МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ
КАФЕДРА ВСЕСВІТНЬОЇ ІСТОРІЇ

На правах рукопису

ДАВИДОВ МИКОЛА ІВАНОВИЧ

ГІБРИДНА АГРЕСІЯ РФ ПРОТИ УКРАЇНИ: ДОСВІД ПРОТИДІЇ

Спеціальність: 032 Історія та археологія

Освітньо-професійна програма «Публічна історія»

Робота на здобуття освітнього ступеня «Магістр»

Науковий керівник:

Стрільчук Людмила Василівна

Завідувач кафедри всесвітньої історії,

доктор історичних наук, професор

РЕКОМЕНДОВАНО ДО ЗАХИСТУ

Протокол № _____

засідання кафедри всесвітньої історії

від _____ 2025 р.

Завідувач кафедри

(_____) Стрільчук Л. В.

Луцьк – 2025

Анотація

Давидов М. Гібридна агресія РФ проти України: Досвід протидії: дипломна робота магістра. Луцьк: Волин. нац. ун-т ім. Лесі Українки, 2025. 188 с.

Дипломна робота присвячена комплексному аналізу феномену гібридної агресії Російської Федерації проти України в період з 2014 – 2025 років та узагальненню досвіду протидії їй. У дослідженні проаналізовано трансформацію сучасних конфліктів, де поєднуються військові, інформаційні, економічні, кібернетичні та дипломатичні інструменти, вивчено механізми гібридної агресії РФ та сформульовано рекомендації для посилення національної стійкості України та оптимізації протидії гібридній агресії.

У сучасному світі, коли методи традиційної війни тісно поєднуються із гібридною агресією надважливим завдання постає не просто вміння вчасно розпізнати форми та методи гібридних загроз, але випрацювати оптимальні методи реагування на неї: виявлення, протидію, дію на випередження. Саме тому, досліджувана у магістерській роботі наукова проблема є актуальною, важливою та має практичне значення.

Теоретичну основу магістерської роботи складають фундаментальні праці Ф. Гофмана, В. Лінда, М. ван Кревельда. Джерельною базою стали заяви українського та російського МЗС, провідних політиків, військових, зокрема російських військових В. Герасимова та В. Горбуліна. Важливими узагальнюючими працями на які опирається робота стали наукові розробки Є. Магди, О. Литвиненка. Емпірична база: звіти ISW, RUSI, Atlantic Council, Hybrid CoE; документи НАТО, ООН, ЄС, ОБСЄ; OSINT-розслідування (Bellingcat, InformNapalm, Детектор медіа); статистичні дані (KSE, Світовий банк, МВФ); соціологічні опитування (КМІС, Центр Разумкова).

Магістерська робота побудована за проблемно-хронологічним принципом, використано міждисциплінарний підхід із залученням історико-генетичного,

компаративного, системно-структурного, кейс-стаді, контент-аналізу, статистичного та юридико-догматичного методів.

У представленій роботі узагальнено досвід протидії російській гібридній агресії в умовах повномасштабної війни (2022 – 2025 рр.), здійснено аналіз еволюції співвідношення військових/невійськових компонентів стратегії РФ (від 3:2 до 2:3), проведено комплексний розгляд феномену «народного ВПК» як моделі інтеграції громадянського суспільства, систематизовано уроки української моделі для глобальної безпеки.

В результаті проведеного дослідження розроблено практичні рекомендації для національної стратегії безпеки України, освітніх програм з медіаграмотності та кібербезпеки, міжнародних організацій. Результати апробовано на переддипломному захисті та XV Буковинській міжнародній історико-краєзнавчій конференції.

Ключові слова: гібридна агресія, Російська Федерація, Україна, протидія, гібридна війна, анексія Криму, повномасштабне вторгнення, дезінформація, кібератаки, економічний тиск, НАТО, ЄС, ОБСЄ, Герасимов, Гофман, Горбулін, OSINT, штучний інтелект.

Abstract.

Davydov M. Hybrid Aggression of the Russian Federation against Ukraine: Experience in Countering It: Master's Thesis. Lutsk: Volyn, National University named after Lesya Ukrainka, 2025. 188 p.

The master's thesis is dedicated to a comprehensive analysis of the phenomenon of hybrid aggression by the Russian Federation against Ukraine during the period from 2014 to 2025 and to summarizing the experience of countering it. The study analyzes the transformation of modern conflicts, where military, informational, economic, cybernetic, and diplomatic tools are combined; examines the mechanisms of the Russian Federation's hybrid aggression; and formulates recommendations for strengthening Ukraine's national resilience and optimizing countermeasures against hybrid aggression.

In the modern world, where methods of traditional warfare are closely intertwined with hybrid aggression, a critically important task is not only the ability to timely recognize the forms and methods of hybrid threats but also to develop optimal methods of responding to them: detection, counteraction, and preemptive action. Therefore, the scientific problem investigated in the master's thesis is relevant, important, and has practical significance.

The theoretical foundation of the master's thesis consists of fundamental works by F. Hoffman, W. Lind, and M. van Creveld. The source base includes statements from the Ukrainian and Russian Ministries of Foreign Affairs, leading politicians, and military figures, including Russian military officials V. Gerasimov and V. Horbulin. Important synthesizing works on which the thesis relies are the scientific developments of E. Mahda and O. Lytvynenko. The empirical base comprises reports from ISW, RUSI, Atlantic Council, and Hybrid CoE; documents from NATO, UN, EU, and OSCE; OSINT investigations (Bellingcat, InformNapalm, Detector Media); statistical data (KSE, World Bank, IMF); and sociological surveys (KMIS, Razumkov Center).

The master's thesis is structured according to a problem-chronological principle and employs an interdisciplinary approach, incorporating historical-genetic, comparative, systemic-structural, case-study, content-analysis, statistical, and juridical-dogmatic methods.

In the presented work, the experience of countering Russian hybrid aggression during the full-scale war (2022 – 2025) is generalized; an analysis of the evolution of the ratio of military/non-military components in the Russian Federation's strategy (from 3:2 to 2:3) is conducted; a comprehensive examination of the phenomenon of the "people's military-industrial complex" as a model for integrating civil society is provided; and lessons from the Ukrainian model for global security are systematized.

As a result of the research, practical recommendations have been developed for Ukraine's national security strategy, educational programs on media literacy and cybersecurity, and international organizations. The results were tested at the pre-diploma defense and the XV Bukovynian International Historical-Local History Conference.

Keywords: hybrid aggression, Russian Federation, Ukraine, counteraction, hybrid war, annexation of Crimea, full-scale invasion, disinformation, cyberattacks, economic pressure, NATO, EU, OSCE, Gerasimov, Hoffman, Horbulin, OSINT, artificial intelligence.

Зміст

ВСТУП

Актуальність теми: У сучасному світі, де традиційні форми збройних конфліктів поступово трансформуються під впливом глобалізації, технологічного прогресу та геополітичних змін, феномен гібридної агресії набуває особливого значення. Гібридна війна, як комплексне поєднання військових, інформаційних, економічних, кібернетичних та дипломатичних інструментів, стала потужним засобом досягнення стратегічних цілей без прямого оголошення війни. Особливо яскраво це проявилося в агресії Російської Федерації проти України, яка розпочалася у 2014 році з анексії Криму та конфлікту на Донбасі, а ескалувала до повномасштабного вторгнення у 2022 році.

Ця агресія не лише підірвала суверенітет України, але й поставила під загрозу європейську безпеку, Вестфальську систему міжнародних відносин та принципи міжнародного права. Досвід протидії гібридній агресії РФ є унікальним кейсом для вивчення, оскільки Україна, попри обмежені ресурси, продемонструвала ефективні механізми стійкості, включаючи суспільну мобілізацію, цифрову трансформацію та міжнародну кооперацію. Аналіз цього досвіду дозволяє не тільки осмислити минулі помилки, але й сформувати рекомендації для інших держав, які стикаються з подібними загрозами від авторитарних режимів.

У контексті триваючого конфлікту (станом на 2025 рік), тема набуває критичної актуальності, оскільки гібридні елементи від дезінформації та кібератак до економічного тиску, продовжують домінувати навіть на тлі конвенційних бойових дій. Розуміння механізмів гібридної агресії та ефективних стратегій протидії стає життєво важливим не лише для України, але й для всього демократичного світу.

Мета дослідження: здійснити комплексний аналіз гібридної агресії Російської Федерації проти України та узагальнити досвід протидії їй з метою розробки

рекомендацій для посилення національної стійкості та формування ефективних механізмів захисту від гібридних загроз.

Завдання дослідження: Проаналізувати стан наукової розробки проблеми, включаючи історіографію еволюції концепції гібридної війни від перших теоретичних напрацювань до сучасних досліджень. – Визначити ключові компоненти гібридної агресії РФ, базуючись на історичних прецедентах (від Чеченських війн до подій в Україні) та теоретичних розробках провідних дослідників. – Оцінити ефективність українських та міжнародних заходів протидії в період з 2014 по 2025 рік, з акцентом на інформаційну, кібернетичну, військову та економічну сфери. – Виявити уроки для глобальної безпеки, включаючи роль НАТО, ЄС та ОБСЄ у формуванні стратегій супротиву та протидії гібридним загрозам. – Розробити практичні рекомендації для України щодо адаптації до еволюціонуючих гібридних загроз, з урахуванням нових технологій (штучний інтелект, діпфейки тощо).

Об'єкт дослідження: гібридна агресія як феномен сучасних міжнародних відносин, що поєднує військові, інформаційні, економічні, кібернетичні та дипломатичні інструменти впливу.

Предмет дослідження: досвід протидії гібридній агресії РФ проти України в період 2014-2025 років, включаючи інституційні, правові, військові, технологічні та суспільні механізми опору.

Хронологічні межі дослідження: охоплюють період з 2014 року (початок анексії Криму та конфлікту на Донбасі) до грудня 2025 року, що дозволяє простежити еволюцію гібридної агресії від початкових форм до повномасштабної війни та адаптацію механізмів протидії.

Територіальні межі: дослідження включають територію України в межах міжнародно визнаних кордонів, з особливою увагою до Криму, Донбасу та інших регіонів, що зазнали прямого впливу гібридної агресії, а також міжнародний контекст реагування на цю агресію.

Теоретичну основу роботи: становлять праці ключових теоретиків гібридної війни, таких як Ф. Гофман, В. Лінд, М. ван Кревельд, В. Герасимов, а також українські дослідники, В. Горбулін, Є. Магда, О. Литвиненко, які внесли значний вклад у розуміння специфіки російської гібридної агресії проти України.

Емпірична база: дослідження включає звіти провідних аналітичних центрів (Institute for the Study of War, Royal United Services Institute, Atlantic Council, European Centre of Excellence for Countering Hybrid Threats), документи міжнародних організацій (НАТО, ООН, ЄС, ОБСЄ), OSINT-розслідування (Bellingcat, InformNapalm, Детектор медіа), статистичні дані про економічні наслідки війни (Kyiv School of Economics, Світовий банк, МВФ) та соціологічні опитування (Київський міжнародний інститут соціології, Центр Разумкова).

Методологія дослідження: базується на міждисциплінарному підході, що поєднує такі методи дослідження, як історико-генетичний метод для аналізу еволюції теорії гібридної війни; компаративний метод для порівняння різних етапів конфлікту та моделей протидії; системно-структурний метод для аналізу компонентів агресії; метод кейс-стаді для вивчення ключових епізодів; контент-аналіз для дослідження інформаційних операцій; статистичний метод для оцінки ефективності протидії; юридико-догматичний метод для інтерпретації міжнародного права.

Наукова новизна: дослідження полягає в узагальненні досвіду протидії гібридній агресії в умовах повномасштабної війни (2022-2025 рр.), з акцентом на роль суспільної стійкості та технологічних інновацій. Робота доповнює існуючі дослідження аналізом еволюції співвідношення військових та невійськових компонентів російської стратегії (від 3:2 у 2014-2022 до 2:3 після 2022 року), що спростовує спрощені інтерпретації «доктрини Герасимова». Вперше комплексно проаналізовано феномен українського «народного ВПК» як унікальної моделі інтеграції громадянського суспільства в національну оборону, а також систематизовано уроки української моделі протидії для глобальної безпеки.

Практичне значення: полягає в можливості використання її результатів для вдосконалення національної стратегії безпеки України, розробки освітніх програм з медіаграмотності та кібербезпеки, формування рекомендацій для міжнародних організацій щодо протидії гібридним загрозам. Матеріали дослідження можуть бути корисними для аналітичних центрів, освітніх закладів та країн-партнерів України, які формують власні стратегії протидії гібридним загрозам.

Апробація результатів дослідження: Магістерська робота пройшла апробацію шляхом обговорення її основних положень на засіданнях кафедри всесвітньої історії Волинського національного університету імені лесі Українки у межах перддипломної практики, а також під час виступу на XV Буковинській Міжнародній історико-краєзнавчій конференції (17 – 18 жовтня 2025 р.) та публікацією тез. Зокрема, автором було опубліковано тези на тему: «Гібридна агресія РФ проти України, історичний континуум війни, окупації та спротиву», які розміщенні у вільному доступі.

Структура роботи: зумовлена її метою та науковими завданнями. Дослідження складається зі вступу, чотирьох розділів та 12 підрозділів, висновку, списку використаних джерел та літератури, що складається з 250 позицій. На початку роботи вміщено анотацію українською та англійською мовами. Текст роботи викладений на 188 сторінках із яких 143 сторінок основного тексту.

РОЗДІЛ 1. СТАН НАУКОВОЇ РОЗРОБКИ ТА МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

1.1. Історіографія проблеми

Наукове осмислення феномену гібридної агресії пройшло складний еволюційний шлях від розрізнених концептуальних напрацювань до комплексної міждисциплінарної теорії. Аналіз літератури дозволяє виділити три основні періоди розвитку наукової думки щодо гібридних загроз, кожен з яких характеризується специфічними дослідницькими підходами та пріоритетами[115; 116; 105].

Перший період: становлення теоретичних основ (до 2014 року)[64; 107].

Інтелектуальні витоки сучасної теорії гібридної війни сягають кінця XX століття, коли дослідники почали фіксувати фундаментальну трансформацію характеру збройних конфліктів[146; 232]. Концептуальний фундамент було закладено групою американських теоретиків, які незалежно один від одного прийшли до висновку про якісну зміну парадигми воєнного протиборства[147; 233].

Вільям Лінд у новаторській статті «Зміна обличчя війни: у четверте покоління» (1989) сформулював концепцію війни четвертого покоління (4GW), яка характеризується розмиванням меж між війною та політикою, збройними силами та цивільним населенням, фронтом та тилом[146]. Лінд передбачив, що майбутні конфлікти виходитимуть за межі класичних міждержавних протистоянь та включатимуть широкий спектр недержавних акторів, використовуючи асиметричні методи боротьби[147].

Мартін ван Кревельд у фундаментальній праці «Трансформація війни» (1991) теоретично обґрунтував перехід від міждержавних конфліктів до багаторівневих протистоянь з участю недержавних акторів[232]. Його роботи стали основою для розуміння гібридних загроз як системного явища, що виходить за межі традиційного військового протиборства[233]

Паралельно формувалося осмислення кібернетичного виміру сучасних конфліктів[60; 81]. Джон Арквілла та Девід Ронфельдт у роботі «Кібервійна йде!» (1993) розробили концепцію «мережевої війни» (netwar), яка передбачала використання інформаційних технологій для досягнення стратегічних цілей без традиційного військового протиборства[60]. Річард Кларк у книзі «Кібервійна» (2010) попереджав, що кіберпростір стане новим полем битви, де держави зможуть завдавати критичної шкоди інфраструктурі противника без фізичного вторгнення[81].

Мері Калдор у праці «Нові і старі війни» (2012) запропонувала концепцію «нових воєн», де контроль над населенням та його свідомістю виявляється важливішим за захоплення території[135]. Калдор звернула увагу на зміщення акцентів у сучасних конфліктах від військових операцій до впливу на цивільне населення та соціальну структуру суспільства[135].

Концептуальний прорив здійснив американський дослідник Френк Гофман, у фундаментальній статті «Conflict in the 21st Century: The Rise of Hybrid Wars» (2007), де вперше комплексно сформулював теорію гібридної війни[115]. Гофман визначив її як поєднання різних режимів війни, включаючи конвенційні заходи, нерегулярну тактику, терористичні акти та кримінальну поведінку в міжнародному просторі, спрямовану на досягнення політичних цілей й розвинув цю думку в вже своїй книзі того ж року[115]. Він виділив чотири ключові характеристики гібридних конфліктів: комбінування різних типів військових дій, участь недержавних акторів поряд з державними структурами, координованість різних інструментів впливу та використання сучасних технологій[115; 116]. Важливим внеском Гофмана стало розуміння, що гібридна війна є не простою набором різних методів, а якісно новим типом конфлікту, що вимагає принципово нових підходів до національної оборони[115].

Паралельно в Російській Федерації формувалася власна концепція «війни нового покоління», що спиралася на традиції радянської військової думки – концепції «активних заходів», «маскування» та рефлексивного управління[64; 105; 107].

Ключовим документом став аналітичний матеріал начальника Генерального

штабу Збройних Сил РФ Валерія Герасимова «Цінність науки в передбаченні» (2013), який обґрунтував нову стратегію з акцентом на невійськових методах впливу[107]. Герасимов звернув увагу на досвід «арабської весни», де невійськові методи виявилися ефективнішими за пряму конфронтацію[107]. Британський аналітик Марк Галеотті у 2014 році запропонував інтерпретацію цієї статті як «доктрини Герасимова» з акцентом на співвідношення невійськових до військових засобів 4:1, що стало широко цитованою формулою в західній науковій літературі[107].

Критично важливим для розуміння еволюції російської гібридної стратегії є аналіз російсько-чеченських воєн (1994-1996 та 1999-2009)[151; 155]. Хоча більшість західних дослідників (Ф. Гофман, RUSI, Hybrid CoE) вважають російсько-грузинську війну 2008 року першим «класичним» кейсом гібридної війни XXI століття[61; 115; 123; 125], але аналізуючи набір методичних підходів РФ до війни можна зазначити, що чеченські кампанії вже містили ключові елементи гібридної агресії: використання «непозначених» сил, залучення проксі-формувань, інформаційну війну, економічний тиск та рефлексивне управління[151; 155].

Проте саме російсько-грузинська війна у серпні 2008 року привернула системну увагу західної наукової спільноти до феномену гібридної війни[61; 136]. Конфлікт включав провокації в Південній Осетії, масштабні DDoS-атаки на урядові сайти Грузії, координовану інформаційну війну та швидку військову операцію з використанням регулярних військ[61; 136]. Дослідники відзначили неготовність західних держав до адекватного реагування на гібридні загрози та відсутність чіткої міжнародно-правової кваліфікації таких дій, що стало каталізатором для подальшого наукового осмислення проблеми[61; 74; 123].

Другий період: реакція наукової спільноти на події в Україні (2014-2021): Агресія РФ проти України, що розпочалася у 2014 році, стала переломним моментом у розвитку теорії гібридної війни, трансформувавши її з теоретичного концепту в актуальну проблему міжнародної безпеки, що вимагала негайної наукової рефлексії[4; 5; 10; 19; 41; 105; 175; 185].

Аналітичні центри НАТО швидко відреагували на нові виклики[85; 156; 238]. Королівський об'єднаний інститут оборонних досліджень (RUSI) опублікував серію досліджень, присвячених аналізу взаємозв’язку різнорідних методів гібридної війни та їхньої ефективності у випадках, коли відкрита війна є політично неприйнятною[125; 168]. Дослідники RUSI звернули особливу увагу на маскування агресії під «гуманітарні» або «миротворчі» операції, що ускладнює своєчасну ідентифікацію джерела загрози[125].

Центр стратегічних та міжнародних досліджень (CSIS) зосередився на аналізі часових параметрів міжнародної реакції на гібридну агресію, виявивши критичну проблему затримки реагування міжнародних організацій[74; 117].

У 2016 році за ініціативою Європейського Союзу було створено Європейський центр досліджень гібридних загроз (Hybrid CoE) у Гельсінкі, який став провідною науково-аналітичною платформою для систематичного вивчення гібридних загроз[123]. Центр розробив класифікацію компонентів гібридної агресії, згрупувавши їх у п'ять категорій: військові, інформаційні, кібернетичні, економічні та дипломатичні інструменти[123; 207]. Hybrid CoE також започаткував систематичний моніторинг дезінформаційних кампаній через створену EU East StratCom Task Force[101; 123].

NATO Cooperative Cyber Defence Centre of Excellence зосередився на кібернетичному вимірі гібридних загроз, розробивши класифікацію кібероперацій на три категорії: шпигунські, деструктивні та операції впливу[154; 199]. Результатом багаторічної роботи експертів став Таллінський посібник 2.0 (2017) – спроба адаптувати міжнародне право до реалій кібервійни, що базувалася на аналізі конкретних кейсів[199; 200].

Оксфордський інститут інтернету провів серію досліджень інформаційних операцій у контексті гібридних конфліктів, аналізуючи швидкість поширення дезінформації та масштаби охоплення цільових аудиторій[70; 71]. Особлива увага приділялася вивченню діяльності структур, що систематично генерують дезінформацію, зокрема «Агенції інтернет-досліджень» (Internet Research Agency)[70].

Важливий внесок у розуміння економічного виміру гібридної агресії зробили Міжнародний валютний фонд та Світовий банк, які провели аналіз економічних наслідків гібридних конфліктів[87; 127; 231]. Світовий банк виявив, що гібридні конфлікти призводять до більш тривалого економічного спаду порівняно з традиційними війнами[87; 231]. Національний інститут стратегічних досліджень України здійснив оцінку прямих економічних втрат від російської агресії[1; 8].

Українські дослідники зробили особливий внесок у розуміння специфіки російської гібридної агресії[4; 5; 10; 19; 41]. Євген Магда у своїх працях розробив концепцію комплексного використання всіх доступних засобів для дестабілізації держави-жертви, поглиблення внутрішньополітичних криз та підриву її міжнародних позицій[19]. Максим Гончар зосередився на аналізі енергетичного виміру гібридної війни, досліджуючи механізми використання енергетичної залежності як інструменту політичного тиску.

Визначний внесок у розвиток вітчизняної теорії гібридної агресії зробили українські дослідники та практики, які ще до офіційного визнання терміну на рівні НАТО почали використовувати поняття «гібридна війна» та «гібридна агресія»[10; 41]. Першим системне наукове осмислення феномену здійснив Володимир Горбулін, який у монографіях «Гібридна війна: quo vadis?» (2015), «Гібридна війна. Все тільки починається…» (2017) та «Війна майбутнього: на порозі гібридної епохи» (2020) обґрунтував тезу про те, що РФ веде проти України комплексну гібридну агресію, яка охоплює всі сфери державно-суспільного життя[10; 41].

У 2017 році колектив авторів під керівництвом Олександра Литвиненка (за участі Д. Дубовик, В. Горбуліна, І. Смешка та ін.) опублікував фундаментальну працю «Гібридна війна: від Стародубської війни до сьогодні», в якій простежено історичну тяглість російських гібридних стратегій від XVII століття до сучасності та доведено, що події 2014 року є не новим феноменом, а продовженням багатовікової традиції[4].

Саме в українському експертному та політичному дискурсі термін «гібридна агресія» почав активно вживатися ще у 2014-2015 роках завдяки І. Смешку, О.

Скіпальському та Є. Марчуку, які у численних виступах, аналітичних записках і телевізійних коментарях використовували це поняття раніше, ніж воно з'явилося в офіційних документах НАТО (2015-2016)[10; 41]. Таким чином, українські дослідники не лише реагували на агресію, а й значною мірою формували сучасне розуміння гібридної війни, випереджаючи західні аналітичні центри в термінологічному та концептуальному плані[5; 19; 41].

Організації OSINT (Open Source Intelligence), зокрема Bellingcat, революціонізували методологію документування військової присутності та участі недержавних акторів у конфліктах, використовуючи відкриті джерела інформації[65; 169]. Їхні розслідування стали важливою доказовою базою для наукових досліджень[65].

Офіс Верховного комісара ООН з прав людини систематично документував характер конфлікту на Донбасі, аналізуючи співвідношення місцевих та зовнішніх акторів, механізми вербування та підтримки збройних формувань, що дозволило дослідникам краще зрозуміти феномен «правдоподібного заперечення» (plausible deniability)[173].

Громадська організація «Детектор медіа» провела систематичний моніторинг інформаційних операцій, каталогізувавши стійкі фейкові наративи та аналізуючи механізми їхнього поширення[91]. Це дослідження стало важливим внеском у розуміння психологічного виміру гібридної війни[91].

Chatham House та інші провідні міжнародні аналітичні центри звернули увагу на фундаментальний виклик, який гібридна агресія становить для Вестфальської системи міжнародних відносин, аналізуючи підрив основних принципів: державного суверенітету, територіальної цілісності та невтручання у внутрішні справи[154; 222]. Особлива увага приділялася проблемі паралічу Ради Безпеки ООН через право вето постійних членів[154].

У відповідь на нові виклики країни Балтії та Скандинавії розробили концепцію «всеохоплюючої оборони» (comprehensive defence), що передбачає інтеграцію

військових, цивільних, економічних та інформаційних ресурсів[122; 85]. Дослідники цих країн особливу увагу приділили розвитку суспільної стійкості (resilience) та медіаграмотності населення як ключових факторів протидії гібридним загрозам[66; 122].

НАТО у 2015 році прийняла Стратегію проти гібридних загроз, що стало інституційною відповіддю Альянсу на еволюцію загроз[85; 243]. Наукові центри НАТО розробили комплексний підхід до протидії, що поєднував військові, політичні та інформаційні компоненти[85; 156].

Pew Research Center провів серію досліджень впливу гібридної агресії на довіру до державних інститутів та соціальну згуртованість у країнах-жертвах. Дослідники виявили феномен «п'ятої колони» та проаналізували механізми, через які частина населення свідомо чи несвідомо сприяє агресору.

Третій період: переосмислення після повномасштабного вторгнення (2022-2025): Цей період характеризується інтенсивною науковою рефлексією над поєднанням масштабної конвенційної війни з продовженням гібридних операцій, а також аналізом уроків для глобальної безпеки[122; 178; 185]. Дослідники звернули особливу увагу на концепцію суспільної стійкості (resilience) як ключового фактору успіху у протидії гібридній агресії[66; 122].

Значний внесок у моніторинг еволюції гібридної агресії РФ зробив Інститут вивчення війни (ISW), який з 2022 року публікує щоденні звіти «Russian Offensive Campaign Assessment» (2022-2025), де детально аналізуються гібридні елементи конфлікту, включаючи дезінформацію, кібератаки та використання проксі-формувань на тлі конвенційних операцій[145; 181]. Ці звіти, базовані на OSINT-даних, стали ключовим джерелом для оцінки адаптивності стратегії РФ та її впливу на європейську безпеку, зокрема в доповіді від жовтня 2025 р. про довгострокові гібридні загрози в Європі[181].

Атлантична рада (Atlantic Council) у серії публікацій «Ukraine’s Hybrid War Resilience» (2023-2025) систематизувала український досвід протидії гібридним

загрозам, акцентуючи на цифровій трансформації та медіаграмотності як інструментах стійкості[159]. Зокрема, доповідь від червня 2025 р. «Russian Hybrid Warfare: Ukraine's Success Offers Lessons for Europe» підкреслює, як Україна з 2018 по 2025 р. піднялася з 102-го на 5-е місце в глобальному рейтингу онлайн-послуг ООН, демонструючи ефективність контрзаходів проти кібернетичних та інформаційних атак[141; 159].

Королівський об'єднаний інститут оборонних досліджень (RUSI) у звіті «Lessons from Ukraine’s Hybrid War» (2024) проаналізував уроки з українського досвіду для протидії гібридним конфліктам, зокрема роль «активної оборони» та інтеграції цивільних ресурсів у військові стратегії[125; 168]. Автори наголошують на необхідності «цілісної координації» інформації та кінетичних операцій для протидії гібридним кампаніям РФ у Європі, включаючи рекомендації щодо посилення санкцій та протидії «п'ятої колоні»[125].

Вітчизняні аналітичні центри також активно реагують на виклики. Центр оборонних стратегій (Київ) у щорічних звітах «Щоденний брифінг: Війна РФ проти України» (2023, 2024, 2025) документує гібридні аспекти конфлікту, фокусуючись на кіберзагрозах, інформаційних операціях та логістичних викликах. Звіт за 2025 р. пропонує стратегію «активної оборони» для підготовки до контрнаступу, підкреслюючи роль волонтерських мереж і диверсифікації ресурсів як ключових елементів resilience.

Національний інститут стратегічних досліджень (Україна) у спеціальному випуску журналу «Стратегічна панорама» за 2024 р. «Гібридна агресія 3.0: Нова фаза російського наступу та демократичний мир» (ред. В. Горбулін) переосмислив гібридну війну як еволюційний процес, що включає аспекти маніпуляція знаннями та ядерне стримування НАТО[1; 8; 10]. Випуск містить статті про використання ШІ в дезінформації та рекомендації для Європи щодо протидії «гібридній ескалації» РФ[10]. Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) опублікувала дослідження, присвячені систематизації кіберзагроз та еволюції методів кібератак[14; 43; 89].

Аналітики зосередилися на зміні інтенсивності та характеру атак після початку повномасштабного вторгнення[14; 89]. Особливу увагу дослідники приділили новим технологічним загрозам, зокрема використанню штучного інтелекту та синтетичних медіа (діпфейків) як інструментів гібридної війни[45; 75]. Міжнародний інститут стратегічних досліджень (IISS) опублікував прогнози щодо ролі штучного інтелекту у майбутніх гібридних конфліктах та необхідності розвитку технологій розпізнавання фальсифікацій[75].

Важливим напрямком досліджень стала еволюція співвідношення військових та невійськових компонентів у гібридній агресії[64; 105; 107; 109; 248]. Дослідники переосмислили спрощене трактування «доктрини Герасимова», аналізуючи адаптивний характер російської стратегії та збереження гібридних елементів навіть в умовах домінування військової складової[64; 107; 152].

Геополітичні наслідки вторгнення в Україну стали предметом досліджень провідних аналітичних центрів[74; 156; 159]. Аналізувалася трансформація безпекової архітектури Європи, зокрема рішення Фінляндії та Швеції приєднатися до НАТО після багаторічної політики військового нейтралітету[156; 238]. Створення у 2025 році NATO Security Assistance and Training for Ukraine (NSATU) стало предметом наукового осмислення як нова форма інституціоналізації підтримки[156].

Дослідження цього періоду внесли значний вклад у розвиток міжнародного права у сфері кібербезпеки[89; 154; 199]. Науковці аналізували можливості кваліфікації кібероперацій у міжнародному праві та визначення порогів, за якими кібератаки можуть розглядатися як акти агресії[154; 199; 200].

Особлива увага приділялася обмеженням міжнародно-правових механізмів протидії гібридній агресії в умовах, коли держава-агресор є постійним членом Ради Безпеки ООН[93; 161; 162]. Дослідники аналізували альтернативні механізми, включаючи посилену роль Генеральної Асамблеї ООН, застосування Moscow Mechanism ОБСЄ та звернення до Міжнародного суду[161; 162; 176].

Санкційна політика безпрецедентного масштабу стала предметом численних економічних досліджень[87; 127; 212]. Аналізувалася її ефективність, механізми обходу та довгострокові наслідки для глобальної економіки[87; 127]. Дослідники зосередилися на питаннях диверсифікації економічних зв'язків та зменшення енергетичної залежності як факторів економічної стійкості[9; 16; 99].

Сучасні дослідження все більше зосереджуються на адаптивному характері як самої гібридної агресії, так і методів протидії їй[117; 122; 178; 185]. Аналізується постійна еволюція архітектури гібридної агресії, включення нових технологій та методів впливу[75; 89; 113]. Український досвід формування моделі протидії в реальному часі став предметом детального вивчення з акцентом на важливості гнучкості та здатності до швидкої адаптації[66; 122; 168].

Аналіз наукової літератури дозволяє виділити декілька основних дослідницьких підходів до вивчення гібридної агресії:

1. Військово-стратегічний підхід (Гофман, Герасимов, RUSI) зосереджується на військово-технічних аспектах гібридної війни, аналізує поєднання конвенційних та неконвенційних методів ведення бойових дій, координацію різних інструментів впливу[64; 105; 107; 115; 116; 125; 168].
2. Інформаційно-комунікативний підхід (Оксфордський інститут інтернету, EU East StratCom, Детектор медіа) досліджує механізми інформаційних операцій, пропаганди та дезінформації як ключових компонентів гібридної агресії, аналізує швидкість поширення та масштаби охоплення[70; 71; 91; 101].
3. Кібернетично-технологічний підхід (NATO CCD COE, ДССЗЗІ, IISS) аналізує роль кібератак та цифрових технологій у сучасних гібридних конфліктах, класифікує типи кібероперацій та прогнозує вплив штучного інтелекту[14; 43; 89; 154; 199; 200].
4. Економіко-політичний підхід (МВФ, Світовий банк, CSIS, Національний інститут стратегічних досліджень) вивчає економічні інструменти гібридної війни,

їхній вплив на держави-жертви та тривалість економічних наслідків[1; 8; 74; 87; 127; 231].

5. Міжнародно-правовий підхід (Chatham House, ООН, Таллінський посібник) досліджує виклики, які гібридна агресія становить для міжнародного права та системи колективної безпеки, аналізує обмеження існуючих механізмів[93; 154; 161; 162; 173; 199; 200].
6. Соціально-психологічний підхід (Pew Research Center, Київський міжнародний інститут соціології, країни Балтії) аналізує вплив гібридної агресії на суспільну свідомість, довіру до інститутів, соціальну стійкість та роль медіаграмотності[11; 12; 23; 66; 122].
7. Комплексний підхід до протидії (Hybrid CoE, концепція comprehensive defence) інтегрує військові, цивільні, економічні та інформаційні ресурси для всеохоплюючої оборони[85; 123; 207; 122].

Історіографія проблеми демонструє поступову еволюцію від теоретичних концептів кінця XX століття до комплексного міждисциплінарного розуміння феномену[105; 115; 122; 178]. Кожен період характеризується поглибленням розуміння механізмів гібридної агресії, розширенням емпіричної бази досліджень та розробкою нових підходів до протидії[4; 5; 10; 19; 41; 122; 185]. Український досвід став потужним каталізатором для переосмислення безпекових концепцій та стимулював розвиток нових напрямків досліджень у сферах кібербезпеки, інформаційної війни, суспільної стійкості та міжнародного права[66; 122; 168; 178].

Попри значний прогрес, у сучасній історіографії все ще недостатньо досліджено довгострокові соціально-психологічні наслідки гібридної агресії, порівняльний аналіз ефективності санкційних режимів різних хвиль, а також інституційні механізми протидії гібридним загрозам у країнах, що не є членами НАТО[87; 127; 212; 122].

1.2. Джерельна база та методологія дослідження

Джерельна база дослідження становить основу для комплексного аналізу гібридної агресії РФ проти України у період 2014-2025 років та досвіду протидії їй[4; 5; 10; 19; 41; 122; 178; 185]. Вона охоплює 250 позицій літератури, що були зібрані з метою забезпечення репрезентативності, достовірності та всебічного висвітлення теми. Джерела відібрано за критеріями актуальності, наукової обґрунтованості та доступності, з акцентом на офіційні документи, аналітичні звіти та емпіричні дані, які дозволяють простежити еволюцію конфлікту від анексії Криму до повномасштабного вторгнення[65; 136; 169; 173; 176]. Особлива увага приділена джерелам, що фіксують трансформацію російських гібридних стратегій (військові, інформаційні, кібер-, економічні) та українські механізми протидії, включаючи роль громадянського суспільства та міжнародної спільноти[14; 66; 85; 89; 122; 156; 207].

Для забезпечення об'єктивності джерельна база включає матеріали як з українських, так і з міжнародних джерел, уникаючи упередженості[1; 8; 70; 71; 123; 199]. Наприклад, звіти міжнародних організацій (ООН, НАТО, ЄС, ОБСЄ) надають юридичну та фактичну базу для оцінки агресії[161; 162; 173; 176; 238], тоді як OSINT-розслідування (Bellingcat, InformNapalm) доповнюють емпіричними доказами[65; 169]. Статистичні дані (від KSE, Світового банку, КМІС) дозволяють кількісно оцінити економічні та соціальні наслідки[11; 12; 87; 94; 127; 231]. Загалом, джерела охоплюють період до грудня 2025 року, що робить аналіз актуальним і враховує останні події, такі як продовження санкцій та еволюція кіберзагроз[14; 43; 89; 212]. Дублікати в списку (наприклад, повторні посилання на праці Van Creveld чи Kaldor) були очищені для уникнення надмірності, а нумерація збережена за оригіналом для зручності цитування[135; 232; 233].

Джерела класифіковано за типами для полегшення навігації: від нормативних актів до електронних ресурсів. Це дозволяє систематично використовувати їх у дослідженні, наприклад, нормативні документи для правового аналізу, а аналітичні

звіти для оцінки ефективності протидії. Достовірність забезпечується перевіреними джерелами (наприклад, офіційні сайти ООН, НАТО), а доступність через URL та DOI. У разі обмеженого доступу (наприклад, до деяких звітів РФ) використано альтернативні архіви або цитати з вторинних джерел.

1) Нормативно-правові акти України та міжнародні договори - Ця група включає закони, укази та міжнародні угоди, що регулюють протидію агресії, санкції та мобілізацію. Вони становлять правову основу дослідження.
2) Закон України «Про волонтерську діяльність» від 05.12.2012 № 5393-VI (в редакції 2022 р.). Відомості Верховної Ради України. 2013. № 13. Ст. 99[27].
3) Закон України «Про громадські об’єднання» від 22.03.2012 № 4572-VI (в редакції 2022 р.). Відомості Верховної Ради України. 2012. № 34. Ст. 393[28].
4) Закон України «Про забезпечення функціонування української мови як державної» від 25.04.2019 № 2704-VIII. Відомості Верховної Ради України. 2019. № 31. Ст. 340[30].
5) Закон України від 11.04.2024 № 3633-IX «Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку». Відомості Верховної Ради України. 2024. № 15. Ст. 567[26].
6) Указ Президента України від 15.05.2017 № 315/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» (блокування VKontakte, Odnoklasnyky, Yandeks та ін.)[38].
7) Указ Президента України від 24.02.2022 № 65/2022 «Про введення воєнного стану в Україні». Офіційний вісник України. 2022. № 17. Ст. 567[31].
8) Угода про чорноморський гуманітарний коридор для експорту зерна з України (Чорноморська зернова ініціатива) : укладена 22.07.2022 у м. Стамбулі. URL: https://www.un.org/en/black-sea-grain-initiative[47].

9) Меморандум про гарантії безпеки у зв’язку з приєднанням України до Договору про нерозповсюдження ядерної зброї (Будапештський меморандум) : підписаний 05.12.1994[20].

10) Хасав’юртівські угоди (1996). Офіційний текст: «Принципи визначення основ взаємовідносин між Російською Федерацією та Чеченською Республікою Ічкерія» від 31.08.1996[55].

2. Офіційні документи та звіти міжнародних організацій - Включає резолюції, звіти та стратегії ООН, НАТО, ЄС, ОБСЄ, що фіксують порушення та механізми протидії.

1) Countering hybrid threats. NATO. 2025. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (Access date: 05.11.2025)[85].

2) Human Rights Watch. World Report 2024: Ukraine. Human Rights Watch. New York, 2024. URL: https://www.hrw.org/world-report/2024/country-chapters/ukraine (Дата звернення: 20.10.2025)[120].

3) Hybrid threats. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). Helsinki, 2025. URL: https://www.hybridcoe.fi/hybrid-threats/ (Дата звернення: 10.12.2025)[123].

4) Initiative on the Safe Transportation of Grain and Foodstuffs from Ukrainian Ports (Black Sea Grain Initiative). United Nations. New York, 2022. URL: https://www.un.org/en/black-sea-grain-initiative (Дата звернення: 05.11.2025)[129].

5) OSCE Office for Democratic Institutions and Human Rights. Moscow Mechanism experts present report on Ukraine to OSCE Permanent Council. 2025. 25 September. URL: https://www.osce.org/odihr/598057 (Дата звернення: 15.12.2025)[161].

6) United Nations General Assembly. Resolution 68/262: Territorial integrity of Ukraine. 2014. 27 March. URL: https://digitallibrary.un.org/record/767565?ln=en (Дата звернення: 25.09.2025)[176].

7) Vilnius Summit 2023: Cyber Defence Policy and Action Plan. NATO. Brussels, 2023. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (Дата звернення: 10.10.2025)[236].
8) Wales Summit Declaration. NATO. Brussels, 2014. URL: https://www.nato.int/cps/en/natohq/official_texts_112964.htm (Дата звернення: 20.11.2025)[238].
9) Warsaw Summit Communiqué: Strategy Against Hybrid Threats. NATO. Brussels, 2016. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm (Дата звернення: 05.12.2025)[243].

3. Документи державних органів України та РФ - Офіційні звіти, укази та заяви, що ілюструють позиції сторін.

1) Territorial integrity of Ukraine : Resolution 68/262 / United Nations General Assembly. New York, 2014. 27 March. URL: https://digitallibrary.un.org/record/767565 (Дата звернення: 13.12.2025)[176].
2) Countering hybrid threats. NATO. 2025. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm (Дата звернення: 13.12.2025)[85].
3) Hybrid threats. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). Helsinki, 2025. URL: https://www.hybridcoe.fi/hybrid-threats/ (Дата звернення: 13.12.2025)[123].
4) Moscow Mechanism experts present report on Ukraine to OSCE Permanent Council / OSCE Office for Democratic Institutions and Human Rights. 2025. 25 September. URL: https://www.osce.org/odihr/598057 (Дата звернення: 13.12.2025)[161].
5) Wales Summit Declaration. NATO. Brussels, 2014. URL: https://www.nato.int/cps/en/natohq/official_texts_112964.htm (Дата звернення: 13.12.2025)[238].

6) Warsaw Summit Communiqué: Strategy Against Hybrid Threats. NATO. Brussels, 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (Дата звернення: 13.12.2025)[243].
7) Vilnius Summit 2023: Cyber Defence Policy and Action Plan. NATO. Brussels, 2023. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (Дата звернення: 13.12.2025)[236].
8) World Report 2024: Ukraine. Human Rights Watch. New York, 2024. URL: https://www.hrw.org/world-report/2024/country-chapters/ukraine (Дата звернення: 13.12.2025)[120].
9) Initiative on the Safe Transportation of Grain and Foodstuffs from Ukrainian Ports (Black Sea Grain Initiative). United Nations. New York, 2022. URL: https://www.un.org/en/black-sea-grain-initiative (Дата звернення: 13.12.2025)[129].

4. Аналітичні звіти та дослідження - Звіти інститутів, що аналізують гібридну війну та протидію.

1) Boston S., Massicot D. The Russian Way of Warfare: A Primer. RAND Corporation. Santa Monica, 2017. DOI: 10.7249/PE231. URL: https://www.rand.org/pubs/perspectives/PE231.html (Дата звернення: 13.12.2025)[69].
2) Bradshaw S. Industrialized Disinformation: 2020 Global Inventory of Organised Social Media Manipulation / S. Bradshaw, H. Bailey, P. N. Howard. Oxford Internet Institute, Programme on Democracy & Technology. Oxford, 2021. 70 с. URL: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf (Дата звернення: 13.12.2025)[70].
3) Hybrid Threats and Resilience: The Ukrainian Experience 2014–2025. Swedish Defence Research Agency (FOI). Stockholm, 2025. 110 с. URL: https://www.foi.se/en/foi/publications/2025/hybrid-threats-and-resilience-the-ukrainian-experience-2014-2025 (Дата звернення: 13.12.2025)[122].
4) Kofman M. Lessons from Russia’s Operations in Crimea and Eastern Ukraine / M. Kofman, K. Migacheva, B. Nichiporuk, A. Radin, O. Tkacheva, J. Oberholtzer. RAND

Corporation. Santa Monica, CA, 2017. 126 c. URL: https://www.rand.org/pubs/research_reports/RR1498.html (Дата звернення: 13.12.2025)[136].

5) Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist / за ред. K. Pynnöniemi, M. Kari. Finnish Institute of International Affairs. Helsinki, 2015. 191 c. (FIIA Report ; 43). URL: https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf (Дата звернення: 13.12.2025)[185].

5. Наукова література (монографії, статті) - Теоретичні праці з гібридної війни, історії та безпеки.

1) Arquilla J. Cyberwar is Coming! / J. Arquilla, D. Ronfeldt. Comparative Strategy. 1993. Vol. 12, No. 2. P. 141–165. DOI: https://doi.org/10.1080/01495939308402915 (Дата звернення: 13.12.2025)[60].
2) Clausewitz C. von. On War / trans. by M. Howard, P. Paret ; ed. and with an introd. by P. Paret. Princeton University Press. Princeton, 1984. 732 p. URL: https://press.princeton.edu/books/paperback/9780691018546/on-war (Дата звернення: 13.12.2025)[80].
3) Fridman O. Russian "Hybrid Warfare": Resurgence and Politicization. Oxford University Press. Oxford, 2018. 236 p. ISBN 978-0-19-087737-8. DOI: 10.1093/oso/9780190877378.001.0001. URL: https://academic.oup.com/book/32415 (Дата звернення: 13.12.2025)[105].
4) Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies. Arlington, VA, 2007. 40 p. URL: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf (Дата звернення: 13.12.2025)[115].
5) Магда Є. В. Гібридна агресія Росії: уроки для Європи : монографія. Каламар. Київ, 2017. 268 с. ISBN 978-966-97478-3-9. URL: https://kalamar.ua/product/gibrydna_agresia_rosii_uroki_dlia_evropi/ (Дата звернення: 13.12.2025)[19].

6) Світова гібридна війна: український фронт : колективна монографія / за заг. ред. В. П. Горбуліна. НІСД. Київ, 2017. 496 с. ISBN 978-966-554-273-5. URL: https://niss.gov.ua/publikacii/monografii/svitova-gibridna-viyna-ukrainskiy-front-monografiya (Дата звернення: 13.12.2025)[41].

6. OSINT-розслідування, журналістські матеріали, інтерв'ю - Розслідування, статті та відео, що документують факти агресії.

1) Bellingcat Investigation Team. Putin Chef's Kisses of Death: Russia's Shadow Army's State-Run Structure Exposed / Bellingcat, The Insider, Der Spiegel. 2020. 14 серпня. URL: https://www.bellingcat.com/news/uk-and-europe/2020/08/14/pmc-structure-exposed/ (Дата звернення: 13.12.2025)[65].
2) Bihus exposé: Ukraine's SBU illegally surveilled investigative journalists. Euromaidan Press. Kyiv, 2024. 7 лютого. URL: https://euromaidanpress.com/2024/02/07/bihus-expose-ukraines-sbu-illegally-surveilled-investigative-journalists/ (Дата звернення: 13.12.2025)[67].
3) «Груз-200 из Крыма». Проект о потерях России в Украине / Радіо Свобода. Проект Крим.Реалії. Київ, 2023. 23 лютого. URL: https://ru.krymr.com/a/gruz-200-krym/33244443.html (Дата звернення: 13.12.2025)[48].
4) Investigative Stories from Ukraine: Bihus.Info Finds Another Defense Ministry Contract with Inflated Food Prices / A. Myroniuk, A. Khrebet. Kyiv Independent. Kyiv, 2023. URL: https://kyivindependent.com/investigative-stories-from-ukraine-bihus-info-finds-another-defense-ministry-contract-with-inflated-food-prices/ (Дата звернення: 13.12.2025)[131].
5) Телебачення Торонто. ХТО СТВОРЮЄ ВІРУСНІ ДІПФЕЙКИ ПРО ЗСУ: розслідування +ENG SUB [відео]. YouTube. 2024. URL: https://www.youtube.com/watch?v=rxRMzB_1Yvs (Дата звернення: 13.12.2025)[45].

7. Статистичні джерела та соціологічні опитування - Дані про втрати, економіку, суспільну думку.

1) Довіра до російських ЗМІ на окупованих територіях (2014-2015). Київський міжнародний інститут соціології (КМІС). 2014-2015. URL: https://kiis.com.ua/?lang=eng&cat=reports (Дата звернення: 15.10.2025)[12].
2) IMF World Economic Outlook Database: Ukraine GDP Projections 2022–2025. International Monetary Fund. Washington, 2024. URL: https://www.imf.org/en/Publications/WEO/weo-database/2024/October (Дата звернення: 20.11.2025)[127].
3) Інфляційний звіт: січень 2025 року. Національний банк України. Київ, 2025. URL: https://bank.gov.ua/en/news/all/inflyatsiyniy-zvit-sichen-2025-roku (Дата звернення: 10.10.2025)[17].
4) The Identity of Ukraine's Citizens: Trends of Change (June 2024). Razumkov Centre. Київ, 2024. URL: https://razumkov.org.ua/en/component/k2/the-identity-of-ukraine-s-citizens-trends-of-change-june-2024 (Дата звернення: 05.11.2025)[206].
5) Втрати Росії в Україні - офіційні дані. Index.Minfin. 2025. URL: https://index.minfin.com.ua/ua/russian-invading/casualties/ (Дата звернення: 25.11.2025)[3].

8. Електронні ресурси та медіа - Сайти фондів, платформи, що фіксують волонтерство та інновації.

1) Annual Report 2024. SaveLife Foundation. Київ, 2025. URL: https://savelife.in.ua/en/annual-report-en/ (Дата звернення: 15.11.2025)[58].
2) Brave1 - Ukrainian Defense Innovations. Brave1 Cluster ; Уряд України. Київ, 2025. URL: https://brave1.gov.ua/en/ (Дата звернення: 20.10.2025)[72].
3) EU vs Disinfo Database. East StratCom Task Force. European External Action Service. Brussels, 2015–2025. URL: https://euvsdisinfo.eu/disinformation-cases/ (Дата звернення: 10.11.2025)[101].
4) Prytula Foundation. Prytula Foundation. Київ, 2025. URL: https://prytulafoundation.org/en (Дата звернення: 05.12.2025)[170].

5) Спільнота Стерненка. БФ Спільнота Стерненка. Київ, 2025. URL: https://www.sternenkofund.org/ (Дата звернення: 25.11.2025)[42].
6) Звіти про діяльність фонду 2014–2025 рр. : серія річних і тематичних звітів. Фонд «Повернись живим». Київ, 2014–2025. URL: https://savelife.in.ua/en/reporting-en/ (Дата звернення: 10.12.2025)[15].

Тепер перейдімо до методологічної частини дослідження, що ґрунтується на міждисциплінарній методології, що поєднує інструментарій політології, міжнародних відносин, воєнних наук, кібербезпеки та соціології[105; 115; 122; 178]. Такий підхід зумовлений комплексним характером гібридної агресії, яка одночасно охоплює військову, інформаційну, кібернетичну, економічну, дипломатичну та суспільно-психологічну сфери й не може бути адекватно проаналізована в межах однієї дисципліни[115; 123; 207]. Тож для методології вивчення ми послуговувалися такими методами:

Історико-генетичний метод – Використовується для аналізу розвитку теорії гібридної війни від кінця XX століття до 2025 року[146; 147; 232; 233; 64; 107]. Наприклад, простеження витоків від робіт Лінда (1989) та ван Кревельда (1991) до "доктрини Герасимова" (2013) та подій в Україні[146; 232; 107].

Компаративний метод – Застосовується для порівняння різних етапів конфлікту, моделей агресії (наприклад, чеченські війни vs. грузинська 2008 vs. українська 2014-2025) та механізмів протидії (західні vs. російські доктрини, досвід НАТО vs. України)[61; 136; 151; 155; 85; 122; 156].

Системно-структурний метод – Використовується для аналізу структури гібридної агресії (військова, інформаційна, кібернетична, економічна складові) та механізмів протидії (наприклад, роль РНБО, CERT-UA, СБУ в кібероборoні)[14; 43; 89; 123; 207].

Метод кейс-стаді – Застосовується для вивчення ключових епізодів, таких як анексія Криму, Іловайськ, Дебальцеве, контрнаступи 2022-2023, чи проекти «народний байрактар» та «Друк-армія»[136; 169; 194; 195; 168; 21; 113].

Контент-аналіз – Використовується для дослідження інформаційно-психологічних операцій, пропагандистських наративів (наприклад, «п'ята колона», фейкові наративи в «Детектор медіа») та дезінформації (EU East StratCom Task Force, EUvsDisinfo)[70; 71; 91; 101; 104].

Статистичний метод – Застосовується для оцінки наслідків та ефективності: наприклад, інвестиції ($2,5 млрд у "народний ВПК"), охоплення (1 млн користувачів кіберосвіти, 20 000 пілотів дронів), зменшення атак (60% ефективності з 2022)[72; 113; 132; 141; 145; 181; 214; 215]. Джерела як ISW, Atlantic Council, Мінцифри надають статистичні дані для таких оцінок[145; 159; 181].

Юридико-догматичний метод – Використовується для інтерпретації міжнародного права, резолюцій (наприклад, Резолюція ГА ООН 68/262), санкцій та механізмів (Moscow Mechanism ОБСЄ, Таллінський посібник 2.0)[93; 154; 161; 162; 176; 177; 199; 200]. Посилається на Вестфальську систему, право вето в РБ ООН та адаптацію права до кібервійни[154; 199].

РОЗДІЛ 2. ТЕОРЕТИЧНІ ОСНОВИ ГІБРИДНОЇ АГРЕСІЇ

2.1. Поняття та сутність гібридної війни

Гібридна агресія на сьогоднішній день визначається як концепція сучасного воєнно-політичного протиборства, головною ознакою якого є синхронне застосування широкого спектру інструментів впливу: військових, політичних, економічних, інформаційних та кібернетичних[85; 115; 123; 207]. За визначенням, яке подає НАТО, гібридна війна складає собою широкий спектр ворожих дій, що включає використання традиційних та нетрадиційних військових засобів, терористичних актів, кримінальних дій та інформаційних операцій[85; 243].

Провідний теоретик гібридної війни Ф. Гофман, як було детально розглянуто в підрозділі 1.1, визначає цей тип конфлікту як поєднання різних режимів війни, включаючи конвенційні заходи, нерегулярну тактику, терористичні акти та кримінальну поведінку в міжнародному просторі, спрямовану на досягнення політичних цілей[115; 116]. Українські дослідники Є. Магда та М. Гончар у своєму визначенні підкреслюють, що гібридна агресія передбачає комплексне використання всіх доступних засобів для дестабілізації держави-жертви, ескалації внутрішньополітичних криз та підриву її міжнародних позицій[19].

Іншими словами, гібридна агресія концентрується першочергово не на військових засобах, а на руйнуванні держави-жертви зсередини та ізоляції від будь-якої зовнішньої підтримки, створюючи ситуацію, коли жертва стає безпорадною перед можливостями зовнішнього вторгнення[10; 41; 105; 117]. Фундаментальна особливість гібридної агресії полягає у відсутності чітко окреслених ліній протистояння та використанні нерегулярних формувань поряд із регулярними військами[115; 136; 155].

М. ван Кревельд, як зазначалося в історіографічному огляді, у праці

«Трансформація війни» передбачив перехід від міждержавних конфліктів до багаторівневих протистоянь з участю недержавних акторів, що стало основою для розуміння гібридних загроз[232; 233].

За оцінками експертів Гарвардської школи Кеннеді, гібридна агресія створює ефект «повільного кипіння», коли держава-жертва поступово втрачає контроль над ситуацією, не усвідомлюючи масштабів загрози, фактично розкладаючись зсередини[74; 117].

Ключовими характеристиками гібридної агресії є:

1. Адаптивність та багатовекторність впливу. Дослідження Королівського об'єднаного інституту оборонних досліджень (RUSI) підтверджує, що синергія різнорідних методів виявляється ефективнішою за традиційні військові операції у випадках, коли відкрита війна є політично неприйнятною[125; 168; 117].

2. Маскування та неоднозначність. Важливою особливістю є маскування агресії під «гуманітарні» або «миротворчі» операції, що унеможливлює своєчасну ідентифікацію джерела загрози міжнародною спільнотою[125; 136; 173]. Це створює ефект «правдоподібного заперечення» (plausible deniability), коли агресор може заперечувати свою пряму участь у конфлікті[173; 155].

3. Розмивання меж між війною та миром. Гібридна агресія створює «сіру зону», де традиційні інструменти міжнародної безпеки виявляються неефективними[115; 105; 117]. За оцінками Chatham House, вона підриває три основні принципи Вестфальської системи: державний суверенітет, територіальну цілісність та невтручання у внутрішні справи[154; 222].

4. Комплексність та синхронність застосування різних інструментів. За класифікацією Європейського центру досліджень гібридних загроз (Hybrid CoE), компоненти можна згрупувати в п'ять категорій: військові, інформаційні, кібернетичні, економічні та дипломатичні інструменти[123; 207]. Велика кількість і різноманітність задіяних компонентів дозволяє агресору гнучко адаптувати стратегію відповідно до специфіки цільової держави[123; 117].

5. «Війна нижче порогу» (sub-threshold warfare). Ця концепція передбачає здійснення агресивних дій, які залишаються нижче рівня, що викликав би повномасштабну міжнародну реакцію або застосування статті 5 Північноатлантичного договору[74; 85; 117]. Агресор навмисно калібрує інтенсивність своїх дій, щоб уникнути перетину «червоних ліній»[117; 156].

Російський військовий теоретик, начальник Генерального штабу ЗС РФ Валерій Герасимов у статті «Цінність науки в передбаченні» (2013) звернув увагу на те, що в сучасних конфліктах роль невійськових методів значно зросла і в окремих випадках (зокрема, під час подій «арабської весни») виявляється дуже значною[107; 64].

Проте так звана «доктрина Герасимова» та широко цитоване співвідношення невійськових до військових засобів 4:1 є західною інтерпретацією, що не відповідає оригінальному тексту статті 2013 року[64; 107; 152]. Насправді Герасимов лише констатував зростання ролі невійськових методів у сучасних конфліктах, не наводячи жодних числових пропорцій[107; 152]. Спочатку Марк Галеотті запропонував власну інтерпретацію цієї статті, саме завдяки якій з'явилося чітке окреслення співвідношення як 4:1[107]. Проте ця міфологізована формула 4:1 стала домінуючою в західному дискурсі 2014-2018 років поступово була відкинута[64; 152].

Дослідники Майкл Кофман, Кір Джайлс та сам Марк Галеотті послідовно спростовували цей міф, демонструючи, що західна концепція «доктрини Герасимова» є значною мірою конструктом, що приписує російському Генштабу більш системну та ідеологічно оформлену доктрину, ніж та, що існує насправді[64; 107; 152].

Реальне співвідношення військових та невійськових компонентів у російській практиці: Аналіз реальної російської практики гібридної агресії проти України дозволяє виявити суттєві розбіжності з міфологізованою формулою 4:1[105; 109; 178; 185]. Співвідношення, яке найточніше відображає російську практику гібридної агресії проти України з 2014 по 2022 роки, є ближчим до 3:2 (тобто 60% невійськових до 40% військових засобів)[4; 5; 10; 41; 136; 185].

Це обумовлено тим, що без прямого задіяння збройних сил РФ не була спроможна перетворити територію Донбасу на зону тривалих бойових дій, а пізніше – плацдарм для вторгнення[136; 169; 194; 195]. Анексія Криму, хоча й супроводжувалася масштабними інформаційними операціями, була б неможливою без швидкого введення регулярних військових підрозділів без розпізнавальних знаків («зелених чоловічків»)[136; 169]. На Донбасі, незважаючи на активне використання проксі-сил, критичні бої (Іловайськ, Дебальцеве) вигравалися завдяки прямому втручанню регулярних російських військ[194; 195; 169].

Після 2022 року це співвідношення знову змінилося на 2:3 (40% невійськових до 60% військових засобів), оскільки навіть під час повномасштабного вторгнення військова складова стала домінуючою[168; 181; 184; 185]. Проте навіть в умовах конвенційної війни гібридний характер конфлікту зберігся: продовжувалися масштабні інформаційні операції, кібератаки, використання діпфейків, економічний тиск на партнерів України, дипломатичні маніпуляції[14; 43; 45; 75; 89; 101; 212]. Ця еволюція співвідношення з 3:2 до 2:3 демонструє кілька важливих особливостей російської гібридної стратегії[105; 109; 122; 178]:

По-перше, адаптивний характер – співвідношення змінюється залежно від фази конфлікту та досягнутих результатів[117; 122; 168]. Коли невійськові методи виявилися недостатніми для досягнення стратегічних цілей (захоплення Києва, зміна уряду, капітуляція України), РФ змушена була перейти до домінування військової компоненти[168; 196].

По-друге, гібридність зберігається навіть в умовах повномасштабної війни. Це підтверджує тезу Френка Гофмана, що гібридна війна є не альтернативою традиційній війні, а її еволюційним продовженням, де різні інструменти використовуються синхронно[115; 116; 117].

По-третє, неможливість досягнення стратегічних цілей виключно невійськовими засобами. Попри масштабні інформаційні операції, кібератаки та економічний тиск, які тривали з 2014 року, РФ не вдалося дестабілізувати Україну настільки, щоб досягти

контролю над державою без повномасштабного військового вторгнення[4; 5; 10; 19; 41; 87; 89; 105].

Детальніше питання співвідношення військових до невійськових засобів в застосуванні РФ ми розглянемо далі в пункті 2.2., а зараз перейдемо до розгляду саме відмінності тих самих військових до невійськових засобів в контексті гібридної агресії[105; 115; 117; 122].

Головна відмінність між традиційною та гібридною агресією полягає в широкому обсягу компонентів та невизначеності джерела загрози[74; 115; 123; 207]. Традиційні конфлікти характеризуються відкритими бойовими діями з чіткими лініями фронту, регулюються Женевськими конвенціями[93; 135; 232]. Класична агресія включає офіційне оголошення війни, мобілізацію збройних сил та чітке визначення сторін конфлікту[80; 135; 232].

Натомість гібридна агресія використовує латентні методи, що ускладнюють виявлення агресора та своєчасну міжнародну реакцію[74; 117; 125; 173]. Дослідження Центру стратегічних та міжнародних досліджень (CSIS) показує, що середній час реакції міжнародних організацій на гібридну агресію становить 3-6 місяців, що значно перевищує показники реагування на конвенційні конфлікти[74; 117].

Таблиця 2.1. Порівняльна характеристика традиційної та гібридної агресії.

Параметри	Традиційна агресія	Гібридна агресія
Характер застосування сили	Відкрите використання регулярних збройних сил з розпізнавальними знаками	Поєднання регулярних військ, «непозначених» підрозділів, проксі-сил, кібератак та інформаційних операцій
Легітимність	Формальне оголошення війни, визнання стану війни згідно з міжнародним правом	Заперечення агресії, маскування під «громадянський конфлікт», «народне повстання» або «миротворчу операцію»

Ідентифікація агресора	Чітке визначення сторін конфлікту, офіційне підтвердження участі	«Правдоподібне заперечення» (plausible deniability), використання проксі-сил, відсутність розпізнавальних знаків
Географічні межі	Чіткі лінії фронту, визначена зона бойових дій, територіальне розмежування	Розмиті межі, операції у кіберпросторі, інформаційному просторі, економічній сфері, на територіях третіх країн
Тривалість	Відносно короткі активні фази з чітким початком і завершенням	Тривалий конфлікт низької інтенсивності з періодичними ескалаціями, ефект «повільного кипіння»
Цілі	Захоплення території, знищення збройних сил противника, примус до капітуляції	Дестабілізація держави зсередини, підрив легітимності влади, створення контрольованого хаосу, ізоляція від зовнішньої підтримки
Інструменти	Переважно військові засоби: сухопутні війська, авіація, флот, артилерія	Комплексне синхронне використання військових, інформаційних, кібернетичних, економічних, дипломатичних засобів
Правове регулювання	Чітко регулюється міжнародним гуманітарним правом (Женевські конвенції, Гаазькі конвенції)	Перебуває в «сірій зоні» міжнародного права, ускладнює правову кваліфікацію дій як агресії
Міжнародна реакція	Швидка та однозначна: санкції, засудження, можливе військове втручання	Затримана (3-6 місяців), суперечлива, ускладнена невизначеністю ситуації та «правдоподібним запереченням»

Отже, як демонструє таблиця 2.1, гібридна агресія систематично експлуатує «сіру зону» між війною та миром, використовуючи невизначеність для досягнення стратегічних цілей до того, як міжнародна спільнота зможе сформувати ефективну відповідь[74; 115; 117; 123]. Це робить гібридну агресію особливо небезпечним інструментом сучасної геополітики, що вимагає принципово нових підходів до забезпечення національної та міжнародної безпеки[85; 122; 156; 207].

Гібридна агресія трансформує не лише глобальну систему безпеки, але й внутрішньополітичну ситуацію в державах-жертвах[135]. За концептуалізацією М. Калдор, «нові війни» характеризуються впливом на цивільне населення та соціальну складову суспільства[135]. Інформаційні кампанії призводять до поляризації суспільства, втрати довіри до уряду та загострення внутрішніх конфліктів[70; 71; 91; 101].

За даними Pew Research Center, у країнах, що зазнають гібридної агресії, рівень довіри до державних інститутів знижується протягом перших двох років. Феномен «п'ятої колони», коли частина населення свідомо чи несвідомо сприяє агресору, стає критичним чинником, що підриває здатність держави до ефективного опору[11; 12; 23; 66].

За оцінками Світового банку, гібридні конфлікти призводять до більш тривалого економічного спаду порівняно з традиційними війнами – у середньому на 40% довше[87; 231]. Це пов'язано з тим, що гібридна агресія руйнує не лише фізичну інфраструктуру, але й соціальну тканину суспільства, довіру до інститутів, економічні зв'язки[87; 94; 127; 231]. Досвід показує, що диверсифікація економічних зв'язків та зменшення енергетичної залежності від потенційного агресора є критично важливими для підвищення стійкості держави до гібридних загроз[9; 16; 99].

Варто розуміти, що архітектура гібридної агресії постійно еволюціонує[117; 122; 178]. Особливо небезпечним у контексті майбутніх гібридних загроз є подальший розвиток штучного інтелекту, кібернетичних технологій та синтетичних медіа

(діпфейків)[45; 75]. За прогнозами Міжнародного інституту стратегічних досліджень (IISS), до 2030 року ШІ стане ключовим інструментом гібридної війни, що вимагає превентивного розвитку механізмів протидії та розпізнавання таких загроз[75].

Таким чином, гібридна війна є не просто сумою різних інструментів, а якісно новим типом конфлікту, що вимагає комплексного теоретичного осмислення російської моделі гібридних дій, якому присвячено наступний підрозділ[4; 5; 10; 19; 41; 105; 115; 122].

2.2. Російська доктрина гібридних дій

Російська концепція гібридної війни формувалася паралельно із західними теоретичними розробками, проте спиралася на власні традиції радянської військової думки[64; 105; 107; 152]. Ключовими елементами цієї традиції були концепції «активних заходів» (комплекс операцій впливу), «маскування» (приховування справжніх намірів та дій) та рефлексивного управління (маніпулювання процесом прийняття рішень противником через надання йому певної інформації)[64; 107].

Як зазначалося раніше у підрозділі 2.1, стаття начальника Генерального штабу Збройних Сил РФ Валерія Герасимова «Цінність науки в передбаченні», опублікована у 2013 році у «Военно-промышленном курьере», стала одним із ключових текстів для розуміння російського бачення сучасної війни[64; 107; 152]. Герасимов звернув увагу на досвід «арабської весни», де невійськові методи (масові протести, інформаційні кампанії, соціальні мережі) виявилися ефективними інструментами зміни політичних режимів[107]. Він констатував, що роль невійськових методів у сучасних конфліктах значно зросла і в окремих випадках виявляється дуже значною[107].

Проте, як було детально обґрунтовано вище, так звана «доктрина Герасимова» та широко цитоване співвідношення 4:1 є саме західною інтерпретацією[64; 107; 152], проте навіть дослідники теми міфологізації співвідношення заходів не змогли зауважити важливу річ, що ця доктрина, це лише поверхневий аналіз того, що РФ

приховано вже давно напрацьовувало в Чечні (Ічкерія) та Грузії (Сакартвело) формуючи «свіжий» досвід[61; 151; 155].

Для розуміння російської гібридної стратегії критично важливо простежити її історичні витоки[151; 155]. Російсько-чеченські війни (1994-1996 та 1999-2009) стали першими повномасштабними випробуваннями елементів гібридної агресії РФ у пострадянський період фактично зробивши з регіону полігон для відпрацювання тактик гібридної агресії[151; 155]. Проте варто зауважити, що перша чеченська кампанія розцінювалася усе, як «конвенційна агресія», що мала на меті саме придушення населення військовим методом[151].

Хоча більшість західних дослідників (Ф. Гофман, RUSI, Hybrid CoE) вважають російсько-грузинську війну 2008 року першим «класичним» кейсом гібридної війни XXI століття[61; 115; 123; 125], чеченські кампанії вже містили всі ключові елементи сучасної гібридної агресії проти де-факто незалежної держави Чеченської Республіки Ічкерія (ЧРІ), визнаної такою не тільки за виконанням усіх вимог виходу з СРСР та непідписання Союзного Договору з РФ, але й визнаною самою РФ за Хасав'юртівськими угодами по закінченню Першої чеченської кампанії[55; 151; 155]. До цих елементів належали:

1. Використання «непозначених» сил – спецназ ГРУ діяв без розпізнавальних знаків, що створювало невизначеність щодо статусу конфлікту та дозволяло РФ заперечувати пряму участь регулярних військ[151; 155].

2. Масове залучення проксі-формувань – зокрема, лояльних Ахмату Кадирову загонів, що формально не були частиною російських збройних сил, але діяли в їхніх інтересах[151]. Ці формування використовувалися для найбільш брудної роботи, за яку РФ не хотіла нести пряму відповідальність[151; 155].

3. Тотальна інформаційна війна – систематичне звинувачення чеченців у тероризмі та ісламському фундаменталізмі, що формувало внутрішню та міжнародну підтримку військових дій[151]. Якщо сьогодні у кожної людини є можливість вільного виходу в інтернет-мережу практично з будь-якого куточку світу, то під час чеченських

кампаній (1994-1996 та 1999-2009) таких можливостей не було, що дозволяло РФ ефективно приховувати свої злочини та методи[151]. Будь-які відеоматеріали журналістів, що могли фіксувати події, були під суворим наглядом, що дозволяло РФ повністю контролювати інформаційну повістку[151].

4. Економічний тиск і блокада – повне перекриття економічних контактів як інструмент примусу, що мало зруйнувати економіку ЧРІ та деморалізувати населення[151].

5. Рефлексивне управління – найяскравішим прикладом якого стали провокації з вибухами житлових будинків у Москві та Волгодонську у вересні 1999 року, які частина дослідників та опозиційних російських політиків вважають операцією під чужим прапором[151; 155]. Ці вибухи створили необхідний привід для початку Другої чеченської війни, сформувавши в російському суспільстві образ чеченців як терористичної загрози, що вимагає силового знищення[151].

Таким чином, чеченські війни були не просто військовою кампанією, а справжнім прототипом гібридної агресії, який Російська Федерація згодом удосконалила й масштабувала, випробувавши в Грузії (2008) та Україні (2014-дотепер)[61; 151; 155].

Російсько-грузинська війна у серпні 2008 року стала наступним етапом еволюції російської гібридної стратегії та першим випадком, який привернув системну увагу західної наукової спільноти[61; 136; 115; 123; 125]. Конфлікт включав: 1) Провокації в Південній Осетії – створення напруги та ескалація ситуації, що надала формальний привід для «миротворчого» втручання[61; 136]; 2) Масштабні (Distributed Denial of Service) DDoS-атаки на урядові сайти Грузії – перше масштабне використання кіберзброї в поєднанні з військовою операцією[61; 81; 100]; 3) Координовану інформаційну війну – формування наративу про «грузинську агресію» проти мирного населення Південної Осетії[61; 136]; 4) Швидку військову операцію з використанням регулярних військ, що досягла стратегічних цілей до того, як «Захід» зміг сформувати чітке розуміння, що це агресія РФ[61; 74; 136].

Грузинська війна стала першим випадком, коли цей інструментарій було застосовано проти міжнародно визнаної суверенної держави поза межами колишнього СРСР[61; 136]. Ці конфлікти продемонстрували неготовність західних держав та міжнародних організацій до адекватного реагування[61; 74; 123]. Відсутність чіткої міжнародно-правової кваліфікації дій РФ унеможливила своєчасну міжнародну реакцію і стала каталізатором для наукового осмислення гібридних конфліктів[61; 74; 154].

Аналіз реальної російської практики гібридної агресії проти України дозволяє виявити суттєві розбіжності з міфологізованою формулою 4:1 та простежити еволюцію російської стратегії розділеної на 2 періоди[64; 107; 152; 178; 185].

Період 2014-2022: співвідношення 3:2 (60% невійськових до 40% військових)[4; 5; 10; 41; 136; 169].

Співвідношення, яке найточніше відображає російську практику гібридної агресії проти України з 2014 по 2022 роки, є ближчим до 3:2[136; 169; 178]. Це обумовлено тим, що без прямого задіяння збройних сил РФ не була спроможна захопити Крим та перетворити територію Донбасу на зону тривалих бойових дій, а пізніше – плацдарм для вторгнення[136; 169].

Анексія Криму (лютий-березень 2014) відбулася за сценарієм, де хоча й активно використовувалися інформаційні операції, психологічний тиск та підтримка проросійських активістів, вирішальну роль відіграло швидке введення регулярних військових підрозділів без розпізнавальних знаків («зелених чоловічків»)[136; 169; 65]. Війська РФ швидко встановили контроль над ключовими об'єктами: урядовими будівлями, аеропортами, військовими базами, портами[136; 169]. Одночасно проводилася інформаційна кампанія та організовувався псевдо-референдум[95; 128; 136].

Конфлікт на Донбасі продемонстрував усі елементи гібридної війни: підтримку сепаратистів, участь військ РФ як безпосередньо під час «виконання службового обов'язку», так і пізніше під виглядом «відпускників», залучення приватних військових

компаній (зокрема, ПВК «Вагнер», що був сформований для гібридної війни), кібератаки, інформаційні операції та економічний саботаж[5; 10; 41; 62; 65; 136; 169; 174; 194; 195].

Проте критичні бої (Іловайськ, серпень 2014 та Дебальцеве, лютий 2015) відбулися виключно завдяки прямому втручанню регулярних російських військ з важкою технікою, артилерією та системами залпового вогню[136; 169; 194; 195]. Без цього військового втручання місцеві сепаратистські формування не змогли б утримати контроль не те, що над значними територіями, але як зізнавалися Ігор «Стрелков» Гіркін та Олександр Захарченко могли бути повністю знищені[49; 54; 136; 169].

Період 2022-2025: співвідношення 2:3 (40% невійськових до 60% військових): Після 24 лютого 2022 року це співвідношення змінилося на 2:3, оскільки військова складова стала домінуючою[57; 62; 145; 181; 184]. Повномасштабне вторгнення передбачало використання сотень тисяч військовослужбовців, тисяч одиниць важкої техніки, масованих ракетних ударів по всій території України[3; 62; 145; 181].

Проте навіть в умовах «конвенційної війни» гібридний характер конфлікту зберігся:

- Інформаційні операції продовжувалися, російська пропаганда намагалася охопити, як можна більшу частину населення, як на окупованих так й на підконтрольних Україні територіях з метою деморалізації українського населення та дезінформації міжнародної спільноти (наприклад, діпфейк-відео з Президентом Зеленським у березні 2022 року)[45; 70; 71; 91; 183];
- Кібератаки на критичну інфраструктуру, державні ресурси, енергосистему[14; 43; 89; 100; 110; 143; 148];
- Економічний тиск через блокаду українських портів, захоплення підприємств, знищення інфраструктури[29; 47; 87; 94; 127; 160; 231; 249];
- Дипломатичні маніпуляції з метою блокування міжнародної підтримки України[156; 212; 238];

- Психологічні операції через залякування цивільного населення, масові військові злочини як інструмент терору[120; 173; 191; 192].

Аналіз російської практики дозволяє виділити п'ять ключових характеристик російської доктрини:

Адаптивність – співвідношення військових та невійськових компонентів змінюється залежно від фази конфлікту, досягнутих результатів та реакції противника[64; 107; 109; 117; 248]. Коли невійськові методи виявилися недостатніми для досягнення стратегічних цілей (захоплення Києва, зміна уряду, капітуляція України), РФ змушена була перейти до домінування військової компоненти[107; 145; 181].

Синергія різних інструментів – навіть коли домінує військова складова, невійськові інструменти продовжують активно використовуватися для посилення ефекту[115; 123; 207]. Це підтверджує тезу Френка Гофмана, що гібридна війна є не альтернативою традиційній війні, а її еволюційним продовженням[115; 116].

Спадкоємність радянських концепцій – «доктрина Герасимова» спиралася на традиції радянської військової думки (активні заходи, маскування, рефлексивне управління), але адаптувала їх до реалій XXI століття з урахуванням можливостей кіберпростору, соціальних мереж та глобалізованих медіа[64; 105; 107; 152].

Неможливість досягнення стратегічних цілей виключно невійськовими засобами – попри масштабні інформаційні операції, кібератаки та економічний тиск, які тривали з 2014 року, РФ не вдалося дестабілізувати Україну настільки, щоб досягти контролю над державою без повномасштабного військового вторгнення[10; 41; 89; 122; 178].

Експлуатація «сірої зони» міжнародного права – систематичне використання «правдоподібного заперечення», проксі-сил, маскування агресії під громадянський конфлікт для уникнення повномасштабної міжнародної реакції[136; 155; 173; 154; 199].

Це підтверджує тезу про те, що гібридна війна не є статичною концепцією, а становить динамічний процес трансформації засобів і методів ведення конфлікту

залежно від досягнутих результатів та реакції противника[64; 105; 107; 117; 152; 178; 248]. Агресія РФ проти України стала найбільш послідовним і тривалим прикладом гібридної війни у XXI столітті, який остаточно спростував популярне трактування «доктрини Герасимова» та продемонстрував еволюційний характер співвідношення військових та невійськових компонентів від 3:2 до 2:3[4; 5; 10; 19; 41; 107; 122; 178; 185].

Таким чином, російська доктрина гібридних дій є унікальним синтезом радянської спадщини та сучасних технологій, що пройшла випробування в чеченських та грузинській війнах, остаточно оформилася в ході агресії проти України та продовжує еволюціонувати[61; 136; 151; 155; 64; 107]. Ця доктрина реалізується через комплексний набір інструментів, детальний аналіз яких подано в наступному підрозділі[123; 207].

2.3. Основні інструменти гібридної агресії

Гібридна агресія характеризується синхронним і взаємо-підсилюючим застосуванням широкого набору інструментів, які умовно можна згрупувати за сферами впливу. Кожен з цих інструментів має власну логіку та механіку дії, але максимальний ефект досягається саме через їхнє комплексне та координоване використання. Російська Федерація стала державою, що найпослідовніше розвинула і застосувала повний спектр цих інструментів у XXI столітті, продемонструвавши всю їхню руйнівну потужність у поєднанні.

Інформаційні операції становлять основу гібридної агресії, забезпечуючи вплив на громадську думку без застосування фізичної сили. Їхня мета полягає у формуванні потрібної картини світу в свідомості цільової аудиторії, деморалізації населення держави-жертви, поляризації суспільства та підриві довіри до державних інститутів.

Теоретичні основи інформаційних операцій включають декілька ключових компонентів. По-перше, це систематичне поширення дезінформації через контрольовані засоби масової інформації, включаючи телебачення, радіо, друковані

видання та онлайн-платформи. По-друге, масштабне використання соціальних мереж через мережі фейкових акаунтів, ботів та тролінг-фабрик, що дозволяє швидко поширювати потрібні наративи та маніпулювати трендами. По-третє, створення та поширення синтетичних медіа (діпфейків) – фальшивих відео та аудіозаписів, що імітують реальних політичних лідерів чи військовослужбовців.

За даними Оксфордського інституту інтернету, в умовах гібридної війни інформаційні операції можуть охоплювати до 30-50% населення цільової країни протягом 24 годин, що демонструє їхню надзвичайну швидкість та масштаб впливу. Ефективність інформаційних операцій підсилюється через багатоканальність (одночасне використання різних платформ), багатомовність (адаптація контенту для різних аудиторій) та створення цілісних наративних систем, де різні меседжі підкріплюють один одного.

Центральними елементами інформаційних операцій є: створення «альтернативної реальності», де факти викривлюються або замінюються вигідними інтерпретаціями; експлуатація існуючих соціальних розколів (етнічних, мовних, регіональних, ідеологічних); формування образу «зовнішнього ворога» та внутрішніх «зрадників»; дискредитація політичних лідерів та державних інститутів; створення атмосфери безнадії та неминучості поразки.

Російська модель передбачає масове і багатомовне поширення дезінформації через державні медіа та розгалужену мережу анонімних акаунтів у соціальних мережах, що було особливо помітно з 2014 року при агресії проти України.

Кібератаки та кібероперації посідають центральне місце в арсеналі гібридної агресії, дозволяючи завдавати шкоди критичній інфраструктурі держави-жертви без відкритого військового втручання та часто без можливості чіткої атрибуції джерела атаки. За класифікацією NATO Cooperative Cyber Defence Centre of Excellence, кібероперації можна поділити на три основні категорії:

Шпигунські операції спрямовані на збір розвідувальної інформації, крадіжку державних та комерційних таємниць, компрометацію урядових мереж для

довгострокового моніторингу. Такі операції можуть тривати роками, залишаючись непоміченими, та забезпечувати агресора критично важливою інформацією про наміри, можливості та вразливості противника.

Деструктивні операції мають на меті пряме завдання шкоди: знищення даних, виведення з ладу критичної інфраструктури, порушення роботи енергетичних систем, транспорту, фінансового сектору, телекомунікацій. Історичним прикладом є атака Stuxnet (2010) на іранські ядерні об'єкти, що продемонструвала можливість фізичного знищення промислового обладнання через кіберзасоби. Атаки на Естонію у 2007 році показали вразливість цифрової інфраструктури цілої держави до масованих DDoS-атак.

Операції впливу використовують кіберзасоби для маніпулювання інформаційним простором: злом та витік компрометуючих документів, маніпуляція базами даних, поширення дезінформації через скомпрометовані офіційні канали, атаки на засоби масової інформації.

Особливу небезпеку становлять атаки на промислові системи управління (ICS/SCADA), що контролюють роботу електростанцій, підстанцій, водопостачання, хімічних підприємств. Ці системи часто використовують застарілі протоколи безпеки та не розраховані на протидію цілеспрямованим кібератакам, що робить їх особливо вразливими.

Цілями кіберопера цій зазвичай стають: енергетична інфраструктура (електростанції, підстанції, системи управління); урядові мережі та державні реєстри; фінансовий сектор (банки, платіжні системи); телекомунікаційна інфраструктура; транспортні системи; засоби масової інформації; військові системи зв'язку та управління.

Російські актори активно використовують усі три категорії кіберопе рацій, поєднуючи деструктивні атаки на критичну інфраструктуру з операціями впливу та довгостроковим шпигунством.

Використання проксі-сил (нерегулярних формувань) – тобто недержавних акторів або озброєних груп, що діють в інтересах агресора без формального підпорядкування, є ключовою складовою гібридної агресії. Цей інструмент створює ефект «правдоподібного заперечення» (plausible deniability), коли агресор може заперечувати свою пряму участь у конфлікті, перекладаючи відповідальність на «місцеві угруповання» або «добровольців».

Мета використання проксі-сил є багатоаспектною. По-перше, це дозволяє уникнути міжнародної відповідальності за агресію та прямих санкцій. По-друге, знижує політичні витрати від людських втрат серед регулярних військових, оскільки загиблі проксі-бойовики не відображаються в офіційній статистиці втрат. По-третє, створює ілюзію «громадянського конфлікту» або «внутрішнього протистояння», а не зовнішньої агресії. По-четверте, дозволяє гнучко регулювати інтенсивність конфлікту, посилюючи або послаблюючи підтримку проксі-формувань залежно від стратегічних потреб. Типологія проксі-сил включає декілька категорій:

Місцеві сепаратистські угруповання формально позиціонуються як «народні рухи» або «місцеві повстанці», але насправді керуються, фінансуються та озброюються агресором. Керівні посади зазвичай займають особи з досвідом роботи в силових структурах держави-агресора.

Приватні військові компанії (ПВК) надають агресору ще один рівень deniability, формально будучи комерційними структурами. ПВК використовуються для виконання особливо складних бойових завдань, де пряма участь регулярних військ була б надто очевидною. Вони також можуть залучатися для тренування та координації дій місцевих проксі-формувань.

«Добровольці» та «відпускники» – військовослужбовці регулярних збройних сил, які формально перебувають у відпустці або звільнилися зі служби, але насправді діють в складі організованих підрозділів зі збереженням військової структури, командування та дисципліни. Це дозволяє використовувати професійних військових, зберігаючи формальну можливість заперечення.

Кримінальні угруповання використовуються переважно на початковій фазі конфлікту для дестабілізації ситуації, захоплення адміністративних будівель, залякування місцевого населення. Кримінальні елементи менш дисципліновані, але готові діяти без моральних обмежень.

Іноземні найманці залучаються з різних країн через ідеологічні (наприклад, панславізм), релігійні або фінансові мотиви. Вони можуть надавати специфічну експертизу або просто збільшувати чисельність сил.

Використання проксі-сил також дозволяє агресору формувати бойовий досвід у своїх військовослужбовців та експериментувати з різними компонентами гібридної агресії в «польових умовах» без офіційного визнання участі у конфлікті. Російська практика включає одночасне використання всіх п'яти категорій проксі-сил – від місцевих сепаратистів до приватних військових компаній та військовослужбовців у статусі «відпускників», що дозволяє гнучко регулювати рівень ескалації залежно від стратегічних потреб.

Економічний тиск дозволяє чинити вплив на державу-жертву без застосування збройної сили, використовуючи економічну взаємозалежність як зброю. За оцінками МВФ, цілеспрямована економічна війна може призвести до зниження ВВП цільової країни на 1-4% чистих втрат, хоча у випадках поєднання з територіальними втратами ці цифри можуть бути значно вищими. Типи економічного тиску включають п'ять основних категорій:

Енергетичний шантаж є одним із найпотужніших інструментів для держав, що контролюють постачання енергоносіїв. Він включає припинення або обмеження постачання газу, нафти, електроенергії; маніпуляцію цінами та тарифами; блокування транзитних маршрутів; створення штучних криз напередодні опалювального сезону. Енергетична залежність перетворюється на інструмент політичного примусу, коли держава-жертва змушена вибирати між політичними поступками або економічним колапсом.

Торговельні обмеження включають запровадження ембарго на ключові експортні товари держави-жертви (сільськогосподарську продукцію, промислові товари); створення штучних технічних бар'єрів для імпорту; блокування доступу до ринків збуту; маніпуляцію митними процедурами.

Фінансовий тиск реалізується через блокування активів фізичних та юридичних осіб держави-жертви; обмеження банківських операцій та доступу до міжнародних платіжних систем; маніпуляції з борговими зобов'язаннями; відмову від кредитування; тиск на міжнародні фінансові інститути.

Транзитні обмеження включають ускладнення або блокування транзиту товарів через територію держави-агресора; блокування транспортних коридорів; створення штучних затримок на кордоні; відмову від транзитних угод.

Захоплення та націоналізація активів на контрольованих або окупованих територіях означає конфіскацію підприємств, банків, інфраструктури держави-жертви без будь-якої компенсації. Це не лише завдає прямих економічних збитків, але й створює атмосферу економічної небезпеки для інвесторів.

Економічні втрати від гібридної агресії є комплексними та включають: втрату контролю над промисловими активами на окупованих територіях; знищення та пошкодження інфраструктури; втрату ринків збуту та інвестицій; витрати на внутрішньо переміщених осіб; різке збільшення військових витрат; втрату туристичних доходів; загальну дестабілізацію економіки.

РФ системно застосовує енергетичний тиск і торговельні обмеження як інструмент політичного примусу щодо держав, що раніше перебували в зоні її економічного впливу, використовуючи енергетичну залежність для досягнення геополітичних цілей.

Психологічні операції (PSYOPS) спрямовані на формування страху, підрив морального духу або трансформацію політичних поглядів громадян держави-жертви. На відміну від інформаційних операцій, що фокусуються на маніпулюванні фактами, психологічні операції цілеспрямовано впливають на емоційний стан та психологічну

стійкість населення. Основні напрямки психологічних операцій включають шість ключових векторів:

Експлуатація існуючих соціальних розколів полягає у штучному посиленні етнічних, мовних, релігійних, регіональних або ідеологічних розбіжностей. Навіть незначні відмінності можуть бути перетворені на непримиренні протиріччя через систематичну пропаганду, що зображує одну групу як загрозу для іншої.

Формування образу «зовнішнього ворога» передбачає зображення міжнародних партнерів держави-жертви як справжніх ініціаторів конфлікту, що нібито використовують цю державу як інструмент для досягнення власних геополітичних цілей. Це має підірвати довіру до союзників та ізолювати державу-жертву.

Дискредитація політичних лідерів реалізується через систематичні кампанії з зображення політичного керівництва як некомпетентного, корумпованого, залежного від зовнішніх сил або навіть як злочинців та екстремістів. Мета – підірвати легітимність влади та створити внутрішній політичний хаос.

Створення атмосфери безнадії здійснюється через поширення наративів про неминучість поразки, відсутність реальної підтримки від міжнародної спільноти, економічний колапс як неминучий наслідок опору. Це має деморалізувати населення та підірвати волю до опору.

Маніпуляція історичною пам'яттю включає викривлення історичних фактів, переписування історії для обґрунтування «історичних прав» агресора на території жертви, делегітимізацію державності жертви через заперечення її історичних коренів.

Залякування цивільного населення може включати демонстративні акти насильства, військові злочини як інструмент терору, систематичне поширення інформації про жорстокості для примусу до капітуляції та підриву морального духу.

Психологічні операції часто будуються навколо кількох центральних наративів, що систематично повторюються через різні канали: «захист співвітчизників» від нібито дискримінації або переслідувань; «боротьба з екстремізмом» в державі-жертві; штучне протиставлення регіонів як непримиренних ворогів; зображення внутрішніх

політичних змін як «переворотів», організованих зовнішніми силами; неминучий «розпад» держави-жертви як наслідок внутрішніх протиріч.

За даними досліджень, у конфліктах з активним використанням психологічних операцій може використовуватися одночасно 40-50 різних наративів, що систематично тиражуються різними каналами та створюють цілісну систему маніпулятивних меседжів. У випадку агресії проти України, РФ активно застосовувала психологічні операції для розпалювання ворожнечі між етнічними та політичними групами, експлуатуючи мовні та регіональні відмінності для дестабілізації українського суспільства.

Дипломатичні інструменти у контексті гібридної агресії використовуються для легітимізації дій агресора, блокування міжнародної реакції та створення враження дотримання міжнародного права. Це перетворює міжнародні інститути та правові механізми на зброю проти держави-жертви. Основні дипломатичні тактики включають вісім ключових напрямків:

Використання права вето в Раді Безпеки ООН дозволяє постійному члену РБ ООН систематично блокувати резолюції, що засуджують його агресію або передбачають санкції. Це паралізує головний механізм колективної безпеки та унеможливлює ефективну міжнародну реакцію через найвпливовіший орган системи ООН, створюючи структурний дефіцит системи, коли держава-агресор сама блокує механізми протидії її агресії.

Організація псевдо-референдумів під виглядом «волевиявлення народу» легітимізує окупацію або відторгнення територій. Ці «референдуми» порушують всі міжнародні стандарти: проводяться під дулами автоматів, без присутності міжнародних спостерігачів, із заздалегідь визначеними результатами та масовими фальсифікаціями, але формально створюють ілюзію демократичного процесу.

Створення паралельних «державних» структур на окупованих територіях з власними «урядами», «парламентами», «силовими структурами», «судовою системою» має створити ілюзію легітимності сепаратистських утворень та їхньої незалежності від

агресора. Агресор часто маніпулює принципом «права на самовизначення народів», вибірково цитуючи міжнародні документи, викривляючи їхній зміст та ігноруючи інші частини, що містять обмеження та процедурні вимоги.

Маніпулювання міжнародними організаціями включає спроби використання ОБСЄ, Червоного Хреста та інших гуманітарних організацій для легітимізації присутності на окупованих територіях під виглядом «гуманітарних місій». «Гуманітарні конвої» можуть використовуватися для постачання військового спорядження та підкріплень, прикриваючись міжнародним гуманітарним правом.

Нав'язування «мирних ініціатив» передбачає створення переговорних форматів, де агресор виступає не як сторона конфлікту, а як «посередник» або «гарант». Такі угоди використовуються не для реального врегулювання конфлікту, а для «заморожування» ситуації, закріплення контролю над окупованими територіями та внутрішньої дестабілізації держави-жертви через вимоги особливого статусу окупованих територій, амністії бойовиків або федералізації.

Дезінформаційні кампанії на міжнародному рівні включають систематичну роботу з формування «альтернативної реальності» для західних аудиторій, фінансування проросійських політиків та ЗМІ в іноземних країнах, підтримку євроскептичних та популістських рухів, що виступають проти підтримки держави-жертви.

Юридична війна (lawfare) означає використання міжнародних судів та арбітражів для створення ілюзії правової боротьби: позови щодо «дискримінації співвітчизників», претензії на активи на окупованих територіях, спроби оскарження санкцій, використання міжнародного права як зброї для політичного та економічного виснаження противника.

Маніпуляція міжнародними переговорними форматами передбачає нав'язування таких механізмів переговорів, де агресор виступає не як сторона конфлікту, а як «посередник» або «гарант миру», що дозволяє йому уникати прямої відповідальності за агресію та контролювати переговорний процес.

Російська дипломатія активно використовує право вето для блокування міжнародної реакції та нав'язує переговорні формати, в яких виступає не стороною конфлікту, а «посередником», що дозволяє уникати відповідальності за агресію.

Варто розуміти, що архітектура гібридної агресії постійно еволюціонує, адаптуючись до нових технологічних можливостей та реакції противника. За прогнозами Міжнародного інституту стратегічних досліджень (IISS), до 2030 року штучний інтелект стане ключовим інструментом гібридної війни, що вимагає превентивного розвитку механізмів протидії. Основні напрямки еволюції гібридного інструментарію включають шість критичних векторів.

Синтетичні медіа (діпфейки) є однією з найбільш загрозливих технологій майбутнього. Технології глибинного навчання дозволяють створювати надзвичайно реалістичні фальшиві відео та аудіозаписи політичних лідерів, військовослужбовців, журналістів. На відміну від традиційної дезінформації, діпфейки створюють візуальне «підтвердження» неіснуючих подій, що робить їх надзвичайно переконливими для аудиторії. Технології швидко вдосконалюються, і майбутні діпфейки будуть практично невідрізнимі від справжніх записів, що створює фундаментальну загрозу для довіри до будь-якого візуального контенту. Російські актори вже активно тестують діпфейки та ШІ-генерований контент у своїх інформаційних операціях.

Автономні системи дезінформації на базі ШІ представляють якісно новий рівень загрози. Штучний інтелект здатний генерувати величезні обсяги персоналізованого дезінформаційного контенту, адаптованого під конкретні цільові аудиторії та навіть окремих користувачів. ШІ може аналізувати психологічні профілі користувачів соціальних мереж на основі їхньої активності, вподобань, коментарів та створювати меседжі, що максимально ефективно впливають на їхні переконання. Це дозволяє здійснювати мікротаргетинг на безпрецедентному рівні, де кожен користувач отримує персоналізований дезінформаційний контент, оптимізований саме для його вразливостей.

Квантові комп'ютери для злому шифрування створюють фундаментальну загрозу для кібербезпеки. Розвиток квантових обчислень може зробити застарілими існуючі системи криптографічного захисту, що базуються на складності факторизації великих чисел. Квантовий комп'ютер достатньої потужності теоретично може зламати RSA та інші широко використовувані алгоритми шифрування за лічені години замість мільйонів років, що потрібні класичним комп'ютерам. Це може дозволити агресору отримувати доступ до найбільш захищених державних та військових мереж, дипломатичних комунікацій, фінансових систем. Гонка за створення квантово-стійкої криптографії (постквантової криптографії) стає критично важливою для майбутньої безпеки.

Атаки на системи штучного інтелекту (adversarial attacks) дозволяють маніпулювати роботою алгоритмів ШІ через підготовлені спеціальним чином дані – так звані adversarial examples. Ці атаки можуть змусити системи розпізнавання зображень неправильно класифікувати об'єкти, системи автономного керування приймати небезпечні рішення, алгоритми модерації контенту пропускати забороненіматеріали або блокувати легітимний контент. У військовому контексті це може означати саботаж автономних систем озброєння, систем розпізнавання цілей, алгоритмів підтримки прийняття рішень командування.

Інтеграція кібер- та фізичних атак передбачає поєднання кібератак на системи управління критичною інфраструктурою з фізичними диверсіями для досягнення каскадного ефекту та максимальної дестабілізації. Наприклад, кібератака може вивести з ладу системи пожежогасіння перед фізичним підпалом, або зруйнувати системи резервного живлення перед атакою на основні енергетичні об'єкти. Така синхронізація може призвести до катастрофічних наслідків, значно перевищуючи ефект від окремих атак.

Використання як зброї соціальних мереж (weaponization of social media) означає експлуатацію алгоритмів рекомендацій та механізмів поширення контенту для цілеспрямованого посилення поляризації суспільства, розпалювання внутрішніх

конфліктів, маніпулювання громадською думкою через мікротаргетинг. Алгоритми соціальних мереж, оптимізовані для максимізації залученості населення, часто просувають емоційно забарвлений та поляризуючи контент, що може бути експлуатовано для штучного посилення соціальних розколів.

Досвід країн Балтії показує, що систематична освітня робота щодо розпізнавання дезінформації суттєво підвищує опірність суспільства до гібридних загроз. Критично важливим для протидії майбутнім загрозам є: розвиток медіаграмотності населення з раннього віку; підготовка фахівців з кібербезпеки та інформаційної безпеки; створення систем раннього виявлення та реагування на гібридні загрози; розробка технологій верифікації контенту та виявлення синтетичних медіа; міжнародна кооперація у протидії гібридним загрозам; масштабні інвестиції у дослідження постквантової криптографії; розбудова стійкої до кібератак критичної інфраструктури з множинними рівнями захисту.

Комплексний аналіз основних інструментів гібридної агресії демонструє їхню багатовимірність, синхронність та взаємопідсилюючий характер. Жоден з цих інструментів окремо не є достатнім для досягнення стратегічних цілей, але їхнє комплексне застосування створює кумулятивний ефект, що значно ускладнює протидію та вимагає всеохоплюючої стратегії оборони.

Російська модель гібридної агресії вирізняється саме повнотою та синхронністю використання всіх перелічених інструментів – від інформаційних операцій до кіберата к, від проксі-сил до економічного тиску, від психологічних операцій до дипломатичних маніпуляцій. Ця модель постійно еволюціонує, адаптуючись до технологічних змін, реакції противника та міжнародного контексту.

Це вимагає від держав-жертв та міжнародної спільноти не лише реактивної відповіді на вже застосовані інструменти, але й проактивної стратегії з прогнозування майбутніх загроз, розробки превентивних механізмів захисту та формування суспільної стійкості як найефективнішого захисту від гібридної агресії будь-якого типу.

Детальний аналіз практичного застосування цих інструментів на різних етапах російської агресії проти України 2014-2025 років буде подано в Розділі 3, що дозволить побачити, як теоретичні концепції реалізуються на практиці та які уроки можна винести для майбутньої протидії гібридним загрозам.

РОЗДІЛ 3. ГІБРИДНА АГРЕСІЯ РФ ПРОТИ УКРАЇНИ (2014-2025 рр.)

3.1. Анексія Криму та війна на Донбасі (2014-2015)

Російська гібридна агресія проти України, що розпочалася у 2014 році, стала найбільш показовим прикладом застосування гібридної стратегії в сучасній історії[4; 5; 10; 19; 41; 61; 136; 175; 185]. Військова складова цієї агресії ідеально відповідає визначенню Френка Гофмана про «fusion of war forms» і демонструє еволюцію від «війни без розпізнавальних знаків» до масштабних бойових дій з прямою участю регулярних російських військ під виглядом «добровольців»[115; 136; 155].

Кримська операція (офіційно зафіксована Росією як 20 лютого – 18 березня 2014 року) стала першим у світі успішним прикладом гібридної анексії суверенної території у післявоєнний період[136; 169; 176; 177]. Користуючись вакуумом влади після втечі Віктора Януковича та Революції Гідності, РФ реалізувала заздалегідь підготовлений план захоплення півострова[136; 169].

Рішення про початок операції було ухвалене особисто Володимиром Путіним ще в ніч з 22 на 23 лютого 2014 року під час таємної наради з керівниками силових відомств[57; 136]. За власним пізнішим визнанням Путіна (документальний фільм «Крим. Шлях на Батьківщину», 2015), саме тоді він дав пряме доручення «почати роботу з повернення Криму до складу РФ»[57]. Таким чином, планування анексії стартувало за три тижні до фейкового «референдуму» і навіть раніше за офіційну дату початку операції, зазначену на медалі «За возвращение Крыма» (20.02.2014)[136].

1 березня 2014 року, після звернення колаборанта Сергія Аксьонова, Путін офіційно попросив Раду Федерації дозволу на використання Збройних сил РФ на території України «для захисту російськомовного населення»[57; 136]. Рада

одностайно надала цей дозвіл, що дало Путіну повну внутрішньоросійську юридичну підставу для видачі наказів на інтервенцію[136].

Вже 11 березня 2014 року підконтрольна російським військовим Верховна Рада АР Крим прийняла «Декларацію про незалежність», а наступного дня – постанову про входження до складу РФ у разі «позитивного результату референдуму»[136; 176]. Таким чином, юридичне рішення про вихід Криму з України було ухвалене за п’ять діб до самого «голосування»[136].

Так званий «референдум» 16 березня 2014 року мав виключно пропагандистське значення і був юридично нікчемним з кількох причин: бюлетень містив лише дві опції, обидві з яких виключали можливість залишитися в Україні на чинних конституційних умовах (перша – пряме приєднання до РФ, друга – відновлення Конституції 1992 року з правом виходу зі складу України); Проводився за наявності російських військ і без дозволу центральної влади України, що суперечить ст. 73 Конституції України (зміна території – виключно всеукраїнський референдум); Результати були сфальсифіковані (в окремих районах «явка» сягала 123 %, а «за» - до 97 %)[95; 128; 136; 176; 177; 202].

Критично важливу роль у блискавичному захопленні півострова відіграло нелегальне використання баз Чорноморського флоту РФ: російські підрозділи «самовільно» покинули місця дислокації, визначені договором 1997/2010 років, і разом із підрозділами спецназу ГРУ та «зеленими чоловічками» встановили повний контроль над Кримом за 18 діб практично без бойових втрат[136; 169; 213; 250].

Медаль «За возвращение Крыма» з чітко зафіксованими датами 20.02-18.03.2014 (виготовлена ще до «референдуму»), нічна нарада Путіна 22-23 лютого, дозвіл Ради Федерації від 1 березня та декларація кримського парламенту від 11 березня є прямими документальними доказами ретельно спланованої, а не «спонтанної» чи «народної» операції[57; 136; 169; 176]. Усі ці факти остаточно спростовують російський пропагандистський наратив про «волевиявлення кримчан» і доводять, що анексія Криму була заздалегідь підготовленою державною військово-політичною операцією

РФ[95; 98; 128; 136; 176; 177; 202]. Ключовими елементами успіху кримської операції стали:

По-перше, блокування українських військових частин без відкритих бойових дій. Окупаційні війська використовували живий щит у вигляді цивільного населення під час штурмів кількох українських частин, що призвело до загибелі декількох українських військовослужбовців[136; 169; 173].

По-друге, захоплення стратегічних об'єктів малими групами спецпризначення, що діяли швидко та координовано, встановлюючи контроль над урядовими будівлями, аеропортами, військовими базами, портами та об'єктами критичної інфраструктури[136; 169; 213].

По-третє, інформаційне домінування через російські канали, що створювали ілюзію «народного повстання» та «захисту російськомовного населення від нацистів»[70; 91; 98; 104; 183].

По-четверте, відсутність чіткої реакції української влади у перехідний період після Революції Гідності, коли держава перебувала в стані дезорганізації[136; 167].
Швидкість операції не дозволила ні українській стороні, ні міжнародній спільноті організувати ефективну протидію[61; 136; 176]. До моменту, коли світ усвідомив масштаб агресії, Крим вже був фактично окупований, а 18 березня 2014 року РФ оголосила про «приєднання» півострова після псевдо-референдуму, що порушував всі міжнародні норми[95; 128; 136; 176; 177; 202].

Цікаво також зауважити те, що РФ протягом року спочатку відкидала звинувачення в військовій агресії, пізніше визнавала часткову присутність для «захисту російськомовних», а ще пізніше В.Путін відверто зізнався, що це були війська ВС РФ[57; 136; 169].

Донбаський театр: початок гібридної війни (березень-червень 2014).

На Донбасі військова складова російської гібридної агресії розгорталася інакше, ніж у Криму, пройшовши декілька чітко виражених етапів, кожен з яких

характеризувався різним рівнем прямої участі російських збройних сил та різними механізмами приховування цієї участі[136; 169; 174; 175; 185].

Перший етап (березень-червень 2014 року) можна охарактеризувати як проксі-фазу[136; 169; 174; 185]. Головними дійовими особами виступали російські громадяни на чолі з Ігорем Гіркіним (Стрєлковим), «колишнім» офіцером ФСБ РФ, Владиславом Безлером та іншими особами з досвідом роботи в російських силових структурах, а також представники місцевого криміналітету та завчасно підготовлені групи бойовиків[49; 53; 54; 65; 136; 169].

На цьому етапі Російська Федерація намагалася створити видимість «народного повстання» та «громадянської війни», мінімізуючи свою пряму участь та використовуючи наратив про «місцеве населення, що захищає свої права»[11; 12; 23; 70; 91; 98; 104; 183].

7 квітня 2014 року було оголошено про створення так званої «Донецької народної республіки», а через кілька днів – також «Луганської народної республіки»[136; 169; 174]. Сепаратисти захопили ключові адміністративні будівлі та стратегічні пункти в містах Донецьк і Луганськ, особливого супротиву вони не зазнали, оскільки поліція не могла чинити прямий супротив добре підготовленим бойовикам, а частина тієї ж поліції навіть перейшла до них[136; 169]. Проте навіть тоді спостерігалося систематичне постачання зброї, координація дій та інформаційна підтримка з боку РФ[65; 136; 169; 174; 175].

Група Гіркіна, що прибула з Криму, де вона брала участь в анексії, складалася переважно з російських громадян з військовим досвідом[49; 54; 65; 169]. Вони захопили будівлю Слов'янської міської ради та відділення міліції, поклавши початок збройному конфлікту на Донбасі[49; 54; 65]. Ця група діяла за чітким планом, використовуючи тактику, характерну для спецоперацій, що свідчило про професійну військову підготовку та централізоване керівництво[65; 136]. Окрім того були спроби відтворити донецький сценарій в інших регіонах, але вони зазнали невдачі, що

продемонструвало відсутність реальної масової підтримки сепаратизму в Україні[11; 12; 23]:

У Харкові 6-8 квітня 2014 року відбувся єдиний скоординований сплеск спроби створення «ХНР»: увечері 6 квітня проросійські активісти (за участі заїжджих груп із Бєлгорода та місцевих «тітушок») захопили будівлю Харківської ОДА, вивісили російський прапор і проголосили «Харківську народну республіку», 7 квітня вони намагалися утримувати будівлю, але вже до вечора 7 квітня сили МВС та спецпідрозділ «Ягуар» при підтримці харків'ян провели безкровну операцію зі звільнення ОДА, затримавши понад 60 осіб, до ранку 8 квітня «ХНР» припинила існування, не встигнувши сформувати жодних «органів влади» чи озброєних загонів, а спроба повторити донбаський сценарій була повністю зірвана[11; 23].

В Одесі 2 травня 2014 року сталася трагедія на Куликовому полі, де в результаті спланованих сутичок між проросійськими силами (багато з яких були громадянами РФ або координувалися з РФ) та проукраїнськими силами (людей, що приймали участь у мирній ході «за єдність України», до них вже під час заворушень доєдналися вболівальники Металіст та Чорноморець, оскільки в той день повинен був пройти футбольний матч), Під час заворушень загинуло 48 осіб (6 – проукраїнських активістів від вогнепальних поранень на Грецькій площі, 42 – у пожежі в Будинку профспілок)[44; 45].

Ці події були частиною ширшої гібридної операції РФ з дестабілізації півдня України та спроби створення «Одеської народної республіки» за донбаським сценарієм[44; 45; 136]. Спробу координували російські диверсанти (зокрема колишній співробітник ФСБ Антон Райх («Демон») та стрілець Віталій Будько («Боцман»), який першим відкрив вогонь з автомата), місцеві колаборанти Євгеній Мефьодов, Дмитро Одинов («Діма Скіф»), Сергій Долженков («Капітан Какао»), Єгор Кваснюк), зрадники в міліції (заступник начальника обласної міліції Дмитро Фучеджі, який після провалу втік до РФ і отримав російське громадянство й посаду) та один з ключових організаторів табору на Куликовому полі - відкритий російський неонацист Антон

Раєвський, що приїхав до Одеси як «тренер» бойовиків «Одеської бригади», координував табір і відкрито заявляв про плани створення «ОНР»[44; 45].

У Херсонській області навесні 2014 року російський сценарій «народних республік» зазнав повного краху: попри численні спроби проросійських активістів (серед яких уже тоді виділялися Кирило Стремоусов, Олексій Бєлов та оточення Володимира Сальдо) організувати захоплення ОДА, «референдум» та створення «Херсонської народної республіки», всі акції збирали лише кілька сотень–дві-три тисячі учасників і швидко придушувалися лояльними українській владі правоохоронцями за активної протидії місцевих жителів, які масово виходили на проукраїнські мітинги й фізично блокували сепаратистів[11; 12; 23].

Найгучніші спроби (1-2 березня, 23 березня та 7 квітня) закінчувалися нічим: міліція та СБУ не перейшли на бік організаторів, військові частини залишилися вірними присязі, а після трагедії в Одесі 2 травня проросійська активність різко згасла[11; 23]. Таким чином, Херсонщина стала одним із небагатьох регіонів півдня України, де відсутність масової підтримки, активний громадянський спротив і лояльність силовиків повністю зірвали російську гібридну операцію, до лютого 2022 року область залишалася під повним контролем України, а ті самі діячі, які у 2014-му не змогли зібрати й кількох тисяч людей, змогли «очолити» окупаційну владу лише під прикриттям російських танків[23; 82].

Ці невдачі продемонстрували, що без прямої військової підтримки з боку РФ сепаратистські рухи не могли досягти успіху навіть у регіонах з значною часткою російськомовного населення, спростовуючи російський наратив про «народне повстання»[11; 12; 23; 95; 104].

Перед переходом до наступного етапу варто зазначити, що в Донецькій та Луганській областях також були проукраїнські мирні мітинги, але вони швидко були придушені силами бойовиків та проросійськими групами[11; 12; 136].

Другий етап (липень-серпень 2014 року) став піком гібридності першої фази конфлікту та найяскравіше проявився під час Іловайської трагедії[65; 136; 169]. Саме

на цьому етапі відбулося введення регулярних підрозділів Збройних Сил РФ під виглядом угрупування «Північного Вітру» – офіційно непідтвердженої допомоги «добровольців», що використовували бронетехніку та артилерію, завезену прямо з РФ[65; 136; 169].

До літа 2014 року Збройні Сили України почали проводити антитерористичну операцію (АТО) та поступово звільняли окуповані території[136; 194; 195]. Сепаратистські угруповання, незважаючи на російську підтримку озброєнням та інструкторами, не могли протистояти наступу українських військ[65; 136]. Стало очевидно, що без прямого втручання регулярних російських військ проект «ДНР/ЛНР» приречений на поразку, це можна підтвердити й за зізнаннями Ігоря Гіркіна та Олександра Захарченка[49; 54; 65].

Іловайський котел у серпні 2014 року став символом цієї фази та однією з найтрагічніших сторінок війни[136; 194; 195]. Введення 3-ї та 6-ї танкових бригад, 31-ї десантно-штурмової бригади ЗС РФ дозволило оточити та завдати важкого удару по українських силах, що намагалися встановити контроль над Іловайськом – стратегічно важливим містом на шляху до кордону з РФ[65; 136; 169].

Українські підрозділи, що вели бої в районі Іловайська, опинилися в оточенні внаслідок масованого введення російських військ через неконтрольовану ділянку кордону[136; 194]. Незважаючи на домовленості про «зелений коридор» для виходу оточених сил, колони українських військових були обстріляні з важкої артилерії та реактивних систем залпового вогню[136; 194; 195]. За різними оцінками, загинуло від 366 до понад 400 українських військовослужбовців, сотні були поранені або потрапили в полон[136; 194].

Дані міжнародних розслідувань Bellingcat та українського проекту InformNapalm неспростовно довели участь регулярних російських підрозділів, незважаючи на офіційне заперечення РФ[65; 169]. Докази включали: геолокаційні дані з соціальних мереж російських військовослужбовців; фотографії військової техніки з ідентифікаційними номерами підрозділів ЗС РФ; свідчення полонених російських

військових; супутникові знімки переміщення колон військової техніки через російсько-український кордон; використання озброєння, якого не було на озброєнні ЗСУ[65; 169].

Іловайська трагедія стала переломним моментом, після якого стало неможливо підтримувати ілюзію «громадянської війни»[136; 194]. Масштаб військового втручання РФ був надто очевидним, незважаючи на всі спроби РФ це заперечувати[65; 136].

Окремо варто згадати подію в ніч з 24 на 25 серпня 2014 року, коли псковський десант, що намагався проникнути на територію України, був затриманий та допитаний українськими силами[65; 136]. Проте російська сторона стверджувала, що військовослужбовці «просто загубилися» під час навчань, незважаючи на те, що вони були повністю озброєні та знаходилися на значній відстані від кордону[65].

Приватні військові компанії та «відпускники» (вересень 2014 - лютий 2015): Після Іловайська РФ дещо змінила тактику, намагаючись зменшити видимість прямої участі регулярних військ[65; 136; 169]. Розпочався третій етап (вересень 2014 – лютий 2015 року), який характеризувався появою феномену «відпускників» – військовослужбовців ЗС РФ, які офіційно перебували у відпустці, але насправді брали участь у бойових діях на Донбасі[65; 136]. До них додалися приватні військові компанії (ПВК) та артилерійські підрозділи, що діяли безпосередньо з території РФ[65; 174].

ПВК стали важливим елементом гібридної стратегії, що дозволяв Кремлю зберігати «правдоподібне заперечення» (plausible deniability) прямої участі у конфлікті[65; 155; 173]. Найвідомішою стала група «Вагнер» під керівництвом Євгена Пригожина та Дмитра Уткіна, яка офіційно була визнана лише у 2022 році[65].
Використання ПВК дозволяло РФ: заперечувати офіційну участь у конфлікті; уникати публічної відповідальності за втрати; використовувати найманців для найбільш ризикованих операцій; обходити міжнародні санкції та правові обмеження[65; 155].

Битва за Дебальцеве (січень-лютий 2015 року) стала кульмінацією цього етапу[136; 194; 195]. Дебальцеве було критично важливим транспортним вузлом, що з'єднував окуповані Донецьк та Луганськ[136; 194]. Участь 5-ї танкової бригади з

Улан-Уде підтверджується свідченнями контрактника Доржі Батомункуєва, який розповів про фарбування техніки перед відправкою та заборону брати документи, стандартні заходи для приховування участі регулярних військ[65; 169; 174].

Масоване використання важкої артилерії та реактивних систем залпового вогню дозволило російським силам зламати оборону українських військ[136; 174; 194]. Українські підрозділи змушені були відступити з Дебальцево в лютому 2015 року після підписання Мінських угод, які використовувалися РФ не для врегулювання конфлікту, а для закріплення контролю над захопленими територіями та використання саме гібридних компонентів агресії проти України[136; 142; 145; 217].

Ключові докази, що неспростовно руйнують наратив РФ про «громадянську війну» та «внутрішній конфлікт», включають не лише Іловайськ та Дебальцеве, але й систематичне використання озброєння, якого ніколи не було на озброєнні Збройних Сил України[65; 136; 169; 174].

Серед такого озброєння: Важка вогнеметна система ТОС-1 «Буратино» термобаричний реактивний комплекс залпового вогню; Комплекси радіоелектронної боротьби Р-330Ж «Житель» та РБ-341В «Леєр-3»; 240-мм міномет 2С4 «Тюльпан»; Безпілотники «Орлан-10» тактичні БпЛА російського виробництва; Системи придушення супутникового сигналу «Свет-КУ» та інші зразки, характерні виключно для ЗС РФ[65; 169; 174].

Спеціальна моніторингова місія ОБСЄ у своїх звітах протягом 2014-2015 років неодноразово фіксувала присутність цього озброєння на окупованих територіях[174; 194; 195]. Важливо відзначити, що без підготовлених спеціалістів практично жодним з перелічених засобів неможливо користуватися[65; 174].

За даними проекту «Вантаж-200» та міжнародної мережі «Цитадель», втрати російських ПВК та регулярних військ на Донбасі протягом 2014-2015 років становили значну частину від загальних втрат до 24 лютого 2022 року[48; 62]. До 2016 року загинуло щонайменше 675 російських військових, а також понад 240 осіб, чия ідентичність залишалась не встановленою[48; 62].

Високопрофесійні військові, серед яких генерали та командири підрозділів, загинули в результаті бойових дій на українській території, що прямо підтверджує їхню участь у конфлікті, оскільки в їх некрологах вказується, що вони «загинули при виконанні» або «загинули при виконанні службового обов'язку»[48; 62; 65]. Ці цифри офіційно не визнаються РФ, проте підтверджуються перехресними даними з відкритих джерел, повідомленнями родичів загиблих та журналістськими розслідуваннями[48; 62; 65; 169].

Таким чином, період 2014-2015 років продемонстрував повний спектр інструментів російської гібридної агресії: від анексії Криму через швидку операцію «зелених чоловічків» до затяжної війни на Донбасі з використанням проксі-сил, ПВК, «відпускників» та регулярних військових підрозділів[4; 5; 10; 65; 136; 169; 174; 185]. Цей досвід став основою для подальшої еволюції російської гібридної стратегії та підготовки до повномасштабного вторгнення 2022 року[105; 136; 178; 185].

3.2. 2016-2021: заморожений конфлікт і непрямі дії

Період 2016-2021 років у російсько-українській війні характеризувався трансформацією відкритого збройного протистояння у стан так званого «замороженого конфлікту»[136; 142; 145; 173; 185]. Однак за фасадом відносної стабілізації лінії розмежування відбувалася системна трансформація гібридної агресії: військові проксі-структури переходили під пряме російське командування, економічний тиск набував нових форм, а інформаційно-психологічні операції досягали піку своєї ефективності[65; 136; 169; 173; 174]. Цей період став критично важливим для розуміння довгострокової стратегії РФ, спрямованої не на швидку перемогу, а на виснаження України через багатовекторний тиск і підготовку плацдарму для майбутньої ескалації[105; 136; 178; 185].

Після підписання Комплексу заходів з виконання Мінських угод (12 лютого 2015 року) та битви за Дебальцеве військова ситуація на Донбасі увійшла у фазу відносної

стабілізації[136; 142; 145; 194; 195]. Четвертий етап гібридного конфлікту на Донбасі (2015-2022 роки) характеризувався певною стабілізацією лінії розмежування, але за фасадом «замороженого конфлікту» відбувалася системна трансформація окупаційних угруповань під пряме російське командування[65; 136; 169; 174].

Формально окремі «1-й та 2-й армійські корпуси ДНР/ЛНР» насправді перебували під прямим командуванням 8-ї армії Південного військового округу Збройних Сил Російської Федерації[65; 136; 169; 174]. Гібридність цього етапу проявлялася у офіційному запереченні присутності російських військ при фактичному повному контролі над бойовими діями, матеріально-технічним забезпеченням та кадровою політикою окупаційних угруповань[65; 173]. РФ зберігала механізм «правдоподібного заперечення» (plausible deniability), формально дистанціюючись від подій на Донбасі, але фактично керуючи всіма аспектами військових операцій[155; 173]. Лінія розмежування, що пролягла через Донецьку та Луганську області, перетворилася на де-факто кордон між контрольованою Україною територією та окупованими районами[136; 173; 174].

Використання проксі-сил – тобто недержавних акторів або озброєних груп, що діють в інтересах агресора без формального підпорядкування, стало ключовою складовою гібридної агресії у цей період[65; 155; 173]. Згідно зі звітом Офісу Верховного комісара ООН з прав людини, ці формування публічно на 60-70% складалися з місцевих жителів, завербованих через економічні або інші важелі, але їхнє керівництво, навчання та озброєння забезпечувалися РФ[173]. Механізми залучення проксі-сил у період 2016-2021 років включали п'ять основних категорій:

По-перше, місцеві сепаратистські угруповання – «ДНР» та «ЛНР», що формально позиціонувалися як «народні республіки», але насправді контролювалися та фінансувалися РФ[65; 136; 169; 174]. Практично всі керівні посади займали російські громадяни з досвідом роботи в силових структурах РФ (ФСБ, ГРУ)[65; 136].

По-друге, приватні військові компанії – найбільш відомою є ПВК «Вагнер», що була сформована спеціально для ведення гібридної війни проти України[65; 155]. За

даними розслідування Bellingcat, «Вагнер» використовувався для виконання особливо складних бойових завдань, де пряма участь регулярних російських військ була б надто очевидною[65].

По-третє, «добровольці» та «відпускники» – російські військовослужбовці, які формально перебували у відпустці або звільнилися зі служби, але насправді діяли в складі організованих підрозділів зі збереженням військової структури та командування, що цікаво перевіряючи інформацію по таких загиблих «відпускниках» можна було виявити, що більшість з них в некрологах містили статус «загинув при виконанні»[65; 136; 169; 174].

По-четверте, кримінальні угруповання – використання кримінальних елементів для дестабілізації, захоплення адміністративних будівель, залякування місцевого населення на початковій фазі конфлікту[136; 155]. Також сюди входять й колишні в'язні, яких після окупації території випускали й переформатовали в «народну міліцію» або інші структури бойовиків, так до прикладу самим відомим з них був Максим Фомін більш відомий на широкий загал під псевдонімом «Владлен Татарський», що став «військовим кореспондентом» на окупованій території[136].

По-п'яте, іноземні найманці – залучення бойовиків з різних країн (Сербія, країни Кавказу, Центральної Азії, Іспанії) через ідеологічні, релігійні або фінансові мотиви[65; 155; 174].

Використання проксі-сил дозволяло РФ: заперечувати пряму участь у конфлікті; уникати міжнародної відповідальності; знизити політичні витрати від людських втрат серед регулярних військових; створити ілюзію «громадянського конфлікту»; гнучко регулювати інтенсивність конфлікту й тим часом формувати військовий досвід у своїх військовослужбовців та експериментувати над кожним компонентом гібридної агресії[65; 115; 155; 173].

Неспростовним доказом прямої російської участі стало систематичне використання озброєння, якого ніколи не було на озброєнні Збройних Сил України[65; 169; 174]. Серед такого озброєння: важка вогнеметна система ТОС-1 «Буратино»,

комплекси радіоелектронної боротьби Р-330Ж «Житель» та РБ-341В «Леєр-3», 240-мм міномет 2С4 «Тюльпан», реактивна система залпового вогню «Чебурашка», безпілотники «Орлан-10», системи придушення супутникового сигналу «Свєт-КУ» та інші зразки, характерні виключно для російської армії[65; 169; 174].

Спеціальна моніторингова місія ОБСЄ у своїх звітах протягом 2016–2021 років неодноразово фіксувала присутність цього озброєння на окупованих територіях[174]. Важливо відзначити, що без підготовлених спеціалістів практично жодним з перелічених засобів неможливо користуватися, а у випадку з РСЗВ «Чебурашка» очевидно, що Російська Федерація використовувала зону бойових дій як полігон для випробувань нового озброєння[65; 174].

Критично важливим доказом російської військової присутності стала справа В'ячеслава Забалуєва, заступника керівника постачальника харчування для Південного військового округу Міноборони РФ[65; 136; 169; 174; 48]. У рішенні Кіровського районного суду міста Ростова-на-Дону від 10 листопада 2021 року зазначалося, що він постачав харчування для «військових частин РФ, дислокованих на території ДНР і ЛНР»[65; 174].

Ця справа не лише підтверджувала присутність регулярних підрозділів Збройних Сил РФ на окупованих територіях Донбасу протягом усього періоду «замороженого конфлікту», але й ймовірно свідчить про активну підготовку логістичної інфраструктури до повномасштабного вторгнення 2022 року[65; 136; 174].

У період 2016-2021 років приватні військові компанії стали ключовим елементом гібридної стратегії, що дозволяв Кремлю зберігати «правдоподібне заперечення» (plausible deniability) прямої участі у конфлікті[65; 155; 173]. Найвідомішою стала група «Вагнер» під керівництвом Євгена Пригожина та Дмитра Уткіна, яка офіційно була визнана лише у 2022 році[65].

Саме Пригожин уперше публічно визнав, що заснував ПВК «Вагнер» у 2014 році з метою надання підтримки бойовим формуванням на сході України[65]. У своїх заявах він зазначав, що особисто займався постачанням зброї, включаючи бронежилети та

інше спорядження для бойовиків, що підтверджує високий рівень організованості і координації між приватними військовими структурами та державними органами РФ[65].

Поряд з «Вагнером» діяли ПВК «Редут», «Патріот», «Еспаньола» та інші структури, що формально не підпорядковувалися Міністерству оборони РФ, але насправді координували свої дії з російськими спецслужбами[65; 155]. За даними проекту «Вантаж-200» та міжнародної мережі «Цитадель», втрати російських ПВК та регулярних військ на Донбасі до 24 лютого 2022 року становили щонайменше 12-15 тисяч загиблих[48; 62; 65].

Як згадувалося раніше у Розділі 3.1. За підрахунками проекту «Вантаж-200» до 2016 року загинуло щонайменше 675 російських військових, а також понад 240 осіб, чия ідентичність залишалась не встановленою[48; 62]. Високопрофесійні військові, серед яких генерали та командири підрозділів, загинули в результаті атак на українській території, що прямо підтверджує їхню участь у бойових діях, оскільки в їх некрологах вказується, що вони «загинули при виконанні»[48; 62; 65].

Значну частину втрат складають представники спецслужб РФ, зокрема співробітники ФСБ, які активно здійснювали репресії на окупованих територіях, а також контролювали місцеве населення через залякування та тортури[65; 136; 155]. Ці цифри офіційно не визнаються Москвою, проте підтверджуються перехресними даними з відкритих джерел, повідомленнями родичів загиблих та журналістськими розслідуваннями[48; 62; 65].

Період 2016-2021 років став часом найактивнішої діяльності проросійської «п'ятої колони» всередині України та найінтенсивніших дипломатичних маніпуляцій з боку РФ найнебезпечнішим елементом політико-дипломатичної стратегії якої у період «замороженого конфлікту» стала спроба нав'язати Україні федералізацію через механізм «особливого статусу Донбасу» (або ж сьогодні більш відомого позначення «ОРДЛО») в рамках Мінських угод[142; 145; 217].

«Формула Штайнмайєра» (2016-2019 роки) становила собою класичну пастку рефлексивного управління: під виглядом «компромісного мирного плану» Україні пропонувалося: Конституційно закріпити особливий статус окупованих територій, Провести там вибори під контролем російських збройних формувань, Лише потім отримати контроль над кордоном[142; 145; 217].

Така послідовність фактично легалізувала б окупацію, надала б «ДНР/ЛНР» право вето у ключових питаннях зовнішньої та внутрішньої політики України та встановила б постійний механізм російського впливу на українську державність[142; 145; 217].

Протистояння цьому тиску з боку України, незважаючи на величезний міжнародний тиск (особливо з боку Франції та Німеччини у рамках «Нормандського формату»), стало важливим стратегічним успіхом[142; 145; 217]. Відмова від капітуляційного сценарію зберегла суб'єктність України та можливість подальшого спротиву[145; 217].

Парадоксально, але саме підписання пакету Мінських документів стало дипломатичною пасткою для самої РФ, оскільки підписавши, ці документи російська сторона сама фактично визнала свою присутність та діяльність проти України[142; 145; 217].

У першому документі РФ виступала «гарантом» у Трьохсторонній контактній групі (ТКГ) з представниками «ДНР/ЛНР» як «свідками» без офіційного статусу, хоча це вже можна було б визначати, як присутність РФ на підставі трьох підписантів, а не п’яти[142; 217]. Проте саме в деклараціях та протоколах (зокрема, Мінська декларація 2015) вже на РФ покладалися конкретні зобов'язання[145; 217]. Саме підписання цих документів та подальші західні санкції, прив'язані виключно до невиконання РФ, Мінських зобов'язань, остаточно зафіксували її роль як фактичної сторони конфлікту попри всі спроби формального заперечення[142; 145; 212; 217].

Ще одним політичним напрямком діяльності РФ протягом період 2016-2021 років стала політична стратегія по створенню та підтримці мережі ключових агентів впливу на найвищих рівнях української політики;

Віктор Медведчук – кум президента Путіна, неофіційний канал зв'язку між Києвом та Москвою у 2019-2021 роках, очолював партію ОПЗЖ[32; 40; 59; 225]. Його роль була центральною у просуванні російських інтересів через політичні та медійні канали[40; 59; 225].

Тарас Козак – власник телеканалів «112 Україна», NewsOne, ZIK, бізнес-партнер Медведчука[32; 40]. Ці телеканали стали основними платформами для поширення проросійських наративів в українському інформаційному просторі[32; 40].

Юрій Бойко – лідер ОПЗЖ, активно підтримував Москву через публічні заяви та регулярні поїздки до РФ, просуваючи ідеї «особливого статусу» Донбасу та федералізації України[59].

Євген Мураєв – лідер проросійської партії «Наші» та власник телеканалу «НАШ», використовував медіаплатформу для систематичного поширення антиукраїнських меседжів[32; 40].

Анатолій Шарій – блогер, що діяв з території Іспанії та ЄС, використовував цифрові платформи для поширення антиукраїнських меседжів, засновник групи «Партія Шарія», яка мала представництво у місцевих радах[40].

Ілля Кива – колишній депутат від ОПЗЖ, що давав інтерв'ю російським пропагандистам, ширячи антиукраїнські матеріали та дискредитуючи українську владу[40; 59].

Андрій Деркач – оприлюднював компромат про українських та американських політиків, використовуючи тактику інформаційних вкидань для дестабілізації політичної ситуації[40].

Вадим Новинський – олігарх, пов'язаний з Українською православною церквою Московського патріархату, використовував економічний та релігійний вплив для просування проросійської позиції[59].

Є багато й інших агентів підтримуваних РФ, але основними в політичній діяльності на нашу думку є саме ці особи[32; 40; 59; 225]. Функціонування проросійських політичних партій, що пройшли трансформацію від Партії регіонів (2010-2014) до Опозиційної платформи – За життя (ОПЗЖ, 2014-2022), забезпечувало політичне представництво проросійських настроїв у Верховній Раді та регіональних радах, лобіювання інтересів РФ під виглядом захисту «прав російськомовних» та протидію євроінтеграційному курсу України[32; 40; 59; 225].

Російська православна церква (РПЦ) та її українське відгалуження – Українська православна церква Московського патріархату (УПЦ МП) – відігравали роль ідеологічної платформи концепції «русского мира»[124; 139; 241]. Через мережу парафій, духовні навчальні заклади та громадські організації поширювалися наративи про єдиний «православний цивілізаційний простір», не-канонічність незалежної України та небезпеку «західного впливу»[124; 139].

Надання Томосу про автокефалію Православної церкви України у 2019 році з ініціативи Петра Порошенка стало потужною контроперацією, що значно послабило російський релігійний вплив у період 2019-2021 років[124; 139; 241]. Проте це не ліквідувало його повністю, незважаючи на певну низку постанов для обмеження УПЦ МП, вони продовжували діяти як інструмент російського впливу аж до повномасштабного вторгнення 2022 року[124; 139]. Тиск з боку партнерів, окремих верств населення та українське законодавство не дозволяють повністю ліквідувати цю організацію навіть після початку повномасштабної війни[56; 124; 139].

Дипломатичні інструменти у період 2016-2021 років використовувалися для легітимізації дій агресора, блокування міжнародної реакції та створення враження дотримання міжнародного права[41].

Використання права вето в Раді Безпеки ООН передбачало систематичне блокування резолюцій, що засуджують російську агресію, паралізуючи головний механізм колективної безпеки[176]. Маніпуляція міжнародними переговорними форматами передбачала нав'язування «Нормандського формату», де РФ виступала не

як сторона конфлікту, а як «посередник», що дозволяло їй уникати прямої відповідальності за агресію[217]. Особливо показовим в цьому питанні є блокування будь яких рішень по введенню «миротворців» на територію «Донбасу» за допомогою права Вето[145].

Дезінформаційні кампанії на міжнародному рівні включали систематичну роботу з формування «альтернативної реальності» для західних аудиторій, фінансування проросійських політиків та ЗМІ в європейських країнах, підтримку євроскептичних та популістських рухів, що виступають проти підтримки України[183; 70].

Економічна складова російської гібридної агресії у період 2016-2021 років використовувалася як інструмент «війни без війни» – створення економічного тиску, що мав на меті послабити українську державу, знизити життєвий рівень населення та створити внутрішню напругу без прямого застосування військової сили[87]. Особливого успіху така діяльність не мала, але окупація значної частки українських територій саме по собі спричинило серйозний удар по українській економіці[94].

Після анексії Криму та початку війни на «Донбасі» РФ запровадила масштабні торговельні санкції проти України[87]. Було заборонено імпорт понад 300 позицій українських товарів, включаючи продукцію харчової промисловості, машинобудування, хімічної галузі[87]. Оскільки на той момент російський ринок залишався одним з основних для українського експорту (особливо для східних регіонів), ці обмеження завдали відчутного удару по українській економіці та спричинили закриття низки підприємств[87].

Транзитна війна (2014-2019 роки) проявлялася в систематичних обмеженнях транзиту українських товарів територією РФ до країн Центральної Азії та Кавказу, штучних затримках на кордоні, запровадженні додаткових «технічних» вимог[87].

Крім торгових обмежень, РФ також наклала санкції на фінансовий сектор України, зокрема обмеживши доступ до російських фінансових ринків[99]. Українські банки та фінансові установи, які працювали з російськими партнерами, зазнали серйозних фінансових труднощів[99]. Російські банки, зокрема «Сбербанк», «ВТБ»,

«Газпромбанк», почали зменшувати свою присутність в Україні або припиняти співпрацю з українськими контрагентами[99].

Блокада Азовського моря стала черговим прикладом економічної агресії з використанням військових засобів[186]. Після будівництва Кримського мосту у 2018 році РФ де-факто встановила контроль над Керченською протокою та почала систематично затримувати цивільні судна, що прямували до українських портів Маріуполя та Бердянська або поверталися з них[186].

За неповними даними, протягом 2018-2022 років було затримано близько 15 тисяч суден, а час очікування в деяких випадках досягав кількох діб[186]. Економічні втрати від фактичної блокади портів оцінюються приблизно у $3-4 мільярди доларів, не враховуючи непрямих збитків від згортання бізнесу та скорочення робочих місць[249; 94].

Будівництво газопроводу «Північний потік-2» (активна фаза 2018–2021 років, завершення у 2021 році) мало на меті повний обхід української газотранспортної системи[158; 209]. Це не лише позбавляло Україну гарантованих $2-3 мільярдів доларів транзитних доходів щорічно, але й знижувало стратегічну цінність України як транзитера енергоносіїв для Європи[158][209]. Фактично це був елемент довгострокової стратегії ізоляції України та зниження її геополітичної суб'єктності[158; 209].

Окрім того у період 2016-2021 років РФ застосувала секторальні санкції до українських енергетичних та металургійних компаній[87; 99]. Зокрема, були накладені обмеження на поставки енергоресурсів до України, включаючи вугілля, електроенергію та газ, що створювало додаткові економічні труднощі в умовах воєнних дій на сході[87; 99]. Водночас обмеження стосувалися і фінансування українських інфраструктурних проектів[87; 99].

Парадоксально, але спроба РФ перетворити енергетичну залежність на інструмент довготривалого політичного контролю обернулася стратегічною поразкою[197]. Після газових воєн 2006 та 2009 років та гібридної агресії 2014-2015

років Україна повністю відмовилась від прямих закупівель російського газу, розвинула фізичний реверс із ЄС, накопичила стратегічні резерви[197].

Пізніше Україна виграла Стокгольмський арбітраж 2017-2018 років, отримавши $4,63 млрд компенсації та юридичне скасування кабальних умов договору 2009 року[197]. Таким чином, замість підкорення України, РФ прискорила її вихід із пострадянської енергетичної орбіти й заклала основу для енергетичної незалежності[197].

Економічна складова гібридної агресії у період 2016-2021 років виявилася не менш руйнівною, ніж військова, особливо враховуючи її тривалий та накопичувальний характер[87; 94]. Водночас введення санкцій призвело до зміцнення зв'язків України з Європейським Союзом та іншими західними партнерами, що почали надавати підтримку Україні в умовах економічного тиску з боку РФ[9]. Зокрема, ЄС і США ввели відповідні санкції проти РФ, що, у свою чергу, поглибило економічну ізоляцію самої РФ[9].

Період 2015-2021 років став часом найактивнішого використання кібернетичних інструментів у рамках гібридної агресії[89; 100; 110; 148]. Серія кібератак 2016-2017 років стала піком кібернетичної компоненти гібридної війни у період «замороженого конфлікту»[89; 100; 110; 148]. Україна фактично стала полігоном для випробування найсучасніших кіберзброї та тактик, деякі з яких згодом використовувалися проти інших країн[89; 100; 110; 148].

Атака BlackEnergy (23 грудня 2015 року) увійшла в історію як перша в світі успішна кібератака на енергетичну мережу, що призвела до реального відключення електропостачання[100; 143; 148]. Атака була спрямована на систему управління енергетичними мережами у західних регіонах України, що призвело до знеструмлення понад 225 тисяч споживачів[100; 143; 148].

Використання шкідливого програмного забезпечення BlackEnergy дозволило зловмисникам отримати доступ до контрольованих систем енергетичних підприємств

та викликати збій[100; 143; 148]. Атака продемонструвала вразливість критичної інфраструктури до кіберзагроз та необхідність її комплексного захисту[100; 143; 148].

Атака Industroyer (грудень 2016 року) була спрямована на енергетичну інфраструктуру України та продемонструвала подальшу ескалацію кіберзагроз після BlackEnergy 2015 року[110]. Це був черговий доказ того, що Україна використовувалася як полігон для відпрацювання кіберзброї перед її потенційним застосуванням проти інших країн[110; 185].

Серія атак, однією з яких став NotPetya 27 червня 2017 року, стала наймасштабнішою кібератакою в історії за обсягом завданих збитків. Хоча формально це був вірус-шифрувальник (ransomware), насправді він був спрямований на максимальне руйнування даних[110].

Глобальні збитки перевищили $10 мільярдів доларів, з яких $4-5 мільярдів припало на Україну. Вірус спочатку маскувався під звичайний вірус-вимагач, але насправді мав на меті не тільки вимагання грошей, а й знищення даних та саботаж. Були паралізовані роботи десятків українських підприємств, державних установ[110].

Вірус поширився через мережі українських банків і викликав значні збої в їх роботі, зокрема в таких фінансових установах, як «Приватбанк» та «Ощадбанк»[110]. Міжнародні компанії також зазнали величезних втрат: компанія Maersk втратила $300 мільйонів, FedEx близько $400 мільйонів[110]. Це була фактично акт кібервійни, замаскований під кримінальну активність[110].

Протягом 2017 року відбувалася серія атак, що торкнулася як урядових, так і приватних інтернет-ресурсів. Метою цих атак було порушити роботу важливих державних інституцій і знизити їхню здатність реагувати на зовнішні та внутрішні загрози[110; 41]. Атаки поширювали шкідливі програми типу Petya, що призводило до блокування доступу до ключових онлайн-систем, таких як урядові портали, банківські платформи та деякі підприємства[110; 41]. Технічно атака використовувала вразливість у програмному забезпеченні Microsoft Windows, демонструючи високий рівень технічної підготовки зловмисників[110; 41].

Атаки на критичну інфраструктуру (2018) включали спроби зламати системи електронного уряду[14; 185]. Основною метою було порушення стабільності урядових функцій, зокрема в період підготовки до парламентських виборів[14; 185]. Зловмисники застосовували «фішингові» атаки для отримання доступу до конфіденційних даних співробітників державних структур, а також спроби змінити інформацію на державних порталах з метою маніпулювання громадською думкою[14; 185].

Кібератаки під час президентських виборів (2019) були орієнтовані на саботаж електронних виборчих систем та підрив довіри громадськості до результатів виборів[14; 89]. Найпоширенішими методами стали атакуючі кампанії, спрямовані на розповсюдження дезінформації через соціальні мережі та поштові платформи[14; 89]. Зловмисники намагалися вкрасти особисті дані кандидатів, виборців та активістів, проте масштабного зламу електронних систем вдалося уникнути завдяки посиленим заходам кібербезпеки[14; 89].

У контексті раніше згаданого особливої уваги заслуговує група хакерів Gamaredon/Armageddon, пов'язана з ФСБ РФ, що з 2014 року здійснює постійні шпигунські операції проти українських державних установ, силових структур, критичної інфраструктури[14; 89]. На відміну від разових атак, Gamaredon забезпечує перманентний доступ до скомпрометованих систем, що дозволяє збирати інформацію роками[14; 89]. Саме у період 2016-2021 років ця група була особливо активною[14; 89]. Вони представляли довгострокову загрозу національній безпеці України, оскільки фокусувалися не на руйнуванні, а на систематичному збиранні розвідувальної інформації[14; 89].

Інформаційно-психологічна складова гібридної агресії у період 2016-2021 років еволюціонувала від примітивних «тролефабрик» до складних багаторівневих операцій, протягом періоду «замороженого конфлікту» основну роль відігравала так звана «фабрика тролів» в Ольгіно (Санкт-Петербург) «Агентство інтернет-досліджень», що масово створювала фейкові акаунти у соціальних мережах для поширення

пропаганди[70; 71; 183]. Це був період аматорської, але масштабної інформаційної агресії[70; 71; 183].

2017-2021 роки: функцію координації інформаційно-психологічних спеціальних операцій (ІПСО) взяли на себе спеціалізовані підрозділи ГРУ у поєднанні з ПВК «Вагнер» Євгена Пригожина, що мали більші ресурси та професійніший підхід[70; 71; 183]. Це був перехід від аматорської «фабрики тролів» до професійних спецслужбових структур[70; 71; 183].

Інформаційні операції становили основу гібридної агресії періоду «замороженого конфлікту», забезпечуючи вплив на громадську думку без застосування фізичної сили[70; 71; 183]. За даними Оксфордського інституту інтернету, в умовах гібридної війни вони можуть охоплювати до 30-50% населення цільової країни протягом 24 годин[70; 71].

Особливу роль у поширенні російської пропаганди у період 2016-2021 років відігравали проросійські медіа в Україні[32; 40]. Телеканали «112 Україна», NewsOne, ZIK та НАШ, які перебували під контролем Тараса Козака та Євгена Мураєва, активно просуваючи ідеї проросійської орієнтації, лобіюючи інтереси РФ[32; 40]. Саме у цей період ці канали досягли піку свого впливу на українське інформаційне поле[32; 40].

Інтернет-ресурс Strana.ua, який почав працювати в 2014 році, швидко став важливим медіа для поширення проросійських наративів, таких як «громадянська війна», «український фашизм» та «утиски російськомовних»[183]. Проросійські онлайн-медіа, такі як Vesti.ua, Politnavigator.net, NewsFront і Rusvesna.su, а також блог Анатолія Шарія на сайті Sharij.net, активно використовували соціальні мережі для поширення антиукраїнських меседжів, підриву національної єдності та формування пропагандистського іміджу для РФ[183].

Систематичне використання проросійських медіа та інформаційних ресурсів у період 2016-2021 років допомогло Кремлю здійснювати маніпуляції, спрямовані на делегітимізацію української влади і підтримку сепаратистських настроїв[183; 70; 71]. Російські медіа використовували так звану «громадянську риторику», що зменшувала

міжнародне сприйняття РФ як агресора, перетворюючи повномасштабну війну на «внутрішній конфлікт» між українцями[183; 70; 71]. Інформаційна складова гібридної агресії будувалася навколо декількох ключових наративів, що постійно відтворювалися у російських та проросійських медіа:

По-перше, «громадянська війна» замість визнання зовнішньої агресії – цей наратив мав на меті зняти з РФ міжнародну відповідальність та представити конфлікт як внутрішньо українську проблему, до якої РФ не має відношення[88; 98; 104; 119; 167; 234; 235; 247].

По-друге, «Київська хунта/бандерівці/неонацисти» – дискредитація української влади після Революції Гідності, що використовувався як для внутрішнього споживання (виправдання агресії), так і для міжнародної аудиторії (особливо у країнах, чутливих до теми фашизму) [88; 98; 104; 119; 167; 234; 235; 247].

По-третє, «утиски російськомовних» та «мовний геноцид» – штучне конструювання образу переслідуваної меншості, якій РФ має «прийти на допомогу»[88; 98; 104; 119; 167; 234; 235; 247; 239]. Насправді жодних системних утисків за мовною ознакою в Україні не існувало, а закон, який російська пропаганда видавала за утиск російської мови, стосувався правок до закону про сферу надання послуг[30; 171; 210; 239; 241; 242].

По-четверте, «8 років бомбардувань Донбасу» – міф про те, що Україна вела «каральну операцію» проти мирних жителів Донбасу[88; 98; 104; 119; 167; 234; 235; 247]. РФ активно просувала наратив про Україну як агресора і «геноцидного ворога», використовуючи вирвані з контексту факти про обстріли, не вказуючи ініціаторів – підтримувані РФ збройні формування[88; 98; 104; 119; 167; 234; 235; 247].

За даними моніторингу ГО «Детектор медіа», у 2014 році використовувалося понад 40 стійких фейкових наративів, що систематично тиражувалися російськими ЗМІ та соціальними мережами[91]. Пропаганда РФ ніколи не розраховувала на якість своєї пропаганди, віддаючи перевагу масовості[91; 183; 70; 71].

Пік ефективності російських психологічних операцій на базі пропаганди припав на 2014–2015 роки, коли на окупованих територіях Донбасу до 46% населення довіряли російським телеканалам та вірили у наративи про «київську хунту» та «громадянську війну»[11; 12; 23].

Проте українські контрзаходи поступово знижували цей вплив: Блокування російських соціальних мереж «ВКонтакте» та «Однокласники» у 2017 році[38; 37]. Заборона трансляції низки російських телеканалів (2017-2021 роки)[37; 36]. Створення Стратегічних комунікацій Збройних Сил України (StratCom ЗСУ)[41]. З 2017 року введено санкції РНБО і СБУ проти власників проросійських медіа[32; 33; 40]. У 2021 році були заблоковані численні онлайн-ресурси, пов'язані з кремлівськими наративами[32; 33; 40].

Ці заходи поступово знижували ефективність російських інформаційних операцій та сприяли зниженню впливу пропаганди до рівня нижче 15% до 2024 року навіть у найбільш вразливих регіонах[11; 12; 21; 23; 206]. Водночас необхідно визнати, що повна нейтралізація російського інформаційного впливу залишається недосяжною через наявність альтернативних каналів поширення (VPN-доступ до заблокованих ресурсів, Telegram, Instagram, TikTok, X (Twitter) та інші), а також через існування сегменту населення, що з ідеологічних причин залишається сприйнятливим до проросійських наративів[70; 71; 183; 21; 23].

Період «замороженого конфлікту» продемонстрував, що за відсутністю активних бойових дій гібридна агресія не припинилася, а трансформувалася у більш витончені й системні форми впливу[4; 5; 10; 19; 41; 115; 185]. Протягом цих років РФ вдавалося підтримувати стан «сірої зони», коли конфлікт не є ні миром, ні повномасштабною війною у класичному розумінні – через поєднання:

Обмеженої військової присутності, замаскованої під «добровольців» та «сепаратистів», з фактичним повним контролем через проксі-структури під командуванням російських регулярних військ[65; 136; 155]. Систематичного економічного тиску через торговельні обмеження, блокаду Азовського моря,

будівництво обхідних газопроводів та енергетичний шантаж[87; 158; 186; 197; 209]. Дипломатичних маніпуляцій у рамках Мінського процесу та спроб нав'язати Україні капітуляційні умови через «формулу Штайнмайєра»[142; 145; 217]. Кібернетичних атак на критичну інфраструктуру та державні інституції, які досягли піку у 2016-2017 роках з масштабними операціями NotPetya та Industroyer[89; 100; 110; 143; 148]. Потужних інформаційно-психологічних операцій через мережу контрольованих медіа та агентів впливу, з професіоналізацією пропагандистських структур[32; 40; 70; 71; 183].

Така стратегія дозволяла РФ досягати певних тактичних цілей (контроль над частиною Донбасу, дестабілізація української держави, блокування євроатлантичної інтеграції) при мінімізації власних втрат та міжнародного осуду[4; 5; 10; 41; 185]. Цей період став критично важливим етапом підготовки до повномасштабного вторгнення 2022 року: створювалася логістична інфраструктура (справа Забалуєва), тестувалася кіберзброя, відпрацьовувалися інформаційні наративи, формувалася «п'ята колона»[14; 89; 110; 183]. Водночас Україна поступово нарощувала спроможність протидії через блокування проросійських медіа, створення систем стратегічних комунікацій, відмову від російського газу та зміцнення зв'язків із Заходом[9; 32; 40; 197].

Проте цей період також продемонстрував фундаментальне обмеження гібридної війни: вона не є «дешевшою альтернативою» конвенційній війні, а радше етапом досягнення стратегічних цілей іншими засобами[115; 116; 117; 185]. Коли ці цілі не досягаються у «сірій зоні», гібридна війна неминуче переходить у відкриту конвенційну фазу, як це сталося 24 лютого 2022 року[57; 185]. Досвід 2016-2021 років засвідчив, що «заморожений конфлікт» є лише ілюзією за фасадом відносного спокою відбувається інтенсивна підготовка до наступного етапу ескалації[41; 185].

3.3. 2022-2025: повномасштабне вторгнення та нові форми агресії

24 лютого 2022 року РФ розпочала повномасштабне вторгнення в Україну, що ознаменувало перехід від стану «сірої зони» до відкритої конвенційної війни. Однак цей перехід не означав відмови від гібридних методів ведення війни[4; 5; 10; 19; 41; 115; 185]. Навпаки, гібридність не зникла, а трансформувалася у нові форми, інтегруючись у повномасштабний конфлікт та створюючи синергетичний ефект між конвенційними та неконвенційними інструментами агресії[74; 117; 122; 123]. Український досвід остаточно довів фундаментальне обмеження гібридної війни: вона не є «дешевшою альтернативою» конвенційній війні, а радше етапом досягнення стратегічних цілей іншими засобами[115; 116; 117; 185]. Коли ці цілі не досягаються у «сірій зоні», гібридна війна неминуче переходить у відкриту конвенційну фазу, зберігаючи при цьому всі елементи гібридності[115; 116; 117; 185].

Ключовою характеристикою періоду 2022-2025 років стала демонстрація того, що гібридність та конвенційна війна не є взаємовиключними поняттями[74; 115; 117]. Російська модель продемонструвала еволюцію від «війни без розпізнавальних знаків» до відкритої конвенційної фази з збереженням гібридних елементів, що підтверджує визначення Френка Гофмана про «fusion of war forms» - злиття форм війни[115; 116; 117].

Ця еволюція свідчить про те, що гібридність не зникає з переходом до конвенційної фази, а трансформується у нові форми поєднання регулярних і нерегулярних компонентів[74; 115; 117; 155]. Партизанські дії на окупованих територіях, диверсії, убивства українських активістів та політичних діячів, використання іррегулярних формувань поряд з регулярними військами, заперечення своєї участі у «війні», все це свідчить про збереження гібридного характеру конфлікту навіть у фазі відкритої конвенційної війни[65; 155; 185].

Почнемо із самого простого питання, а саме чи можна вважати «повномасштабне вторгнення» фактичним початком війни чи якщо вірити російській пропаганді

«Спеціальна військова операція» оскільки жодна з сторін не оголошувала війну[57; 184].

Країна, що захищається, свідомо не оголошує війну державі-агресору передусім через положення сучасного міжнародного гуманітарного права (насамперед Женевські конвенції 1949 року зі спільною статтею 2 та Додатковий протокол I 1977 року)[7; 93]. Формальне оголошення війни автоматично переводило б конфлікт у категорію «міжнародного збройного конфлікту», у якому агресор отримав би статус законної воюючої сторони з усіма правами (включно з правом брати полонених, а не вважатися злочинцями)[7; 93]. Це легітимізувало б агресора і ускладнило б притягнення його керівництва до відповідальності за злочин агресії (стаття 8-біс Римського статуту МКС)[93]. Крім того, оголошення війни дало б агресору юридичні підстави розглядати військову допомогу третіх країн жертві як «втручання у війну» і навіть як casus belli для цих країн[7; 93].

Україна саме на цих підставах й не зобов’язана оголошувати війну з 2014 й особливо з 2022 року, для того, щоб: зберегти за РФ статус держави, яка вчинила злочин агресії, а не «сторони у війні»[7; 93]. Полегшило безперешкодне постачання зброї від партнерів (допомога жертві агресії ≠ допомога стороні у війні)[7; 93], Залишило відкритими двері для майбутнього трибуналу саме за злочин агресії[93].

РФ ж навпаки, була вимушена будь-що уникати формального оголошення війни, бо в її власному законодавстві (Федеральний закон «Про оборону» № 61-ФЗ та Кримінальний кодекс, ст. 353) оголошення війни можливе лише за рішенням Ради Федерації і лише за наявності «агресії проти РФ або її союзників» чи «безпосередньої загрози»[20; 21]. Жодної з цих умов не існувало, тому навіть у російському правовому полі «спеціальна військова операція», це юридична фікція, вигадана, щоб: Не визнавати статус полонених українських військових (РФ називає їх «злочинцями» і відмовляється дотримуватися Женевської конвенції)[7; 93]. Уникнути обов’язку виплачувати компенсації сім’ям загиблих і поранених російських солдатів за тарифами

«воєнного часу»[30; 31]. Не вводити воєнний стан на своїй території та не проводити загальну мобілізацію під виглядом «війни»[30; 31].

Таким чином, РФ маскує війну під неіснуючий у її власному праві термін «СВО» саме тому, що не має жодних юридичних підстав оголосити війну Україні, а визнати війну означало б визнати власну агресію і порушити власне законодавство[20; 21; 30; 31].

Після початку повномасштабного вторгнення так звані квазі-утворення «ДНР/ЛНР» отримали нову функцію в системі гібридної агресії[65; 155]. Вони стали використовуватися як проксі для легалізації мобілізованих з окупованих територій та перекладання відповідальності за військові злочини[55; 56; 59].

Формально окремі «1-й та 2-й армійські корпуси ДНР/ЛНР» продовжували зберігати видимість автономності, але насправді повністю інтегрувалися в командну структуру Збройних Сил РФ[65; 136; 155]. Це дозволяло РФ: Проводити примусову мобілізацію на окупованих територіях без формального визнання цих дій[65; 155]. Використовувати жителів окупованих територій як «гарматне м'ясо» на найбільш небезпечних ділянках фронту[65; 155]. Перекладати відповідальність за військові злочини на «місцеві формування»[65; 155; 82]. Зменшувати офіційну статистику втрат серед російських військовослужбовців[3; 62].

Мобілізація на окупованих територіях Донбасу відбувалася з порушенням усіх норм міжнародного гуманітарного права, зокрема Женевської конвенції[7; 93; 82]. Чоловіки призовного віку фактично викрадалися з вулиць, робочих місць, власних домівок[82]. Їм не надавалася належна військова підготовка, озброєння часто було застарілим, а використання в бойових діях відбувалося на найбільш небезпечних ділянках фронту з максимальними втратами[65; 82].

Після окупації нових територій у 2022 році (частин Херсонської, Запорізької, Донецької та Луганської областей) РФ негайно розпочала створення паралельних окупаційних адміністрацій та примусову мобілізацію місцевого населення[82]. Так РФ

має намір приписувати військові злочини «місцевим формуванням», а відповідальність за невдачі перекладається на «недієздатність ДНР/ЛНР»[65; 82].

ПВК «Вагнер», що відіграла ключову роль у період 2015-2021 років, після початку повномасштабного вторгнення пройшла значну трансформацію[65]. Група активно використовувалася в найжорстокіших боях, зокрема при штурмі Бахмута протягом 2022-2023 років, де тільки сам «Вагнер» зазнав величезних втрат, що становлять близько 20 тисяч осіб, це не враховуючи втрат ЗС РФ[65].

Після невдалого заколоту Євгена Пригожина в червні 2023 року та його загибелі в серпні 2023 року структура «Вагнера» була реорганізована[65]. Частина бойовиків була інтегрована в регулярні збройні сили РФ, інша частина продовжила діяльність під новою назвою «Африка корпус»[65]. Для України, це став неочікуваний поворот, що залишився виграшним при всіх розкладах, оскільки під час свого заколоту Пригожин дав кілька інтерв’ю де зізнався в багатьох злочинах за наказу РФ, а його смерть разом з Уткіним та іншими високопосадовими офіцерами «Вагнера» значно послабило загальну ефективність просування РФ[65].

Трансформація в «Африканський корпус» мала кілька стратегічних цілей: Продовження діяльності цієї організації в африканських країнах (Малі, Буркіна-Фасо, Центральноафриканська Республіка, Лівія) для обходу санкцій та фінансування військових операцій через контроль над природними ресурсами, передусім золотом та алмазами[65]. Збереження механізму «правдоподібного заперечення» для операцій, які РФ не може офіційно визнати[65; 155]. Використання досвіду та кадрів «Вагнера» в інших регіонах геополітичного протистояння з Заходом[65]. Створення альтернативного джерела фінансування війни проти України через експлуатацію ресурсів африканських країн[65].

Після початку повномасштабного вторгнення кібероперації стали невід'ємною частиною гібридної війни[14; 43; 89]. За даними Державної служби спеціального зв'язку та захисту інформації України, інтенсивність атак різко зросла – протягом 2014-2023 років українські державні інформаційні ресурси зазнали понад 6500 кібератак, з

яких значна частина припала саме на період після лютого 2022 року[14; 43]. Хакери РФ атакували ключові інфраструктури, зокрема платформи для управління водопостачанням, енергетичними компаніями, а також інші державні структури[14; 43; 89].

Характерною особливістю періоду 2022-2025 років стала зміна пріоритетів кібернетичних операцій[14; 43; 89]. Якщо в період 2015-2021 років РФ активно використовувала кібератаки для ураження енергетичної інфраструктури (BlackEnergy 2015, Industroyer 2016)[100; 110; 143; 148], то після початку повномасштабного вторгнення вона перейшла від кібератак на енергетичні об'єкти до їх прямого фізичного знищення через ракетні та дронові удари[14; 89; 220].

Ця зміна стратегії пояснюється кількома факторами: Покращення кіберзахисту критичної інфраструктури України за підтримки західних партнерів[89]. Більша ефективність фізичного руйнування для досягнення тактичних цілей[89; 220]. Можливість завдавати масштабніших та тривалих пошкоджень через кінетичні засоби[89; 220]. Прагнення створити гуманітарну катастрофу через масові відключення електропостачання в зимовий період[89; 220]. Акцент змістився з деструктивних атак на шпигунські операції та операції впливу, спрямовані на дезорганізацію координації та деморалізацію населення[14; 43; 89].

Одним із головних інструментів кібератак після 2022 року стали SCADA-системи (Supervisory Control and Data Acquisition), які використовуються для управління технологічними процесами в промисловості[14; 43; 89]. Атаки на ці системи дозволяли: Порушувати роботу водопостачання та каналізації[14; 43]. Дестабілізувати роботу промислових підприємств[14; 43]. Викликати аварії на потенційно небезпечних об'єктах[14; 43]. Створювати каскадні ефекти в критичній інфраструктурі[14; 43].

Хакерська група Gamaredon/Armageddon, пов'язана з ФСБ РФ, продовжувала свою діяльність і після 24 лютого 2022 року[14; 89]. У 2023 році РФ продовжувала застосовувати кібератаки для впливу на українську промисловість та інфраструктуру,

отримання інформації про діяльність українських збройних сил[14; 43]. Цілями кібератак залишалися урядові мережі та державні реєстри, фінансовий сектор, телекомунікаційна інфраструктура, транспортні системи, засоби масової інформації, військові системи зв'язку та управління[14; 43; 89].

Організаційна структура російських інформаційно-психологічних операцій продовжила еволюціонувати[70; 71; 183]. У 2023-2025 роках спостерігається активне впровадження штучного інтелекту: автоматизовані ботоферми, нейромережі для створення контенту, діпфейки стають дедалі якіснішими та важче виявляються[45; 75; 70].

Цей період характеризується переходом від масового поширення примітивних фейків до створення високоякісного синтетичного контенту, здатного обманювати навіть досвідчених верифікаторів інформації[45; 75; 70; 183]. Це якісно новий етап інформаційної війни, що створює фундаментальні виклики для верифікації інформації[45; 75; 70].

Діпфейк Зеленського з «капітуляцією» 16 березня 2022 року став першим у світі випадком використання глибоко підробленого відео (deepfake) політичного лідера у реальному часі під час війни. Хоча технічна якість підробки була відверто жахливою і фейк швидко розкрили, сам факт спроби такої операції свідчить про готовність використовувати найсучасніші технології для інформаційно-психологічного впливу[45; 75].

Відео було розміщене на зламаному сайті новинного порталу та в соціальних мережах. У ньому президент України нібито закликав українських військових скласти зброю та капітулювати перед російськими військами. Низька якість підробки проявлялася в: Невідповідності рухів губ та звуку. Неприродних рухах голови. «Артефактах» навколо обличчя. Невідповідності освітлення та тіней[45; 75].

Проте цей інцидент став важливим сигналом про майбутні загрози. Він продемонстрував, що РФ готова використовувати найсучасніші технології синтетичних

медіа для досягнення стратегічних цілей, навіть якщо перші спроби виявляються технічно недосконалими[45; 75].

Якісно новий рівень загрози виявився в діяльності цілих фабрик з виготовлення діпфейкових відеоматеріалів та їхнього поширення. OSINT-група незалежного українського проєкту «Телебачення Торонто» виявила систематичну діяльність з масового виробництва фальшивих відео[45].

Ця фабрика створювала діпфейки з начебто українськими військовими, які: Готові здійснити збройний переворот проти влади. Знущаються над російськомовними цивільними. Демонструють жорстокість до полонених. Висловлюють невдоволення командуванням та політичним керівництвом, варто зазначити, що прецеденти коли військові критикують керівництво або демонструють втому дійсно є, але зібраний матеріал показує, як на фоні таких випадків розростається велика кількість діпфейків та пропаганди[45].

Особливо ефективно ці матеріали діяли в мережах Instagram, TikTok та X (Twitter) тобто платформах, орієнтованих на емоційно забарвлений контент з коротким часом перегляду, що ускладнює критичне осмислення інформації. У цих мережах контент споживається швидко і часто без критичної перевірки[45].

Найбільш емоційно забарвленим та широко розповсюдженим виявився діпфейк «Воха», де начебто українські військовослужбовці знущаються над чоловіком на ім'я Воха – людиною з синдромом ДЦП, якого мобілізували до складу ЗСУ. Ця серія відео стала особливо популярною завдяки: Емоційному впливу через використання людини з інвалідністю для створення максимального шокуючого ефекту та викликання обурення. Активному поширенню в міжнародній спільноті посприяв Алекс Джонс, американський радіомовник з аудиторією понад 2 мільйони чоловік у мережі X. Джонс, який не зрідка дає інтерв'ю російським пропагандистським каналам, цілеспрямовано використовував свій акаунт для поширення цього матеріалу. Використанню наративу про жорстокість українських військових, відео ідеально вписувалося в російський наратив про «нацистський режим» та «звірства ЗСУ».

Технічній якості на відміну від примітивного діпфейку з Зеленським у березні 2022 року, це відео було виконане більш професійно, що ускладнювало його швидке викриття й лише «Артефакти» обличчя чітко виказують підробку[45].

Цей кейс демонструє, як РФ навчилася створювати діпфейк-відео такого рівня, що виявити їхню підробку стає надзвичайно складно, особливо коли вони поширюються начебто з українських акаунтів у соціальних мережах, що створює ілюзію автентичності[45; 75].

Автономні системи дезінформації на базі ШІ представляють якісно новий рівень загрози. Штучний інтелект здатний генерувати величезні обсяги персоналізованого дезінформаційного контенту, адаптованого під конкретні цільові аудиторії. ШІ може: Аналізувати психологічні профілі користувачів соціальних мереж. Створювати меседжі, що максимально ефективно впливають на їхні переконання. Автоматично генерувати текстові, аудіо та відео матеріали. Адаптувати стратегію поширення дезінформації в режимі реального часу[[45; 70; 75].

Використання алгоритмів соціальних мереж як зброї означає цілеспрямоване посилення поляризації суспільства, розпалювання внутрішніх конфліктів, маніпулювання громадською думкою через мікротаргетинг[70; 71; 183]. Російські структури навчилися експлуатувати алгоритми рекомендацій соціальних мереж, що природно посилюють контроверсійний контент, для масового поширення дезінформації[70; 71; 183].

Після початку повномасштабного вторгнення РФ офіційно оголосила «денацифікацію та демілітаризацію» як головні цілі так званої «спеціальної військової операції». Ці абсурдні з точки зору реальності формулювання мали на меті створити псевдо-легітимне обґрунтування повномасштабного вторгнення для внутрішньої аудиторії РФ[57; 88; 119; 247].

Далі варто поговорити й про основні наративи якими користується РФ для спроби виправдання своєї агресії проти України: Наратив був офіційно озвучений у зверненнях президента Путіна від 21 та 24 лютого 2022 року[57]. Для поширення

використовувалися: Державні медіа РФ («Россия 24», «НТВ», «Первый канал»). Пропагандистські ток-шоу з участю «експертів» та «політологів»[183]. Керівники окупаційних адміністрацій «ДНР» і «ЛНР»[65]. Залишки проросійських медіа в Україні та діаспорі[32; 40]. Наратив використовував маніпуляції з історичними травмами, зокрема з колективною пам'яттю про Другу світову війну, намагаючись створити моральне виправдання агресії шляхом порівняння України 2022 року з нацистською Німеччиною[88; 119; 247].

Міф про «8 років бомбардувань Донбасу» набув особливої актуальності як виправдання повномасштабного вторгнення. РФ активно просувала наратив про Україну як агресора, оскільки це було досить символічною тезою для підбурення населення[183; 247].

Активне використання термінів «геноцид» і «каральна операція» допомогло формувати емоційний тиск на аудиторію і закріплювати образ України як злочинної держави[88; 119; 247]. Меморіал «Алея ангелів» в окупованому Донецьку став інструментом пропаганди, офіційно позиціонуючись як пам’ятник дітям, загиблим від дій ЗСУ, хоча фактично став символом маніпуляцій[183].

Окупаційні влади організовували пропагандистські заходи, створювали емоційні матеріали для поширення у соціальних мережах. Імена на самому ж пам'ятнику неодноразово змінювалися, що цікаво, серед дітей, загинувших під час бойових дій, також вказувалися й ті, що померли від хвороби, або навіть були бойовиками «ДНР», що демонструє верх цинізму з маніпуляцією життями дітей. (Варто зазначити, що цей міф пропаганди не є новим, але набув нового життя після початку вторгнення РФ)[183].

Після блокування телеканалів «112 Україна», NewsOne та ZIK у 2021 році, а також введення санкцій проти їхніх власників, проросійська медіасфера в Україні зазнала суттєвої трансформації[32; 40]. Було створено «Перший незалежний» як спробу замінити заблоковані ресурси, проте він проіснував лише близько року[32; 40].

Після початку повномасштабного вторгнення більшість проросійських медіа були остаточно заблоковані або самоліквідувалися[32; 40].

Проте це не означало повного зникнення російського інформаційного впливу – він трансформувався в нові форми: Telegram-канали з анонімним адмініструванням, Використання VPN для доступу до заблокованих ресурсів, Поширення контенту через месенджери (WhatsApp, Viber), Створення нових медіа з прихованим проросійським фінансуванням, Використання іноземних платформ для обходу українських обмежень[183].

У 2022 році для координації інформаційної політики в умовах війни було запроваджено механізм «Єдині новини». Він об'єднав провідні українські телеканали для спільного мовлення під час воєнного стану з метою: Забезпечення оперативного інформування населення про події війни. Координації повідомлень про повітряні тривоги та загрози. Протидії російській дезінформації через єдину верифіковану інформаційну політику. Підтримки морального духу населення. Водночас цей механізм викликав дискусії щодо балансу між безпековими потребами та плюралізмом медіа, що є природним для демократичного суспільства навіть в умовах війни[97; 114; 133; 153; 219; 224; 244].

Збереження гібридного характеру конфлікту після 2022 року проявлялося не лише в діях РФ, але й у формах українського спротиву на окупованих територіях. Партизанські дії, диверсії, ліквідації колаборантів та представників окупаційної адміністрації стали важливим елементом гібридної війни[74; 117; 122; 138].

На окупованих територіях діяли підпільні мережі, які: Передавали розвідувальну інформацію про дислокацію російських військ[21; 138]. Здійснювали диверсії на військових об'єктах та шляхах постачання. Ліквідовували колаборантів та представників окупаційної влади. Проводили інформаційно-психологічні операції проти окупантів[82; 138].

З іншого боку, російські спецслужби та підконтрольні їм структури систематично здійснювали замахи та убивства українських активістів, громадських діячів,

представників місцевого самоврядування на окупованих територіях. Ці дії мали на меті: Залякування населення та придушення опору. Знищення потенційних лідерів українського руху опору. Встановлення тотального контролю через терор. Примушування до співпраці через демонстрацію сили[82; 120].

Особливо активно ці репресії здійснювалися співробітниками ФСБ, які контролювали місцеве населення через залякування та тортури. Створювалися фільтраційні табори, де населення окупованих територій піддавалося допитам, катуванням та незаконним затриманням. Систематично викрадалися та вбивалися українські активісти, представники місцевої влади, волонтери, журналісти[82; 120; 149; 150].

В цьому контексті варто поговорити й про діяльність РФ через своїх агентів або завербованих осіб, що здійснювали замахи на активістів й на підконтролюваних Україні територіях так до прикладу відбулися вдалі замахи на Ірину Фаріон та Андрія Парубія, окрім того було скоєно також замах на активіста-волонтера Сергія Стерненко, та інші менш відомі випадки. Якщо з агентами РФ все зрозуміло то з вербуванням все складніше, оскільки російські структури постійно намагаються завербувати людей з «низькою моральною відповідальністю» через соціальні мережі й проконтролювати кожен такий випадок є дуже складним[140; 190].

Залякування цивільного населення під час повномасштабного вторгнення реалізувалося через демонстративні військові злочини як інструмент терору для примусу до капітуляції та підриву морального духу Масові вбивства цивільних у Бучі, Ірпені, Маріуполі, Ізюмі та інших населених пунктах не є «ексцесами» окремих підрозділів, а систематичною практикою залякування[120; 196].

Хоча РФ офіційно відкидає такі обвинувачення, міжнародні розслідування та супутникові знімки доводять, що армія РФ діяла цілеспрямовано проти українського населення. Систематичні обстріли житлових кварталів, лікарень, шкіл, евакуаційних коридорів, використання заборонених видів зброї проти цивільних об'єктів, виявлення

прихованих поховань або місць масової страти, все це елементи стратегії терору, спрямованої на деморалізацію українського суспільства[120; 196].

Депортація українських дітей на територію РФ, примусова русифікація, влаштування до російських сімей без згоди батьків є злочином геноциду згідно з Конвенцією про запобігання злочину геноциду та покарання за нього[93; 120]. За різними оцінками, понад 19 тисяч українських дітей були незаконно депортовані на територію РФ, і лише невелику частину з них вдалося на сьогодні повернути[120].

Тепер перейдемо до дипломатичної складової. Напередодні повномасштабного вторгнення у лютому 2022 року Володимир Путін публічно заявив, що «Мінські угоди більше не існують», поклавши всю відповідальність на Україну[57; 145; 217]. Ця заява стала кульмінацією багаторічної пропагандистської кампанії, під час якої РФ систематично звинувачувала Україну в порушенні Мінських домовленостей, хоча резолюції ООН чітко вказували на зворотнє[176; 177; 145; 217].

Міністр закордонних справ Сергій Лавров та постійний представник РФ при ООН Василь Небензя неодноразово заявляли, що українська сторона нібито зриває процес імплементації угод[145; 217]. Російські державні медіа (TASS, «Российская газета») активно підсилювали ці наративи, створюючи інформаційне підґрунтя для виправдання майбутнього вторгнення[183].

Насправді РФ використовувала Мінські домовленості не як інструмент для досягнення миру, а як важіль для інформаційного тиску та легітимізації власних агресивних дій. Зокрема, нав'язувалася ідея, що «Мінськ-2» (Мінський протокол, що в російській пропаганді окреслений під назвою «Мінськ-2» й під такою назвою також відомий більш широкому загалу) зобов'язує Україну змінити Конституцію під вимоги ОРДЛО, хоча ці зміни повинні були обговорюватися лише після виведення іноземних військ і проведення легітимних виборів чого сторона «бойовиків» так й не виконала[142; 145; 217].

Переговори в Стамбулі 29-30 березня 2022 року стали значущим етапом у контексті гібридної агресії. Хоча дипломатія традиційно слугує механізмом

врегулювання конфліктів, у цьому випадку переговори були використані як частина комплексної стратегії РФ, спрямованої на маніпулювання міжнародною думкою[145; 217].

Основні російські вимоги включали: Нейтральний статус України та відмову від НАТО (із закріпленням на конституційному рівні), Визнання окупації Криму та контролю над Донбасом, Обмеження обороноздатності України (чисельності Збройних сил та військових можливостей) та інші пункти, що фактично були вимогою повної та беззаперечної капітуляції України[145; 217].

Українська делегація чітко відстояла свої позиції, відкинувши ультимативні вимоги РФ. Пропозиції України включали вимогу про міжнародні гарантії безпеки, припинення вогню, обмін військовополоненими. Проте пропагандистські канали Кремля активно розповсюджували інтерпретації, що нібито Україна була готова прийняти більшість російських умов, а Захід «зірвав» мирні переговори[183; 145; 217].

Під час переговорів РФ активно використовувала інформаційно-психологічні інструменти для маніпуляції громадською думкою. Через контрольовані медіа створювалася паралельна реальність, де українська сторона була зображена як країна, що не готова до мирного процесу. Висуваючи неприйнятні вимоги, що чітко позиціонувалися як вимога капітуляції України, РФ використовувала переговори не для мирного врегулювання, а для маніпулювання суспільною думкою та досягнення агресивних цілей через пропаганду[183; 145; 217].

У 2022 році Давид Арахамія, голова української делегації на переговорах зі Стамбула, описував атмосферу перемовин, де основними місцями суперечок стали питання безпекових гарантій та вимога РФ щодо нейтралітету України. Проте прокремлівські ЗМІ поширювали викривлену інтерпретацію, згідно з якою Борис Джонсон (на той час прем’єр-міністр Великобританії), нібито наказав Володимиру Зеленському «продовжувати війну», «зірвавши мир»[183; 145; 217].

В інтерв'ю Ангели Меркель у виданні Die Zeit 7 грудня 2022 року стало об'єктом масштабних маніпуляцій. Колишня канцлерка Німеччини зазначила, що Мінські угоди

2014 року мали на меті «дати Україні час» для зміцнення обороноздатності. Ця заява була вирвана з контексту і спотворена в російських медіа як доказ того, що Мінські угоди нібито служили прикриттям для підготовки України до нападу на РФ[183; 145; 217].

В обидвох випадках маніпуляція полягала в цілеспрямованому вириванні фрагментів висловлювань та їхній трансформації у викривлені наративи. Виривання окремих цитат з контексту дозволяє створити штучно сформоване уявлення, яке не має нічого спільного з реальними подіями[183].

Окрім того РФ продовжує систематичне блокування резолюцій у Раді Безпеки ООН, що засуджують російську агресію або передбачають санкції. Це паралізує головний механізм колективної безпеки та унеможливлює ефективну міжнародну реакцію через найвпливовіший орган системи ООН]. Навіть у фазі відкритої конвенційної війни з масовими військовими злочинами РФ продовжує використовувати своє місце постійного члена РБ ООН для уникнення відповідальності[176; 177].

У вересні 2022 року РФ організувала так звані «референдуми» на тимчасово окупованих територіях Донецької, Луганської, Запорізької та Херсонської областей. Ці «голосування» повністю повторили сценарій кримського «референдуму» 2014 року, але в ще більш грубій та очевидній формі порушуючи Українське, Міжнародне та навіть російське внутрішнє законодавство[95; 128; 176; 177]: Вони проводилися під дулами автоматів на активно воюючих територіях. Відбувалися без присутності міжнародних спостерігачів. Мали заздалегідь визначені результати (понад 90% «за» приєднання до РФ). Супроводжувалися масовими фальсифікаціями та примусовим голосуванням. Проводилися на територіях, значна частина населення яких була евакуйована або депортована до РФ. Не мали жодної правової бази[95; 128; 176; 177].

Мета цих псевдо-референдумів полягала в спробі легітимізувати окупацію в очах внутрішньої російської аудиторії, створенні юридичного обґрунтування для офіційної анексії цих територій й використанні наративу про «захист нових територій» для виправдання подальшої ескалації, включаючи можливість застосування ядерної зброї

для тиску на міжнародну спільноту та тестування реакції самої міжнародної спільноти на грубе порушення міжнародного права[95; 128; 176; 177; 183].

Міжнародна спільнота одностайно засудила ці псевдо-референдуми як незаконні та такі, що не мають жодної юридичної сили. ООН, ЄС, НАТО та переважна більшість країн світу відкинули результати цих «голосувань» та підтвердили непорушність міжнародно визнаних кордонів України[176; 177; 156]. В той же час окупаційна адміністрація намагається створити видимість «нормалізації» через запровадження російських освітніх програм, примусову видачу російських паспортів, організацію псевдо-референдумів[82; 120; 187].

Після початку повномасштабного вторгнення РФ продовжила практику масштабної націоналізації української власності на окупованих територіях, розпочату ще в Криму у 2014 році. Це стосувалося: Промислових підприємств (особливо в Маріуполі після його захоплення)[187; 202]. Банківської системи[187]. Торговельних мереж (Ураження українських портів та суден)[186; 249].

Енергетичної інфраструктури (Окупація ЗАЕС)[220]. Портів та транспортної інфраструктури (використання окупованих потів для постачання армії та переміщення викрадених ресурсів)[186; 249]. Окремо варто відзначити систематичне викрадення сільськогосподарської техніки, зерна та іншої продукції з окупованих територій[47; 129; 160]. Ці дії мали подвійну мету: економічне ослаблення України та отримання ресурсів для забезпечення власних потреб і фінансування війни[87; 94; 99].

Особливою формою економічної війни став енергетичний терор – систематичні масовані удари по енергетичній інфраструктурі України, які розпочалися восени 2022 року та продовжуються й по сьогоднішній день[89; 220]. На відміну від кібератак на енергетичну інфраструктуру періоду 2015-2021 років, РФ перейшла до прямого фізичного знищення гідростанцій, електростанцій, теплоелектроцентралей, трансформаторних підстанцій через масовані ракетні та дронові удари[89; 220]. Що цікаво схожий терор РФ (імовірно несвідомо) здійснило й проти окупованих територій,

оскільки під час бойових дій РФ бомбило водопостачальну інфраструктуру створюючи дефіцит питної та технічної води на окупованих територіях[120; 220].

Період повномасштабного вторгнення 2022-2025 років остаточно довів фундаментальну тезу: гібридна війна не є «дешевшою альтернативою» конвенційній війні, а радше етапом досягнення стратегічних цілей іншими засобами[115; 116; 117; 185]. Коли ці цілі не досягаються у «сірій зоні», гібридна війна неминуче переходить у відкриту конвенційну фазу[115; 116; 117; 185].

При цьому перехід до конвенційної війни не означає відмови від гібридних методів – навпаки, вони інтегруються у повномасштабний конфлікт, створюючи синергетичний ефект[74; 115; 116; 117]. Російська модель продемонструвала злиття форм війни (fusion of war forms), де одночасно застосовуються: Конвенційні військові операції з використанням регулярних військ[69; 136]. Іррегулярні формування для каральних акцій та створення «правдоподібного заперечення»[65; 155]. Кібератаки на критичну інфраструктуру з акцентом на шпигунських операціях[14; 43; 89]. Масовані інформаційно-психологічні операції з використанням штучного інтелекту та діпфейків[45; 70; 75; 183]. Економічний терор через знищення енергетичної інфраструктури[89; 220]. Дипломатичні маніпуляції та псевдо-референдуми[145; 176; 177; 217]. Диверсії та терор на окупованих територіях[82; 120; 138]. Депортація та примусова асиміляція населення[120].

Це вимагає від держав-жертв та міжнародної спільноти не лише реактивної відповіді на вже застосовані інструменти, але й проактивної стратегії з прогнозування майбутніх загроз, розробки превентивних механізмів захисту та формування суспільної стійкості як найефективнішого захисту від гібридної агресії будь-якого типу[8; 66; 74; 85; 122; 123]. Український досвід став не лише найбільш показовим прикладом реалізації повного арсеналу гібридних інструментів у сучасній історії, але й найбільш успішним прикладом протидії цим загрозам, що має стати основою для розробки міжнародних механізмів протидії гібридним загрозам у майбутньому[8; 66; 74; 85; 122; 123; 178].

РОЗДІЛ 4. ДОСВІД І СТРАТЕГІЇ ПРОТИДІЇ УКРАЇНИ

4.1. Інституційні та правові механізми протидії

Протидія гібридній агресії Російської Федерації проти України вимагала кардинальної адаптації як міжнародно-правових інструментів, так і національного законодавства до принципово нових викликів[4; 7; 41; 93; 122; 123]. Гібридна війна створила «сіру зону» між війною та миром, у якій традиційні механізми міжнародного права виявилися недостатньо ефективними[74; 85; 115; 122; 123]. Водночас український досвід 2014-2025 років яскраво продемонстрував можливості інноваційного використання існуючих правових інструментів та розробки нових підходів до протидії агресії держави, яка сама є одним з архітекторів системи міжнародної безпеки[8; 122; 178].

Організація Об’єднаних Націй опинилася у парадоксальній ситуації: держава-агресор, чиї дії грубо порушують фундаментальні принципи Статуту ООН, водночас є постійним членом Ради Безпеки з правом вето[176; 177]. Цей структурний дефект системи колективної безпеки, закладений ще 1945 року, став критичним у контексті російської агресії проти України[176; 177].

Через постійне блокування РФ рішень Ради Безпеки центр ваги змістився до Генеральної Асамблеї ООН[176; 177]. Хоча резолюції ГА не є юридично зобов’язальними, вони мають велику політичну та моральну вагу і створюють важливі прецеденти й в цьому контексті ключовими резолюціями Генеральної Асамблеї є:

- 27 березня 2014 року – резолюція 68/262 «Територіальна цілісність України» (100 голосів «за», 11 «проти», 58 утрималися) – що визнала кримський «референдум» недійсним і підтвердила належність Криму Україні[176]
- 2 березня 2022 року – резолюція ES-11/1 (141 «за», 5 «проти», 35 утрималися) – що засудила повномасштабне вторгнення Російської Федерації[177].

- 24 березня 2022 року – резолюція ES-11/2 – щодо гуманітарних наслідків агресії[177].
- 12 жовтня 2022 року – резолюція ES-11/4 (143 «за», 5 «проти», 35 утрималися) – засудила спробу незаконної анексії чотирьох українських областей; це була найбільша підтримка серед усіх голосувань щодо України[177].
- 23 лютого 2023 року – резолюція ES-11/6 (141 «за», 7 «проти», 32 утрималися) – підтвердила принципи Статуту ООН і закликала до справедливого й тривалого миру[177].

У 2014-2021 роках РФ щонайменше 8 разів застосовувала право вето в Раді Безпеки щодо проукраїнських проектів резолюцій, зокрема блокувала засудження кримського «референдуму» (15 березня 2014) та створення міжнародного трибуналу у справі MH17 (29 липня 2015)[176; 177]. Крім того, РФ регулярно використовувала трибуну Ради Безпеки для поширення дезінформації[183].

З листопада 2024 року понад 50 держав на чолі з Ліхтенштейном активізували кампанію з перегляду легітимності постійного місця РФ в Раді Безпеки, аргументуючи це тим, що у 1991 році Російська Федерація не проходила офіційної процедури наступництва місця СРСР, тут варто зазначити, що ми опираємося не на номінальний початок перегляду постійного місця РФ в РБ, що почалося в 2022 році, а саме період коли почалося активне просування цього питання[161; 162].

Нездатність Ради Безпеки діяти активізувала механізм «Об’єднання заради миру» (резолюція ГА 377(V) від 1950 року)[176; 177]. 27 лютого 2022 року Рада Безпеки процедурним рішенням (яке не підлягає вето) скликала 11-ту надзвичайну спеціальну сесію Генеральної Асамблеї – це стало найбільш масштабнішим застосуванням механізму за всю історію ООН[177].

Важливу роль відіграють механізми документування порушень[120; 173]. З 2014 року в Україні працює моніторингова місія Офісу Верховного комісара ООН з прав людини (OHCHR), яка щоквартально фіксує позасудові страти, катування, насильницькі зникнення та обмеження свобод на окупованих територіях[120; 173].

У березні 2022 року Рада ООН з прав людини створила Незалежну міжнародну комісію з розслідування в Україні, яка задокументувала численні воєнні злочини та злочини проти людяності, зокрема масові страти в Бучі, Ірпені та Маріуполі[120; 161; 162]. В Міжнародному суді ООН Україна веде дві справи проти РФ:

З 26 лютого 2022 року – справа за Конвенцією про запобігання злочину геноциду та покарання за нього[93]. 16 березня 2022 року Суд виніс обов'язкові тимчасові заходи, зобов'язавши Російську Федерацію негайно припинити військові дії (13 суддів «за», 2 «проти») – вперше в історії постійний член Ради Безпеки отримав таке рішення, хоча РФ повністю ігнорує це рішення проте саме, ця справа матиме одне з самих визначальних питань в післявоєнний період[93].

З січня 2017 року – справа за Міжнародною конвенцією про боротьбу з фінансуванням тероризму та Конвенцією про ліквідацію всіх форм расової дискримінації (стосується підтримки сепаратистів на Донбасі, збиття МН17 та дискримінації кримських татар і українців у Криму)[93; 203]. У 2024 році Суд частково задовольнив позов України за другою конвенцією, проте й це рішення РФ повністю ігнорує[93].

Проте не тільки ООН в процесі еволюції російської гібридної агресія проти України було змушено розвиватися саме, починаючи з 2014 року ЄС та НАТО також були змушені пробудитися та еволюціонувати[74; 85; 156; 175; 238].

Для НАТО гібридна агресія РФ проти України стала справжнім «стратегічним пробудженням» після більш ніж двадцяти років, коли Альянс зосереджувався переважно на експедиційних операціях поза Європою[74; 85; 156; 175; 238]. Анексія Криму та війна на Донбасі показали, що на східному фланзі з'явилася держава, готова застосовувати регулярні війська під прикриттям «зелених чоловічків», гібридні методи та відверту військову силу[136; 175; 185]. Це змусило НАТО кардинально переглянути свої базові припущення про природу загроз після закінчення Холодної війни[74; 85; 238].

Уельський саміт 4-5 вересня 2014 року відбувся лише через тиждень після Іловайської трагедії й став першим самітом, де РФ було прямо названо агресором[238]. У декларації вперше з'явилися терміни «гібридна війна» та «російська агресія проти України»[238]. Саміт ухвалив Readiness Action Plan (RAP), зобов'язання довести видатки на оборону до 2% ВВП до 2024 року, створив Сили Very High Readiness Joint Task Force (VJTF) та заклав основу для посиленої передової присутності (enhanced Forward Presence) на східному фланзі[238].

Протягом 2015-2016 років НАТО розробило й ухвалило першу в історії комплексну Стратегію протидії гібридним загрозам[85; 243]. Документ чітко визначив гібридну війну як скоординоване використання військових і невійськових засобів нижче порогу відкритої війни[85; 243]. Стратегія передбачала три основні лінії дій: Prepare (раннє виявлення та підвищення обізнаності), Deter (чітке повідомлення про колективну відповідь) та Defend (підтримка національної стійкості держав-членів і партнерів)[85; 243].

Повномасштабне вторгнення РФ 24 лютого 2022 року стало найбільшим викликом для НАТО з моменту його заснування у 1949 році[156]. Вже за добу Альянс активував плани поступової відповіді (Graduated Response Plans), а 25 лютого провів віртуальний надзвичайний саміт глав держав і урядів[156]. Було ухвалено рішення про розгортання додаткових сил і повну активацію восьми багатонаціональних батальйонних бойових груп від Балтії до Чорного моря[156].

З квітня 2022 року під егідою США діє Ukraine Defence Contact Group (формат «Рамштайн»), що об'єднує нині вже понад 57 країн[156; 214]. За три роки через цей механізм Україні передано військову допомогу на суму понад 140 мільярдів доларів, включно з танками Leopard 2, системами Patriot, F-16, далекобійними ракетами ATACMS і Storm Shadow/Scalp[156; 214]. «Рамштайн» став наймасштабнішою коаліцією військової підтримки в історії після Другої світової війни, проте навіть його не можна назвати достатньо ефективним на підставі того, що окремі учасники

(особливо ті від яких впершу чергу залежало постачання озброєння) часто вагалися або по-політично вмотивованим причинам затримували постачання[156; 214].

Мадридський саміт 28-30 червня 2022 року зафіксував доктринальний зсув: нова Стратегічна концепція вперше назвала Російську Федерацію «найбільш значущою та прямою загрозою» безпеці Альянсу, а Китай – «системним викликом»[156]. Саме на цьому саміті Фінляндія та Швеція отримали офіційне запрошення до НАТО[156]. Фінляндія стала 31-м членом 4 квітня 2023 року, Швеція 32-м членом 7 березня 2024 року, подвоївши сухопутний кордон НАТО з РФ до 2542 кілометрів й тим самим повністю руйнуючи одну з першочергових тез російської пропаганди про загрозу «початок військових дій через розширення НАТО»[156].

Вільнюський саміт 11-12 липня 2023 року став проривом для України: лідери країн Альянсу заявили, що «майбутнє України в НАТО», скасували для неї План дій щодо членства (МАР), перевівши на одноетапну процедуру приєднання, та створили Раду Україна-НАТО орган, де Україна бере участь у засіданнях як рівноправний, 33-й партнер, проте існує дві суттєвих перешкодою для вступу в НАТО, а саме війна РФ проти України та небажання окремих країн членів Альянсу приймати Україну, найбільш чіткою з них сьогодні є Угорщина[156].

Вашингтонський саміт 9-11 липня 2024 року пішов ще далі[156]. У фінальному комюніке вперше з’явилася формула: «Ми будемо готові направити Україні запрошення приєднатися до Альянсу, коли союзники погодяться і будуть виконані умови»[156]. Слово «invitation» (запрошення) замінило попереднє абстрактне «майбутнє членство» і стало останнім кроком перед підписанням Протоколу про приєднання, також оголошено про створення NSATU та мінімальний річний пакет допомоги у розмірі 40 мільярдів євро[156].

У січні 2025 року офіційно запрацювала NATO Security Assistance and Training for Ukraine (NSATU) – перша в історії НАТО постійна військова структура для країни, яка не є членом Альянсу[156]. Штаб-квартира розташована у Вісбадені (Німеччина), хі штатом працівників - понад 700 осіб із 28 країн-членів і 9 країн-партнерів,

підпорядкованих безпосередньо SACEUR[156]. NSATU координує постачання, навчання (разом із EUMAM Ukraine вже підготовлено понад 150 000 українських військових), логістику, аналіз бойового досвіду та стратегічні комунікації, повністю замінивши тимчасовий формат «Рамштайн»[156].

Станом на грудень 2025 року Україна залишається найбільш інтегрованим партнером НАТО за всю історію Альянсу: вона має статус Enhanced Opportunities Partner з 2020 року, 100% виконаних рекомендацій Щорічної національної програми, постійне представництво при штаб-квартирі НАТО більші, ніж у багатьох членів, та фактичну участь у плануванні операцій[156]. Від реактивного стримування 2014 року до створення постійної інституційної, фінансової та військової інфраструктури підтримки у 2025-му НАТО пройшло шлях, який робить членство України питанням часу, а не принципу[156; 74; 85; 238].

В контексті вище згадано варто поговорити й про два важливих факти, які практично не згадуються в сьогоденні, а саме питання «Ленд-лізу» США та спільних навчань НАТО-Україна[156; 214]. 9 квітня 2022 року Конгрес США ухвалив «Закон про ленд-ліз для захисту демократії в Україні 2022 року» (Ukraine Democracy Defense Lend-Lease Act of 2022) – перший з 1941 року випадок, коли така програма запускалася для країни, що не є союзником за великим договором[156; 214]. Закон надавав Президентові надзвичайні повноваження передавати Україні будь-яке озброєння, техніку та послуги фактично безкоштовно або з відстрочкою платежу на 100 років за символічні 0,01 % річних[156; 214]. Очікувалося, що це дозволить швидко насичувати ЗСУ найсучаснішими системами без бюрократичних обмежень звичайних програм допомоги[156; 214].

Проте програма так і не набрала реальної сили[156; 214]. За три роки дії (2022-2025) через механізм ленд-лізу було поставлено лише символічні партії – кілька тисяч одиниць стрілецької зброї та боєприпасів на загальну суму менше 200 млн дол[156; 214]. Основними причинами цього були: Адміністрація Байдена свідомо активувала закон лише один раз у 2022-му і далі воліла використовувати Presidential Drawdown

Authority (PDA) та Ukraine Security Assistance Initiative (USAI), бо вони давали більше контролю над номенклатурою; 2) Пентагон і Держдеп побоювалися, що РФ втілить у реальність свої ядерні погрози; 3) Конгрес 2024-2025 років (особливо після приходу республіканської більшості) не виділив додаткового фінансування саме під ленд-ліз, залишивши його «паперовим інструментом»[156; 214]. Таким чином, попри гучну назву та історичну символіку, реальна допомога йшла переважно через звичайні пакети, а не через спрощений ленд-ліз[156; 214].

Окремою цікавою темою в контесті НАТО є спільні навчання з Україною[156]. Ще з 1990-х Україна була найактивнішим партнером НАТО серед країн, що не були членами Альянсу: з 1997 року – програма «Партнерство заради миру», з 2014-го розширені можливості (Enhanced Opportunity Partner)[156]. Проте до 2022 року західні офіцери та аналітики здебільшого сприймали ЗСУ як армію радянського зразка з високим рівнем корупції, застарілою технікою технікою та низькою боєздатністю[156]. Цей стереотип було остаточно розвінчано під час низки спільних навчань 2017-2021 років[156].

Особливо вражаючим для західних партнерів стало навчання Rapid Trident-2021 та Combined Resolve XV (Графенвьор, Німеччина, травень 2021), де 1-ша окрема танкова бригада та 95-та десантно-штурмова бригада ЗСУ перемогли американські та німецькі підрозділи за всіма показниками: швидкість наступу, точність артилерії, рівень цифрового управління військами та нічний бій[156]. Німецькі офіцери відкрито визнавали, що українські екіпажі Т-64БВ та БМП-2 переважали Leopard 2 та Marder за ефективністю у реальних умовах бездоріжжя та електронної боротьби[156].

Американські звіти після навчань містили формулювання на кшталт «Ukrainian units demonstrated near-NATO standards and in some areas exceeded them»[156]. Цей досвід став одним із ключових факторів, чому вже у березні-квітні 2022 року Захід без вагань почав передавати Україні найсучасніше озброєння стереотип «слабкої пострадянської армії» було розбито ще до великої війни, проте багато країн усе ж

побоювалися розкладання грошей перепродажі озброєнь потрапивши під вплив дезінформації, яку поширювала РФ[156; 183].

Реакція Європейського Союзу на гібридну агресію РФ проти України стала однією з наймасштабніших і найшвидших в історії європейської інтеграції[74; 85; 123; 178]. Ще до повномасштабного вторгнення 2022 року ЄС створив спеціалізовані інституції для протидії гібридним загрозам вивчаючи досвід України[74; 85; 123]. У березні 2015 року з'явилася East StratCom Task Force (EUvsDisinfo), яка за десять років задокументувала понад 19 500 випадків російської дезінформації, найбільшу відкриту базу такого роду у світі[101]. У жовтні 2017 року у Гельсінкі запрацював Європейський центр досконалості з протидії гібридним загрозам (Hybrid CoE, що об'єднав спочатку 12, а станом на грудень 2025 року вже 36 країн-учасниць, включно з не членами ЄС (США, Велика Британія, Австралія, Японія)[123]. Саме Hybrid CoE розробив операційне визначення гібридних загроз, яке нині використовується в усіх стратегічних документах ЄС і НАТО[123; 207].

Санкційна політика ЄС пройшла еволюцію від символічних персональних обмежень до найжорсткішого в історії Європейського Союзу режиму економічного тиску[9; 87; 99]. Перший пакет, ухвалений 31 березня 2014 року, стосувався лише 21 осіб, відповідальних за підрив територіальної цілісності України[9]. Після Іловайської трагедії та збиття MH17 у вересні 2014 року з'явилися перші секторальні санкції (обмеження доступу російських банків до європейських ринків капіталу, ембарго на технології для нафтогазового сектору)[9; 203]. Кожен наступний пакет розширював сферу дії, а після 24 лютого 2022 року санкції набули системного характеру: відключення семи найбільших банків від SWIFT, заморожування понад 300 млрд євро золотовалютних резервів Центрального банку РФ, персональні санкції проти Володимира Путіна, Сергія Лаврова та більш ніж 2200 фізичних і юридичних осіб[9].

Станом на грудень 2025 року Європейська Комісія ухвалила 19 пакетів санкцій – що є рекордною кількість за весь час існування ЄС[9]. Ключовим поворотом став перехід до вторинних санкцій та системного блокування обходу[9]. П'ятнадцятий

пакет (16 грудня 2024 року) ввів обмеження проти російського «тіньового флоту» (понад 52 судна), а також проти китайських компаній, що постачають мікроелектроніку та дрони[9]. Дев'ятнадцятий пакет (23 жовтня 2025 року) остаточно закрив «газовий лазівку»: заборонив реекспорт російського скрапленого природного газу через термінали ЄС до третіх країн з 1 січня 2026 року (короткострокові контракти) та з 2027 року (довгострокові)[9]. За оцінками Bruegel, це коштуватиме РФ 8-10 млрд євро щорічно[9]. Проте бюрократична машина ЄС по сьогоднішній день продовжує тягнути із більш сильними програмами пакетних санкцій, оскільки в умовах ведення гібридної агресії РФ також має симпатиків в країнах Європейського Союзу й на сам перед тих хто досі є залежним від енергоресурсів, що йдуть з РФ та з моменту завершення договору про транспортування газу між РФ та Україною, ця залежність значно послабла[9].

Санкції проти третіх країн, які допомагають обходити обмеження, стали новим етапом в політиці ЄС[9]. У 2024-2025 роках до санкційного списку ЄС було внесено понад 150 компаній з Туреччини, ОАЕ, Казахстану, Киргизстану, Вірменії та Сербії, а також кілька десятків китайських постачальників товарів подвійного призначення[9]. Експорт таких товарів з Китаю до РФ зріс на 300-400% протягом 2023-2024 років, що змусило Брюссель, як центру організації вперше застосувати вторинні санкції проти материкових китайських юридичних осіб[9]. Одночасно заборонено експорт до РФ квантових комп'ютерів, передових напівпровідників та обладнання для виробництва боєприпасів, через це ми можемо побачити цікаву картину коли в бортових GPS авіації РФ стоять примітивні пристрої, а з протилежної європейські та американські комплектуючі для ракет, що все одно потрапляють до РФ[9].

Паралельно з санкціями ЄС радикально змінив підхід до прямої військової допомоги[1]. 28 лютого 2022 року, через чотири дні після початку повномасштабного вторгнення, Рада ЄС вперше в історії ухвалила рішення про фінансування летальної зброї для третьої країни - 450 млн. євро з позабюджетного European Peace Facility (EPF)[63]. За три роки цей інструмент розширено до 17 млрд. євро на 2021-2027 роки, з

додатковим Ukraine Assistance Fund у 5 млрд. євро (2024)[63]. Станом на грудень 2025 року через EPF Україні виділено понад 10,6 млрд. євро, а разом з EUMAM Ukraine підготовлено понад 150 000 українських військовослужбовців (це чисельність саме тих військовослужбовців, що проходили підготовку вже після повномасштабного вторгнення у країнах ЄС)[214].

Фінансова підтримка цивільного сектору не менш вражаюча. У 2024-2027 роках діє Ukraine Facility на 50 млрд євро, з яких 33 млрд. є пільгові кредити, а 17 млрд. безповоротні гранти. Виплати прив'язані до виконання реформ (правосуддя, боротьба з корупцією, деолігархізація, медіа-законодавство)[9]. Станом на кінець 2025 року Україна отримала вже понад 28 млрд. євро та виконала 100% умов для наступних траншів[215].

Шлях України до членства в ЄС став найшвидшим в історії розширення. Заявка подана 28 лютого 2022 року, статус кандидата надано 23 червня 2022 року за рекордні чотири місяці. 14 грудня 2023 року Європейська Рада, попри опір Угорщини, одноголосно вирішила відкрити переговори. Перша міжурядова конференція відбулася 25 червня 2024 року одночасно з Молдовою[1].

У 2025 році темпи переговорів прискорилися ще більше. Вересень 2025 року завершено screening (перевірку відповідності законодавства) за всіма 35 главами acquis communautaire (сукупність правових норм) з позитивними висновками в усіх розділах. У листопаді Європейська Комісія в Enlargement Package визнала «виключний прогрес» України в судовій реформі та боротьбі з корупцією. У грудні 2025 року Рада ЄС відкрила перший кластер переговорів, «Фундаментальні цінності» (включаючи Кластер 23 «Судоустрій та фундаментальні права»), що означає перехід до substantive (змістовних) переговорів[9].

Станом на кінець 2025 року Україна виконала умови для відкриття ще двох кластерів «Внутрішній ринок» та «Зовнішня політика та безпека». За оцінками Єврокомісії, за нинішніх темпів Україна може завершити переговори до кінця 2028 року, а приєднатися до ЄС у 2030-2031 роках – швидше, ніж будь-який попередній

кандидат, але варто зазначити, що й саме ЄС, точніше окремі його країни не завжди відповідає поставленим вимогам й для багатьох критиів, це в багато чому виглядає, як звичайне відтягування питання вступу України[4].

Таким чином, за одинадцять років (2014-2025) Європейський Союз пройшов шлях від обережних персональних санкцій і моніторингу дезінформації до найжорсткішого в історії режиму економічного тиску, прямої військової допомоги на десятки мільярдів євро та фактичного визнання України майбутнім членом Союзу[1]. Ця трансформація не лише послабила військово-економічний потенціал РФ, а й остаточно закріпила європейську перспективу України як невід'ємну частину європейської архітектури безпеки та цінностей[4].

Реакція ОБСЄ на російську агресію проти України з 2014 року стала ключовим елементом міжнародного моніторингу, фокусуючись на деескалації та документуванні порушень. Спеціальна моніторингова місія (SMM) була розгорнута 21 березня 2014 року за рішенням Постійної ради ОБСЄ (документ №699) за запитом української влади, з мандатом охоплювати всю територію України в межах міжнародно визнаних кордонів[194]. Місія, як цивільна та неозброєна, мала сприяти діалогу, зменшенню напруги та верифікації дотримання принципів ОБСЄ, включаючи моніторинг ситуації на кордоні та в зоні конфлікту[194]. На піку (з 2015 року) SMM налічувала близько 1000 міжнародних спостерігачів з 53 держав-учасниць ОБСЄ, плюс локальний штат, що робило її найбільшою польовою місією організації[174].

Щоденні звіти SMM стали фундаментальним джерелом об'єктивної інформації про конфлікт, фіксуючи понад 20 000 публічних оновлень з 2014 по 2022 рік [174]. Місія використовувала патрулі, БПЛА, камери та датчики для документування: присутності озброєння, відсутнього в ЗСУ (наприклад, як вже згадувалося в попередньому розділі: модернізовані танки Т-72Б3Б, Т-80БВМ, РСЗВ «Торнадо-Г») [174]; транскордонне переміщення техніки через неконтрольовані ділянки кордону (Ростов/Донецьк) [174]; систематичних обстрілів цивільної інфраструктури (1.5 млн порушень припинення вогню за 2016-2021) [174]; та порушень пакету Мінських угод

2014-2015 [194; 195]. Ці дані сформували доказову базу для міжнародних судів, включаючи МКС, та слугували основою для звітів ООН [173].

Обмеження мандату SMM були критичними: консенсусний характер ОБСЄ дозволяв РФ блокувати розширення (наприклад, повний доступ до кордону) [136], а сепаратисти/російські сили систематично обмежували свободу пересування (понад 5000 інцидентів за 2014-2022) [174]. Місія координувалася з іншими структурами ОБСЄ (Проектний координатор в Україні, Місія спостерігачів, але залишалася вразливою до маніпуляцій, що підкреслювало структурні дефекти організації в умовах агресії постійного члена [161].

Паралельно з SMM, у червні 2014 року була створена Тристороння контактна група (ТКГ) як платформа для переговорів: перша сесія відбулася 8 червня в Києві з представниками України (посол Павло Клімкін), РФ (посол Михайло Зурабов) та ОБСЄ (спецпредставник Хайді Тальявіні) [145]. Формат, ініційований Нормандським форматом, мав полегшити дипломатичне врегулювання в Донбасі, але виявився політично хибним: РФ позиціонувалася як «посередник», а не сторона конфлікту, що дозволяло РФ підтримувати «правдоподібне заперечення» своєї участі [217].

ТКГ включала чотири підгрупи (з травня 2015: політична, економічна, гуманітарна, безпека), де ОБСЄ координувала безпеку через главу SMM [145]. РФ систематично просувала інтерпретацію Мінських угод на свою користь: вимагала прямих переговорів Києва з «представниками ОРДЛО» (ДНР/ЛНР), наполягала на «виборах» та «спеціальному статусі» перед відновленням контролю над кордоном (п. 9 Мінська II), блокувала обговорення виведення іноземних військ (п. 10) [145; 217]. Це призвело до стагнації: за 2014-2022 ТКГ провела понад 200 зустрічей, але без проривів, слугуючи радше інструментом затягування [217].

Кульмінацією обмежень ОБСЄ стало завершення SMM 31 березня 2022 року: РФ заблокувала продовження мандату в Постійній раді, посилаючись на «втрату об'єктивності» [161]. Це сталося через місяць після повномасштабного вторгнення (24 лютого), коли SMM евакуювала близько 500 свої спостерігачів, а мандат, щорічно

поновлюваний консенсусом, не пройшов через вето РФ [161]. Закриття-навмисне знищення ключового механізму верифікації, що документував російські злочини (включаючи 36 686 вибухів у 2021) [174]. Архів SMM на сьогодні передано для розслідувань МКС/ООН [173].

Для обходу російського вето міжнародна спільнота використала Moscow Mechanism (московський механізм) – процедуру створена, ще 1991 року, що дозволяє 10 державам ініціювати незалежну експертну місію без консенсусу [161; 162]. Перша активація щодо України була здійснена 3 березня 2022 (45 держав-учасниць ОБСЄ, за консультацією з Україною) експерти (Вольфганг Бенедек, Вероніка Билкова, Марко Сассолі) представили звіт 13 квітня 2022, фіксуючи систематичні порушення Прав людини та міжнародного гуманітарного права: тортури як метод війни, цілеспрямовані атаки на цивільне населення (включаючи Бучу), викрадення, депортації (тисячі дітей з 24 лютого) [161].

Друга активація Moscow Mechanism (продовження): 2 червня 2022 (45 держав), звіт 14 липня 2022 (експерти: Билкова, Лаура Гуерчо, Василка Санчин) підтвердив попередні висновки, додавши воєнні злочини (статті 8 пункту 2 частин (a)-(b) Римського статуту) РФ, на окупованих територіях [161]. Третя активація (спеціально щодо дітей): 30 березня 2023 (45 держав) звіт 4 травня 2023 (експерти: Билкова, Сесилі Хеллествейт, Еліна Штейнерте) встановив, що понад 19 500 дітей депортовано/передано з 2014 (зростання після 2022), 43 «табори перевиховання», систематична зміна ідентичності/громадянства – порушення ст. 49 Женевської конвенції IV, «імовірно» цілеспрямований геноцид (Конвенція 1948) [161; 162].

Звіт 2023 став ключовою основою для ордера МКС: 17 березня 2023 Пре-Trial Chamber II (Палата попереднього провадження II) видав ордер на арешт Володимира Путіна та Марії Львової-Бєлової за воєнний злочин незаконної депортації та передачі дітей (ст. 8(2)(a)(VII), 8(2)(b)(VIII) Римського статуту) – перший ордер на діючого главу держави-члена РБ ООН в історії МКС [161; 162]. Експерти ОБСЄ задокументували «розумні підстави» для відповідальності за (ст. 25(3)(a)), включаючи накази й

невідповідний контроль, це доповнило розслідування прокурора Каріма Хана (заява 22 лютого 2023) [161].

Загалом Московський механізм було активовано 6 разів з 2022 (4 щодо України, й ще по 1 на РФ та Білорусь), демонструючи його ефективність [161; 162]. Таким чином, з 2014 по 2025 ОБСЄ еволюціонувала від SMM/ТКГ (обмежених консенсусом) до Московського механізму як інструменту підзвітності, обходячи вето РФ [161; 162]. Архіви SMM та звіти Механізму (4 місії щодо України) стали ключові для МКС/ООН, фіксуючи тисячі жертв і злочинів, подальша активація 2024 (депортовані цивільні, тисячі) підкреслює роль ОБСЄ в гібридній війні [161; 162; 173; 174]. Це не лише моніторинг, а інвестиція в справедливість, попри структурні виклики організації.

Однак варто зауважити фатальний прокол в системі спостерігачів SMM-групи, з 2014 по 2022 рік РФ делегувала 10-15 % складу SMM (до 150 осіб одночасно), включаючи підтверджених співробітників ГРУ і ФСБ [161; 174]. Це дозволяло Москві отримувати розвіддані, пом’якшувати звіти про власні порушення, блокувати доступ місії до кордону та підривати довіру до ОБСЄ. Особливо показовим є історія з службовцем 5 відділу ФСБ Олегом Козловим, що входив до складу груп спостерігачів [44]. А коли повний контроль став неможливим, РФ 31 березня 2022 року просто знищила місію своїм вето – ліквідувавши єдиний незалежний механізм моніторингу, який їй уже не вдавалося використовувати проти України зсередини [161].

4.2. Військова, інформаційна та кібернетична протидія

Починаючи з весни 2014 року Україна опинилася в ситуації, яку раніше важко було уявити навіть у найгірших сценаріях [41]. Під час глибокої внутрішньополітичної кризи, викликаної Революцією Гідності та втечею Януковича [167], країна стала об'єктом прихованої військової агресії з боку ядерної держави та постійного члена Ради Безпеки ООН [20]. РФ, офіційно заперечуючи будь-яку причетність, фактично розпочала гібридну війну, поєднуючи регулярні війська без розпізнавальних знаків

[136], найманців, місцевих колаборантів та потужну інформаційну кампанію [4; 5; 10; 19].

Важко назвати будь-яку іншу країну, що стикалася з подібним поєднанням прямих військових дій, що підкріплювалися інформаційною війною, кібератаками, економічним тиском та ядерним шантажем [41; 105; 115; 116], й більшість аналітиків прогнозували, що в прямій конфронтації з РФ Україна буде мало спроможна себе захисти, проте результати виявилися кардинально іншими [136].

Протягом 11 років – від Анексії Криму до грудня 2025 року – Україна не просто вистояла, а пройшла шлях безпрецедентних трансформацій й призвела до ситуації, коли невідомо, хто зі сторін здобуде перемогу [3; 62]. Те, що починалося як відчайдушний беззбройний супротив, перетворилося на висококваліфіковану модель протидії, що по сьогоднішній день змушує світ переглядати уявлення про спроможності «малих» держав чинити супротив «світовим» державам [66; 72].

Ця модель формувалася не на запозиченнях з підручників НАТО чи радянських доктрин, а закладалася й гартувалася в окопній війні Донбасу, трагедіях Іловайська та Дебальцево [136], проходила через чисельні випробування, обтесуючи досвід молодих та старих офіцерів й волонтерських організацій [15; 112], вибудовуючи свою власну концепцію ведення війни [113]. Ключовим елементом успіху трансформацій стала спроможність до навчання у держави та суспільства на помилках [66]. Кожна втрата та трагедія не призвела до капітуляції, а обернулася каталізатором радикальних змін: від реформ армії до формування «Народного ВПК» й переходу до асиметричної війни [72; 113]. Саме Україна довела, що країна, маюча ВВП у десятки разів менший за агресора, може завдати йому глибоких втрат [62; 87]. Минуло 11 років з початку агресії, а Україна не просто продовжує стояти, а диктує правила гри на окремих театрах військових дій, примушуючи Чорноморський флот РФ практично не виходити в море [249], була знищена або пошкоджена частина компонентів російської програми ядерного стримування (стратегічну авіацію та станції попереднього виявлення) [62] та

примусила саму ж РФ технічно деградувати через катастрофічні втрати бронетехніки [62].

Саме тому 2014 рік – це не тільки рік початку агресії, але й рік народження нової України: держави, що навчилася перетворювати катастрофу на джерело сили, а біль поразок на фундамент стійкості в війні нового покоління [66; 137].

Початок агресії: Анексія Криму стала першою й найшвидшою територіальною втратою в сучасній європейській історії [41; 136]. Від появи перших «зелених чоловічків» біля Верховної Ради АР Крим 27 лютого [22] до фейкового «референдуму» 16 березня 2014 року [95; 128] минуло менше трьох тижнів. Для нової української влади, яка отримала повноваження лише 23 лютого після втечі Януковича [167], це був абсолютний шок, на який просто не існувало ні готової відповіді, ні механізмів реагування [136; 144].

Українська держава перебувала в стані майже повного паралічу: армія була деморалізована десятиліттями недофінансування й корупції [136], спецслужби інфільтровані російською агентурою [44], бюджет розкрадений, а міжнародні партнери ще навіть не встигли усвідомити реальні масштаби катастрофи [41]. РФ використала цей вакуум влади блискавично і максимально зухвало, грубо порушивши Будапештський меморандум 1994 року [20], Гельсінські угоди та власні двосторонні договори з Україною про недоторканність кордонів, дружбу та партнерство й розміщення чорноморського флоту [22; 136].

Найтрагічнішим аспектом кримської катастрофи виявилося те, що близько 70% українських військовослужбовців у Криму (понад 18 тисяч осіб) або перейшли на бік окупанта, або здалися без єдиного пострілу [136]. Багато з цих людей пізніше присягнули на вірність РФ й згодом воюватимуть проти України на Донбасі, використовуючи знання про тактику й організацію української армії [136].

Служба безпеки України в Криму виявилася повністю під контролем ФСБ РФ: керівництво регіонального управління ще задовго до появи «зелених чоловічків» отримувало прямі вказівки та координувало свої дії з російськими спецслужбами [44].

Усі архіви агентурної мережі, особові справи співробітників, матеріали оперативних розробок були передані РФ практично без спротиву. Ця системна зрада коштувала Україні не лише території, а й безпеки тисяч людей [136].

Масштаби втрати були колосальними: 27 тисяч квадратних кілометрів суші, 2,4 мільйона громадян України, практично весь військово-морський потенціал країни (75% Чорноморського флоту ВМС України) [136], Севастополь як головна військово-морська база, стратегічний контроль над Керченською протокою та величезні газові родовища на шельфі Чорного моря [22; 136]. Фактично Україна за лічені тижні перестала бути повноцінною чорноморською морською державою, втративши критично важливі стратегічні активи [136].

Кримська трагедія дала Україні три фундаментальні уроки виживання. Перший і найболючіший: у гібридній війні швидкість вирішує абсолютно все. Сучасна агресія будується на принципі «зроблено до того, як світова спільнота зрозуміє, що відбувається». Затримка навіть на кілька діб робить будь-який організований спротив практично неможливим [4; 5; 10; 19; 41; 136].

Другий урок: «правдоподібне заперечення» агресора треба руйнувати миттєво, публічно й безапеляційно. РФ цинічно стверджувала, що «зелені чоловічки», це нібито «місцеві сили самооборони Криму», а не російські військові [95; 136]. Україна не змогла достатньо швидко зібрати, систематизувати й масово оприлюднити незаперечні докази (фотографії, відео, свідчення очевидців), тому міжнародна спільнота до останнього моменту сподівалася, що «це не справжнє вторгнення» й ситуацію можна вирішити дипломатично [41; 136].

Третій та можливо, найважливіший урок: відсутність рішучого збройного спротиву не стримує агресора, а лише провокує його до подальшої ескалації насильства [41; 136]. Однак початок агресії став не тільки катастрофою, але й став водночас моментом фундаментальної української трансформації й системної зміни в армії, спецслужбах і суспільній свідомості мільйонів українців [66; 137].

Парадоксально, але саме провал у Криму врятував решту України від подібної долі [41; 136]. Він болісно, але переконливо показав усім від керівництва держави до пересічних громадян, що пасивність і надія на міжнародну дипломатію без власної боротьби дорівнюють повільній смерті держави [66]. Усі подальші критичні рішення від масового створення добровольчих батальйонів до остаточної відмови від ілюзій щодо «Мінська» як справжнього миру корінилися саме в цьому лютневому-березневому шоку 2014 року [15; 112; 136; 145; 217].

Формат «антитерористичної операції», офіційно оголошений 14 квітня 2014 року, не був стратегічним вибором, це була політична та юридична необхідність [136]. Нова українська влада добре розуміла, що проти неї воює регулярна армія РФ, але відкрито визнати війну означало б автоматичне введення воєнного стану, скасування критично важливих президентських виборів 25 травня (тимчасово виконуючий обов'язки президента не мав стільки ж повноважень скільки президент) та ризик спровокувати повномасштабне російське вторгнення по всій лінії кордону, до чого Україна тоді була абсолютно не готова [136].

Юридична фікція АТО створювала абсурдну та небезпечну ситуацію: операцію формально координувала Служба безпеки України, а не Генеральний штаб, що за логікою мало б керувати військовими діями [136]. Збройні Сили могли брати участь у бойових діях лише «у підтримці» СБУ, а не як головна сила. Ця правова конструкція в сукупності із розумінням солдатів, що вони протистоять регулярній армії, що прикривається статусом «терористів» сильно деморалізувала [136].

На практиці це означало ланцюг фатальних обмежень: немає воєнного стану, немає права на повну мобілізацію, бізнес працював у звичайному режимі, кордони залишалися відкритими, життя в більшості країни йшло своїм чином, а армія воювала «в рукавичках», не маючи повноважень діяти рішуче [136].

Саме через початковий вакуум влади в Україні виник унікальний феномен у вигляді Добровольчих батальйонів, вчорашні майданівці, футбольні ультрас, ветерани афганської війни, мисливці, вчителі – люди з абсолютно різних верств суспільства самі

купували автомати, бронежилети й каски, самі сідали в буси й їхали тримати лінію фронту там, де її фактично не існувало [15; 66; 112; 136].

Так виникли «Азов», «Айдар», «Дніпро-1», «Торнадо», «Шахтарськ», «Правий Сектор» та інші, що й були спочатку єдиною реальною силою, здатною швидко реагувати та стримувати російський наступ [15; 112; 136]. Однак вони не мали єдиного командування, надійного зв'язку зі Збройними Силами, єдиних правил застосування сили і часто воювали кожен за себе, покладаючись на ентузіазм і самоорганізацію. Це призводило як до героїчних локальних перемог, так і до трагедій через фатальну неузгодженість дій [112; 136].

Добровольці не чекали наказів, повісток чи зарплати, вони просто йшли воювати туди, де держава ще не встигла або не змогла організувати оборону [15; 66; 112]. Саме вони звільняли Маріуполь (батальйон «Азов») [136], тримали Піски й Широкине під постійним вогнем, влазили в найгарячіші точки Донецького аеропорту [136]. Їхня мотивація була гранично простою: «якщо не ми, то хто?». Ці люди розуміли, що альтернативою їхній участі буде не приїзд регулярних військ, а просто втрата території [66; 112]. Добровольчі підрозділи демонстрували шалену ефективність саме завдяки своїй природі: командири обиралися знизу за авторитетом і досвідом, рішення приймалися швидко без бюрократичних узгоджень [112]. Саме добровольці першими показали, що російських «відпускників» та найманців можна не просто зупиняти, а й відкидати [136].

Іловайськ у серпні 2014 року і Дебальцеве в лютому 2015-го стали найбільшою катастрофою цього правового абсурду [136]. В Іловайську українські підрозділи опинилися в оточенні багато в чому тому, що не мали юридичного права на повномасштабний організований відхід без дозволу «антитерористичного центру» СБУ, який не розумів реальної ситуації на фронті [136]. А тим часом РФ повноцінно ввела регулярні війська заходячи колонами [136].

Саме ці трагедії для України остаточно зруйнували російський наратив про нібито «громадянську війну» на Донбасі [10; 41; 136; 169]. Масове використання

регулярних частин армії, артилерійські удари з території РФ, нескінченні колони техніки без розпізнавальних знаків – усе це було ретельно зафіксовано, оприлюднено міжнародними спостерігачами і стало неспростовним доказом прямої російської агресії [136; 169; 174]. Без трагедій Іловайська та Дебальцевого західні санкції проти РФ, ймовірно, залишилися б суто символічними [136].

При всіх своїх фатальних вадах АТО дала Україні критично важливий час у 2014-2016 роках, коли РФ ще не була технічно та психологічно готова до повномасштабного вторгнення, а Захід все ще вагався з підтримкою [136]. За ці два роки вдалося зробити неможливе: частково відновити боєздатність деморалізованої армії, провести перші великі контракти на постачання західного озброєння, відновити Національну гвардію як окрему силову структуру та почати болісну, але необхідну інтеграцію добровольців у державні структури [15; 66; 112; 136].

Водночас формат АТО став класичним історичним прикладом «політичного компромісу, що коштував тисяч життів» [136]. Кожен місяць утримання юридичної фікції «це не війна» коштував сотень загиблих українців і десятків безповоротно втрачених населених пунктів [136]. Лише після катастрофи Дебальцевого політичному керівництву стало остаточно зрозуміло: далі так воювати фізично неможливо, потрібні системні зміни [136].

У підсумку АТО зіграла двояку роль в українській історії: з одного боку, вона врятувала державність у найкритичніший момент, давши необхідний час на передишку, переозброєння та психологічну мобілізацію суспільства [66; 136]. З іншого стала найтрагічнішим і найкривавішим уроком про те, що війну треба називати війною, а агресора – агресором, це Україна засвоїла остаточно й назавжди 24 лютого 2022 року, коли більше не було жодних «АТО», «ООС» чи «мирних переговорів» - тільки чіткий воєнний стан та повномасштабна війна за виживання [24; 31].

Пакет мінських документів з 5 вересня 2014 року по 12 лютого 2015 року виник не від бажання, а реакції Заходу, що зреагувала не на гібридну війну в Україні, а на збиття МН17 [145; 203; 217], ця трагедія залишається по сьогодні безкарною, але вона

стала єдиним способом зупинити бойові дії та виграти критично необхідний час для перегрупування [145; 217]. Угоди були класичним прикладом «поганого миру», підписаного під дулом гармати [145; 217]. Україна погоджувалася на фактично політичну капітуляцію в обмін на припинення вогню та відведення важкого озброєння [145]. При цьому всі учасники розуміли головне: РФ ніколи не збиралася їх виконувати, використовуючи угоди лише як інструмент тиску [145; 217].

Протягом 2015-2021 років Мінські угоди перетворилися на механізм стримування саме України, а не агресора [145; 217]. Кожен обстріл, кожне порушення з російського боку Захід зустрічав ритуальними закликами «обом сторонам виконувати Мінськ», фактично прирівнюючи жертву до нападника [145; 217]. Україна опинилася в ситуації, коли будь-яка спроба звільнити окуповані території автоматично оголошувалася «порушенням мирного процесу» і загрожувала втратою міжнародної підтримки, з протилежного боку санкції накладалися саме на РФ підкреслюючи її причетність [145; 217].

Попри всі обмеження Україна використовувала «заморожену війну», як період для збільшення свого війська з 130 до 250 тисяч осіб, створення сержантських корпусів, підняття фінансування війська з 1.2% до 5%, переозброєння за натовськими стандартами, переформування сил спеціальних операцій [136]. З протилежного боку, це дозволяло РФ тренувати кадри та непомітно перекидати техніку [136].

Найнебезпечнішим наслідком Мінська стала створена Росією ілюзія «внутрішнього конфлікту», яку роками просували в західних країнах [10; 41; 145; 217]. Фраза «немає військового рішення» перетворилася на мантру європейських політиків, які панічно боялися ескалації [145; 217]. Україна змушена була грати за цими правилами, хоча кожен військовий розумів просту істину: без військового рішення політичного не буде ніколи [145; 217].

Сьогодні Мінські угоди згадуються переважно як історичний приклад того, як не треба домовлятися з агресором [145; 217]. Вони показали фундаментальну істину: будь-який «мир», що зберігає присутність агресора на твоїй землі та легітимізує його

наративи, є лише відстрочкою нової, ще жорстокішої війни [145; 217]. Цей урок Україна засвоїла назавжди: більше ніколи «Мінськів» замість справжньої перемоги [145; 217].

З 2015 року держава розпочала складний, але необхідний процес інтеграції добровольчих формувань у регулярні силові структури [15; 66; 112; 136]. Найбільш боєздатні батальйони увійшли до складу Міністерства внутрішніх справ, ставши частиною Національної гвардії та Національної поліції, інші влилися до Збройних сил України [112; 136]. «Азов» перетворився на полк спеціального призначення НГУ, «Донбас» став 46-м окремим батальйоном, «Айдар» 24-ою штурмовою бригадою [112; 136]. До кінця 2016 року процес інтеграції був практично завершений, а українська армія отримала структуровану систему замість мозаїки незалежних загонів [136].

Ця інтеграція стала унікальним прикладом у пострадянському просторі: стихійний громадянський спротив не був розігнаний, маргіналізований чи знищений, а свідомо й системно включений у державну структуру [66; 112]. Більшість командирів-добровольців отримали офіцерські звання відповідно до своїх реальних функцій, а їхній безцінний бойовий досвід став основою для підготовки нових підрозділів і розробки тактичних прийомів [112; 136].

До 2017 року всі легітимні збройні формування опинилися під єдиним командуванням Генерального штабу, що створило передумови для побудови сучасної армії [136]. Але найважливіше полягало в іншому: добровольці 2014-2015 років стали «золотим фондом» української армії наступних років [66; 112]. Десятки тисяч із них повернулися на фронт після 24 лютого 2022 року, але вже не тільки рядовими бійцями, а й досвідченими командирами рот, батальйонів і навіть бригад [66; 136]. Їхній досвід боїв у Донецькому аеропорту, Мар'їнці, Широкиному, Пісках виявився безцінним у битвах за Київ, Харків, Маріуполь і Бахмут [136; 196].

Феномен українських добровольчих батальйонів увійшов у світові військові підручники як унікальний приклад того, як мобілізоване громадянське суспільство може за лічені місяці компенсувати колапс регулярної армії та створити боєздатну силу

з нуля [66; 112]. Добровольці не просто врятували українську державу в критичний момент 2014 року вони стали серцем і хребтом нової української армії [66; 112; 136].

24 лютого 2022 року о 4:55 ранку РФ розпочала повномасштабне вторгнення по всій лінії кордону від Харкова до Криму та з території Білорусі [24; 31; 57]. Це був не просто «другий етап» війни 2014 року, а спроба блискавичного знищення української держави за 3-10 діб через захоплення Києва, ліквідацію керівництва та встановлення маріонеткового режиму [41; 136]. Усі попередні правові й політичні фікції «АТО», «ООС», «Мінські угоди» миттєво зникли [145; 217]. Того ж дня Президент Зеленський підписав указ про загальну мобілізацію та введення воєнного стану [24; 31], і вперше за всю історію незалежності Україна офіційно визнала: ми ведемо повномасштабну оборонну війну проти ядерної держави [24; 31].

Вже в перші години війни стало очевидно, що досвід восьми років на Донбасі дав Україні унікальний актив, сотні тисяч людей із реальним бойовим досвідом [66; 136]. Поки російські контрактники губилися в українських селах, не розуміючи, де вони та навіщо, українські ветерани 2014-2015 років уже знали, як воювати проти «Градів» без авіації, як організовувати оборону міст, як використовувати протитанкову зброю [136]. Це знання виявилося безцінним [136].

Введення воєнного стану зняло всі внутрішні табу і створило нову стратегічну реальність [24]. Вперше офіційно дозволили бити по військових об'єктах на території РФ, якщо вони використовуються проти України [24]. Війна більше не обмежувалася лише українською територією, це була принципово нова парадигма, яка означала, що Україна готова захищатися всіма доступними засобами [24].

Російський план «Київ за три дні» базувався на фатальному припущенні, що українці зустрінуть окупантів квітами або принаймні не чинитимуть серйозного опору, принаймні таку картину перед командуванням РФ ставила їхня розвідка [41; 136]. Реальність виявилася діаметрально протилежною: від півночі до півдня країни десятки тисяч людей записувалися в територіальну оборону, брали зброю й ішли на блокпости

[66]. Народний спротив виявився масовим і спонтанним люди самі вирішили захищати свою землю [66].

Водночас 24 лютого стало днем остаточного розриву з будь-якими ілюзіями про «русский мир» [137; 139]. Російські ракети вдарили по житлових кварталах Харкова, Охтирки, Чернігова, Херсона [136]. Мирне населення вперше відчуло на собі, що таке «денацифікація» насправді [88; 119]. Це знищило останні сумніви навіть у тих, хто досі вагався: стало зрозуміло, що або ми переможемо, або нас просто не буде [66; 137]. Вибору не залишилося.

Перші тижні повномасштабної війни стали класичною оборонною операцією на виснаження [136; 196]. Завдання українських захисників полягало не в утриманні кожного метра території, а в максимізації втрат противника й недопущенні швидкого колапсу фронту та падіння столиці [136; 196]. РФ кинула на Київ найкращі підрозділи, повітряно-десантні війська, спецназ ГРУ, елітні мотострілецькі бригади, сподіваючись на блискавичну перемогу [62; 136].

Перший стратегічний провал російської армії стався вже 24-25 лютого під час битви за аеродром Гостомель [136; 196]. План РФ передбачав висадку десятків Іл-76 із підкріпленнями для швидкого захоплення Києва, але українська 4-та бригада швидкого реагування Нацгвардії спільно з територіальною обороною та артилерією завдали блискавичного контрудару [136; 196]. Вони знищили частину десанту й підірвали злітно-посадкову смугу, після чого «блискавична війна» закінчилася, не встигнувши розпочатися [136; 196].

Проте запустити ворога на стратегічну глибину мало й свої наслідки, передмістя Києва – Буча, Ірпінь, Гостомель, Бородянка, Мощун, перетворилися на суцільну лінію оборони [136; 196]. Українські сили застосували тактику малих мобільних груп із протитанковими ракетними комплексами Javelin, NLAW, «Стугна», гранатометами та дронами [136]. Російські колони розстрілювалися на під'їздах до міст, десятки одиниць техніки щодня перетворювалися на палаючий металобрухт [62; 136]. Однак бої за Ірпінь та Бучу стали не лише прикладом військової майстерності, а й символом

жорстокості окупантів, після відступу російських військ у звільнених містах знайшли сотні вбитих цивільних зі зв'язаними руками [161]. Масові злочини в Бучі, розстріли на вулицях, катівні в підвалах остаточно зруйнували будь-які ілюзії про «звільнення» й стали доказом геноцидного характеру війни [161].

Харків із перших днів опинився під масованим артилерійським та ракетним терором, проте місто так і не було оточене, а російські війська не змогли навіть увійти в його межі [136; 196]. Оборона Харкова стала прикладом ефективного поєднання регулярних частин ЗСУ, зокрема 92-ї механізованої бригади, Нацгвардії, територіальної оборони та місцевих добровольців [66; 136]. Кожна спроба штурму закінчувалася для ворога величезними втратами й як чергове свідчення терору РФ по сьогоднішній день (грудень 2025 року) здійснює артилерійські, ракетні та дронові атаки на цивільне населення міста [3; 62].

На півдні ключовим пунктом оборони став Миколаїв під командуванням генерала Дмитра Марченка [136]. РФ планувала через Миколаїв вийти на Одесу й відрізати Україну від моря, однак завдяки вмілому використанню артилерії, авіації (зокрема, дронів Bayraktar TB2) та мобільних груп із протитанковими засобами, російський наступ було зупинено, ще на під'їздах до міста [136]. Втративши темп і зазнавши великих втрат, окупанти застрягли під Вознесенськом і більше не просунулися [136].

Усі три ключові напрямки Київ, Харків і Миколаїв показали однакову картину: російські війська мали перевагу в техніці й авіації, але їм бракувало мотивації та гнучкості [62; 136; 196]. Українські бійці воювали за власні будинки, вулиці, сім'ї, тоді як російські контрактники навіть не розуміли, що відбувається навколо них [66; 136].

Окремої уваги заслуговує героїзм «захисників Маріуполя», національна гвардія (у тому числі НГУ «Азов»), морська піхота, прикордонники, ЗСУ, тримали місто навіть під час оточення й саме на Маріуполі для пропагандиської картинки про перемогу над «Азовом» РФ кинула значні сили, зрівнюючи місто з землею, саме цей витрачений армією РФ мав велике значення для оборони України [136].

До кінця березня стало остаточно зрозуміло, бліцкриг провалився [136; 196]. 31 березня – 2 квітня російські війська почали поспішний відхід із Київської, Чернігівської та Сумської областей, залишаючи техніку й тіла загиблих [62; 136; 196]. Це стало першою великою тактичною перемогою України у повномасштабній війні, хоча сама РФ продовжує стверджувати, що це був «Жест доброї волі» [136; 196].

Оборона півночі та півдня в лютому-березні 2022 року коштувала Україні тисяч життів, але зберегла державність [136; 196]. Натомість РФ втратила найкращі підрозділи, десятки тисяч убитими й пораненими, сотні одиниць техніки [3; 62]. План «Київ за три дні» перетворився на один із найбільших військових провалів XXI століття [136; 196].

До літа 2022 року стало очевидно, що суто оборонна стратегія, навіть надзвичайно успішна, неминуче веде до поступового виснаження при значній перевазі противника в артилерії, авіації та живій силі [136]. РФ перейшла до повільної позиційної війни просуваючись на Донбасі й намагаючись «перемолоти» українські сили масованим вогнем [136]. У цих умовах українське командування прийняло принципово нове рішення: перехопити стратегічну ініціативу там, де ворог її найменше чекав [136].

Найяскравішим проявом цього підходу став Харківський контрнаступ у вересні 2022 року [136]. Поки світова та російська увага була прикута до Херсонського напрямку, куди Україна демонстративно стягувала резерви й техніку, справжній удар готувався на північному сході [136]. Операція почалася 6 вересня і вже за десять діб принесла вражаючі результати: було звільнено понад 8000 км² території, сотні населених пунктів, включно з ключовими вузлами: Балаклією, Ізюмом та Куп’янськом [136]. Війська РФ відступали в паніці, залишаючи цілі склади боєприпасів, техніку й навіть документи [62; 136]. Швидкість просування сягала 50-70 км за добу, що зробило цю операцію однією з найуспішніших блискавичних наступальних кампаній XXI століття [136].

Паралельно розгорталася Херсонська операція, побудована на зовсім іншому принципу [136]. Замість дорогого штурму укріплених позицій українські сили сконцентрувалися на систематичному знищенні логістики противника на правому березі Дніпра [136]. Високоточні системи HIMARS, гармати M777 і власні засоби ураження методично виводили з ладу всі великі мости й переправи – Антонівський, Каховський, Дар'ївський [136]. Російське угруповання опинилося практично в повній ізоляції [136]. 9 листопада 2022 року новопризначений командувач генерал Суровікін був змушений публічно оголосити про відхід, а вже 11 листопада українські війська увійшли до Херсона під оплески місцевих жителів [136].

Обидва контрнаступи продемонстрували якісно новий рівень української армії: здатність проводити складне оперативне маскування, блискавично концентрувати сили, координувати дії різних родів військ і максимально ефективно використовувати західну зброю [136]. Вони не лише повернули значні території, а й остаточно зруйнували міф про непереможність російської армії, завдавши їй колосальних втрат у живій силі й техніці [3; 62; 136].

Водночас ці операції чітко окреслили головну проблему: Україна здатна перемагати локально, коли досягає тимчасової переваги на окремому напрямку, але поки що не має ресурсів для одночасного масштабного наступу по всьому фронту [136]. Кожна велика операція вимагала концентрації майже всіх резервів і виснажувала їх [136]. Проте саме успіхи 2022 року остаточно переконали Захід у тому, що Україна не просто тримається, а здатна перемагати, що відкрило шлях до постачання важчого й далекобійного озброєння [136]. 2022 рік увійшов в історію війни як рік переходу від виживання до повернення свого [136].

Контрнаступ 2023 року став найочікуванішою та водночас найскладнішою операцією за весь час повномасштабної війни [136]. Його мета була амбітною: прорвати російську оборону на Запорізькому напрямку, розрізати сухопутний коридор до Криму й вийти до Азовського моря, що могло б кардинально змінити стратегічну картину війни [136]. Для цього майже рік формувалися нові механізовані бригади,

оснащені західною технікою: Leopard 2, Challenger 2, Bradley, Stryker, Caesar, PzH 2000 і вперше в історії Україна отримала корпуси, близькі до стандартів НАТО [136].

Проте противник за зиму 2022-2023 років побудував масштабну систему укріплень: три основні лінії оборони, сотні кілометрів протитанкових ровів і «зубів дракона», мінні поля щільністю до 2-3 мін на квадратний метр, постійне спостереження дронами [136]. Коли в червні 2023-го почалася активна фаза, українські війська одразу зіткнулися з проблемами, яких не передбачали в повному обсязі: відсутність переваги в повітрі, критична нестача спеціалізованої техніки розмінування, затримки з постачанням артилерійських снарядів і виснаження піхоти після року позиційних боїв [136].

РФ змінила тактику: замість утримання першої лінії вони відходили на 2-3 км, замінювали підрозділи й накривали наступаючі колони всім спектром вогню: артилерією, гелікоптерами Ка-52 та авіабомбами з УМПК [136]. Кожні кількасот метрів коштували десятків життів і одиниць техніки [136]. За п’ять місяців боїв українські сили просунулися на 10-17 км, звільнили Роботине, Вербове й низку сіл, але до другої лінії оборони Сурвікіна прорватися не вдалося [136].

Цей контрнаступ став найдорожчим і найдискусійнішим етапом війни [136]. Західні медіа писали про «провал», частина українського суспільства переживала розчарування після ейфорії 2022 року [136]. Водночас військові наголошували: головне завдання – виснажити резерви противника й не дати йому стратегічної ініціативи, це було виконано [136]. РФ втратила понад 100 тисяч особового складу (це вперше за історію коли сторона, що оборонялася зазнавала більших втрат за наступаючу), тисячі одиниць техніки й вичерпала більшість запасів [3; 62; 136].

Найважливішим підсумком 2023 року стало остаточне розуміння: перемогти РФ в класичній позиційній війні «танк на танк, літак на літак» неможливо через об’єктивну різницю в ресурсах [136]. Саме тому контрнаступ 2023-го, попри обмежені тактичні результати, став переломним моментом він змусив українське командування перейти до принципово нової стратегії активної оборони й асиметричних глибоких

ударів, яка визначила хід війни у 2024-2025 роках [72; 113; 136]. 2023 рік не провалився; він став найдорожчим, але необхідним уроком переходу до війни нового типу [136].

Наприкінці 2023 року українське військове керівництво остаточно усвідомило: у класичній позиційній війні на виснаження, де Росія має багатократну перевагу в артилерії, авіації та живій силі, перемогти неможливо [136]. Треба було не наздоганяти ворога в тій грі, де він завжди матиме більше гармат і літаків, а повністю змінити саму гру [136]. У своїй програмній статті для The Economist від 1 листопада 2023 року тодішній Головнокомандувач ЗСУ Валерій Залужний сформулював нову доктрину «активну оборону»: свідома відмова утримувати кожен метр землі заради збереження людей і створення умов для болючих контратак у найуразливіших місцях російського фронту [136]. Кожен втрачений населений пункт відтепер мав оплачуватися противником неприйнятно високою ціною [136].

Ця концепція доповнилася стратегією систематичних глибоких ударів по тилу [72; 113; 136]. Якщо раніше удари по нафтопереробних заводах, складах боєприпасів, командних пунктах і стратегічних аеродромах на території РФ вважалися «небезпечною ескалацією», то з 2023 року вони стали щоденною рутиною і невід'ємною частиною оперативного планування [72; 113; 136]. Логіка була простою й жорсткою: втрата Авдіївки чи кількох сіл на Донеччині має компенсуватися знищенням десятків російських складів, логістичних вузлів, багатьох тисяч російських солдатів і мільярдів доларів інфраструктури [136].

Технологічною основою цього перелому стало стрімке нарощування власного виробництва високоточних і далекобійних систем [72; 113; 132; 221]. Україна почала випускати сотні й тисячі FPV-дронів, що довели свою вражаючу ефективність й на полі бою розпочавши нову еру безпілотних технологій війни, окрім того Україна почала виробляти й десятки дронів-камікадзе середньої та великої дальності (800-2000+ км), модернізувала ракети «Нептун», розгорнула серійне виробництво власних далекобійних систем типу «Паляниця», «Бобер», «Лють» і «Трембіта» [72; 113; 132;

221]. Паралельно партнери надали Storm Shadow/SCALP, ATACMS [136]. Водночас морські дрони Magura V5 і Sea Baby остаточно вигнали Чорноморський флот РФ із західної частини моря, знищивши або серйозно пошкодивши понад третину його бойового складу [136; 249].

Дрон за кілька сотень доларів знищував танк за мільйони, безпілотний катер за чверть мільйона, фрегат за пів мільярда [62; 72; 113]. До 2025 року ця модель досягла зрілості: щомісяця Україна виводила з ладу російської техніки та інфраструктури на суми, що перевищували весь її власний місячний оборонний бюджет [62; 72; 113]. Війна остаточно перемістилася з площини територіальних здобутків у площину економічного та логістичного подавлення агресора [72; 113]. РФ була змушена витрачати мільярди доларів на захист кожного НПЗ і кожного аеродрому і кожного разу ці гроші не йшли на нові ракети чи танки, а НПЗ все одно зазнавали уражень [62; 136].

Таким чином, період 2023-2025 років став народженням унікальної української воєнної доктрини XXI століття: замість спроби перемогти гіганта його ж зброєю Україна навчилася повільно, методично й невідворотно руйнувати його економічно й технологічно, воюючи за власними правилами [72; 113; 132; 136]. Це вже не просто оборона, це війна у якій маленька країна змусила ядерну наддержаву платити неприйнятну ціну за кожен день агресії [66; 136].

За 11 років безперервної війни українська військова стратегія пройшла чотири чітко виражені фази, кожна з яких стала не просто реакцією на обставини, а кроком до створення унікальної моделі протистояння ядерній наддержаві [136]. Спочатку, з 2014 до 2022 року, панувало юридичне заперечення самої війни: формат АТО та ООС, реактивне планування, заборона бити по території агресора й відчайдушне утримання лінії розмежування будь-якою ціною [136]. Це був період виживання й таємного накопичення сил під прикриттям «це не війна» [136]. Потім, у 2022-му, настав час класичної оборони й перших локальних контрнаступів: блискавичне відбиття штурму Києва, Харкова й Миколаєва, а згодом звільнення Харківщини та правобережжя

Херсона [136; 196]. Вперше Україна показала, що може не лише тримати удар, а й перехоплювати ініціативу й повертати своє [136].

2023 рік приніс найамбітнішу спробу «великого прориву» за класичними канонами: десятки нових бригад, сотні одиниць західної техніки, план розрізати сухопутний коридор до Криму [136]. Результатом стало болісне зіткнення з глибоко ешелонованою російською обороною й розуміння: перемогти в стилі Другої світової війни неможливо [136]. Саме ця невдача народила четверту, зрілу фазу (кінець 2023-2025): активну оборону на фронті, поєднану з систематичними глибокими ударами по всій глибині РФ та окупованих територій [72; 113; 136]. Війна остаточно перестала бути боротьбою за кілометри й перетворилася на боротьбу за економічне й логістичне виснаження противника [72; 113; 136].

Таким чином Україна створила першу в історії гібридну доктрину, яка органічно поєднує класичну оборону, партизанські рейди, високотехнологічні удари на тисячі кілометрів і економічну війну через інфраструктуру ворога [4; 5; 72; 113; 136].

У 2015-2016 роках ухвалили нову редакцію Закону «Про національну безпеку», який остаточно закріпив курс на НАТО, запровадив цивільний контроль над силовими структурами, розмежував функції між ЗСУ, Нацгвардією та іншими відомствами і створив посаду Головнокомандувача ЗСУ – крок, який різко підвищив ефективність управління [136].

Найбільш революційним стало створення професійного сержантського корпусу за програмами JMTG-U (США), UNIFIER (Канада), Orbital (Велика Британія) та іншими [136]. Десятки тисяч молодших командирів пройшли навчання за стандартами НАТО і навчилися приймати рішення на місці, керувати малими групами й працювати з сучасною технікою [136]. Саме ці сержанти стали справжнім «хребтом» української армії в 2022-2025 роках [136].

Інтеграція західного озброєння відбувалася прямо на полі бою й часто виглядала як справжній «франкенштейн»: на радянські БМП-1 встановлювали Javelin, на старі БТР-80 – супутниковий зв’язок Starlink, радянську артилерію підключали до планшетів

із програмним забезпеченням НАТО [136]. Цей гібридний підхід виявився надзвичайно ефективним і дозволив максимально швидко використати сильні сторони обох систем [136].

У результаті до 2025 року Україна створила унікальну гібридну армію: за організаційною структурою, стандартами підготовки й управління вона наблизилася до найкращих армій НАТО, за реальним бойовим досвідом високої інтенсивності перевищує більшість із них, а за озброєнням являє собою органічний сплав радянської технічної бази, власних інноваційних розробок і західних високоточних систем [72; 113; 136]. Ця трансформація відбувалася не за заздалегідь написаним мирним планом, а під постійним бойовим стресом, коли кожна помилка коштувала життів і виправлялася миттєво [66; 136]. Саме тому за одинадцять років Збройні Сили України пройшли шлях, на який у мирний час знадобилося б кілька десятиліть, і стали однією з найефективніших, найтехнологічніших і найадаптивніших армій континенту, армією, здатною одночасно вести позиційну війну, глибокі рейди в тил ворога й масштабні асиметричні операції [66; 136].

На початку 2014 року в Україні фактично не існувало сучасних сил спеціальних операцій [136]. Були окремі спецпідрозділи СБУ («Альфа»), розвідки Сухопутних військ, ВМС, але вони були розпорошені, недофінансовані й часто скомпрометовані проросійськими кадрами [136]. Рішення про створення єдиних Сил спеціальних операцій (ССО ЗСУ) ухвалено в 2015-му, офіційно оформлено в 2016-му [136]. Основою стали 8-й полк (Хмельницький) і 140-й центр [136]. З першого дня ССО будувалися за американсько-британською моделлю: жорсткий відбір, автономність, акцент на дії за лінією фронту [136]. Навчання велося інструкторами США (Green Berets), Великої Британії (SAS), Польщі, Литви [136]. Вже до 2019-2020 ССО отримали окремий статус роду військ, власне фінансування й командування [136]. До лютого 2022 чисельність сягнула 4-5 тисяч бійців вищої категорії готовності [136].

Паралельно, під керівництвом Василя Бурби, а з 2020 року особливо Кирила Буданова, відбулася не менш вражаюча трансформація Головного управління розвідки

Міноборони [136]. З традиційної військової розвідки ГУР перетворилося на структуру, що поєднує глибоку агентурну й технічну розвідку з власними ударними підрозділами («Артан», «Кабул-9», «Шаман», Timur, Kraken) [136].

Після стабілізації фронту навесні 2022 року роль ССО та ГУР остаточно змінилася: із захисників столиці вони стали головним інструментом глибоких операцій на окупованих територіях і всередині самої РФ [136]. Рейди, ліквідація колаборантів, викрадення офіцерів, підриви залізничних мостів і складів поступово перетворилися на систематичні удари по стратегічних об'єктах агресора [136]. Найрезонанснішими стали атаки дронами на авіабази «Енгельс-2», «Дягілєво», «Оленья», «Морозовськ» та інші, внаслідок яких РФ втратила десятки стратегічних бомбардувальників Ту-95, Ту-22М3 і літаків А-50 [62], а операція «Павутина» стала історичною подією в світі спеціальних операцій [136].

Особливе місце посіли морські операції: потоплення флагмана «Москва» у квітні 2022 року, знищення підводного човна «Ростов-на-Дону» безпосередньо в сухому доці Севастополя, ураження великих десантних кораблів «Саратов», «Цезарь Куніков», «Новочеркасськ», «Оленегорський горняк» і багатьох інших [62; 136]. Усі ці операції виконувалися невеликими групами спецпризначення за допомогою морських дронів Magura та Sea Baby власного виробництва [72; 113; 136]. До кінця 2024 року Чорноморський флот РФ втратив здатність контролювати західну частину Чорного моря, що дало змогу Україні відновити повноцінний зерновий експорт без участі РФ [136; 249].

Таким чином, ССО та ГУР МО стали втіленням асиметричної відповіді на масовану агресію: замість спроб протистояти РФ в класичній війні вони завдавали точкових, але стратегічно руйнівних ударів по найдорожчих і найуразливіших активах ворога – від авіації за Уралом до флоту в окупованому Криму [72; 113; 136].

З 2014 року, коли РФ розпочала гібридну агресію, кіберпростір став одним із ключових фронтів війни проти України [4; 5; 14; 41; 43; 89; 110; 111; 143]. За 11 років (станом на 2025) країна пережила тисячі атак від NotPetya 2017-го до масованих DDoS

і шпигунських кампаній Sandworm [14; 43; 89; 110; 143]. У відповідь Україна сформувала багатошарову систему внутрішньодержавних структур, що поєднує оборону, розвідку та наступальні можливості, з акцентом на швидке реагування та міжнародну інтеграцію [14; 43; 89]. Ця модель еволюціонувала від реактивних команд до проактивної кіберсили, здатної не лише захищатися, а й контратакувати, як показують операції IT Army у 2022-2025 роках [89].

Центральним координатором національної кібербезпеки є Рада національної безпеки і оборони України (РНБО), яка затверджує стратегічні документи, такі як Стратегія кібербезпеки 2021-2025 років та план заходів на 2025 рік [14; 43]. РНБО визначає пріоритети: захист критичної інфраструктури (енергетика, транспорт, фінанси), протидію державним загрозам і розвиток людського ресурсу [14; 43]. У 2025 році план передбачає посилення кіберстійкості через інвестиції в AI-моніторинг і навчання 50 тисяч фахівців, координуючи зусилля всіх відомств для уникнення дублювання [14; 43].

Державна служба спеціального зв'язку та захисту інформації (Держспецзв'язку) – ключовий орган у сфері технічної оборони [14; 43]. Як регулятор кібербезпеки критичної інфраструктури, вона сертифікує засоби захисту, проводить аудити та координує 17 секторів економіки (від банків до водоканалів) [14; 43]. У 2025 році Держспецзв'язку впровадила нову систему раннього попередження, яка виявила понад 3 тисячі інцидентів за перше півріччя, зменшивши час реагування на 40% порівняно з 2024-м [14; 43].

Національна CERT-UA (Комп'ютерна надзвичайна ситуаційна команда України), підпорядкована Держспецзв'язку, є фронтлайн реагування на інциденти [14; 43]. Заснована в 2007-му, до 2025 року вона обробила понад 10 тисяч атак, включаючи атаки на енергосистему в 2022-2023 роках [14; 43; 89; 143]. CERT-UA фокусується на аналізі загроз (наприклад, від Sandworm), поширенні індикаторів компрометації та співпраці з приватним сектором [14; 43]. У 2025 році команда розширилася до 300

фахівців, інтегруючи AI для автоматизованого виявлення, і провела спільні навчання з НАТО [14; 43].

Служба безпеки України (СБУ) відповідає за контррозвідку в кіберпросторі: протидію кібершпигунству, тероризму та гібридним операціям [14]. Кібервідділ СБУ, створений у 2017-му, у 2025 році відбив понад 2300 атак, включаючи спроби проникнення в урядові мережі та дезінформаційні кампанії [14]. СБУ координує з ГУР для наступальних операцій, як-от хакерські контратаки на російські мережі, і співпрацює з ЦРУ та MI6, обмінюючись розвідданими про загрози [14].

Кіберполіція України, частина Національної поліції при МВС, зосереджена на кримінальних аспектах: розслідування фішингу, ransomware та кібершахрайства [14]. Заснована в 2015-му, до 2025 року вона розкрила понад 5 тисяч злочинів, пов'язаних з російськими угрупованнями, і розвинула інструменти для перевірки даркнет-активності [14]. Кіберполіція інтегрується з Europol та INTERPOL, проводячи спільні операції й в 2025 році запустила платформу для анонімних повідомлень про загрози від бізнесу [14].

Міністерство цифрової трансформації (Мінцифри) координує цивільний сегмент: впровадження Дія для безпечних послуг і стратегії кібергігієни [14]. У 2025 році Мінцифри запустило національну кампанію з кіброосвіти, охопивши 1 млн користувачів, і інтегрувало NIST-фреймворк для стандартизації захисту [14]. Воно також модерує міжвідомчий центр кібербезпеки, де обмінюються даними СБУ, Держспецзв'язку та приватні компанії [14].

Загалом, українська система кібероборони 2025 року – це адаптивна мережа, де РНБО задає стратегію, а CERT-UA, СБУ, та Держспецзв'язку забезпечують оперативну реалізацію [14; 43; 89]. За даними Atlantic Council, ця модель зменшила ефективність російських атак на 60% з 2022-го, завдяки інвестиціям у $100 млн. і міжнародній підтримці (Tallinn Mechanism, EU Cyber Dialogue) [89]. Україна перетворилася з жертви на кіберсилу, демонструючи, як невелика держава може протистояти наддержаві через інтеграцію державних, приватних і волонтерських зусиль [89].

За 11 років безперервної війни (2014-2025) Україна створила унікальну в світовій історії модель протидії гібридній агресії ядерної держави – модель, яку ніхто заздалегідь не планував і не прописував у доктринах, а викувала сама реальність [4; 5; 41; 66; 136]. Ця модель охоплює всі виміри сучасної війни. Військовий: від армії, яка у 2014-му ледве могла виставити один боєздатний батальйон, до однієї з найефективніших, найтехнологічніших і найгнучкіших армій континенту, що органічно поєднує радянську технічну базу, західні високоточні системи та власні дрони, РЕБ і морські безпілотники [66; 72; 113; 136]. Стратегічний: від реактивного утримання лінії розмежування до активної оборони й систематичних глибоких ударів, які перенесли війну на територію та в економіку агресора [72; 113; 136]. Технологічний: від повної залежності від радянських запасів до світового лідерства у бойових дронах, морських безпілотниках і асиметричних системах, що дають максимальний ефект за мінімальну ціну [72; 113; 132; 221].

Зазначимо, що це модель не ідеальна – вона має втрати, помилки й величезну ціну в людських життях, в самій армії виникають системні проблеми, а затяжна війна змушує стагнувати та деградувати, це стає помітним протягом 2025 року, але проблемні питання піднімається та поступово вирішуються, за ініціативи Сергія Паліси, досвідченого ветерана й колишнього командира 93-бригади «Холодний Яр», кандидатуру якого розглядають на призначення заступником офісу президента [136].

Незважаючи на проблеми, ця система працює [66; 136]. Вона довела головне: невелика держава може не просто виживати, а й змушувати ядерну наддержаву платити неприйнятну ціну щодня ставлячи перед загрозою внутрішнього розвалу за умови постійної адаптації, технологічної винахідливості й абсолютної єдності [66; 136]. Кожного разу, коли РФ вважала, що знайшла остаточний ключ до перемоги, Україна за кілька місяців видавала нову відповідь і війна продовжувалася вже за українськими правилами [136].

Сьогодні ця модель стала не лише способом виживання України, а й новою парадигмою безпеки для всього демократичного світу [66]. Від Вест-Пойнта до Тайбея

її вивчають як живий доказ: коли ти не можеш бути сильнішим – будь розумнішим, швидшим і безжаліснішим у захисті своєї свободи [66]. Україна заплатила за цей урок своєю кров'ю, але подарувала світу рецепт, як більше ніколи не програвати гібридну війну [66]. І Україна доводить, що він працює [66; 136].

4.3. Суспільна стійкість та роль громадянського суспільства

Особливої уваги під час гібридної агресії заслуговує роль громадського суспільства що не тільки не зневірилося під тиском, але й залишається по сьогоднішній день головним двигуном державних процесів [15; 66; 76; 77; 78; 79; 112]. Починаючи з 2014 року в Україні формується потужний волонтерський рух, що підтримував державу, яка виявилася не готова до гібридної агресії виконуючи функцію «швидкої допомоги» [15; 66; 112].

Саме волонтери початково забезпечували армію та добровольців всім початково необхідним, збирала гроші на бронежилети, каски, аптечки, їжу, комплектуючі для техніки, а пізніше тепловізори, пікапи та навіть озброєння й бронетехніку (останнє починаючи з 2022) [15; 66; 112]. Ця діяльність врятувала тисячі життів й закрила частину потреб держави й виграла час для переформатування [15; 66; 112]. Особливо важливою в цьому контексті стали трагедії Іловайська та Дебальцево, що нанесли глибокі психологічні травми суспільству, але й одночасно активізували нові хвилі підтримки волонтерських рухів [136].

Проте вже до 2017-2018 років стає зрозуміло, що просте «закриття прогалин» більше не є достатнім, війна ставала дедалі технологічною [15; 66; 72; 113]. Повномасштабне вторгнення 2022 року радикально змінило масштаби та характер запитів [15; 66; 72; 113]. Якщо у 2014-му волонтери купували зі складнощами купували, щось на кшталт телевізора то після 24 лютого волонтерські рухи стали спроможні забезпечувати цілі батальйони комплексами РЕБ, озброєнням, бронетехнікою, дронами, супутниковими терміналами (понад 40 000 станом на 2025

рік), мобільні ситуаційні центри та навіть розробку нових видів озброєнь [15; 21; 39; 58; 72; 113; 170].

Ключовими зсувами став перехід від закупівель готових виробів до інвестування у власне комплексне виробництва, з'явився феномен «народного ВПК»: сотні невеликих приватних компаній, гаражних майстерень та стартапів почали масове виробництво дронів, виробництво РЕБ, антидронових рушниць, автономних майстерень (до прикладу проект «Locker») [18], морських безпілотників, боєприпасів, маскувальних сіток з вуглецевого волокна, тактичні медичні засоби й інше програмне забезпечення військового призначення [72; 113; 132].

За оцінками Мінцифри та Генштабу, станом на початок 2025 року понад 70% всіх БПЛА, що використовуються на фронті (особливо FPV та розвідувальні), є Українського виробництва й 90% з них пройшли через приватний або волонтерсько-приватний сектор (особливо велику роль в цьому питанні грав спочатку активіст Сергій Стерненко та його спільнота, а нині вже повноцінний «Фонд спільнота Стерненка», що організовує забезпечення якісними дронами багатьох бригад та просуває ініціативи на кшталт «Дронів-перехоплювачів» проти розвідувальних та ударних дронів РФ) [42; 72; 113; 132], щомісячно українські компанії виробляв близько 100 тисяч FPV-дронів та дронів-бомбардувальників середньої дальності [72; 113; 132].

«Друк-армія» також став феномен децентралізованого народного ВПК, що виник в Україні з весни 2022 року [72; 113]. Тисячі волонтерів на 3D-принтерах у квартирах, гаражах і офісах масово виготовляли та виготовляють критичні пластикові компоненти для FPV-дронів, РЕБ, систем скидання гранат та іншої техніки [72; 113]. У піковий період 2023-2024 в цьому проекті працювало до 15 тисяч принтерів одночасно, забезпечивши до 70% потреб фронту в таких деталях і ставши світовим прецедентом народного високотехнологічного виробництва під час війни високої інтенсивності [72; 113].

Окремою подією став від «Фонд Сергія Притули» на проект «народний байрактар», що планувався для закупівлі кількох байрактарів, як результат, ці

байрактари Україна отримала фактично безкоштовно від країн партнерів, а 18 серпня 2022 року фонд оголосив, що за зібрані 600 мільйонів гривень було придбано супутник для розвідки, який передано в користування Головному управлінню розвідки (ГУР) Міноборони [21; 39; 170].

Угода укладена з фінською компанією ICEYE, яка спеціалізується на синтетичній апертурі радару (SAR) технології, що дозволяє знімати поверхню Землі в будь-яку погоду, вдень і вночі з високою роздільною здатністю (до 0,5 м), а також річний доступ до бази даних, ще 40 супутників, ця закупівля відбулася при консультації із держструктурами України й він працює по сьогоднішній день, хоча в цієї дії було також багато критиків, які переживали, що їхні гроші можуть бути вкрадені, проте і Кирило Буданов (керівник ГУР МО України), і Олексій Резніков (тепер вже колишній, екс-міністр оборони України на момент угоди) підтверджували інформацію про купівлю супутника ICEYE й тепер наративом про вкрадені гроші користуються лише інтернет-боти [21; 39; 170].

У 2023 році держава усвідомила масштаб явища й почала його інституалізацію, було створено платформу Brave1 – єдине вікно для розробників військових технологій [72]. За два роки через Brave1 пройшло понад 1800 проектів, 120 з них отримали гранти на суму понад 300 млн. доларів, а більше 70 розробок уже кодифіковано НАТО та прийнято на озброєння ЗСУ [72].

Проєкт «Армія дронів», започаткований у липні 2022 року спільно Мінцифри, Генштабом та UNITED24, став найбільшим у світі державно-громадським проектом у сфері безпілотників [72; 113; 132]. Він поєднує державне фінансування, волонтерські збори, навчання пілотів (понад 20 000 випущено) та системні держконтракти з виробниками [72; 113; 132]. Завдяки йому Україна досягла паритету, а в сегменті FPV – локальної переваги над противником [72; 113; 132].

Кластерний підхід став наступним етапом. У 2024–2025 роках сформовано шість великих оборонно-технологічних кластерів: Львівський (РЕБ і зв’язок), Харківський (дрони та боєприпаси), Дніпровський (бронетехніка й важкі дрони), Київський (кібер-

та інформаційні системи), Одеський (морські дрони) та Вінницько-Житомирський (так.мед. і логістика) [72; 113; 132]. Кожен кластер об’єднує десятки компаній, університети, випробувальні полігони й має прямі контракти із ЗСУ [72; 113; 132].

Прикладом ефективності кластерного підходу є морські дрони Magura V5/V7 [72; 113; 136]. Від ідеї до першого бойового застосування пройшло менше року [72; 113]. Приватні компанії «Спецтехноекспорт» і кілька невеликих стартапів за підтримки волонтерських фондів та СБУ створили безпілотник, який знищив або важко пошкодив понад 30% бойового складу Чорноморського флоту РФ, включно з підводним човном «Ростов-на-Дону» та кількома десантними кораблями [62; 72; 113; 136].

Швидкість інновацій у приватному секторі в рази перевищує державні процедури [72; 113; 132]. Якщо традиційний цикл розробки та прийняття на озброєння в держсекторі триває 5-12 років, то в приватно-волонтерському від 3 до 9 місяців [72; 113; 132]. Приклад: після появи російських «Ланцетів» у 2022-му українські аналогічні баражуючі боєприпаси («Сокіл-300», «Паляниця») з’явилися вже у 2023-му й у 2024-2025 роках досягли дальності понад 300 км [72; 113; 132; 221].

Фінансування цього «народного ВПК» здійснюється за трьома основними каналами: прямі збори найбільших фондів («Повернись живим», «Фонд Притули», «Народний дрон») [15; 58; 170], гранти Brave1 та UNITED24 [72], а також прямі контракти ЗСУ та Міноборони з виробниками [72; 113]. Сумарно за 2022-2025 роки через ці канали пройшло понад $2,5 млрд – сума, порівнянна з державним оборонним замовленням на певні категорії озброєнь [15; 58; 72; 113; 170].

Важливим елементом стала дерегуляція. У 2022-2024 роках скасовано більшість дозвільних процедур для виробництва безпілотників і РЕБ, запроваджено спрощену кодифікацію НАТО для приватних розробок, дозволено експорт окремих видів продукції подвійного призначення або прямого військового призначення (так до прикладу «Повернись живим» закуповувала кулемети для ЗСУ, а «Фонд Сергія Притули» та «Фонд Петра Порошенка» здійснювали закупівлі легких

бронетранспортерів) [15; 58; 72; 113; 170]. Це дало змогу українським компаніям вийти на зовнішні ринки і залучати валютну виручку для подальшого розвитку [72; 113].

Соціальний ефект виявився не менш важливим [66; 76; 77; 78; 79]. Тисячі інженерів, айтівців, підприємців, які у 2021 році працювали на глобальні корпорації, повернулися або переорієнтувалися на військові розробки [66; 72; 113]. У країні сформувався новий прошарок – «оборонні технарі», для яких створення зброї стало не лише бізнесом, а й частиною національної ідентичності [66; 72; 113].

Водночас модель має й вразливості: залежність від імпортних комплектуючих (особливо електроніки з Китаю та Тайваню), проблеми масштабування (багато компаній не готові перейти від 100 до 10 000 одиниць на місяць), ризик корупції при держзамовленнях та вигорання команд через надвисоку інтенсивність роботи [72; 113; 132].

Проте навіть з урахуванням цих проблем волонтерсько-приватний сектор остаточно сформувався як четверта складова оборони України поряд із ЗСУ, територіальною та міжнародною допомогою [66; 72; 113; 136]. У 2025 році саме він забезпечує технологічну перевагу на полі бою в ключових сегментах (FPV, РЕБ, морські дрони, баражуючі боєприпаси) та демонструє унікальний приклад, коли громадянське суспільство та приватний бізнес фактично створили паралельний військово-промисловий комплекс за три роки війни [72; 113; 132].

Отже, український «народний ВПК» став не просто допоміжним елементом, а одним із головних драйверів стійкості держави [66; 72; 113]. Він довів, що в умовах гібридної війни швидкість, гнучкість і масова залученість громадян можуть компенсувати нестачу ресурсів і десятирічне відставання у військових технологіях, перетворивши слабкість на асиметричну перевагу [66; 72; 113; 132].

4.4. Оцінка ефективності та уроки для майбутнього

Одинадцять років безперервної гібридної війни РФ проти України (2014-2025) створили унікальний у світовій історії емпіричний матеріал для аналізу ефективності різних стратегій протидії та визначення критичних уроків для майбутнього [4; 5; 41; 66; 122]. Український досвід став найтривалішим і найбільш комплексним випадком протистояння повному арсеналу інструментів гібридної агресії з боку ядерної держави-постійного члена Ради Безпеки ООН [4; 5; 10; 19; 41]. Цей досвід має фундаментальне значення не лише для України, а й для всієї глобальної системи безпеки, оскільки демонструє як вразливості сучасного міжнародного порядку, так й ефективні механізми протидії, що можуть бути адаптовані іншими державами [41; 66; 122].

Критерії оцінки ефективності протидії для об'єктивної оцінки ефективності української моделі протидії гібридній агресії необхідно встановити чіткі критерії аналізу, що охоплюють усі виміри конфлікту [41; 66; 122]. Ці критерії мають враховувати як тактичні успіхи та невдачі, так і стратегічні наслідки для державності, суспільства та міжнародної позиції України [41; 66].

Територіальний критерій – він є найочевиднішим, але й найсуперечливішим: Україна втратила контроль над Кримом (2014) та близько 18% території після 2022 року (частини Донецької, Запорізької, Херсонської та вся Луганська область), що болісно й неприйнятно [41; 94; 136]. Водночас вдалося зірвати головну мету РФ захоплення Києва, зміну влади та перетворення України на маріонеткову державу; країна зберегла державність, столицю та контроль над більшістю стратегічних регіонів (Харків, Одеса, Дніпро, Запоріжжя) [136; 196].У гібридній війні територіальні втрати не є абсолютним показником поразки, ключове, це збереження суб’єктності, здатності до опору та міжнародної підтримки, а за цими параметрами Україна виявила виняткову стійкість, перетворивши «триденну операцію» на виснажливу війну для агресора [41; 66; 136].

За військово-стратегічним критерієм Україна досягла вражаючої трансформації: від деморалізованої армії 2014 року (130 тис. осіб, корупція та проросійська інфільтрація) до однієї з найбільш боєздатних у Європі до 2025-го (понад 800 тис. у силових структурах) [136]. Якісні зміни охоплюють професійний сержантський корпус за стандартами НАТО, інтеграцію західного озброєння (Leopard, HIMARS, F-16), потужні ССО, унікальний 11-річний досвід високої інтенсивності, перехід до проактивної «активної оборони», а за нею й до «асиметричної війни» з глибокими ударами та створення провідного у світі ВПК безпілотних систем [72; 113; 132; 136]. За оцінками RUSI та ISW, українська армія станом на кінець 2025 року за бойовим досвідом, гнучкістю й технологічною винахідливістю перевершує більшість армій НАТО, попри менші бюджети [136; 168].

Економічний критерій – цей критерій показує вражаючу стійкість України в умовах тривалої війни [16; 17; 87; 94; 99; 127; 231]. Короткострокові наслідки були катастрофічними: після 2014-2015 рр. втрачено близько 20% промислового потенціалу (Крим та промисловий Донбас), гривня девальвувалася з 8 до 24 грн/$, у 2022-му ВВП обвалився на 29%, інфляція перевищила 26%, прямі руйнування перевищують $150 млрд (Світовий банк, 2025) [16; 17; 87; 94; 231].

Водночас з 2023 року економіка відновила зростання (5,3% у 2023-му, 3-4% у 2024-2025 рр.) за умов активних бойових дій [16; 17; 99]. Ключові фактори виживання: переорієнтація експорту на ЄС та DCFTA, понад $100 млрд. міжнародної фінансової допомоги за 2022-2025 рр., швидке відновлення критичної інфраструктури, стійкість ІТ-сектору та успішне розблокування експорту зерна (70-80% довоєнного рівня завдяки власному морському коридору 2023-2024 рр.) [16; 17; 47; 99; 214; 215; 249].

Проблеми залишаються величезними: держ.борг близько 88% ВВП, військові видатки понад 37% бюджету, 6+ млн. біженців, відновлення потребуватиме сотень мільярдів доларів [16; 17; 94; 231]. Проте сам факт економічного виживання, в середньо та довгостроковій перспективі, збереження валютних надходжень й здатності

фінансувати війну проти значно багатшого агресора є видатним досягненням стійкості та адаптації [16; 17; 87; 99].

Соціально-психологічний критерій – можливо, найважливіший у гібридній війні, адже саме на розкол суспільства була спрямована російська стратегія (мовний, регіональний, ідеологічний та релігійний поділи) [11; 12; 23; 66; 137; 139; 171; 179; 206; 210; 241]. У 2014-2015 рр. розколи справді були глибокими: частина Донбасу підтримувала сепаратистів, а центр залишався розгубленим [11; 12; 23].

Повномасштабне вторгнення 2022 року парадоксально стало каталізатором безпрецедентної консолідації: суспільство навіть в усіх регіонах, включно з Півднем та Сходом (що раніше виражали менше довіри) практично одноголосно виступали за єдність (КМІС, Разумков) [11; 66; 137; 206], беззаперечна довіра до ЗСУ та до Президента [66; 137]. Виник феномен «нації волонтерів»: мільйони громадян добровільно зібрали понад $3 млрд (2022-2025), сотні тисяч емігрантів повернулися воювати чи допомагати [15; 58; 66; 76; 77; 78; 79; 170].

Війна завдала тяжких травм: понад 30 тис. загиблих військових (офіційно на кінець 2025р.), десятки тисяч поранених, психологічна травматизація, демографічна криза та ризик «втоми від війни» в тилових регіонах [3; 120]. Проте станом на кінець 2025 року готовність продовжувати боротьбу лишається високою: понад 70% українців категорично проти територіальних поступок заради швидкого миру [66; 206]. Суспільна єдність і воля до опору стали одним із головних стратегічних досягнень України [66; 137].

Міжнародно-політичний критерій – став вирішальним для виживання України проти РФ [9; 156; 214; 215]. У 2014-2015 рр. реакція Заходу була слабкою: символічні санкції, лише нелетальна допомога, Мінські угоди фактично легітимізували російську присутність, євроатлантичні перспективи залишалися заблокованими [145; 217].

Повномасштабне вторгнення 2022 року докорінно змінило ситуацію [156; 214; 215]. Україна отримала безпрецедентну підтримку: військова допомога понад $120 млрд. (2022-2025), з них $85 млрд від США, найжорсткіший в історії санкційний

режим (19 пакетів ЄС та замороження $300 млрд. російських активів), статус кандидата в ЄС (2022) і початок переговорів про вступ (2024), механізми Рамштайн, NSATU, Ukraine Facility (€50 млрд) [156; 214; 215]. Війна спровокувала розширення НАТО: Фінляндія та Швеція вступили в Альянс, подвоївши кордон НАТО з РФ [156]. Україна з країни, якій у 2008-му відмовили в МАР, перетворилася до 2025 року на найбільш інтегрованого партнера НАТО з офіційним визнанням: «Україна буде в НАТО» [156].

Підтримка не є абсолютна: зберігаються «стратегічна терплячість», політичні коливання в США та Європі, «втома від України» в суспільствах, тривале обмеження на далекобійні удари по території РФ [156]. Проте трансформація України з об'єкта допомоги на суб'єкт, який реально захищає європейські цінності та змінює геополітичну карту континенту, є одним із найяскравіших дипломатичних тріумфів за весь час незалежності [156].

Інформаційно-кібернетичний критерій – демонструє одну з найяскравіших трансформацій України [14; 43; 89; 110; 111; 143]. У 2014-2017 рр. країна була практично беззахисною: кібератаки BlackEnergy, Industroyer, NotPetya завдали мільярдних збитків, російські медіа та соцмережі («ВКонтакте», «Одноклассники») домінували на Півдні й Сході, довіра до російських джерел сягала близько 46% [11; 12; 32; 37; 38; 110; 111; 143].

Проте станом на 2025 рік створено потужну систему захисту: Держспецзв'язку, CERT-UA, кібервійська ЗСУ, тісна співпраця з США, Британією та Естонією [14; 43; 89]. Кількість успішних російських кібератак зазнала значного спадання, критична інфраструктура швидко відновлюється після ударів [14; 43; 89]. В інформаційному просторі проведено радикальну санацію: заблоковано російські соцмережі (2017), телеканали та проросійські українські медіа (2021-2022), запущено «Єдині новини», розвинено власні Telegram-канали й платформи [32; 37; 38; 40; 97; 114; 133; 153; 219; 224; 244]. Довіра до російських джерел обвалилася до менше ніж 10% навіть у «російськомовних» регіонах [11; 66; 137; 171; 210].

Виклики лишаються: проникнення дезінформації через VPN і Telegram, нові загрози від діпфейків та AI-контенту, складність захисту діаспори [45; 70; 75; 91; 97]. Проте Україна побудувала ефективний імунітет до російської пропаганди й значно посилила кіберстійкість, перетворившись з однієї з найвразливіших країн на одну з найбільш захищених у Європі [14; 43; 89].

Символічне значення української боротьби для глобальної демократії важко переоцінити [66; 156]. Україна стала уособленням опору авторитаризму, доказом того, що демократичні цінності варті того, щоб за них боротися навіть проти ядерної наддержави [66; 156]. Цей наратив не лише мобілізував безпрецедентну міжнародну солідарність, але й надихнув інші демократії - від Тайваню до країн Балтії - на переосмислення власних стратегій безпеки [156]. Український досвід став живим аргументом проти «втоми від демократії» та «євроскептецизму» у західних суспільствах, демонструючи, що свобода та суверенітет вимагають постійної боротьби та інвестицій [66; 156].

Попри значні успіхи, українська модель протидії гібридній агресії не є ідеальною і містить низку стратегічних невдач та системних проблем, які накопичувалися протягом 11 років війни [41; 66; 136]. Аналіз цих викликів дозволяє не лише об'єктивно оцінити ефективність, але й сформулювати рекомендації для їх подолання [41; 66].

Однією з ключових стратегічних невдач стала недооцінка глибини російської загрози на ранніх етапах [41; 136; 145; 217]. У 2014-2021 роках акцент на "мирному врегулюванні" через Мінські угоди та формат АТО/ООС фактично консервував російську присутність на окупованих територіях, дозволяючи РФ накопичувати сили та ресурси для повномасштабного вторгнення, а також опрацьовувати пропагандою місцеве населення [145; 217]. Це призвело до недооцінки необхідності тотальної мобілізації суспільства та економіки, а також затримки в реформах оборонного сектору [136]. Результатом стали болісні втрати в перші місяці 2022 року, коли ЗСУ, попри героїзм, не були повністю готові до масованого удару по кількох напрямках одночасно [136; 196].

Іншою значною проблемою стала залежність від міжнародної допомоги, яка, хоча й врятувала Україну в критичні моменти, створила вразливості в стратегічному плануванні [9; 156; 214; 215]. Політичні коливання партнерів – від затримок у постачанні важкого озброєння (наприклад, танків Leopard у 2023 році) до обмежень на удари по території РФ (які зберігалися до середини 2025 року) неодноразово уповільнювали українські операції [156]. Це підкреслює ризики «зовнішньої залежності» в гібридних конфліктах, де агресор може маніпулювати міжнародною політикою через енергетичний шантаж чи ядерні погрози [41; 156].

У 2025 році війна високої інтенсивності почала проявляти ознаки стагнації в українській армії, що стало одним з найсерйозніших викликів [136]. Тривалий конфлікт призвів до ерозії професійного ядра ЗСУ: висока інтенсивність боїв, хронічна нестача особового складу через проблеми з мобілізацією (у 2025 році план мобілізації виконано лише на 65-70% за даними Генштабу) та психологічне вигорання бійців спричинили зниження мотивації та ефективності підрозділів [6; 13; 26; 31; 35; 136]. У деяких бригадах фіксувалися випадки деградації дисципліни, зростання дезертирства (на 15-20% порівняно з 2024 роком) та стагнації в тактичному розвитку через брак ротації [136]. Економічна криза посилила ці проблеми: інфляція на рівні 18-20% у 2025 році та зростання державного боргу до 95% ВВП (за прогнозами ЄБРР) обмежили фінансування модернізації, призвівши до затримок у виробництві власних озброєнь [16; 17; 94; 231].

Ці проблеми не залишилися без уваги. У 2025 році вони активно піднімалися в суспільному та політичному дискурсі, зокрема через доповіді незалежних аналітиків (наприклад, Центру оборонних стратегій) та парламентські слухання [136]. Значну роль у вирішенні цих питань відіграла ініціатива Павла Паліси, досвідченого ветерана та колишнього командира 93-ї окремої механізованої бригади "Холодний Яр" [136].

Призначений заступником керівника Офісу Президента 29 листопада 2024 року, Паліса (позивний «Хантер») став ключовим архітектором реформ, спрямованих на подолання стагнації [136]. Його ініціативи включали впровадження нової системи

ротації особового складу (зобов'язуючи бригади проводити ротацію кожні 6-8 місяців), посилення психологічної підтримки (розширення програми «Ветеран» на 50% у 2025 році) та оптимізацію мобілізації через цифровізація призову (за допомогою додатку «Резерв+») [136]. До кінця 2025 року ці заходи вже дали перші результати: рівень дезертирства знизився на 10%, а боєготовність підрозділів підвищилася завдяки кращій ротації [136]. Кандидатура Паліси на посаду заступника ОП була обрана саме через його фронтовий досвід, що дозволило ефективно інтегрувати ветеранські ініціативи в державну політику [136].

Український досвід протидії гібридній агресії РФ надає низку критичних уроків, які можуть бути адаптовані іншими державами, що стикаються з подібними загрозами [41; 66; 122]. Ці уроки охоплюють стратегічні, тактичні та суспільні аспекти.

По-перше, адаптивність є ключем до перемоги в гібридних конфліктах [41; 66; 122; 136]. «Мирні врегулювання», як Мінські угоди, виявилися неефективними [145; 217]; натомість постійна еволюція стратегії (від оборони до глибоких ударів) дозволила Україні нейтралізувати переваги агресора, інвестувати в гнучкі системи, такі як ШІ для аналізу загроз та швидке впровадження інновацій, щоб уникнути стагнації, як це спостерігалося в українській армії на початку 2025 року [72; 113; 136].

По-друге, інтеграція громадянського суспільства та приватного сектора в оборону створює асиметричну перевагу [15; 66; 76; 77; 78; 79; 112]. "Народний ВПК" та волонтерський рух компенсували державні прогалини, виробляючи 70-80% дронів для фронту [72; 113; 132]. Розвивати децентралізовані моделі (наприклад, кластери як у Україні), де бізнес та громадяни стають частиною національної безпеки, посилюючи супротив проти гібридних атак [72; 113; 132].

По-третє, асиметрія перемагає масу [72; 113]. Замість симетричного протистояння (танк на танк), Україна зосередилася на руйнуванні логістики та економіки агресора (удари по НПЗ, флоту) [62; 72; 113; 136]. Для менших держав – пріоритетом є розвиток технологій (дрони, кібер) з низькими витратами – високою ефективністю, уникнення позиційних війн, як у 2023-2025 роках [72; 113; 132].

По-четверте, міжнародна солідарність потребує проактивної дипломатії [9; 156; 214; 215]. Україна перетворила себе з «жертви» на «захисника Європи», забезпечивши $200 млрд. допомоги [156; 214; 215]. Необхідно реформувати глобальні інститути (ООН, ОБСЄ) для швидкої реакції, кваліфікувати кібератаки як агресію, як у Таллінському посібнику 2.0 [154; 199; 200].

По-п'яте, соціально-психологічна стійкість - фундамент успіху [66; 137; 206]. Травми війни (втрати понад 400 000 вбитих/поранених за оцінками Зеленського на січень 2025) посилюють єдність, але ризикують «втомою» (підтримка продовження війни впала до 24% за Gallup, серпень 2025) [3; 120]. Необхідно інвестувати в медіаграмотність, психологічну підтримку та наративи, щоб протидіяти дезінформації [66; 97; 114].

По-шосте, технологічна незалежність - запорука виживання [72; 113; 132]. Залежність від імпорту електроніки виявилася вразливістю [72; 113]. Необхідно розвивати локальний ВПК, інтегруючи AI для протидії діпфейкам, як це робить Україна в 2025 [72; 113; 132].

Одинадцять років гібридної агресії РФ проти України створили модель протидії, яка, попри проблеми та втрати, довела свою ефективність [4; 5; 41; 66; 122; 136]. Україна не просто вижила - вона трансформувалася в сильнішу державу, змусивши агресора платити неприйнятну ціну та ставлячи його перед загрозою внутрішнього розвалу [66; 136]. Прогнози зростання ВВП на 1.9-2.5% у 2025 (ЄБРР, ЄС) свідчать про економічну стійкість, а інтеграція в НАТО (підтримка €35 млрд у 2025) - про геополітичний успіх [16; 17; 99; 156]. Незважаючи на стагнацію в армії на початку 2025, ініціативи на кшталт реформ Паліси дозволяють поступово вирішувати ці проблеми, забезпечуючи постійну адаптацію [136].

Ця система працює, бо базується на технологічній винахідливості, домінуючій єдності суспільства та стратегічній гнучкості [66; 72; 113; 136]. Кожного разу, коли РФ вважала, що знайшла остаточний ключ до перемоги (як у наступах 2025), Україна за кілька місяців видавала нову відповідь – від вдосконалених дронів до посилених

кіберзахистів і війна продовжувалася вже за українськими правилами [72; 113; 136]. Сьогодні ця модель стала не лише способом виживання України, а й новою парадигмою безпеки для всього демократичного світу [66; 156].

ВИСНОВОК

Проведене дослідження гібридної агресії Російської Федерації проти України у період 2014-2025 років дозволяє сформулювати ряд фундаментальних висновків щодо природи, механізмів та наслідків цього феномену, а також ефективності різних моделей протидії. Воно підтвердило, що класичне розуміння війни як відкритого збройного конфлікту між державами з чіткими лініями фронту та формальним оголошенням воєнного стану більше не відповідає реаліям XXI століття. Гібридна війна створює «сіру зону» між миром та війною, де традиційні інструменти міжнародного права та колективної безпеки виявляються недостатньо ефективними. А ключовою характеристикою гібридної агресії є синхронне та взаємопідсилююче застосування військових, інформаційних, кібернетичних, економічних та дипломатичних інструментів. Модель РФ продемонструвала адаптивний характер: співвідношення військових та невійськових компонентів змінювалося від 3:2 у період 2014-2022 років до 2:3 після повномасштабного вторгнення 2022 року, що спростовує спрощені інтерпретації «доктрини Герасимова».

Окрім того дослідження виявило критичні структурні дефекти сучасної системи міжнародної безпеки. Найсерйознішою проблемою виявилася ситуація, коли держава-агресор одночасно є постійним членом Ради Безпеки ООН з правом вето, що створює парадокс: порушник міжнародного права може систематично блокувати механізми відповідальності за власні злочини. Паралізація РБ ООН змусила міжнародну спільноту шукати альтернативні механізми: активізацію Генеральної Асамблеї через «Об'єднання заради миру», використання Moscow Mechanism ОБСЄ, звернення до МС ООН та МКС. Однак ці механізми, попри важливість для документування злочинів, виявилися неспроможними зупинити агресію в реальному часі. Вестфальська система міжнародних відносин зазнала фундаментального виклику через систематичний підрив принципів суверенітету, територіальної цілісності та невтручання через

«правдоподібне заперечення», використання проксі-сил та маскування під «громадянський конфлікт».

На наш погляд найважливішим досягненням дослідження є систематизація унікального українського досвіду протидії гібридній агресії ядерної держави. За одинадцять років Україна пройшла шлях від майже повної беззахисності до створення однієї з найефективніших моделей комплексного опору. Військова трансформація відбулася в чотири фази: від юридичного заперечення війни через АТО/ООС (2014-2022) до класичної оборони та локальних контрнаступів (2022), від амбітного «великого прориву» (2023) до зрілої моделі активної оборони з систематичними глибокими ударами (2024-2025).

Ця еволюція довела можливість перемоги через адаптивність, технологічну винахідливість та асиметричні дії. Кіберстійкість пройшла шлях від повної вразливості (BlackEnergy, Industroyer, NotPetya) до ефективної багатошарової системи захисту. Створення Держспецзв'язку, CERT-UA, кібервійськ ЗСУ дозволило знизити ефективність російських кібератак на 60% порівняно з 2022 роком. Інформаційна стійкість досягнута через радикальну санацію медіапростору та розвиток власних платформ стратегічних комунікацій. Довіра до російських джерел впала з 46% у 2014-2015 роках до менше 10% навіть у «російськомовних» регіонах. Економічна стійкість виявилася однією з найбільш вражаючих складових. Попри втрату 20% промислового потенціалу, обвал ВВП на 29% у 2022 році та руйнування на понад $150 млрд, економіка відновила зростання за умов активних бойових дій.

Також дослідження зафіксувало унікальне явище українського суспільства, як «нації волонтерів» та «народного військово-промислового комплексу». Громадянське суспільство стало повноцінним актором національної безпеки, створивши паралельну систему виробництва військових технологій. Це явище не має аналогів у сучасній історії та демонструє: суспільна єдність й технологічна винахідливість можуть компенсувати багатократну перевагу агресора.

Український досвід радикально змінив підходи міжнародної спільноти. Якщо у 2014-2015 роках реакція обмежувалася символічними санкціями, то після 2022 року відбулася безпрецедентна мобілізація, як внутрішнього суспільна так й міжнародна: понад $200 млрд допомоги, найжорсткіший санкційний режим (19 пакетів ЄС, заморожування $300 млрд. активів), прискорена євроатлантична інтеграція (статус кандидата в ЄС з 2022-го, створення NSATU як першої постійної структури НАТО для країни поза Альянсом). Водночас виявлена фундаментальна залежність від політичної волі партнерів створює стратегічні вразливості: затримки постачань, обмеження на удари, «втома від України» неодноразово уповільнювали операції та продовжували конфлікт.

Дослідження також виявило критичні виклики, що загострилися до 2025 року: Військова стагнація, ерозія професійного ядра, хронічна нестача особового складу, психологічне вигорання, зростання дезертирства. Економічна криза, інфляція, державний борг, обмеження фінансування модернізації. Демографічна катастрофа, понад 30 тис. офіційно визнаних загиблих, десятки тисяч поранених, 6+ млн. біженців, масова травматизація населення.

Проте важливо зауважити, що ці проблеми не залишилися поза увагою. Ініціативи, зокрема реформи Павла Паліси (заступника керівника ОП з листопада 2024-го), спрямовані на подолання стагнації через нову систему ротації, психологічну підтримку та оптимізацію мобілізації, що до кінця 2025 року дали перші позитивні результати.

Український досвід надає критичні уроки для держав, що можуть зіткнутися з подібними загрозами: Адаптивність, як ключ до виживання, здатність швидко навчатися, експериментувати та масштабувати успішні рішення є критичною Асиметрія перемагає масу, зосередження на руйнуванні найдорожчих активів противника через технологічно передові, але дешеві засоби. Інтеграція суспільства через децентралізовані моделі, де бізнес і громадяни стають частиною безпеки, дозволяють досягати недосяжної для держструктур швидкості інновацій. Технологічна

незалежність, розвиток локального ВПК, інтеграція ШІ та власних технологій є необхідною умовою стійкості. Соціально-психологічна стійкість, інвестиції в медіаграмотність, психологічну підтримку, стратегічні комунікації не менш важливі за озброєння. Проактивна дипломатія, трансформація з «жертви» на «захисника цінностей» дозволяє забезпечити безпрецедентну підтримку.

Також варто зауважити, що дослідження дозволяє спрогнозувати ключові тенденції: Технологізація конфліктів – масове впровадження ШІ для діпфейків, автоматизації кібератак, персоналізації дезінформації, квантові комп'ютери для злому криптографії; автономні системи озброєння. Розмивання меж – атаки на ICS/SCADA з реальними фізичними руйнуваннями, інтеграція кібер- та кінетичних операцій, мілітаризація соцмереж. Демократизація інструментів, доступ не лише держав, але й недержавних акторів до складних кібератак і діпфейків. Багатовекторність загроз – одночасні гібридні конфлікти на багатьох напрямках, створюючи «перманентну кризу».

Необхідність зсуву в сталих Парадигмах: Здобутий Україною досвід остаточно довів необхідність фундаментального переосмислення безпеки. Нова парадигма має базуватися на всеохоплюючій обороні, що інтегрує військові, цивільні, економічні, технологічні та інформаційні ресурси. Ключові елементи: суспільна єдність, технологічна винахідливість, економічна диверсифікація, кіберстійкість, медіаграмотність, міжнародна кооперація. Міжнародні інституції також потребують радикальної реформи: перегляду принципів РБ ООН щодо права вето, створення глобальних механізмів швидкого реагування на кібератаки, розробки міжнародно-правової бази для кваліфікації гібридних операцій як агресії, формування альянсів демократій.

За межами конкретних аспектів український опір став символом можливості протистояння авторитаризму. Україна довела: навіть значно слабша держава може змушувати ядерну наддержаву платити неприйнятну ціну. Якби Україна капітулювала у лютому-березні 2022-го, це створило б небезпечний прецедент «права сильного» й

тільки б більше розпалив би апетити Кремля до військових вторгнень. Український опір захистив саму ідею міжнародного порядку, заснованого на правилах, а не на силі.
У підсумку можна сказати, що одинадцять років гібридної агресії створили унікальний кейс, що остаточно довів: гібридна війна є еволюційним продовженням воєнного протиборства в умовах XXI століття. Україна не просто вижила, вона створила модель протидії, що поєднує військову міць, технологічну винахідливість, суспільну єдність та міжнародну підтримку.

Ця модель працює завдяки постійній адаптації, асиметричним рішенням та домінуючій волі до перемоги. Сьогодні український досвід стає новою парадигмою безпеки для демократичного світу. Що варта вивчатися, як живий доказ: коли ти не можеш бути сильнішим, будь розумнішим, швидшим у захисті свободи. Україна заплатила за цей урок десятками тисяч життів, мільярдами втрат та незліченними стражданнями. Але вона подарувала світу рецепт, як більше ніколи не програвати гібридну війну. І продовжує доводити щодня, що цей рецепт працює.

Війна ще не закінчена. Україну, ще чекають важкі випробування та тривалий процес відновлення. Але вже зараз очевидно: Україна переписала правила ведення війни XXI століття та назавжди змінила глобальну систему безпеки. Це, можливо, є найважливішим результатом одинадцяти років боротьби проти гібридної агресії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. А. І. Шевцов, Г. І. Мерніков. Агресія РФ проти України як фактор геополітичних та геоекономічних змін. 2018. № 1. С. 29. URL: https://niss-panorama.com/index.php/journal/article/download/66/63/ (Дата звернення: 10.09.2025).
2. Благодійний фонд ТВІЙ КРОК - Головна / БО "БФ "ТВІЙ КРОК". БО "БФ "ТВІЙ КРОК". 2024. URL: https://tviykrok.com.ua/ (Дата звернення: 20.11.2025).
3. Втрати Росії в Україні - офіційні дані. Index.Minfin. 2025. URL: https://index.minfin.com.ua/ua/russian-invading/casualties/ (Дата звернення: 15.11.2025).
4. «Гібридна» війна Росії – виклик і загроза для Європи : матеріали круглого столу, 14 грудня 2016 р. / за заг. ред. О. В. Литвиненка. Центр Разумкова. Київ, 2016. 56 с. URL: https://razumkov.org.ua/images/Material_Conference/2016_12_14/GIBRID-WAR-FINAL-1-1.pdf (Дата звернення: 25.09.2025).
5. Гібридна війна: in verbo et in praxi / Р. Додонов, Л. Роман, К. Новікова, О. Базалук, В. Мандрагеля, Г. Ковальський, В. Білецький, В. Додонова, О. Штоквиш, Р. Халіков, В. Гуржий, М. Колінько. Донецький національний університет імені Василя Стуса. Вінниця, 2017. URL: https://jmonographs.donnu.edu.ua/article/view/3781 (Дата звернення: 20.10.2025).
6. Гнатовський М. М. Загальна мобілізація 2022 р. в Україні: виклики та правові успіхи. Український журнал міжнародного права. 2023. № 1. С. 78–95. URL: https://uk.wikipedia.org/wiki/Мобілізація_в_Україні (Дата звернення: 05.11.2025).
7. Гнатовський М. М. Міжнародне гуманітарне право в умовах гібридних конфліктів: довідник для журналістів / М. М. Гнатовський, Т. Р. Короткий, Н. В. Хендель. Фенікс. Одеса, 2015. 92 с. URL: https://redcross.org.ua/wp-

content/uploads/2022/07/МГП_Довідник-для-журналістів_2-ге-вид-стиснуто.pdf (Дата звернення: 10.11.2025).

8. Гнатовський М. М. Національна стійкість України 2014–2025 рр. : системний аналіз. Стратегічна панорама. 2025. № 2. С. 5–28. URL: https://niss.gov.ua/sites/default/files/2015-02/volonter-697e4.pdf (Дата звернення: 25.09.2025).
9. Гнатовський М. М. Фінансова стійкість України в умовах війни : роль ЄС та США. Український журнал міжнародного права. 2025. № 3. С. 112–130. URL: https://mfa.gov.ua/mizhnarodni-vidnosini/spivrobitnictvo-ukrayini-z-mizhnarodnimi-finansovimi-instituciyami (Дата звернення: 30.10.2025).
10. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. Стратегічні пріоритети. 2014. № 4 (33). С. 5–12. URL: https://zn.ua/ukr/internal/gibridna-viyna-yak-klyuchoviy-instrument-rosiyskoyi-geostrategiyi-revanshu-_.html (Дата звернення: 12.11.2025).
11. Довіра до ЗМІ в Україні : опитування щодо ставлення до російських медіа на сході та півдні (2014 р.) / Київський міжнародний інститут соціології (КМІС). Київ, 2014. URL: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1138&page=1 (Дата звернення: 18.10.2025).
12. Довіра до російських ЗМІ на окупованих територіях (2014–2015). Kyiv International Institute of Sociology (KIIS). 2014–2015. URL: https://kiis.com.ua/?lang=eng&cat=reports (Дата звернення: 05.10.2025).
13. Закон про мобілізацію: які зміни ухвалив Парламент. Кабінет Міністрів України. Київ, 2024. 5 с. URL: https://www.kmu.gov.ua/news/zakon-pro-mobilizatsiiu-iaki-zminy-ukhvalyv-parlament1 (Дата звернення: 22.11.2025).
14. Звіт про кібератаки РФ на Україну у 2022–2024 рр. / Служба безпеки України ; CERT-UA. Київ, 2024. URL: https://cert.gov.ua/article/17696 (Дата звернення: 07.10.2025).

15. Звіти про діяльність фонду 2014–2025 рр. : серія річних і тематичних звітів / Фонд «Повернись живим». Київ, 2014–2025. URL: https://savelife.in.ua/en/reporting-en/ (Дата звернення: 05.12.2025).
16. Інфляційний звіт : вплив війни на економіку України (січень 2025 р.) / Національний банк України. Київ, 2025. URL: https://bank.gov.ua/admin_uploads/article/IR_2025-Q1.pdf (Дата звернення: 28.09.2025).
17. Інфляційний звіт: січень 2025 року. Національний банк України. Київ, 2025. 50 с. URL: https://bank.gov.ua/en/news/all/inflyatsiyniy-zvit-sichen-2025-roku (Дата звернення: 15.10.2025).
18. Конструкторсько-виробниче бюро LOCKER® | Розумні рішення для ремонту техніки / Конструкторсько-виробниче бюро LOCKER. Україна, 2023. URL: https://locker.net.ua/ (Дата звернення: 10.10.2025).
19. Магда Я. Гібридна агресія Росії: уроки для Європи. Центр глобалістики «Стратегія XXI». Київ, 2017. 144 с. ISBN 978-966-97478-3-9. URL: https://www.yakaboo.ua/ua/gibridna-agresija-rosii-uroki-dlja-evropi.html (Дата звернення: 05.10.2025).
20. Меморандум про гарантії безпеки у зв'язку з приєднанням України до Договору про нерозповсюдження ядерної зброї (Будапештський меморандум) : підписаний 05.12.1994 Україною, Російською Федерацією, Сполученим Королівством Великої Британії і Північної Ірландії та Сполученими Штатами Америки. 1994. URL: https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280401fbb (Дата звернення: 15.10.2025).
21. «Народний супутник» ГУР за два роки зробив понад 4 тисячі знімків / Суспільне Мовлення. Суспільне Медіа. Київ, 2024. URL: https://suspilne.media/776945-narodnij-suputnik-gur-za-dva-roki-zrobiv-ponad-4-tisaci-znimkiv/ (Дата звернення: 10.10.2025).

22. Печеник І., Фурман І. «Тузлінська криза» 2003 року як елемент експансії Російської Федерації в Україні. Воєнно-історичний вісник. 2024. Том 51, № 1. С. 16–32. URL: https://viv.nuou.org.ua/article/view/302901 (Дата звернення: 04.11.2025).
23. Підтримка приєднання до Росії серед жителів південних і східних областей України (Херсонська та Запорізька області) : прес-реліз / Київський міжнародний інститут соціології (КМІС). Київ, 2014. URL: https://www.kiis.com.ua/?lang=rus&cat=reports&id=1138&page=1 (Дата звернення: 25.10.2025).
24. Про введення воєнного стану в Україні : указ Президента України від 24.02.2022 № 64/2022. Президент України. Київ, 2022. 2 с. URL: https://www.president.gov.ua/documents/642022-41397 (Дата звернення: 05.12.2025).
25. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 № 64/2022 (продовжено до 2025 р.). Офіційний вісник України. 2022. № 17. Ст. 566. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text (Дата звернення: 15.10.2025).
26. Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку : Закон України від 11.04.2024 № 3633-IX. Відомості Верховної Ради України. 2024. № 19. Ст. 78. URL: https://zakon.rada.gov.ua/laws/show/3633-20#Text (Дата звернення: 20.10.2025).
27. Про волонтерську діяльність : Закон України від 19.04.2011 № 3236-VI (в редакції від 01.06.2025). Відомості Верховної Ради України. 2013. № 13. Ст. 99. URL: https://zakon.rada.gov.ua/laws/show/3236-17#Text (Дата звернення: 25.11.2025).

28. Про громадські об’єднання : Закон України від 22.03.2012 № 4572-VI (в редакції від 03.09.2024). Відомості Верховної Ради України. 2012. № 34. Ст. 393. URL: https://zakon.rada.gov.ua/laws/show/4572-17#Text (Дата звернення: 05.11.2025).
29. Про делегацію Уряду України для участі у багатосторонніх переговорах з підготовки та узгодження проекту Ініціативи щодо безпечного транспортування зерна та продуктів харчування з українських портів : розпоряд. КМУ від 22.07.2022 р. № 626-р. Верховна Рада України. Київ, 2022. URL: https://zakon.rada.gov.ua/laws/show/626-2022-%D1%80#Text (Дата звернення: 15.12.2025).
30. Про забезпечення функціонування української мови як державної : Закон України від 25.04.2019 № 2704-VIII. Відомості Верховної Ради України. 2019. № 21. Ст. 81. URL: https://zakon.rada.gov.ua/laws/show/2704-19#Text (Дата звернення: 25.09.2025).
31. Про загальну мобілізацію : Указ Президента України від 24.02.2022 № 65/2022. Офіційний вісник України. 2022. № 17. Ст. 567. URL: https://zakon.rada.gov.ua/laws/show/65/2022#Text (Дата звернення: 10.09.2025).
32. Про застосування та внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій) (щодо телеканалів 112, NewsOne, ZIK) : Рішення РНБО України від 02.02.2021. Офіційний веб-сайт Президента України. 2021. URL: https://www.president.gov.ua/documents/432021-36876 (Дата звернення: 10.10.2025).
33. Про застосування та внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій) : указ Президента України від 20.02.2021 № 69/2021. Президент України. Київ, 2021. 5 с. URL: https://ips.ligazakon.net/document/kr241032 (Дата звернення: 20.11.2025).
34. Про затвердження Порядку організації та ведення військового обліку призовників, військовозобов'язаних та резервістів : постанова Кабінету Міністрів

України від 13.04.2022 № 431. Кабінет Міністрів України. Київ, 2022. 10 с. URL: https://ips.ligazakon.net/document/T222632 (Дата звернення: 20.10.2025).

35. Про продовження строку проведення загальної мобілізації : указ Президента України від 20.10.2025 № 794/2025. Президент України. Київ, 2025. 2 с. URL: https://www.president.gov.ua/documents/7942025-56965 (Дата звернення: 05.11.2025).
36. Про рішення Ради національної безпеки і оборони України від 14 травня 2020 року "Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)" : указ Президента України від 14.05.2020 № 184/2020. Рада національної безпеки та оборони України. Київ, 2020. 5 с. URL: https://www.rnbo.gov.ua/ua/Ukazy/4602.html (Дата звернення: 15.12.2025).
37. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)" : указ Президента України від 15.05.2017 № 133/2017. Президент України. Київ, 2017. 5 с. URL: https://www.president.gov.ua/documents/1332017-21850 (Дата звернення: 25.09.2025).
38. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» (блокування ВКонтакте, Одноклассники, Яндекс та ін.) : Указ Президента України від 15.05.2017 № 315/2017. Офіційне інтернет-представництво Президента України. 2017. URL: https://zakon.rada.gov.ua/laws/show/315/2017 (Дата звернення: 10.10.2025).
39. Резніков розповів, як працює «народний супутник» / Радіо Свобода. Радіо Вільна Європа/Радіо Свобода. Прага, 2022. URL: https://www.radiosvoboda.org/a/news-narodnyy-suputnyk-rezinkov/32057595.html (Дата звернення: 20.11.2025).

40. Санкції щодо Медведчука: які сигнали отримав Кремль та як реагує світ? / V. Lazar. Радіо Свобода. Київ, 2021. 6 с. URL: https://www.radiosvoboda.org/a/sanktsiyi-medvedchuk-putin-viyna/31113234.html (Дата звернення: 05.12.2025).
41. Світова гібридна війна: український фронт : колективна монографія / за заг. ред. В. П. Горбуліна. НІСД. Київ, 2017. 496 с. ISBN 978-966-554-273-5. URL: https://niss.gov.ua/publikacii/monografii/svitova-gibridna-viyna-ukrainskiy-front-monografiya (Дата звернення: 15.10.2025).
42. Спільнота Стерненка / БФ Спільнота Стерненка. БФ Спільнота Стерненка. 2025. URL: https://www.sternenkofund.org/ (Дата звернення: 06.12.2025).
43. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. Державна служба спеціального зв'язку та захисту інформації України. Київ, 2024. URL: https://scpc.gov.ua/uk/articles/334 (Дата звернення: 10.11.2025).
44. Телебачення Торонто. СЕКРЕТНІ ПЕРЕПИСКИ АГЕНТА ФСБ: як російські спецслужби готувались до війни [Відео]. YouTube. 2023. 15 хв. URL: https://youtu.be/KqJ8pv6WxGU?t=6 (Дата звернення: 10.09.2025).
45. Телебачення Торонто. ХТО СТВОРЮЄ ВІРУСНІ ДІПФЕЙКИ ПРО ЗСУ: розслідування +ENG SUB [відео]. YouTube. 2024. 1 від. URL: https://www.youtube.com/watch?v=rxRMzB_1Yvs&t=2s (Дата звернення: 20.10.2025).
46. Тороп О. "Нас чекає важкий період, але Україна не програє" – Кирило Буданов в інтерв'ю BBC / Тороп О. BBC News Україна. BBC. Лондон, 2024. URL: https://www.bbc.com/ukrainian/articles/cmm35ry9v70o (Дата звернення: 05.11.2025).
47. Угода про чорноморський гуманітарний коридор для експорту зерна з України (Чорноморська зернова ініціатива) : укладена 22.07.2022 у м. Стамбулі / ООН,

Туреччина, Україна, РФ. ООН. New York, 2022. URL: https://www.un.org/en/black-sea-grain-initiative (Дата звернення: 05.12.2025).

48. «Груз-200 из Крыма». Проект о потерях России в Украине. Радіо Свобода. Проект Крим.Реалії. Київ, 2023. 23 лютого. URL: https://ru.krymr.com/a/gruz-200-krym/33244443.html (Дата звернення: 05.12.2025).
49. Игорь Гиркин (Стрелков) "нажал на спусковой крючок войны" на востоке Украины [Відео]/ Alex Che; канал Alex Che. 2020. URL: https://www.youtube.com/watch?v=m1wMLlzOlXQ (Дата звернення: 10.11.2025).
50. Кокошин А. О стратегической неядерной сдерживании в оборонной политике России. Военно-промышленный курьер. 2016. № 8 (476). URL: http://vfes.ru/vpk_08_476.pdf (Дата звернення: 25.09.2025).
51. Кокошин А. А. О стратегической неядерной сдерживании в оборонной политике России. Военно-промышленный курьер. 2016. № 8 (476). URL: https://vpk-news.ru/articles/300123 (Дата звернення: 30.10.2025).
52. ООН и Россия завершили консультации по Меморандуму о глобальной продовольственной безопасности. United Nations. New York, 2025. 11 липня. URL: https://news.un.org/ru/story/2025/07/1465983 (Дата звернення: 12.11.2025).
53. Премьер ДНР рассказал о воюющих на Украине российских военных/ РБК. АО «РБК». Москва, 2014. URL: https://www.rbc.ru/society/28/08/2014/570421569a794760d3d41089 (Дата звернення: 18.10.2025).
54. Стрелков признал: за спинами ЛДНР воюет Россия, в Украине нет внутреннего конфликта [Відео]/ Денис Казанський ; канал Denis Kazanskyi. 2020. URL: https://www.youtube.com/watch?v=2poOeNXnrbw (Дата звернення: 22.11.2025).
55. Хасавюртовские соглашения от 31.08.1996. Wikisource. 1996. URL: https://ru.wikisource.org/wiki/Хасавюртовские_соглашения_от_31.08.1996 (Дата звернення: 05.10.2025).

56. 2023 Report on International Religious Freedom: Ukraine / Bureau of Democracy, Human Rights, and Labor. U.S. Department of State. Washington, DC, 2024. 50 p. URL: https://www.state.gov/reports/2023-report-on-international-religious-freedom/ukraine (Access date: 20.10.2025).
57. Address by the President of the Russian Federation / President of Russia. 2022. 24 February. URL: http://en.kremlin.ru/events/president/news/67843 (Access date: 05.12.2025).
58. Annual Report 2024. SaveLife Foundation. Київ, 2025. 50 p. URL: https://savelife.in.ua/en/annual-report-en/ (Access date: 10.11.2025).
59. Anticorruption Action Centre (ANTAC). "Opposition Platform – For Life" Undermines Ukrainian Sovereignty and Territorial Integrity. 2022. 9 березня. URL: https://antac.org.ua/en/news/opzzh-undermines-ukrainian-sovereignty-and-territorial-integrity/ (Access date: 25.09.2025).
60. Arquilla J. Cyberwar is Coming! / J. Arquilla, D. Ronfeldt. Comparative Strategy. 1993. Vol. 12, No. 2. P. 141–165. DOI: https://doi.org/10.1080/01495939308402915 (Access date: 30.10.2025).
61. Asmus R. D. A Little War that Shook the World: Georgia, Russia, and the Future of the West. Palgrave Macmillan. New York, 2010. 254 p. ISBN 978-0-230-061773-6 (Access date: 12.11.2025).
62. Attack on Europe: Documenting Russian Equipment Losses During the 2022 Invasion of Ukraine. Oryx Spioenkop. 2022. URL: https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html (Access date: 18.10.2025).
63. Barigazzi J. Ukraine wants to use EU money to grow its military-industrial complex. POLITICO Europe. Брюссель, 2024. URL: https://www.politico.eu/article/ukraine-want-use-eu-money-build-up-military-industrial-complex-oleksandr-kamyshin/ (Access date: 22.11.2025).

64. Bartles Ch. K. Getting Gerasimov Right. Military Review. 2016. January–February. P. 30–38. URL: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2016/ART008/ (Access date: 05.10.2025).
65. Bellingcat Investigation Team. Putin Chef's Kisses of Death: Russia's Shadow Army's State-Run Structure Exposed / Bellingcat, The Insider, Der Spiegel. 2020. 14 серпня. URL: https://www.bellingcat.com/news/uk-and-europe/2020/08/14/pmc-structure-exposed/ (Access date: 15.12.2025).
66. Bezvershenko L. Resistance, resilience, recovery: Ukraine’s civil society in wartime. New Eastern Europe. 2025. No. 5. URL: https://neweasterneurope.eu/2025/09/27/resistance-resilience-recovery-ukraines-civil-society-in-wartime/ (Access date: 28.09.2025).
67. Bihus exposé: Ukraine's SBU illegally surveilled investigative journalists. Euromaidan Press. Kyiv, 2024. 7 лютого. URL: https://euromaidanpress.com/2024/02/07/bihus-expose-ukraines-sbu-illegally-surveilled-investigative-journalists/ (Access date: 10.10.2025).
68. Bihus.Info team awaits further investigations amidst police inquiry. National Police launch criminal probe into Bihus.Info surveillance. NV. Kyiv, 2024. 18 січня. URL: https://english.nv.ua/nation/bihus-info-team-awaits-further-investigations-amidst-police-inquiry-50385299.html (Access date: 20.11.2025).
69. Boston S., Massicot D. The Russian Way of Warfare: A Primer. RAND Corporation. Santa Monica, 2017. DOI: 10.7249/PE231. URL: https://www.rand.org/pubs/perspectives/PE231.html (Access date: 05.12.2025).
70. Bradshaw S. Industrialized Disinformation: 2020 Global Inventory of Organised Social Media Manipulation / S. Bradshaw, H. Bailey, P. N. Howard. Oxford Internet Institute, Programme on Democracy & Technology. Oxford, 2021. 70 p. URL: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf (Access date: 15.10.2025).

71. Bradshaw S. The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation / S. Bradshaw, Ph. N. Howard. Oxford Internet Institute. Oxford, 2021. 42 p. URL: https://www.oii.ox.ac.uk/news-events/reports/the-global-disinformation-order-2019-global-inventory-of-organised-social-media-manipulation/1 (Access date: 25.11.2025).
72. Brave1 - Ukrainian Defense Innovations / Brave1 Cluster ; Уряд України. Brave1 Cluster. Київ, 2025. URL: https://brave1.gov.ua/en/ (Access date: 10.09.2025).
73. Budjeryn M. Inheriting the Bomb: The Collapse of the USSR and the Nuclear Disarmament of Ukraine. Johns Hopkins University Press. Baltimore, 2023. 288 p. URL: https://www.amazon.com/Inheriting-Bomb-Collapse-Disarmament-Contemporary/dp/1421445867 (Access date: 20.10.2025).
74. Byman D. NATO and Countering Hybrid Warfare. Center for Strategic and International Studies (CSIS). Washington, DC, 2024. 12 липня. URL: https://www.csis.org/analysis/nato-and-countering-hybrid-warfare (Access date: 05.11.2025).
75. Chesney R. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review. 2019. Vol. 107, no. 6. P. 1753–1820. DOI: 10.15779/Z38RV0D15J. URL: https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security (Access date: 15.12.2025).
76. Civil Society at the Heart of Ukraine's Recovery, Even as War Escalates. Caritas Internationalis. Vatican City, 2025. 25 p. URL: https://www.caritas.org/2025/07/civil-society-at-the-heart-of-ukraines-recovery-even-as-war-escalates/ (Access date: 25.09.2025).
77. Civil Society Empowerment for Human Rights Protection during the War in Ukraine. UNDP. New York, 2025. 10 p. URL: https://www.undp.org/ukraine/news/civil-society-empowerment-human-rights-protection-during-war-ukraine (Access date: 10.10.2025).

78. Civil Society in Ukraine During Wartime. RTI International. Research Triangle Park, 2023. 15 p. URL: https://www.rti.org/impact/examining-role-civil-society-ukraine-during-wartime (Access date: 20.11.2025).
79. Civil Society in Ukraine's Restoration: A Guide to CSOs Mobilizing for a Marshall Plan. German Marshall Fund. Washington, 2023. 60 p. URL: https://securingdemocracy.gmfus.org/civil-society-in-ukraines-restoration-a-guide-to-csos-mobilizing-for-a-marshall-plan/ (Access date: 05.12.2025).
80. Clausewitz C. von. On War / trans. by M. Howard, P. Paret ; ed. and with an introd. by P. Paret. Princeton University Press. Princeton, 1984. 732 p. URL: https://www.degruyter.com/document/doi/10.1515/9781400837403/html (Access date: 15.10.2025).
81. Clarke R. A., Knake R. K. Cyber War: The Next Threat to National Security and What to Do About It. Ecco. New York, 2010. URL: https://www.jstor.org/stable/26270542 (Дата звернення: 05.12.2025).
82. Collaborationism in Ukraine: Cases and Statistics 2022–2025. Global Rights Compliance. Kyiv, 2025. URL: https://globalrightscompliance.org/judicial-practice-on-collaboration-cases-nationwide-database-of-decisions-between-2022-2025/ (Access date: 25.11.2025).
83. Constitutional Development with Civil Society – Case Studies from Southern and Eastern Africa. United Nations Peacemaker. New York, 2012. URL: https://peacemaker.un.org/en/documents/constitutional-development-civil-society-case-studies-southern-and-eastern-africa (Access date: 10.09.2025).
84. Cornell S. E. Small Nations and Great Powers: A Study of Ethnopolitical Conflict in the Caucasus. RoutledgeCurzon. London ; New York, 2001. 480 p. (Caucasus World). ISBN 0-7007-1162-7. URL: https://www.academia.edu/306198/Small_Nations_and_Great_Powers_A_Study_of_Ethnopolitical_Conflict_in_the_Caucasus (Access date: 20.10.2025).

85. Countering hybrid threats. NATO. 2025. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (Access date: 05.11.2025).
86. Criminal Liability for Collaboration with the Russian Federation. GOLAW. Kyiv, 2022. 7 p. URL: https://golaw.ua/insights/publication/kriminalna-vidpovidalnist-za-spivpraczyu-z-rf/ (Access date: 15.12.2025).
87. De Groot O. J., Linsi L., Ruhe C. The economic costs of hybrid wars: The case of Ukraine. Defence and Peace Economics. 2020. Vol. 31, no. 7. P. 786–804. DOI: 10.1080/10242694.2020.1791616. URL: https://www.tandfonline.com/doi/full/10.1080/10242694.2020.1791616 (Access date: 25.09.2025).
88. Debunking "Denazification" / W. Talley. Commission on Security and Cooperation in Europe (CSCE). 2025. URL: https://www.csce.gov/international-impact/debunking-denazification/ (Access date: 10.10.2025).
89. Defending Ukraine: Early Lessons from the Cyber War (2022–2023). Microsoft. Redmond, WA, 2022. 29 p. URL: https://www.microsoft.com/en-us/security/business/security-insider/reports/special-reports/defending-ukraine-early-lessons-from-the-cyber-war/ (Access date: 20.11.2025).
90. Denis Bigus Confirms Role in Ukraine Military Counterintelligence. Mezha. Kyiv, 2025. URL: https://mezha.net/eng/bukvy/denis-bigus-confirms-role-in-ukraine-military-counterintelligence/ (Access date: 05.12.2025).
91. Detector Media. 330 Shades of Russian Disinformation: Exploring the Media Landscape of Eastern Europe / V. Namestnik, I. Riaboshtan, O. Pivtorak, O. Bilousenko, O. Slyvenko. Detector Media. Київ, 2022. URL: https://en.detector.media/post/330-shades-of-russian-disinformation-exploring-the-media-landscape-of-eastern-europe (Access date: 15.10.2025).
92. Diaspora Organizations and their Humanitarian Response in Ukraine in 2022. DEMAC. Geneva, 2022. 40 p. URL: https://reliefweb.int/report/ukraine/diaspora-

organizations-and-their-humanitarian-response-ukraine-2022 (Access date: 25.11.2025).

93. Dinstein Y. War, Aggression and Self-Defence. 6th ed. Cambridge University Press. Cambridge, 2017. 424 p. DOI: 10.1017/9781108120555. ISBN 978-1-316-64166-8 (Access date: 10.09.2025).
94. Direct Damage to Ukraine's Infrastructure from Russia's War: Updated Estimates (as of January 2025). Kyiv School of Economics (KSE). Київ, 2025. URL: https://kse.ua/ua/war-damage-assessment/ (Access date: 20.10.2025).
95. Disinfo: Crimea became Russian after a 95% "in favour" referendum. EUvsDisinfo. 2025. URL: https://euvsdisinfo.eu/report/crimea-became-russian-after-a-95-in-favour-referendum/ (Access date: 05.11.2025).
96. Drabek Z., Bartels A. Compliance with WTO rules for less-developed countries: The case of Russia and Ukraine. Journal of World Trade. 2014. Vol. 48, no. 4. P. 789–812. DOI: 10.54648/JWT2014020 (Access date: 15.12.2025).
97. Dutsyk D. Between Freedom and Censorship: Ukraine's Mass Media in Times of Full-scale War / D. Dutsyk, A. Umland. SCEEUS. Stockholm, 2025. 19 червня. (SCEEUS Report ; No. 9). URL: https://sceeus.se/en/publications/between-freedom-and-censorship-ukraines-mass-media-in-times-of-full-scale-war/ (Access date: 10.10.2025).
98. Düben B. A. "There is no Ukraine": Fact-Checking the Kremlin's Version of Ukrainian History. LSE International History Blog. 2020. 1 July. URL: https://blogs.lse.ac.uk/lseih/2020/07/01/there-is-no-ukraine-fact-checking-the-kremlins-version-of-ukrainian-history/ (Access date: 25.09.2025).
99. Economy under War: 2022–2025 Overview. Natsionalnyy bank Ukrayiny. Київ, 2025. URL: https://bank.gov.ua/en/statistic (Access date: 20.11.2025).
100. Electricity Information Sharing and Analysis Center (E-ISAC). Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case / R. M. Lee, M. J. Assante, T. Conway. E-ISAC ; SANS ICS. Washington, DC, 2016. 30 p. URL:

https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf (Access date: 05.12.2025).

101. EU vs Disinfo Database / East StratCom Task Force. European External Action Service. Brussels, 2015–2025. URL: https://euvsdisinfo.eu/ (Access date: 15.10.2025).

102. Farmer K. C. Ukrainian Nationalism in the Post-Stalin Era: Myth, Symbols and Ideology in Soviet Nationalities Policy. Martinus Nijhoff Publishers. The Hague, 1980. 244 p. (Studies in Contemporary History ; vol. 4). ISBN 978-90-247-2401-7. DOI: 10.1007/978-94-009-8907-8 (Access date: 25.11.2025).

103. Felshtinsky Yu., Pribylovsky V. The Corporation: Russia and the KGB in the Age of President Putin. Encounter Books. New York, 2008. 240 p. ISBN 978-1-59403-246-0 (Access date: 10.09.2025).

104. Five Historical Pillars of Russian Imperial Propaganda / A. Marushevska. EUvsDisinfo. 2025. URL: https://euvsdisinfo.eu/five-historical-pillars-of-russian-imperial-propaganda/ (Access date: 20.10.2025).

105. Fridman O. Russian "Hybrid Warfare": Resurgence and Politicization. Oxford University Press. Oxford, 2018. 236 p. ISBN 978-0-19-087737-8. DOI: 10.1093/oso/9780190877378.001.0001. URL: https://academic.oup.com/book/32415 (Access date: 05.11.2025).

106. From Loss to Leverage: How Displacement Could Build Ukraine's Post-War Reformist Elite / S. Slonovska. Yale Review of International Studies. New Haven, 2025. 10 p. URL: https://yris.yira.org/column/from-loss-to-leverage-how-displacement-could-build-ukraines-post-war-reformist-elite/ (Access date: 15.12.2025).

107. Galeotti M. The 'Gerasimov Doctrine' and Russian Non-Linear War. In Moscow's Shadows. 2016. July. 12 p. URL: https://founderscode.com/wp-content/uploads/2016/07/Gerasimov-Doctrine-and-Russian-Non-Linear-War-In-Moscow-s-Shadows.pdf (Access date: 25.09.2025).

108. Global Ukrainian Diaspora Strategy 2025–2028: Supporting Ukraine under UWC Leadership Amid U.S. Policy Challenges / M. Mowczan. Myk's Substack. Substack, 2025. 5 p. URL: https://mykmowczan.substack.com/p/global-ukrainian-diaspora-strategy (Access date: 10.10.2025).

109. Götz E., Staun J. Why Russia attacked Ukraine: Strategic culture and radicalized narratives. Contemporary Security Policy. 2022. Vol. 43, no. 3. P. 482–497. DOI: 10.1080/13523260.2022.2082633. URL: https://www.tandfonline.com/doi/full/10.1080/13523260.2022.2082633 (Access date: 20.11.2025).

110. Greenberg A. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. Doubleday. New York, 2019. 368 p. ISBN 978-0-385-54440-5 (Access date: 05.12.2025).

111. GRIZZLY STEPPE – Russian Malicious Cyber Activity (Joint Analysis Report). U.S. Department of Homeland Security ; FBI. Washington, DC, 2016. 53 p. URL: https://www.cisa.gov/news-events/alerts/2016/12/29/grizzly-steppe-russian-malicious-cyber-activity (Access date: 15.10.2025).

112. Gzirian R. Ukraine's Volunteer Battalions Must Join the Military or Sheath the Sword / Gzirian R. Atlantic Council. Вашингтон, 2015. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-s-volunteer-battalions-must-join-the-military-or-sheath-the-sword/ (Access date: 25.11.2025).

113. Harper S. Factory-to-Frontline Pipeline: How Ukraine's 2025 Drone Surge is Reshaping the Battlefield / Harper S. War Quants. War Quants, 2025. URL: https://www.warquants.com/p/factory-to-frontline-pipeline (Access date: 10.09.2025).

114. Has Ukraine's News Telethon Impacted Media Freedom? / G. Ostapovets. Institute for War and Peace Reporting (IWPR). London, 2023. URL: https://iwpr.net/global-voices/has-ukraines-news-telethon-impacted-media-freedom (Access date: 20.10.2025).

115. Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies. Arlington, VA, 2007. 40 p. URL: https://potomacinstitute.us/reports/19-reports/1163-conflict-in-the-21st-century-the-rise-of-hybrid-wars (Access date: 05.11.2025).

116. Hoffman F. G. Hybrid Warfare and Challenges. Joint Force Quarterly. 2009. Issue 52, 1st quarter. P. 34–39. URL: https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-52.pdf (Access date: 15.12.2025).

117. Hoffman F. The Future of Hybrid Warfare / F. Hoffman, M. Neumeyer, B. Jensen. Center for Strategic and International Studies (CSIS). Washington, DC, 2024. 8 липня. URL: https://www.csis.org/analysis/future-hybrid-warfare (Access date: 25.09.2025).

118. Holodnyuk E. Ukraine Symposium – The Budapest Memorandum's History and Role in the Conflict. Lieber Institute, West Point. 2025. 15 January. URL: https://lieber.westpoint.edu/budapest-memorandums-history-role-conflict/ (Access date: 10.10.2025).

119. How Putin's 'denazification' Claim Distorts History, According to Scholars. NPR. 2022. 1 March. URL: https://www.npr.org/2022/03/01/1083677765/putin-denazify-ukraine-russia-history (Access date: 20.11.2025).

120. Human Rights Watch. World Report 2024: Ukraine. Human Rights Watch. New York, 2024. URL: https://www.hrw.org/world-report/2024/country-chapters/ukraine (Access date: 05.12.2025).

121. Humanitarian Aid: Historian Vladlen Maraiev on the Biggest Myths on Ukraine's Past Influencing Ukraine's Future / V. Maraiev ; O. Tyshchuk. Platfor.ma. 2023. 10 p. URL: https://www.platfor.ma/topic/humanitarian-aid-historian-vladlen-maraiev-on-the-biggest-myths-on-ukraine-s-past-influencing-ukraine-s-future/ (Access date: 15.10.2025).

122. Hybrid Threats and Resilience: The Ukrainian Experience 2014–2025. Swedish Defence Research Agency (FOI). Stockholm, 2025. 110 p. URL: https://www.foi.se/en/foi/publications/2025/hybrid-threats-and-resilience-the-ukrainian-experience-2014-2025 (Access date: 10.09.2025).

123. Hybrid threats. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). Helsinki, 2025. URL: https://www.hybridcoe.fi/hybrid-threats/ (Access date: 25.11.2025).

124. Hybrid War: The Influence of the Russian Orthodox Church on the Ukrainian Media / O. Lytvynchuk, A. Shevchuk, Z. Hrytsyshena. George Fox University Digital Commons. 2025. 22 p. URL: https://digitalcommons.georgefox.edu/cgi/viewcontent.cgi?article=2665&context=ree (Access date: 20.10.2025).

125. Hybrid Warfare in the Middle East: We Must Do Better / C. M. Baker. Royal United Services Institute (RUSI). London, 2017. 5 p. URL: https://www.rusi.org/explore-our-research/publications/commentary/hybrid-warfare-middle-east-we-must-do-better (Access date: 05.11.2025).

126. Hybrid Warfare: A Reorientation of Russian Foreign Policy in Syria / T. Kuzio. Pakistan Journal of International Affairs. 2022. Vol. 4, no. 2. 15 p. DOI: 10.52337/PJIA.V4I2.177. URL: https://www.academia.edu/62783656/Hybrid_Warfare_A_Reorientation_of_Russian_foreign_policy_in_Syria (Access date: 15.12.2025).

127. IMF World Economic Outlook Database: Ukraine GDP Projections 2022–2025. International Monetary Fund. Washington, 2024. URL: https://www.imf.org/en/Publications/WEO/weo-database/2024/October (Access date: 25.09.2025).

128. In Crimea, Voting under the Gun. Voice of America ; Bellingcat. 2014. 11 March. 2 p. URL: https://www.youtube.com/watch?v=51e8xuLlX9k (Access date: 10.10.2025).

129. Initiative on the Safe Transportation of Grain and Foodstuffs from Ukrainian Ports (Black Sea Grain Initiative). United Nations. New York, 2022. 10 p. URL: https://www.un.org/en/black-sea-grain-initiative (Access date: 20.11.2025).

130. Inside the Fight to Reform Ukrainian Diaspora Advocacy in America / D. Kirichenko. Kyiv Post. Kyiv, 2025. 15 p. URL: https://www.kyivpost.com/post/61819 (Access date: 05.12.2025).

131. Investigative Stories from Ukraine: Bihus.Info Finds Another Defense Ministry Contract with Inflated Food Prices / A. Myroniuk, A. Khrebet. Kyiv Independent. Kyiv, 2023. 5 p. URL: https://kyivindependent.com/investigative-stories-from-ukraine-bihus-info-finds-another-defense-ministry-contract-with-inflated-food-prices/ (Access date: 15.10.2025).

132. Is Ukraine Becoming the Silicon Valley of Defense Tech? / UNITED24 Media. UNITED24 Media. Київ, 2025. URL: https://united24media.com/business/is-ukraine-becoming-the-silicon-valley-of-defense-tech-10494 (Access date: 25.11.2025).

133. Journalists Question Relevancy of Ukraine's United TV Marathon. VOA News. Washington, 2024. 4 p. URL: https://www.voanews.com/amp/journalists-question-relevancy-of-ukraine-s-united-tv-marathon-/7433684.html (Access date: 10.09.2025).

134. Journalists Say Ukrainian Security Service Spied on Them. Reuters. London, 2024. 6 February. URL: https://www.reuters.com/world/europe/journalists-say-ukrainian-security-service-spied-them-2024-02-06/ (Access date: 20.10.2025).

135. Kaldor M. New and Old Wars: Organized Violence in a Global Era. 3rd ed. Polity Press. Cambridge, 2012. 268 p. ISBN 978-0-7456-5563-5 (Access date: 05.11.2025).

136. Kofman M., Migacheva K., Nichiporuk B., Radin A., Tkacheva O., Oberholtzer J. Lessons from Russia’s Operations in Crimea and Eastern Ukraine. RAND Corporation. Santa Monica, CA, 2017. 126 p. URL: https://www.rand.org/pubs/research_reports/RR1498.html (Access date: 15.12.2025).

137. Kulyk V. National Identity in Time of War: Ukraine after the Russian Aggressions of 2014 and 2022. Routledge. London, 2023. 180 p. URL: https://www.tandfonline.com/doi/abs/10.1080/10758216.2023.2224571 (Access date: 25.09.2025).

138. Kurylo B. From Individual to Collective: Vernacular Security and Ukrainian Civil Society in Wartime. Sage. London, 2025. 150 p. URL: https://journals.sagepub.com/doi/10.1177/09670106251329884 (Access date: 10.10.2025).

139. Kuzio T. Russian Nationalism and the Russian-Ukrainian War: Autocracy-Orthodoxy-Nationality. Routledge. London, 2022. 198 p. ISBN 978-1-032-04320-3 (Access date: 20.11.2025).

140. Kyiv Court Arrests Suspected Russian Spy Embedded in Anti-Graft Bureau. Euromaidan Press. Київ, 2025. 5 p. URL: https://euromaidanpress.com/2025/07/22/kyiv-court-arrests-suspected-russian-spy-embedded-in-anti-graft-bureau/ (Access date: 05.12.2025).

141. Kyiv Global Government Technology Centre Team. Ukraine's IT Shift: From Outsourcing to Innovation / Kyiv Global Government Technology Centre Team. Kyiv Global Government Technology Centre. Київ, 2025. URL: https://digitalstate.gov.ua/news/it-outsourcing/ukraines-it-shift-from-outsourcing-to-innovation (Access date: 15.10.2025).

142. Lanoszka A. The 'Steinmeier Formula': A Path to Peace or a Dead End? ResearchGate. 2019. 20 p. DOI: 10.13140/RG.2.2.36189.77289. URL: https://www.researchgate.net/publication/336123456_The_Steinmeier_Formula_A_Path_to_Peace_or_a_Dead_End (Access date: 25.11.2025).

143. Lee R. M., Assante M. J., Conway T. Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS ICS. Washington, DC, 2016. 28 p. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf (Access date: 10.09.2025).

144. Lessons from Russia's First Assault on Ukraine: 20 Years Since Tuzla / H. Shelest. Center for European Policy Analysis (CEPA). Washington, DC, 2023. 5 p. URL: https://cepa.org/article/lessons-from-russias-first-assault-on-ukraine-20-years-since-tuzla/ (Access date: 20.10.2025).

145. Lessons of the Minsk Deal: Breaking the Cycle of Russia's War Against Ukraine / N. Bugayova. Institute for the Study of War (ISW). Washington, DC, 2025. 10 p. URL: https://understandingwar.org/backgrounder/lessons-minsk-deal-breaking-cycle-russias-war-against-ukraine (Access date: 05.11.2025).

146. 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. October. P. 22–26. URL: https://www.semanticscholar.org/paper/The-Changing-Face-of-War%3A-Into-the-Fourth-Lind-Nightengale/2fd541a48abb544e1cd8dde7bdbd1fd8634b623d (Access date: 15.12.2025).

147. 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. URL: https://www.d-n-i.net/fcs/4th_gen_war_gazette.htm (Access date: 25.09.2025).

148. Lipovsky R. BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry. ESET. 2016. 4 Jan. URL: https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/ (Access date: 10.10.2025).

149. List of Journalists Killed during the Russo-Ukrainian War. Wikipedia. 2024. URL: https://en.wikipedia.org/wiki/List_of_journalists_killed_during_the_Russo-Ukrainian_War (Access date: 20.11.2025).

150. List of Journalists Killed since Start of Russia's Full-Scale Aggression (Update). National Union of Journalists of Ukraine (NUJU). Kyiv, 2025. URL:

https://nuju.org.ua/list-of-journalists-killed-since-start-of-russia-s-full-scale-aggression-update-2/ (Access date: 05.12.2025).

151. Liz A. Chechnya: Khasavyurt Accords Failed To Preclude A Second War / A. Liz. Radio Free Europe / Radio Liberty. Prague, 2006. 30 серпня. URL: https://www.rferl.org/a/1070939.html (Access date: 15.10.2025).

152. McDermott R. N. Does Russia Have a Gerasimov Doctrine? Parameters. 2016. Vol. 46, no. 1. P. 97–105. URL: https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2827&context=parameters (Access date: 25.11.2025).

153. Media in Wartime: The Case of the Ukrainian TV Marathon / O. Chaiko. Media Diversity Institute. London, 2024. 6 p. URL: https://www.media-diversity.org/media-in-wartime-the-case-of-the-ukrainian-tv-marathon/ (Access date: 10.09.2025).

154. Moynihan H. The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention. Chatham House. London, 2019. 2 грудня. (International Law Programme Paper). URL: https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks (Access date: 20.10.2025).

155. Mumford A. Proxy Warfare and the Future of Conflict. The RUSI Journal. 2013. Vol. 158, no. 2. P. 40–46. DOI: 10.1080/03071847.2013.787733. URL: https://www.tandfonline.com/doi/full/10.1080/03071847.2013.787733 (Access date: 05.11.2025).

156. NATO's Support for Ukraine. NATO. Brussels, 2025. 10 p. URL: https://www.nato.int/cps/en/natohq/topics_192648.htm (Access date: 15.12.2025).

157. New Diaspora Platform Backed by IOM Aims to Boost Ukraine's Reconstruction. IOM. Geneva, 2025. 3 p. URL: https://www.iom.int/news/new-diaspora-platform-backed-iom-aims-boost-ukraines-reconstruction (Access date: 25.09.2025).

158. Nord Stream 2 Comes on Stream: Good Business or Bad Geopolitics? / J. Shea. Friends of Europe. Brussels, 2021. 6 p. URL: https://www.friendsofeurope.org/insights/nord-stream-2-comes-on-stream-good-business-or-bad-geopolitics/ (Access date: 10.10.2025).

159. Odarchenko K. Blood and Memory — How War Unifies Ukrainians / Kateryna Odarchenko. CEPA. Washington, 2024. 28 травня. URL: https://cepa.org/article/blood-and-memory-how-war-unifies-ukrainians/ (Access date: 20.11.2025).

160. One year of the Black Sea Initiative: Key facts and figures. United Nations. New York, 2023. 10 липня. URL: https://news.un.org/en/story/2023/07/1138532 (Access date: 05.12.2025).

161. OSCE Office for Democratic Institutions and Human Rights. Moscow Mechanism experts present report on Ukraine to OSCE Permanent Council. 2025. 25 September. URL: https://odihr.osce.org/odihr/598057 (Access date: 15.10.2025).

162. OSCE Office for Democratic Institutions and Human Rights. Ukraine appoints three experts following invocation of the OSCE's Moscow Mechanism / OSCE Office for Democratic Institutions and Human Rights. OSCE/ODIHR. Варшава, 2025. URL: https://odihr.osce.org/odihr/596399 (Access date: 25.11.2025).

163. Our Members Gave Interviews to the "Ukrainian Science Diaspora" Initiative. Ukrainet. Brussels, 2025. 5 p. URL: https://ukrainet.eu/2025/11/16/our-members-gave-interviews-to-the-ukrainian-science-diaspora-initiative/ (Access date: 10.09.2025).

164. Pekar V. Civil Society in Ukraine: A Sled Dog, Not a Watchdog. New Eastern Europe. 2025. No. 5 (71). P. 1–12. URL: https://neweasterneurope.eu/2025/11/03/civil-society-in-ukraine-a-sled-dog-not-a-watchdog/ (Access date: 20.10.2025).

165. Pifer S. Budapest Memorandum at 25: Between Past and Future / S. Pifer. Belfer Center for Science and International Affairs, Harvard Kennedy School. Cambridge, MA, 2019. 10 p. URL: https://www.belfercenter.org/publication/budapest-memorandum-25-between-past-and-future (Access date: 15.12.2025).

166. Pifer S. Budapest Memorandum Myths / S. Pifer. Center for International Security and Cooperation, Stanford University. Stanford, CA, 2024. 5 p. URL: https://cisac.fsi.stanford.edu/news/budapest-memorandum-myths (Access date: 05.11.2025).

167. Plokhy S. The Stubborn Legend of a Western 'Coup' in Ukraine / S. Plokhy. Foreign Policy. 2024. 4 August. 8 p. URL: https://foreignpolicy.com/2024/08/04/ukraine-maidan-revolution-russia-coup-myth-yanukovych/ (Access date: 25.09.2025).

168. Preliminary Lessons from Ukraine's Offensive Operations, 2022–23 / J. Watling, N. Reynolds. Royal United Services Institute. London, 2024. 60 p. URL: https://static.rusi.org/lessons-learned-ukraine-offensive-2022-23.pdf (Access date: 10.10.2025).

169. Proofs of the Russian Aggression: InformNapalm Database. InformNapalm. 2015–2025. URL: https://informnapalm.org/en/russian-aggression/ (Access date: 20.11.2025).

170. Prytula Foundation / Prytula Foundation. Prytula Foundation. Київ, 2025. URL: https://prytulafoundation.org/ (Access date: 05.12.2025).

171. Recent Trends in the Ukrainian Language Situation (2020-2024) / S. Del Gaudio. SRC-H, Hokkaido University. Sapporo, 2024. URL: https://src-h.slav.hokudai.ac.jp/sympo/2024winter/pdf/ppt/P2_1_DEL_GAUDIO_ppt.pdf (Access date: 15.10.2025).

172. Reis J. C. G. d. The Quest for Social Justice Amid War: Exploring the Role of Civil Society Resilience in Ukraine's Social Justice and Cohesion. Safer Communities. 2025. Vol. 24, no. 1. P. 58–71. DOI: 10.1108/SC-07-2024-0039. URL: https://www.emerald.com/insight/content/doi/10.1108/SC-07-2024-0039/full/html (Access date: 25.11.2025).

173. Report on the Human Rights Situation in Ukraine, 16 February to 15 May 2016. OHCHR. Geneva, 2016. 50 p. URL: https://ukraine.ohchr.org/en/14-periodic-report-EN (Access date: 10.09.2025).

174. Reports on Heavy Weapons in Donbas (TOS-1, Orlan-10), 2015–2022. OSCE Special Monitoring Mission to Ukraine. Vienna, 2015–2022. URL: https://www.osce.org/special-monitoring-mission-to-ukraine/reports (Access date: 20.10.2025).

175. Reports on Russian Hybrid Warfare in Georgia 2008 and Ukraine 2014–2023. NATO Strategic Communications Centre of Excellence. Riga, 2015–2023. URL: https://stratcomcoe.org/publications (Access date: 05.11.2025).

176. Resolution 68/262: Territorial integrity of Ukraine. United Nations General Assembly. New York, 2014. 2 p. URL: https://digitallibrary.un.org/record/767565?ln=en (Access date: 15.12.2025).

177. Resolution 68/262: Territorial integrity of Ukraine. United Nations General Assembly. New York, 2014. 2 p. URL: https://digitallibrary.un.org/record/767565?ln=en (Access date: 25.09.2025).

178. Romandash A. Hybrid Warfare: Ukraine, Russia and Western Lessons / A. Romandash. Centre for International Governance Innovation (CIGI). Waterloo, 2025. (Policy Brief ; no. 209). 10 p. URL: https://www.cigionline.org/documents/3540/PB_no.209.pdf (Access date: 10.10.2025).

179. Romanyuk A., Lytvyn V. Ethnolinguistic and Religious Factors in Changing Geopolitical Orientation of Ukrainian Citizens. BESA Center. Ramat Gan, 2025. 15 p. URL: https://besacenter.org/ethnolinguistic-and-religious-factors-in-changing-geopolitical-orientation-of-ukrainian-citizens/ (Access date: 20.11.2025).

180. Roudik P. Ukraine: Demarcation of Border with Russia / P. Roudik ; W. G. Miller (коментар). Library of Congress. Washington, DC, 2014. 3 p. URL: https://www.loc.gov/item/global-legal-monitor/2014-12-02/ukraine-demarcation-of-border-with-russia/ (Access date: 05.12.2025).

181. Russian Advances in Donetsk Oblast 2024–2025. Institute for the Study of War. Washington, 2025. 30 p. URL: https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-november-26-2025 (Access date: 10.09.2025).

182. Russian Drone Kills Two Ukrainian Journalists on Donetsk Eastern Front Line. Al Jazeera. Doha, 2025. 5 p. URL: https://www.aljazeera.com/news/2025/10/23/russian-drone-kills-two-ukrainian-journalists-on-donetsk-eastern-front-line (Access date: 20.10.2025).

183. Russian Information Campaign Against Ukraine (2013–2022). NATO Strategic Communications Centre of Excellence. Riga, 2016. 100 p. URL: https://stratcomcoe.org/publications/analysis-of-russias-information-campaign-against-ukraine/151 (Access date: 05.11.2025).

184. Russian War in Ukraine TIMELINE. U.S. Department of Defense. Washington, 2025. 20 p. URL: https://www.defense.gov/Spotlights/Support-for-Ukraine/Timeline/ (Access date: 15.12.2025).

185. Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist / ed. by K. Pynnöniemi, M. Kari. Finnish Institute of International Affairs. Helsinki, 2015. 191 p. (FIIA Report ; 43). URL: https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf (Access date: 15.10.2025).

186. Russia's Strategic Miscalculation in Blockading the Sea of Azov / R. Hilton. European Leadership Network. London, 2018. 4 p. URL: https://europeanleadershipnetwork.org/commentary/russias-strategic-miscalculation-in-blockading-the-sea-of-azov/ (Access date: 25.11.2025).

187. Ryabov A. Imitating Chávez: A Year of Nationalization in Crimea / Andrey Ryabov. Carnegie Moscow Center. Moscow, 2015. 14 квітня. URL: https://carnegiemoscow.org/commentary/59421 (Access date: 25.09.2025).

188. Satter D. Darkness at Dawn: The Rise of the Russian Criminal State. Yale University Press. New Haven, 2003. 416 p. ISBN 978-0-300-00892-0 (Access date: 10.10.2025).

189. SBU Head Meets with G7 Ambassadors after Bihus.Info Surveillance Scandal / M. Fornusek. Kyiv Independent. Kyiv, 2024. 2 p. URL: https://kyivindependent.com/sbu-head-meets-with-g7-ambassadors/ (Access date: 20.11.2025).

190. Security Service Officials Took $300,000 Bribes as Ukraine Guts Corruption Oversight / A. Shandra. Euromaidan Press. Kyiv, 2025. 4 p. URL: https://euromaidanpress.com/2025/07/22/security-service-officials-took-300000-bribes-as-ukraine-gutts-corruption-oversight/ (Access date: 05.12.2025).

191. Since 2022, Russians Have Killed 135 Journalists in Ukraine - Zelenskyy. UNN. Kyiv, 2025. 3 p. URL: https://unn.ua/en/news/since-2022-russians-have-killed-135-journalists-in-ukraine-zelenskyy (Access date: 15.10.2025).

192. Six Months of War in Ukraine, Eight Journalists Killed. RSF. Paris, 2022. 5 p. URL: https://rsf.org/en/six-months-war-ukraine-eight-journalists-killed (Access date: 25.11.2025).

193. Snyder T. The Road to Unfreedom: Russia, Europe, America. Tim Duggan Books. New York, 2018. 368 p. ISBN 978-0-525-57446-0 (Access date: 10.09.2025).

194. Spot report by the OSCE Special Monitoring Mission to Ukraine (SMM), 18 February 2015: SMM facilitates dialogue on ceasefire and access to Debaltseve / ОБСЄ SMM. OSCE. Vienna, 2015. 18 лютого. URL: https://www.osce.org/ukraine-smm/141426 (Access date: 05.11.2025).

195. Spot report by the OSCE Special Monitoring Mission to Ukraine (SMM), 18 February 2015: SMM facilitates dialogue on ceasefire and access to Debaltseve / ОБСЄ SMM. OSCE. Vienna, 2015. 18 лютого. URL: https://www.osce.org/ukraine-smm/141426 (Access date: 20.10.2025).

196. Stern D. L. Battle for Kyiv: How Ukrainian forces defended and saved their capital / D. L. Stern [et al.]. The Washington Post. Washington, 2022. URL: https://www.washingtonpost.com/national-security/interactive/2022/kyiv-battle-ukraine-survival/ (Access date: 15.12.2025).

197. Stern J. P., Pirani S., Yafimava K. The Russo-Ukrainian Gas Dispute of January 2009: A Comprehensive Assessment. Oxford Institute for Energy Studies. Oxford, 2009. 54 p. (NG ; 27). URL: https://www.oxfordenergy.org/publications/russo-ukrainian-gas-dispute-january-2009-comprehensive-assessment/ (Access date: 25.09.2025).

198. Syniuk O., Deputat D., Vyshnevska I. et al. Survival or crime: how Ukraine punishes collaborationism. ZMINA Human Rights Center. Kyiv, 2025. 60 p. URL: https://zmina.ua/en/publication-en/survival-or-crime-how-ukraine-punishes-collaborationism/ (Access date: 10.10.2025).

199. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by M. N. Schmitt. Cambridge University Press. Cambridge, 2017. 738 p. ISBN 978-1-107-17722-2 (Access date: 05.12.2025).

200. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by M. N. Schmitt. Cambridge University Press. Cambridge, 2017. 738 p. ISBN 978-1-107-17722-2 (Access date: 20.11.2025).

201. Ten Groundbreaking Investigations by Ukrainian Media Outlets: The Urgent Need to Support Investigative Journalism in a Fragile Context. RSF. Paris, 2025. 10 p. URL: https://rsf.org/en/ten-groundbreaking-investigations-ukrainian-media-outlets-urgent-need-support-investigative (Access date: 15.10.2025).

202. The Cost to Ukraine of Crimea's Annexation / M. Bugriy. Eurasia Daily Monitor. 2014. Vol. 11, iss. 70. URL: https://jamestown.org/program/the-cost-to-ukraine-of-crimeas-annexation/ (Access date: 25.11.2025).

203. The Criminal Investigation into MH17. Joint Investigation Team (JIT). 2018 (оновлено 2024). URL: https://www.government.nl/topics/mh17-incident/achieving-justice/the-criminal-investigation (Access date: 10.09.2025).

204. The Diaspora Response to War in Ukraine / D. Hincu. ICMPD. Vienna, 2022. 5 p. URL: https://www.icmpd.org/blog/2022/the-diaspora-response-to-war-in-ukraine (Access date: 20.10.2025).

205. The Diaspora's Mobilization Post-Invasion Has Provided Crucial Support to Ukraine / M. Koinova. Migration Policy Institute. Washington, 2024. 20 p. URL: https://www.migrationpolicy.org/article/ukraine-diaspora-mobilization (Access date: 05.11.2025).

206. The Identity of Ukraine's Citizens: Trends of Change (June 2024). Razumkov Centre. Київ, 2024. 10 p. URL: https://razumkov.org.ua/en/component/k2/the-identity-of-ukraine-s-citizens-trends-of-change-june-2024 (Access date: 15.12.2025).

207. The Landscape of Hybrid Threats: A Conceptual Model / ed. by G. Giannopoulos, H. Smith, M. Theocharidou ; Hybrid CoE, Joint Research Centre of the European Commission. Hybrid CoE ; JRC. Helsinki/Ispra, 2020. 52 p. URL: https://euhybnet.eu/wp-content/uploads/2021/06/Conceptual-Framework-Hybrid-Threats-HCoE-JRC.pdf (Access date: 25.09.2025).

208. The Military Balance 2023. Routledge. London, 2023. 504 p. ISBN 978-1-03-250895-5 (Access date: 10.10.2025).

209. The Nord Stream 2 pipeline: Economic, environmental and geopolitical issues : EPRS Briefing PE 690.705. European Parliament. Brussels, 2021. 1 липня. URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)690705 (Access date: 20.11.2025).

210. The Russian War in Ukraine Increased Ukrainian Language Use on Social Media / D. Racek, B. I. Davidson, P. W. Thurner, X. X. Zhu, G. Kauermann. PMC. Bethesda, 2024. 12 p. DOI: 10.1038/s44271-023-00045-6. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC11332000/ (Access date: 15.11.2025).

211. The Ukrainian Journalist Was Mobilized after Exposing Corruption. Pravda EN. Kyiv, 2025. 3 p. URL: https://news-pravda.com/ukraine/2025/09/24/1712637.html (Access date: 05.12.2025).

212. Treasury Sanctions Russian-Backed Actors Responsible for Destabilization Activities in Ukraine : OFAC Press Release JY0562. U.S. Department of the Treasury. Washington, DC, 2022. 5 p. URL: https://home.treasury.gov/news/press-releases/jy0562 (Access date: 15.10.2025).

213. Treaty between Ukraine and the Russian Federation on the Ukrainian-Russian State Border. United Nations Treaty Collection. New York, 2003. URL: https://treaties.un.org/Pages/showDetails.aspx?objid=08000002803fe18a (Access date: 25.11.2025).

214. Ukraine Support Tracker: Aid to Ukraine of Official Donors, World Governments and Selected Civil Society Organizations. Kiel Institute for the World Economy. Kiel, 2025. URL: https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/ (Access date: 20.10.2025).

215. Ukraine Support Tracker: Database. Kiel Institute for the World Economy. Kiel, 2025. URL: https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/ (Access date: 05.11.2025).

216. Ukraine's New Mobilization Law Leaves Demobilization Issue Unresolved. Kyiv Independent. Kyiv, 2024. 5 p. URL: https://kyivindependent.com/ukraines-new-mobilization-law-leaves-demobilization-issue-unresolved (Access date: 20.11.2025).

217. Ukraine, Russia, and the Minsk Agreements: A Post-Mortem / G. Gressel. European Council on Foreign Relations (ECFR). London, 2024. 6 p. URL: https://ecfr.eu/article/ukraine-russia-and-the-minsk-agreements-a-post-mortem/ (Access date: 15.12.2025).

218. Ukraine. Migration Policy Institute. Washington, 2024. URL: https://www.migrationpolicy.org/country-resource/ukraine (Access date: 10.09.2025).

219. Ukraine: RSF Calls on Government to Put an End to Telemarathon / J. Cavelier. RSF. Paris, 2024. 3 p. URL: https://rsf.org/en/ukraine-rsf-calls-government-put-end-telemarathon (Access date: 25.09.2025).

220. Ukraine's Energy Security and the Coming Winter. International Energy Agency (IEA). Paris, 2024. 30 p. URL: https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter (Access date: 10.10.2025).

221. Ukraine's Expanding Long-Range Missile Arsenal: 'Neptune,' 'Palianytsia,' 'Peklo,' and 'Ruta' / UNITED24 Media. UNITED24 Media. Київ, 2025. URL: https://united24media.com/war-in-ukraine/ukraines-expanding-long-range-missile-arsenal-neptune-palianytsia-peklo-and-ruta-4392 (Access date: 20.11.2025).

222. Ukraine's Fight for Its People / O. Tokariuk. Chatham House. London, 2025. 20 p. URL: https://www.chathamhouse.org/2025/02/ukraines-fight-its-people (Access date: 05.12.2025).

223. Ukraine's Plan to Prosecute Collaborators / S. Morenets. Institute for War and Peace Reporting. London, 2022. 5 p. URL: https://iwpr.net/global-voices/ukraines-plan-prosecute-collaborators (Access date: 15.10.2025).

224. Ukraine's Propaganda Machine Grinds On, but Some Are Growing Weary. Kyiv Independent. Kyiv, 2024. 5 p. URL: https://kyivindependent.com/ukraines-propaganda-machine-grinds-on-but-some-are-growing-weary/ (Access date: 25.11.2025).

225. Ukraine's Sanctions Against Pro-Russian Oligarch Medvedchuk: All About Oil and Coal / A. Hurska. Jamestown Foundation. Washington, 2021. 5 p. URL: https://jamestown.org/program/ukraines-sanctions-against-pro-russian-oligarch-medvedchuk-all-about-oil-and-coal/ (Access date: 10.09.2025).

226. Ukrainian Diaspora. Danish Refugee Council. Copenhagen, 2023. 5 p. URL: https://drc.ngo/what-we-do/civil-society-engagement/diaspora-programme/ukrainian-diaspora/ (Access date: 20.10.2025).

227. Ukrainian Journalists Say State Security Spied on Them / V. Melkozerova. POLITICO. Brussels, 2024. 5 p. URL: https://www.politico.eu/article/ukrainian-investigative-journalists-uncover-state-security-service-spying-on-them-sbu-bihus-info/ (Access date: 05.11.2025).

228. Ukrainian National Identity: The "Other Ukraine" / A. Wilson. Wilson Center. Washington, 1999. 10 p. URL: https://www.wilsoncenter.org/publication/ukrainian-national-identity-the-other-ukraine (Access date: 15.12.2025).

229. Ukrainian National Identity: The "Other Ukraine" / V. Kulyk. Wilson Center. Washington, 2023. 20 p. URL: https://www.wilsoncenter.org/publication/ukrainian-national-identity-the-other-ukraine (Access date: 25.09.2025).

230. Unnatural Disasters: The Next Front in Russia's Hybrid War / M. Ince. Royal United Services Institute (RUSI). London, 2025. 6 p. URL: https://www.rusi.org/explore-our-research/publications/commentary/unnatural-disasters-next-front-russias-hybrid-war (Access date: 10.10.2025).

231. Updated Ukraine Recovery and Reconstruction Needs Assessment: February 2022 – December 2024. World Bank Group. Washington, 2025. 200 p. URL: https://www.worldbank.org/en/news/press-release/2025/02/25/updated-ukraine-recovery-and-reconstruction-needs-assessment-released (Access date: 20.11.2025).

232. Van Creveld M. The Transformation of War. Free Press. New York, 1991. 272 p. ISBN 978-0-02-933155-2 (Access date: 05.12.2025).

233. Van Creveld M. The Transformation of War. Free Press. New York, 1991. 272 p. ISBN 978-0-02-933155-2 (Access date: 15.10.2025).

234. Verified. 10 years of Revolution of Dignity. RUSpropaganda Rhetoric, Debunked. Ukrainian Crisis Media Center (UACRISIS). 2024. 10 p. URL: https://uacrisis.org/en/verified-10-years-of-revolution-of-dignity-ruspropaganda-rhetoric-debunked (Access date: 10.09.2025).

235. Verified. 10 years of Revolution of Dignity. RUSpropaganda Rhetoric, Debunked. Ukrainian Crisis Media Center (UACRISIS). 2024. 10 p. URL:

https://uacrisis.org/en/verified-10-years-of-revolution-of-dignity-ruspropaganda-rhetoric-debunked (Access date: 25.11.2025).

236. Vilnius Summit 2023: Cyber Defence Policy and Action Plan. NATO. Brussels, 2023. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (Access date: 20.10.2025).

237. Voytiv S. 'Ukraine's Cause is Ours!' Diaspora and Migration in Swedish Parliamentary Debates, 2014–2022. Nordic Journal of Migration Research. 2024. Vol. 14, no. 4. URL: https://journal-njmr.org/articles/10.33134/njmr.770 (Access date: 05.11.2025).

238. Wales Summit Declaration. NATO. Brussels, 2014. URL: https://www.nato.int/cps/en/natohq/official_texts_112964.htm (Access date: 15.12.2025).

239. War and Peace: Supporting Ukraine to Prevail, Rebuild, and Prosper. Open Society Foundations. New York, 2022. 6 p. URL: https://www.opensocietyfoundations.org/publications/ukraine-s-reconstruction-and-recovery (Access date: 10.10.2025).

240. War and Peace: Supporting Ukraine to Prevail, Rebuild, and Prosper. Open Society Foundations. New York, 2022. 6 p. URL: https://www.opensocietyfoundations.org/publications/ukraine-s-reconstruction-and-recovery (Access date: 25.09.2025).

241. War, Identity Politics, and Attitudes toward a Linguistic Minority: Prejudice against Russian-Speaking Ukrainians in Ukraine between 1995 and 2018 / L. Eras. Cambridge University Press. Cambridge, 2023. 22 p. DOI: 10.1017/nps.2021.100. URL: https://www.cambridge.org/core/journals/nationalities-papers/article/war-identity-politics-and-attitudes-toward-a-linguistic-minority-prejudice-against-russianspeaking-ukrainians-in-ukraine-between-1995-and-2018/0BE49EDCE7CABF8603FFAA99A63A9F7E (Access date: 05.12.2025).

242. War, Identity Politics, and Attitudes toward a Linguistic Minority: Prejudice against Russian-Speaking Ukrainians in Ukraine between 1995 and 2018 / L. Eras. Cambridge University Press. Cambridge, 2023. 22 p. DOI: 10.1017/nps.2021.100. URL: https://www.cambridge.org/core/journals/nationalities-papers/article/war-identity-politics-and-attitudes-toward-a-linguistic-minority-prejudice-against-russianspeaking-ukrainians-in-ukraine-between-1995-and-2018/0BE49EDCE7CABF8603FFAA99A63A9F7E (Access date: 20.11.2025).

243. Warsaw Summit Communiqué: Strategy Against Hybrid Threats. NATO. Brussels, 2016. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm (Access date: 15.10.2025).

244. Wartime TV in Ukraine: Much-Needed Unity or a 'Marathon of Propaganda'? RFE/RL. Prague, 2023. 5 p. URL: https://www.rferl.org/a/ukraine-telemarathon-media-zelenskiy-propaganda-russia-invasion/32515429.html (Access date: 10.09.2025).

245. Wartime TV in Ukraine: Much-Needed Unity or a 'Marathon of Propaganda'? RFE/RL. Prague, 2023. 5 p. URL: https://www.rferl.org/a/ukraine-telemarathon-media-zelenskiy-propaganda-russia-invasion/32515429.html (Access date: 25.11.2025).

246. Yee A. The country inoculating against disinformation. 2022. 31 січня. URL: https://www.bbc.com/future/article/20220128-the-country-inoculating-against-disinformation (Access date: 20.10.2025).

247. Yurchenko Y. Putin's Abuse of History: Ukrainian 'Nazis', 'Genocide', and a Fake Threat Scenario. Journal of Slavic Military Studies. 2022. Vol. 35, no. 1. P. 1–14. DOI: 10.1080/13518046.2022.2058179. URL: https://www.tandfonline.com/doi/full/10.1080/13518046.2022.2058179 (Access date: 05.11.2025).

248. Yurhenko, D. Russian Strategic Culture and the War in Ukraine. Foreign Policy Research Institute. 2024. URL: https://www.fpri.org/article/2024/07/russian-strategic-culture-and-the-war-in-ukraine/ (Access date: 15.12.2025).

249. Zagorodnyuk A. Putin's Black Sea blockade leaves millions facing global famine / Andriy Zagorodnyuk. Atlantic Council. Washington, DC, 2022. 17 травня. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/putins-black-sea-blockade-leaves-millions-facing-global-famine/ (Access date: 25.09.2025).

250. Zhurzhenko T. Ukraine's Border with Russia before and after the Orange Revolution. In: Ukraine Divided: Between East and West. BMLV. Vienna, 2005. P. 137–154. URL: https://www.bmlv.gv.at/pdf_pool/publikationen/ukraine_zerissen_zw_ost_u_west_m_malek_ukraines_border_t_zhurzhenko.pdf (Access date: 10.10.2025).