 2000-х роках, проте феномен поєднання різних форм ведення бойових дій має давню історію. Сун-Цзі у трактаті «Мистецтво війни» (V ст. до н.е.) стверджував: «Найвища майстерність полягає не у перемозі в ста битвах, а у підкоренні ворога без бою» (Sun Tzu, trans. 1963, p. 77), що, по суті, описує фундаментальний принцип гібридної стратегії [16]. Це свідчить про те, що прагнення досягти перемоги невійськовими засобами не є винаходом сучасності, однак саме технологічний розвиток XXI століття надав цій стратегії якісно нових можливостей.

Концептуалізація гібридної війни як окремого феномену відбувалася поступово, проходячи кілька якісно відмінних етапів. Зародження концепції припадає на період 2000–2006 років, коли Френк

Гоффман у 2005 році запропонував визначення гібридної війни як «конфлікту, в якому противник одночасно і адаптивно використовує комбінацію традиційної зброї, іррегулярної тактики, тероризму та кримінальної поведінки в операційному просторі для досягнення політичних цілей» (Hoffman, 2007, p. 8) [7]. Поштовхом до розробки концепції стала війна Ізраїлю з Хезболлою у 2006 році, коли остання продемонструвала поєднання партизанської тактики, використання сучасних протитанкових систем, кібератак та ефективних інформаційних кампаній (Cordesman & Sullivan, 2007) [2]. Звідси випливає, що початкове розуміння гібридності фокусувалося переважно на військово-тактичному рівні, залишаючи поза увагою більш широкий спектр невійськових інструментів впливу.

Період 2007–2013 років характеризується поглибленою теоретичною розробкою концепції. Дослідники розширили її межі, включивши економічні, дипломатичні та інформаційні компоненти. Маккуен (2008) запропонував розглядати гібридну війну як континуум між традиційною війною та іррегулярним конфліктом, де противник оперує на всьому спектрі можливостей [12]. Це дало можливість зробити висновок про те, що гібридність не є фіксованим набором тактик, а являє собою динамічну адаптивну стратегію, що постійно еволюціонує відповідно до можливостей та обмежень конкретного контексту.

Критично важливим виявився аналіз радянського досвіду «активних заходів» (активные мероприятия) КДБ СРСР у період холодної війни, які включали дезінформацію, підривну діяльність, маніпуляції з медіа та політичне втручання (Rid, 2020) [15]. Ці практики згодом були адаптовані та масштабовані російськими службами безпеки, що свідчить про історичну наступність гібридних стратегій та їх укоріненість у певних геополітичних традиціях.

Якісно новий етап розвитку концепції пов'язаний з публікацією у 2013 році статті начальника Генерального штабу Збройних Сил РФ Валерія Герасимова, що згодом отримала назву «доктрина Герасимова». Він описав концепцію «війни нового покоління», стверджуючи, що «правила війни кардинально змінилися. Роль невійськових засобів у досягненні політичних і стратегічних цілей зросла, і у багатьох випадках вони перевершили за ефективністю силу зброї» (Gerasimov, 2013, p. 2). Герасимов запропонував співвідношення невійськових до військових засобів як 4:1, підкреслюючи пріоритет інформаційного, економічного, дипломатичного та підривного впливу над прямим військовим втручанням.

Парадоксальним є той факт, що Герасимов описував гібридну війну як західну стратегію проти Росії, хоча саме російська агресія проти України у 2014 році стала найяскравішим прикладом застосування цієї доктрини (Galeotti, 2016) [4]. Це дозволяє зробити висновок про те, що концептуалізація гібридної війни у російському дискурсі виконувала подвійну функцію, з одного боку, легітимуючи власні агресивні дії як «оборону» від західної експансії, з іншого — розробляючи стратегічну доктрину для практичного застосування.

Період від 2014 року до сьогодення характеризується практичною апробацією та подальшим розвитком концепції. Російська агресія проти України продемонструвала нову якість гібридної війни, що включає використання «зелених чоловічків» (військових без розпізнавальних знаків), масові кібератаки на критичну інфраструктуру, глобальні кампанії дезінформації, енергетичний шантаж та втручання у демократичні процеси інших держав. З цього випливає, що сучасна гібридна війна являє собою не просто тактичну новацію, а фундаментальну трансформацію самої природи збройного конфлікту, що вимагає переосмислення базових категорій теорії війни та міжнародного права.

У науковій літературі існує плюралізм визначень гібридної війни, що відображає складність та багатогранність цього феномену. Для цілей цього дослідження ми пропонуємо інтегроване визначення:

Гібридна війна — це форма стратегічного протиборства, що характеризується синхронізованим застосуванням військових і невійськових засобів (інформаційно-психологічних, кібернетичних, економічних, дипломатичних, підривних) для досягнення політичних цілей, при якому межі між станом війни і миру, зовнішніми і внутрішніми загрозами, державними і недержавними акторами є розмитими або свідомо приховуються агресором.

Для розуміння глибини трансформації сучасних збройних конфліктів доцільно провести системний порівняльний аналіз класичних та гібридних форм війни.

Аналіз російсько-української війни свідчить про фундаментальні парадигмальні зміни у характері збройних конфліктів XXI століття:

Від фізичного знищення до когнітивного підпорядкування. Якщо у класичних війнах перемога визначалася знищенням збройних сил противника та окупацією території (за принципом Клаузевіца), то у гібридній війні головною метою стає контроль над свідомістю, наративами та процесами прийняття рішень.

За даними NATO StratCom COE (2020), російська Федерація витрачає близько $1.4 млрд. щорічно на зовнішню пропаганду та інформаційні операції, що порівнянно з оборонним бюджетом середньої європейської країни [14]. Це свідчить про стратегічний пріоритет когнітивного виміру війни.

Від лінійного фронту до омнінапрямкового впливу. Гібридна війна не має чіткої лінії фронту. Операції ведуться одночасно:

- У кіберпросторі (атаки на критичну інфраструктуру).
- В інформаційному просторі (глобальні кампанії дезінформації).

Параметр	Класичний збройний конфлікт	Гібридна війна
Оголошення війни	Формальне оголошення війни згідно з міжнародним правом	Відсутність формального оголошення, «війна без війни»
Учасники	Регулярні збройні сили держав з чіткими розпізнавальними знаками	Комбінація регулярних військ, іррегулярних формувань, найманців, кібергруп, без чітких розпізнавальних знаків
Театр військових дій	Географічно визначений фронт, тиловий та прифронтовий райони	Розмиті кордони, одночасні дії на всій території держави та за її межами
Основні засоби	Військова сила (сухопутні війська, авіація, флот)	Інтегровані військові, інформаційні, кібернетичні, економічні, дипломатичні засоби
Цілі ураження	Збройні сили противника, військова інфраструктура	Критична інфраструктура, інформаційний простір, суспільна свідомість, економіка, політична система
Тривалість активної фази	Чітко окреслені фази (початок, ескалація, кульмінація, завершення)	Континуальний характер, відсутність чітких фаз, «війна до війни» та «війна після війни»
Інформаційний простір	Пропаганда як допоміжний інструмент	Інформаційні операції як рівноправний компонент стратегії
Правове регулювання	Женевські конвенції, міжнародне гуманітарне право	Експлуатація прогалин у міжнародному праві, «сіра зона» між війною і миром
Критерій перемоги	Військова перемога, окупація території, капітуляція	Політичні цілі: зміна режиму, контроль над ресурсами, дестабілізація регіону

Рис. 1. Порівняльні характеристики класичних та гібридних збройних конфліктів
Джерело: розроблено В. Дворяновим

- В економічній сфері (енергетичний шантаж, маніпуляції з цінами).
- У політичній площині (підтримка «п'ятої колони», втручання у вибори).
- На кінетичному рівні (військові операції).

Від державоцентричної до мережецентричної моделі. Класичні війни велися між державами з централізованими командними структурами. Гібридні конфлікти залучають розподілені мережі акторів:

- Офіційні військові структури.
- Приватні військові компанії (ПВК «Вагнер», Академія).
- Кібергрупи (APT28 «Fancy Bear», APT29 «Cozy Bear», Sandworm).
- Медіа-холдинги (RT, Sputnik, мережа проксі-сайтів).
- Бот-ферми та «тролів фабрики» (Internet Research Agency).

Від матеріальних ресурсів до інформаційних активів. Якщо у минулому військова могутність визначалася кількістю танків, літаків та солдатів, то у гібридній війні критично важливими стають:

- Контроль над наративами та інформаційними потоками.
- Здатність до кібератак та кіберзахисту.
- Доступ до персональних даних та можливості мікротаргетингу.
- Володіння технологіями AI, deepfake, синтетичних медіа.

Від швидкості до тривалості. Класичні війни прагнули до швидкої перемоги (блискавична війна, Blitzkrieg). Гібридна війна характеризується тривалістю та «ефектом повільного кип'ятіння жаби» — поступовою ескалацією, що не провокує рішучої відповіді.

Російська агресія проти України розпочалася не у 2022, а у 2014 році, і навіть до 2014 року можна ідентифікувати елементи гібридного впливу (енергетичні конфлікти 2006 та 2009 років, підтримка проросійських політичних сил, інформаційні кампанії).

Російсько-українська війна стала найбільш повним та документованим прикладом застосування гібридних стратегій у XXI столітті, демонструючи синхронізоване використання військово-кінетичних, кібернетичних, інформаційних, економічних та дипломатичних інструментів впливу. Аналіз конкретних проявів гібридної агресії дозволяє перейти від абстрактних теоретичних конструктів до емпіричного розуміння механізмів та логіки гібридної війни.

Анексія Автономної Республіки Крим у лютому-березні 2014 р. стала класичним прикладом гібридної військової операції, що поєднувала елементи маскування, швидкості та правдоподібного заперечення. Російські збройні сили без розпізнавальних знаків, які російські ЗМІ евфемістично називали «ввічливі люди», а український дискурс охрестив «зеленими чоловічками», здійснили блокування українських військових об'єктів, захоплення Верховної Ради Криму та інших стратегічних об'єктів за лічені дні.

За даними звіту Міжнародного кримінального суду (ICC, 2016), у операції брали участь підрозділи 45-го полку спеціального призначення ВДВ РФ, 22-ї окремої бригади спецназу ГРУ та військовослужбовці Чорноморського флоту РФ. Офіційно Росія запе-

речувала присутність своїх військ протягом майже двох місяців, і лише 17 квітня 2014 р. президент Путін визнав участь російських військових, коли анексія вже була фактично завершеною. Звідси випливає, що стратегічна мета полягала у створенні fait accompli (свершившегося факта) до того, як міжнародна спільнота зможе відреагувати, уникнувши при цьому правової кваліфікації дій як збройної агресії згідно зі статтею 2(4) Статуту ООН.

Ця операція демонструє ключову особливість гібридної війни: використання розриву у часі між фактичним здійсненням агресії та можливістю її правової кваліфікації для створення незворотних наслідків. Це дозволяє зробити висновок, що швидкість виконання, маскування джерела агресії та експлуатація процедурних обмежень міжнародного права становлять технологічне ядро гібридної військової операції.

На сході України Росія застосувала якісно іншу модель гібридної агресії, офіційно позиціонуючи конфлікт як «громадянську війну» та надаючи підтримку самопроголошеним «ДНР» та «ЛНР». Водночас, дослідження незалежних розслідувальних організацій Bellingcat, InformNapalm та Atlantic Council методами OSINT задокументували присутність регулярних підрозділів Збройних Сил РФ, зокрема 3-ї мотострілецької дивізії, 200-ї окремої мотострілецької бригади та артилерійських підрозділів, а також російської військової техніки, включаючи системи залпового вогню «Град», «Ураган», «Смерч» та танки Т-72Б3, що не перебували на озброєнні України.

За оцінками Міністерства оборони України (2021), у пік конфлікту протягом 2014–2015 років на Донбасі одночасно перебувало до 40000 російських військовослужбовців та найманців. Це дає можливість розвинути бачення проксі-війни не як простого використання третіх сторін, а як складної гібридної конструкції, де офіційне заперечення поєднується з фактичним військовим контролем, створюючи стан «війни, яка офіційно не існує».

З цього випливає, що проксі-модель дозволяє агресору досягати військових цілей, уникаючи міжнародної відповідальності та санкцій, що застосовуються до прямих збройних конфліктів між державами.

24 лютого 2022 р. Росія розпочала повномасштабне вторгнення в Україну, що на перший погляд могло здаватися поверненням до класичної міждержавної війни. Водночас, навіть у цій фазі зберігалися суттєві елементи гібридності, що проявлялися через атаки на цивільну інфраструктуру та енергосистему України, синхронізовані інформаційні операції, використання найманців ПВК «Вагнер» для створення правдоподібного заперечення щодо найбільш брутальних дій, проведення фальшивих референдумів на окупованих територіях для створення видимості легітимності та постійний ядерний шантаж як інструмент стримування західної допомоги Україні.

Це дозволяє зробити висновок, що гібридність не є альтернативою конвенційній війні, а може функціонувати як додатковий рівень операцій навіть у контексті відкритого збройного конфлікту, посилюючи ефективність традиційних військових дій через когнітивний, інформаційний та економічний тиск.

Російсько-українська війна стимулювала розвиток комплексної системи протидії гібридним загрозам в Україні, що охоплює нормативно-правовий, інституційний, технологічний та соціальний виміри. Аналіз українського досвіду дозволяє виявити як успішні практики, так і системні виклики, з якими стикаються держави у протидії гібридній агресії.

Правове підґрунтя протидії гібридним загрозам в Україні формувалося поетапно, відповідаючи на еволюцію характеру російської агресії. Стратегія національної безпеки України, прийнята у 2020 році та оновлена у 2023 році, визначає гібридні загрози як один із пріоритетних викликів національній безпеці. Це дало можливість створити правову основу для координованих дій різних державних органів. Стратегія кібербезпеки України (2021) та Доктрина

Дата	Подія	Актори	Механізм маскування
20.02.2014	Початок «Євромайдану» в Києві	Українські протестувальники	Контекст політичної кризи
27.02.2014	Захоплення Верховної Ради Криму	45-й полк ВДВ РФ	Без розпізнавальних знаків
28.02.2014	Блокування українських військових частин	22-а бригада спецназу ГРУ	«Народна самооборона Криму»
01–15.03.2014	Контроль над критичною інфраструктурою	Чорноморський флот РФ	Офіційне заперечення
16.03.2014	«Референдум» про приєднання до РФ	Окупаційна адміністрація	Легалістична риторика
18.03.2014	Підписання «договору про приєднання»	Кремль	Fait accompli
17.04.2014	Путін визнає участь російських військових	Президент РФ	Ретроспективне визнання

Рис. 2. Хронологія анексії АР Крим: технологія гібридної операції

Джерело: розроблено В. Дворяновим

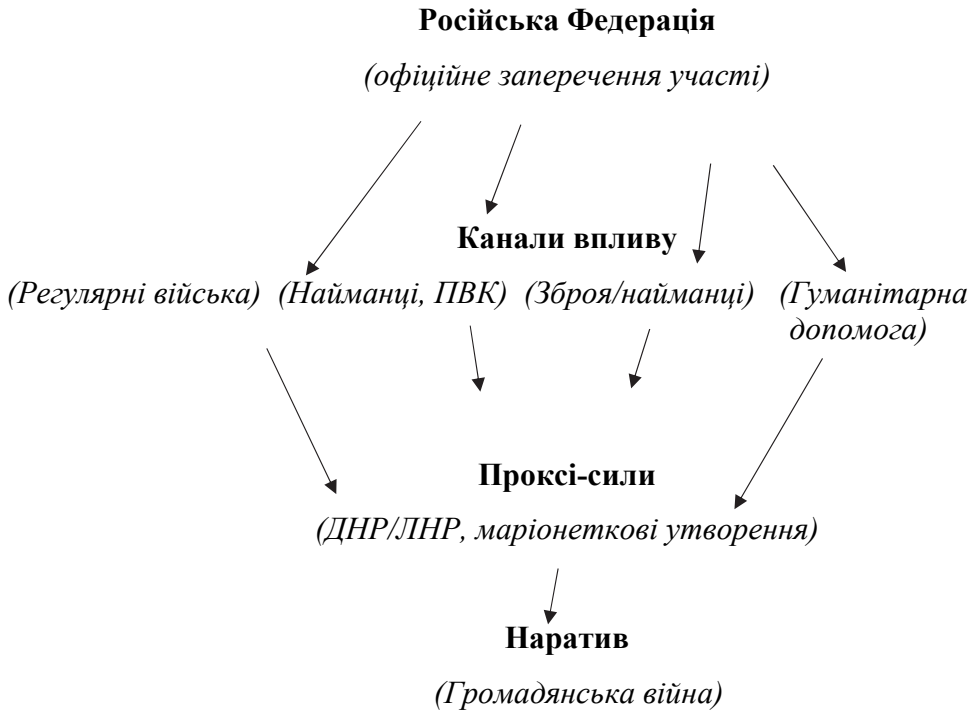

Рис. 3. Структура проксі-конфлікту на Донбасі
Джерело: розроблено В. Дворяновим

інформаційної безпеки (2017) конкретизують напрямки протидії у відповідних сферах, формуючи багаторівневу систему правового регулювання.

Інституційна архітектура протидії гібридним загрозам в Україні характеризується розподіленою моделлю відповідальності з центральною координацією через Раду національної безпеки і оборони. У 2021 році при РНБО було створено Центр протидії дезінформації, функціонал якого охоплює моніторинг інформаційного простору, виявлення дезінформаційних кампаній, координацію з міжнародними партнерами та публічне спростування фейків. Це дозволило централізувати аналітичну роботу та забезпечити швидке реагування на інформаційні загрози.

Служба безпеки України відповідає за контррозвідувальний напрямок, включаючи виявлення та припинення діяльності агентів впливу, боротьбу з диверсійно-розвідувальними групами та захист від підривної діяльності. Міністерство цифрової трансформації координує кібербезпекову складову, зокрема захист критичної інфраструктури та розвиток цифрової резильєнтності. CERT-UA (Computer Emergency Response Team of Ukraine) здійснює оперативне реагування на кіберінциденти, демонструючи вражаючу ефективність: за 2023 рік команда обробила 2,194 інциденти та попередила понад 100 масштабних атак; в 2025 р. опрацювала 5927 інцидентів, що на 37,4% більше ніж в 2024 році (CERT-UA, 2026) [1]. З наведених даних випливає, що розподілена модель відповідальності при належній координації здатна забезпечити гнучке та ефективне реагування на різнопланові гібридні загрози.

Україна розробила ефективну систему стратегічних комунікацій, що стала одним із ключових

Документ	Рік прийняття	Основний фокус	Ключові положення
Закон «Про основи національної безпеки»	2003 (з численними змінами)	Загальні засади нацбезпеки	Визначення загроз, повноваження органів, координація
Доктрина інформаційної безпеки	2017	Інформаційний простір	Протидія пропаганді, медіаграмотність, стратком
Закон «Про кібербезпеку»	2017	Кіберпростір	Захист КІІ, повноваження CERT-UA, міжнародна співпраця
Стратегія національної безпеки	2020 (оновлена 2023)	Комплексна безпека	Інтеграція всіх напрямків протидії гібридним загрозам
Стратегія кібербезпеки	2021	Технічний захист	Розвиток кіберспроможностей, стандарти захисту

Рис. 4. Нормативно-правова база протидії гібридним загрозам в Україні
Джерело: розроблено В. Дворяновим

факторів успішного протистояння російській інформаційній агресії. Координація повідомлень між Офісом Президента, урядом та військовим керівництвом забезпечує так званий «єдиний голос держави», що критично важливо для формування довіри як всередині країни, так і на міжнародній арені. Це дало можливість уникнути суперечливих меседжів та хаотичної комунікації, які могли б підірвати ефективність інформаційної оборони.

Принцип прозорості та відкритості став стратегічним вибором України, що радикально відрізняв її підхід від традиційної закритості воєнної інформації. Щоденні брифінги Міністерства оборони, публікація об'єктивних даних про втрати та ситуацію на фронті, забезпечення доступу міжнародних журналістів до зони бойових дій створили атмосферу довіри та достовірності. Звідси випливає, що прозорість у комунікації може бути не вразливістю, а конкурентною перевагою у протистоянні з противником, що систематично використовує дезінформацію.

Цифрова дипломатія стала інноваційним інструментом, що дозволив Україні обійти традиційні дипломатичні канали та звертатися безпосередньо до громадян інших країн. Це дозволило створити безпрецедентну хвилю глобальної солідарності, що трансформувалася у конкретну політичну, економічну та військову підтримку.

Розвиток медіаграмотності населення став довгостроковою стратегією підвищення суспільної стійкості до дезінформації. Впровадження курсів медіаграмотності у школах та університетах, організація тренінгів для журналістів з фактчекінгу, проведення публічних кампаній з виявлення дезінформації створили системний підхід до формування критичного мислення. Результати цієї роботи є вражаючими: за даними Internews (2023), рівень медіаграмотності в Україні зріс з 34% у 2021 році до 52% у 2023 році, що становить зростання на 53% за два роки.

Це дозволяє зробити висновок, що інвестиції в медіаграмотність приносять вимірні результати у відносно короткі терміни, особливо в умовах активного інформаційного протиборства, коли населення безпосередньо стикається з проявами дезінформації.

Висновки і перспективи подальших досліджень. Проведене дослідження аналізу трансформації сучасних збройних конфліктів та державної протидії дозволяє сформулювати наступні ключові висновки:

1. Гібридна війна трансформує саму природу міжнародної безпеки, перетворюючи її з дискретної (мир/війна) на континуальну категорію, де стан «ні миру, ні війни» стає нормою, а не винятком. Успішність держав у цій новій реальності визначатиметься не лише військовою силою чи економічною потужністю, а здатністю до швидкої адаптації, суспільною згуртованістю та технологічною спроможністю.

2. Держави не можуть розглядати протидію гібридним загрозам як тимчасовий проєкт з визначеним початком і кінцем, а мають інтегрувати її як постійну функцію системи національної безпеки. Держави, що розвинуть ефективні механізми протидії, побудують резильєнтні суспільства з високою медіаграмотністю та критичним мисленням, забезпечать дієву міжнародну координацію, матимуть стратегічну перевагу не лише у відбитті конкретних гібридних атак, а й у довгостроковому геополітичному протиборстві.

3. Україна потребує створення інтегрованого стратегічного документа, що об'єднає всі напрямки протидії гібридним загрозам у єдину систему. Цей документ має містити єдине визначення гібридних загроз, типологію загроз та ризиків, розподіл повноважень між державними органами, механізми координації, систему фінансування та критерії ефективності. Стратегія має бути розрахована на період 2024–2035 років з обов'язковим оглядом кожні три роки для адаптації до еволюції загроз. Це дозволить перейти від фрагментованого реагування на окремі виклики до системного превентивного підходу.

Ключовою інституційною інновацією має стати створення Національного координаційного центру протидії гібридним загрозам як постійно діючого органу при РНБО України. Центр має здійснювати моніторинг гібридних загроз у режимі реального часу, координувати дії державних органів, провадити стратегічне планування, забезпечувати міжнародну співпрацю та функціонувати як ситуаційний центр цілодобово.

Подальші наукові дослідження мають бути спрямовані на підвищення ефективності державних механізмів протидії гібридним загрозам у контексті національної безпеки.

ДОДАТКОВА ІНФОРМАЦІЯ

ВНЕСОК АВТОРІВ: Усі автори зробили внесок порівну.
ФІНАНСУВАННЯ: Автори не отримували фінансування для цього дослідження.
ЗАЯВА ПРО ДОСТУПНІСТЬ ДАНИХ: Не застосовується.
КОНФЛІКТ ІНТЕРЕСІВ: Автори заявляють про відсутність конфлікту інтересів.

Література

1. CERT-UA. (2025). *Звіт про кіберінциденти 2025*. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37 (дата звернення: 27.01.2026).
2. Cordesman A.H., Sullivan W. *Lessons of the 2006 Israeli-Hezbollah War*. Center for Strategic and International Studies. 2007.
3. Russian Disinformation About Ukraine: 2014–2023. Brussels: EU DisinfoLab, 2023.
4. Galeotti M. Russian Political War: Moving Beyond the Hybrid. *Routledge.* 2019.
5. Giles K. Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power. Chatham House, 2016.
6. Glenn R.W. et al. *All Glory Is Fleeting: Insights from the Second Lebanon War*. RAND Corporation, 2009.
7. Hoffman F.G. Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies, 2007.
8. Hoffman F.G. Hybrid Warfare and Challenges. *Joint Force Quarterly.* 2009. 52(1). P. 34–39.
9. Горбулін, В.П. (2017). «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. Київ : НІСД.
10. Ліпкан В.А. Національна безпека України в умовах гібридної війни. Київ : Знання України, 2019.
11. Магда Є.В. Гібридна війна: вижити і перемогти. Київ : Вивчаймо Україну, 2015.
12. McCuen J.J. Hybrid Wars. *Military Review*. 2008. 88(2). P. 107–113.
13. Monaghan A. The 'War' in Russia's 'Hybrid Warfare'. *Parameters.* 2016. 45(4). P. 65–74.
14. NATO Strategic Communications Centre of Excellence. Cognitive Warfare. Riga: NATO StratCom COE, 2020.
15. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. *Farrar, Straus and Giroux*. 2020.
16. Sun Tzu. The Art of War (S.B. Griffith, Trans.). Oxford University Press, 1963. (Original work published ca. 5th century BCE).
17. Власюк О.С., Кононенко С.В. Актуальні проблеми забезпечення національної безпеки України. Київ : НІСД, 2020.
18. Центр протидії дезінформації при РНБО України. Звіти про дезінформаційні кампанії проти України. Київ, 2026. URL: https://cpd.gov.ua/category/reports/ (дата звернення: 27.01.2026).

References

1. CERT-UA. (2025). Report on cyber incidents 2025. State Service of Special Communications and Information Protection of Ukraine. URL: https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37 [in Ukrainian].
2. Cordesman, A.H., & Sullivan, W. (2007). Lessons of the 2006 Israeli-Hezbollah War. Center for Strategic and International Studies.
3. EU DisinfoLab. (2023). Russian Disinformation About Ukraine: 2014–2023. Brussels: EU DisinfoLab.
4. Galeotti, M. (2019). Russian Political War: Moving Beyond the Hybrid. Routledge.
5. Giles, K. (2016). Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power. Chatham House.
6. Glenn, R. W., et al. (2009). *All Glory Is Fleeting: Insights from the Second Lebanon War*. RAND Corporation.
7. Hoffman, F.G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies.
8. Hoffman, F.G. (2009). Hybrid Warfare and Challenges. Joint Force Quarterly, 52(1), 34–39.
9. Gorbulin, V.P. (2017). «Hybrid war» as a key tool of the Russian geostrategy of revenge. Kyiv: NISD [in Ukrainian].
10. Lipkan, V.A. (2019). National security of Ukraine in the conditions of a hybrid war. Kyiv: Knowledge of Ukraine [in Ukrainian].
11. Magda, E.V. (2015). Hybrid warfare: survive and win. Kyiv: Let's study Ukraine [in Ukrainian].
12. McCuen, J.J. (2008). Hybrid Wars. Military Review, 88(2), 107–113.
13. Monaghan, A. (2016). The 'War' in Russia's 'Hybrid Warfare'. Parameters, 45(4), 65–74.
14. NATO Strategic Communications Centre of Excellence. (2020). Cognitive Warfare. Riga: NATO StratCom COE.
15. Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.
16. Sun Tzu. (1963). The Art of War (S.B. Griffith, Trans.). Oxford University Press. (Original work published ca. 5th century BCE).
17. Vlasyuk, O.S., & Kononenko, S.V. (2020). Actual problems of ensuring national security of Ukraine. Kyiv: NISD [in Ukrainian].
18. Center for countering disinformation at the National Security and Defense Council of Ukraine. (2026). Reports on disinformation campaigns against Ukraine. Kyiv. URL: https://cpd.gov.ua/category/reports/ [in Ukrainian].

Дата першого надходження статті до видання: 30.01.2026
Дата прийняття статті до друку після рецензування: 24.02.2026
Дата публікації: 28.02.2026