МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

МАРТИНОВА ВІКТОРІЯ ВОЛОДИМИРІВНА

Допускається до захисту:
завідувач кафедри міжнародних
відносин і зовнішньої політики
д.е.н., професор
_____ Лимар В. В.
«____» _____ 2025 р.

ТРАНСФОРМАЦІЯ МЕТОДІВ ГІБРИДНОЇ ВІЙНИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ (2014-2025 РР.)

Спеціальність 291. Міжнародні відносини, суспільні комунікації та регіональні студії

Магістерська робота

Науковий керівник:
Лещенко Л.В., професор кафедри
міжнародних відносин і зовнішньої політики
д. політ. н., професор

Оцінка: ____ / ___ / _____
(бали/за шкалою ECTS/за національною шкалою)

Голова ЕК:
Гижко А.П., доктор філософії з
політ. наук.

Вінниця- 2025

Мартинова В.В. Трансформація методів гібридної війни Російської Федерації проти України (2014-2025 рр.) Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії», ОП «Міжнародні комунікації та медіація в умовах конфліктного врегулювання». ДонНУ імені Василя Стуса, Вінниця, 2025.

Магістерська робота присвячена дослідженню трансформації ключових компонентів гібридної війни РФ проти України на різних етапах агресії: інформаційно-психологічні операції, кібератаки, політико- економічний тиск, та використання проксі-сил. У роботі здійснено хронологічний аналіз трансформації методів гібридної війни, порівняно особливості періоду після анексії Криму у 2014 році з тактиками, застосованими під час повномасштабного вторгнення 2022 року та наступних років.

Ключові слова: гібридна війна, російсько-українська війна, інформаційна війна, міжнародна безпека.

96 с. Бібліограф.: 128 найм.

Martynova V.V. Transformation of the Russian Federation's hybrid warfare methods against Ukraine (2014-2025). Specialty 291 “International Relations, Social Communications, and Regional Studies,”Educational Program “International Communications and Mediation in Conflict Resolution,”Vasyl’ Stus Donetsk National University, Vinnytsia, 2025.

The master's thesis is devoted to the study of the transformation of key components of the Russian Federation's hybrid war against Ukraine at various stages of aggression: information and psychological operations, cyberattacks, political and economic pressure, and the use of proxy forces. The thesis provides a chronological analysis of the transformation of hybrid warfare methods, comparing the features of the period after the annexation of Crimea in 2014 with the tactics used during the full-scale invasion of 2022 and subsequent years.

Keywords: hybrid war, Russian-Ukrainian war, information warfare, international security.

96 p. Bibliography: 128 items.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Початок XXI століття ознаменувався суттєвою трансформацією форм і методів воєнно-політичного протистояння, у межах яких гібридна агресія набула характеру однієї з найдинамічніших і найменш формалізованих феноменів сучасної міжнародної безпеки. Водночас науковий інтерес становить не стільки сама гібридна війна як явище, скільки процес еволюції її інструментарію, що змінюється під впливом нових технологій, міжнародної кон'юнктури та політичних рішень держав-агресорів. У цьому контексті особливо показовою є гібридна агресія Російської Федерації проти України, методи якої з 2014 року зазнали істотних змін — від прихованих та переважно невійськових операцій до масштабного поєднання військових дій з оновленими інформаційно-психологічними, кібернетичними, економічними й дипломатичними засобами впливу. Дослідження трансформації цих методів є актуальним, оскільки дозволяє встановити закономірності адаптації російської стратегії до змін міжнародного середовища та внутрішніх обмежень, а також окреслити специфіку сучасних багатовимірних загроз, що постають перед Україною та регіональною безпекою.

Теоретична значущість вивчення еволюції методів гібридної агресії РФ полягає в тому, що воно сприяє подальшому розвитку концептуальних підходів до аналізу гібридних конфліктів, дозволяє уточнити межі та зміст категорій, які описують взаємодію військових і невійськових засобів, а також поглиблює розуміння механізмів адаптивної поведінки держав-ревізіоністів у міжнародних відносинах. Крім того, аналіз російської практики розширює теоретичні уявлення про розмитість меж між станами миру, конфлікту й постконфліктного періоду, актуалізує потребу перегляду традиційних моделей стримування та безпекових режимів, що не враховують системного використання інформаційних, кібернетичних та економічних засобів у довготривалих конфліктах.

Практична актуальність дослідження визначається тим, що розуміння трансформації методів російської гібридної агресії створює можливості для більш обґрунтованого прогнозування подальших дій РФ, підвищення ефективності системи національної безпеки України та формування комплексних стратегічних комунікацій, спрямованих на протидію інформаційно-психологічним впливам. Отримані результати також можуть бути використані у вдосконаленні державної політики в галузі кібербезпеки, протидії дезінформації та кризового реагування, а їхнє практичне застосування сприятиме посиленню стійкості України до багатовимірних загроз сучасного конфліктного середовища.

Об'єкт дослідження - гібридна війна Російської Федерації проти України.

Предмет дослідження. Методи та інструменти гібридної агресії РФ, їхня еволюція й трансформація у 2014–2025 роках.

Мета і завдання дослідження. Метою роботи є визначення передумов, змісту та наслідків трансформації методів гібридної агресії Російської Федерації проти України у 2014–2025 роках, а також встановлення ключових чинників, що зумовили еволюцію інструментів гібридного впливу в зазначений період.

Для досягнення мети поставлено такі завдання:

- Розкрити теоретико-концептуальні підходи до розуміння феномену гібридної війни у світовій та українській науковій думці.
- Визначити основні засоби гібридної агресії РФ проти України після 2014 року.
- З'ясувати причини, зміст та наслідки трансформації гібридних методів Росії в умовах повномасштабної агресії 2022 року.
- Охарактеризувати роль нових технологій (кібератак, deepfake, соціальних мереж, ШІ) у сучасних гібридних конфліктах.

- Розкрити українські та міжнародні механізмів протидії гібридним загрозам.
- Розробити рекомендації щодо удосконалення механізмів протидії гібридним загрозам.

Хронологічні рамки дослідження відповідають часу тривалості російсько-української війни, охоплюють період з 2014 року до тепер.

Територіальні межі магістерської роботи охоплюють євроатлантичний регіон в просторовій інтерпретації ОБСЄ.

Наукова новизна дослідження. У роботі здійснено комплексний аналіз трансформації методів гібридної агресії РФ проти України в 2014–2025 рр., визначено етапи еволюції російського гібридного впливу, встановлено кореляцію між зовнішньополітичними подіями та активністю інформаційно-психологічних операцій. Крім того, висвітлено роль новітніх технологій, штучного інтелекту, кібератак, цифрових платформ в контексті досвіду російсько-української війни.

Науково-практична значущість дослідження. Практичне значення дослідження проявляється у його корисності для органів державної влади та безпекових структур, оскільки отримані результати можуть бути використані для вдосконалення стратегій протидії гібридним загрозам, розроблення ефективних підходів до захисту інформаційного простору, формування сучасної інформаційної політики та посилення системи стратегічних комунікацій. Для аналітичних центрів і експертного середовища матеріали роботи становлять підґрунтя для поглибленого аналізу проявів гібридної агресії, підготовки аналітичних звітів, вироблення рекомендацій державним інституціям і моделювання безпекових сценаріїв. У освітньо-науковому вимірі результати дослідження можуть бути використані у навчальних програмах із міжнародних відносин, безпекознавства та комунікацій, слугувати базою для подальших наукових розвідок, розроблення методичних матеріалів, а також сприяти розвитку нових напрямів, орієнтованих на вивчення сучасних форм гібридної агресії.

Апробація магістерського дослідження здійснена у формі наукової публікації:

- Мартинова В.В. Особливості російської концепції гібридної війни та її практичного втілення. *Вісник студентського наукового товариства Донецького національного університету імені Василя Стуса*. Випуск 17. Том 1 / Ред. кол. М.І. Прихненко (голова) та ін. Вінниця : ДонНУ імені Василя Стуса, 2025. Вип.17. Т.1. С.44-48. URL: https://jvestnik-sss.donnu.edu.ua/article/view/17288

- Мартинова В. «Інструменти російських маніпуляцій щодо вступу України до ЄС та механізми протидії». *Десятий збірник наукових статей і тез – «Політичні партії і вибори: українські та світові практики»*.

Структура роботи. Магістерська робота складається зі вступу, чотирьох розділів, 12 підрозділів, висновків, списку джерел і літератури. Її структура обумовлена метою та завданнями дослідження. Загальний обсяг становить 96 с.

РОЗДІЛ 1

СТАН ВИВЧЕННЯ ПРОБЛЕМИ, ДЖЕРЕЛЬНА БАЗА ТА МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

1.1. Основні підходи до розуміння гібридної війни

Поняття гібридна війна стала предметом активного наукового обговорення на Заході з кінця 1990-х років, після розпаду СССР та початком гібридних операцій РФ в Грузії та згодом в Україні. Для аналізу гібридної війни авторка пропонує класифікацію досліджень за основними підходами: західний (концептуально-аналітичний), український (прикладно-оборонний) та російський (доктринально-наступальний).

Одним з авторів західного підходу, хто суттєво сприяв формуванню цієї концепції гібридної війни, вважають Френка Гофмана. Він описував гібридну війну як сукупність різнорідних операцій, від звичайних військових дій до партизанських тактик, терористичних нападів, безпорядків, що разом утворюють єдину операційну стратегію [60]. За Гофманом, противники у гібридних конфліктах прагнуть створити максимальний вплив на державу, поєднуючи різні форми загроз і методів для виявлення та експлуатації її вразливих місць. Ключовою характеристикою таких конфліктів є конвергенція форм ведення бойових дій та дій суб'єктів конфлікту. Це проявляється у взаємопов'язаності військових, політичних, економічних, інформаційних і кіберзасобів, а також у розмиванні меж між державними та недержавними акторами, що ускладнює ідентифікацію джерел загроз та застосування традиційних методів протидії. Гофман підкреслював, що сучасна гібридна війна не обмежується лише прямими військовими діями. Велике значення мають інформаційно-психологічні операції (ІПСО), економічний і політичний тиск, кібератаки, саботаж і пропагандистські кампанії. Це дозволяє агресору послабити стійкість противника, підривати

його економічні й політичні структури, впливати на громадську думку та міжнародну репутацію держави, при цьому залишаючись у межах «сірого» правового простору. Концепція Гофмана стала базовою для подальших досліджень у сфері гібридної війни та була використана при формуванні національних стратегій безпеки у США, НАТО та ЄС. Велике значення мають інформаційно-психологічні операції, економічний і політичний тиск, кібератаки, саботаж і пропагандистські кампанії. Дана стратегія дозволяє агресору послаблювати стійкість противника: підривати роботу критичної інфраструктури й фінансових систем через кібератаки, створювати економічну вразливість через енергетичний шантаж чи торгові обмеження, дискредитувати державні інститути й делегітимізувати керівництво за допомогою цілеспрямованих інформаційних кампаній та технік соціального інженірингу. Одночасно використовуються методи «повзучої ескалації», тобто застосування проксі-формувань, підривних груп та «сірих зон» дій, що забезпечує політичну відмову від прямої відповідальності та ускладнює юридичну кваліфікацію атак[61].

ІПСО становлять одну з центральних складових сучасної гібридної війни. Їхня мета полягає не лише у спотворенні інформаційного простору противника, але й у трансформації сприйняття реальності, у формуванні бажаних моделей мислення, емоцій та поведінки цілих соціальних груп. На відміну від традиційної пропаганди, ІПСО діють комплексно поєднуючи медійний, психологічний, технологічний та культурний вплив. Саме через інформаційно-психологічні механізми Російська Федерація вибудовує свою гібридну стратегію, спрямовану на дестабілізацію супротивника без прямого збройного зіткнення. З позиції практичної протидії, гібридній війні, що були описані Гофманом, особливої уваги потрібно надати підходу «whole-of-society». Який включає в себе поєднання кіберзахисту та інвестування в стійкість критичної інфраструктури; розвиток систем раннього виявлення інформаційних атак; підвищення цифрової грамотності населення та прозорих комунікацій з боку держави; міжнародну координацію

у сфері атрибуції кібератак та запровадження правових механізмів для відповідальності акторів у «сірій зоні»[62].

Питання про те, чи слід вважати гібридну війну принципово новим явищем, залишається предметом наукових дискусій і сьогодні. Деякі дослідники звертають увагу на історичні приклади, де простежуються елементи, схожі на сучасні гібридні методи, зокрема під час Тридцятилітньої війни та наполеонівських кампаній. Так, у працях, таких як монографія В. Мюррея та П. Мансура «Гібридні бойові дії», показано, що комбінація військових операцій із політичними, економічними та пропагандистськими заходами використовувалася ще раніше; автори підкреслюють, що в різних конфліктах тією чи іншою мірою завжди присутній гібридний компонент, оскільки агресор, як правило, використовує наявні внутрішні суперечності суспільства [92].

Концепція «нових війн», запропонована М. Кальдор, є близькою до гібридних конфліктів і виділяється серед традиційних форм війни рядом ключових характеристик. Вона передбачає участь численних державних і недержавних акторів, боротьбу за контроль над владними інститутами замість територіального захоплення, а також прагнення отримати політичні та економічні вигоди без безпосередньої військової перемоги [81]. У сучасних умовах набувають поширення проксі-війни, коли основні держави реалізують свої стратегічні цілі через третіх осіб, що дозволяє досягати результатів без прямого залучення власних сил. Поряд із цим розвиваються «мережеві війни», які фокусуються на впливі в кіберпросторі, проникненні у державні та недержавні структури, а також на використанні інформаційних та технологічних ресурсів для досягнення стратегічних цілей [81]. Історично сформовані концепції непрямої дії, які у XX столітті наголошували на необхідності послаблення стійкості противника, отримали продовження в сучасних теоретичних підходах. Зокрема, Ліддел Гарт у праці про непряму стратегію обґрунтовував ідею, що дезорганізація сил ворога є дієвим засобом підриву їхнього опору [89]. Дж. Кеннан у концепції «політичної війни» (1948)

аргументував доцільність широкого використання невійськових засобів для досягнення політичних результатів, що є витоками розуміння сучасної російсько-української війни [83].

Переходячи до огляду формулювання гібридної війни українськими дослідниками, слід згадати про В.П. Горбуліна. У сучасних гібридних конфліктах особлива увага приділяється тісній інтеграції їхніх компонентів та посиленню ролі інформаційного фактора, що підкреслює В. П. Горбулін [6]. Він розглядає гібридну війну як комплексне явище, що поєднує військові та невійськові засоби для досягнення стратегічних цілей агресора у сучасному міжнародному середовищі. За його оцінкою, сучасні конфлікти, зокрема російсько-українська війна, демонструють поєднання квазімілітарних, дипломатичних, економічних та інформаційних засобів впливу, включно з елементами ядерного шантажу [6]. Горбулін наголошує, що такий підхід є цілеспрямованим і системним, а не випадковим набором тактик: він ґрунтується на використанні сучасних особливостей безпекового середовища, у тому числі територій «сірого простору», де співіснують демократичні та авторитарні режими. Однією з ключових рис сучасної гібридної війни, на думку Горбуліна, є інтеграція різнорідних компонентів конфлікту та посилення ролі інформаційного фактора. Він підкреслює, що гібридні конфлікти розвиваються у системній кризі міжнародного середовища та вимагають міждисциплінарного підходу для ефективного аналізу, особливо у безпековій сфері. При цьому традиційне уявлення про гібридні загрози як асиметричні дії слабшого проти сильнішого втрачає актуальність: досвід російської агресії демонструє, що потужний агресор може використовувати гібридні методи проти держав із відчутним потенціалом [6]. У науковому контексті Горбулін підкреслює, що термін «гібридна війна» є парасольковим, оскільки інтегрує різні форми впливу — від фізичних і психологічних до конвенційних і неконвенційних, державних та недержавних акторів. Ця конвергенція змінює традиційні уявлення про розмежування між тероризмом, іррегулярними військовими діями та класичними конфліктами, що дозволяє

сформувати цілісне розуміння сучасних стратегічних протистоянь і уникнути дублювання термінів [6].

За спостереженням Г. М. Перепелиці, гібридна війна характеризується асиметричністю конфлікту, коли одна зі сторін застосовує стратегії, що враховують дисбаланс сил і ресурсів. Перепелиця наголошує, що сутність гібридного протистояння полягає не лише у використанні нетрадиційних методів ведення бойових дій, але й у комплексному поєднанні військових, політичних, економічних та інформаційних інструментів для досягнення стратегічних цілей [16]. Особливою рисою, на думку Перепелиці, є гнучке використання різних форм сили, серед яких він виділяє «м'яку», «розумну» та «структурну» силу. «М'яка» сила включає культурні, інформаційні та психологічні засоби впливу, «розумна» сила — застосування стратегічного планування та технологій для досягнення цілей, а «структурна» сила передбачає використання політичних, економічних та адміністративних механізмів. Крім того, Перепелиця звертає увагу на зниження порогу для залучення нових суб'єктів у конфлікт, включно з недержавними акторами, що робить гібридну війну більш масштабною та складною для прогнозування.

Є. В Магда у своїх роботах, зокрема монографії «Світова гібридна війна: український фронт», аналізує російську гібридну агресію через призму інформаційної війни та пропагандистських кампаній. Особливу увагу придіяючи інформаційно-психологічним операціям, що становлять одну з центральних складових сучасної гібридної війни. На відміну від традиційної пропаганди, ІПСО діють комплексно, поєднуючи медійний, психологічний, технологічний та культурний вплив. Саме через інформаційно-психологічні механізми Російська Федерація вибудовує свою гібридну стратегію, спрямовану на дестабілізацію супротивника без прямого збройного зіткнення[89].

Поняття «гібридна війна» у російському стратегічному дискурсі має власну специфіку та суттєво відрізняється від західного розуміння. Офіційно російські військові теоретики та політичні діячі уникають вживання самого

терміну «гібридна війна» стосовно дій Росії, натомість активно використовують його для опису політики Заходу. У російському наративі саме США, НАТО та Європейський Союз нібито ведуть «гібридну війну» проти Росії через санкції, інформаційний вплив, підтримку України та розширення військово-політичних альянсів. Такий підхід формує основу для виправдання власних агресивних дій, які в російських джерелах подаються як «відповідь» або «захисна реакція». За не підтвердженими твердженями начальника Генерального штабу РФ Валерія Герасимова, гібридна війна трактується як форма сучасного протиборства, у якій пріоритет віддається «невійськовим засобам», а саме політичному, інформаційному, економічному та культурному впливу[9]. Самі ж московити назвали це трактування нібито «доктриною Герасимова». Вона нібито передбачає поєднання традиційних і нетрадиційних методів впливу, розмивання меж між війною і миром, а також активне використання пропаганди, кібероперацій і дезінформації.

Так звана «Доктрина Герасимова» вважається одним із концептуальних підґрунтів сучасного російського підходу до ведення гібридної війни. Її витоки пов’язують із нібито публікацією начальника Генерального штабу Збройних сил РФ Валерія Герасимова у 2013 році під назвою «Цінність науки у передбаченні»[129]. У цій статті Герасимов наголошував, що «самі правила війни змінилися: роль невійськових засобів досягнення політичних і стратегічних цілей значно зросла, а в багатьох випадках вони за ефективністю перевищують силу зброї»[129]. «Доктрина Герасимова» розглядає сучасний конфлікт як інтегрований процес, у якому військові дії є лише одним із компонентів системи гібридного впливу, що включає політичний, економічний та інформаційно-психологічний тиск. Інформаційне агентство «Оборонно промисловий кур’єр», підкреслює, що ця концепція спирається на постійне створення хаосу та нестабільності у країні-цілі, використовуючи як легальні, так і приховані механізми втручання, включно з проксі-силами, «зеленими чоловічками», бот-мережами та економічним шантажем[100;129]. Ключовою ідеєю цієї схеми є використання невійськових

засобів на ранніх етапах, коли дестабілізація досягається інформаційно-психологічними, політичними, дипломатичними чи економічними інструментами. Військова сила в такій моделі застосовується лише тоді, коли інші методи не забезпечують бажаного результату.

Підводячи підсумок слід сказати, західна та українська інтерпретації «гібридної війни», розглядають її як складне явище, що поєднує різнорідні методи впливу, від прямих військових дій до інформаційно-психологічних операцій, кібератак, економічного та політичного тиску. Ключові автори, такі як Френк Гофман, В. П. Горбулін та Г. М. Перепелиця, наголошують на системності та цілеспрямованості гібридних методів, інтеграції військових і невійськових компонентів, ролі інформаційного фактора, асиметричності конфлікту та використанні проксі-сил і «сірих зон». Українські дослідники підкреслюють необхідність превентивних заходів, включно з розвитком кіберзахисту, стійкості критичної інфраструктури, цифрової грамотності населення та міжнародної координації. У протилежність цьому, російська інтерпретація, відома як «доктрина Герасимова», має практичну та наступальну спрямованість. Вона розглядає сучасний конфлікт як інтегрований процес, де пріоритет віддається невійськовим засобам, а саме політичному, економічному, інформаційному та культурному впливу, а військова сила застосовується лише у разі необхідності. Доктрина Герасимова опирається на традицію радянських «активних заходів» та сучасні цифрові технології, що дозволяє системно створювати хаос і нестабільність у країні-цілі, при цьому легітимізуючи власні агресивні дії як відповідь на зовнішні загрози. Основна відмінність між підходами полягає в ролі та призначенні гібридних методів: на Заході та в Україні вони аналізуються як загроза, що потребує комплексної протидії, тоді як у російському дискурсі виступають інструментом досягнення стратегічних цілей та виправдання наступальної політики.

1.2. Джерельна база дослідження

Проведення комплексного аналізу феномену гібридної війни потребує опори на широку, багатовимірну та міждисциплінарну джерельну базу. Гібридна війна це явище, що поєднує військові, політичні, інформаційні, економічні та технологічні виміри, тому для її всебічного вивчення необхідно залучати документи найрізноманітніших типів від нормативно-правових актів і стратегічних доктрин, офіційних заяв, медійних публікацій і даних соціальних мереж. Такий підхід дозволяє поєднати правовий, політичний, військово-стратегічний і комунікативний аспекти гібридного протистояння, виявити механізми його реалізації та оцінити його наслідки у міжнародному контексті.

Першу групу джерел становлять нормативно-правові та стратегічні документи, у яких визначено офіційні підходи до розуміння та протидії гібридним загрозам. До таких належать Військова концепція протидії гібридній війні НАТО, що стала першим системним документом Альянсу, де було окреслено природу гібридних загроз як поєднання військових, політичних, економічних, інформаційних та кіберінструментів тиску[94]. Важливими доповненнями до неї є Декларація саміту НАТО у Велсі (2014), у якій гібридні загрози вперше були офіційно визнані фактором, що потребує колективної відповіді, та Комюніке Варшавського саміту (2016), де закріплено пріоритет посилення стійкості держав-членів і створення спеціалізованих механізмів для протидії гібридним атакам[95]. Ці документи мають високу джерельну цінність, оскільки відображають еволюцію офіційних підходів НАТО до розуміння гібридної війни як комплексного виклику, що вимагає координації військових, розвідувальних, дипломатичних і комунікаційних інструментів. Не менш важливими є Європейська стратегія протидії гібридним загрозам (EU Joint Framework on Countering Hybrid Threats, 2016) та Стратегія кібербезпеки ЄС (EU Cybersecurity Strategy, 2022), які визначають ключові напрями співпраці держав-членів Європейського

Союзу у сферах кіберзахисту, інформаційної безпеки, стратегічних комунікацій та протидії дезінформації[46]. Вони фіксують формування міжвідомчих механізмів координації, посилення обміну розвідданими між країнами-членами ЄС та НАТО, а також впровадження єдиних стандартів реагування на гібридні загрози. Окрему цінність для аналізу та розуміння гібридної війни, становлять Женевські конвенції 1949 року та додаткові протоколи до неї 1977 року, які заклали міжнародно-правові засади ведення війни, визначили статус комбатантів, цивільного населення та гуманітарних стандартів у збройних конфліктах[11, 8]. У контексті гібридних війн ці документи є важливими орієнтирами для оцінки порушень міжнародного гуманітарного права, зокрема щодо дій, які маскуються під «внутрішні конфлікти» або «миротворчі операції». Використання цих документів дає змогу обґрунтувати юридичну невизначеність гібридних агресій і вказати на необхідність адаптації міжнародного права до нових форм збройних дій, де межа між війною і миром, державним і недержавним актором часто стирається.

Другою групою джерел є документи міжнародних організацій та міждержавних інституцій, у яких відображено колективні зусилля світової спільноти у протидії гібридній агресії. Особливе значення мають аналітичні звіти та стратегічні огляди від Європейського Союзу, Організації Об’єднаних Націй, Гельсінської групи з прав людини та Європейського центру передового досвіду з протидії гібридним загрозам, у яких систематизовано практичний досвід реагування на нові форми конфліктів, а саме гібридну війну. Серед них вирізняються Hybrid CoE Strategic Reports (2021–2024), підготовлені Європейським центром передового досвіду з протидії гібридним загрозам (Гельсінкі), що діє під егідою ЄС. Ці звіти аналізують ключові тенденції розвитку гібридних операцій у XXI столітті, зокрема поєднання інформаційних, енергетичних, економічних та кіберінструментів у межах інтегрованих стратегій впливу. Значна увага приділяється механізмам

протидії дезінформації, розвитку стратегічних комунікацій, удосконаленню інституційної взаємодії держав-членів ЄС у сфері безпеки[74].

Важливим джерелом є щорічні звіти аналітичної ініціативи Європейської служби зовнішніх дій (EEAS), спрямованої на виявлення, документування та спростування гібридних дезінформаційних кампаній. У цих звітах простежується динаміка формування й поширення пропагандистських наративів, аналізуються методи використання соціальних мереж як інструменту впливу на громадську думку, а також окреслюються основні тенденції гібридних інформаційних операцій у контексті агресії Росії проти України[56].Окремий пласт документальної бази становлять звіти Гельсінської групи (Helsinki Commission Reports, 2014–2023), присвячені порушенням прав людини на окупованих територіях України та аналізу методів російської гібридної агресії під час анексії Криму[63]. У цих звітах детально описано механізми проведення гібридної агресії на півострові, а саме використання «зелених чоловічків» без розпізнавальних знаків, інформаційно-психологічні операції для легітимізації окупації, тиск на органи місцевого самоврядування та систематичне порушення норм міжнародного гуманітарного права. Зокрема, у доповіді «Окупація Криму Росією: наслідки для прав людини та міжнародної безпеки» підкреслюється, що анексія супроводжувалася масштабною кампанією дезінформації, спрямованою на створення ілюзії «внутрішнього конфлікту» й прикриття прямої військової участі Росії[64].

Третю групу становлять аналітичні та наукові дослідження, які відображають розвиток теоретичної думки щодо сутності, структури та динаміки гібридної війни як нового типу конфлікту XXI століття. До найважливіших належать праці таких авторів, як Френк Гофман «Гібридна війна та виклики», який увів у науковий обіг сам термін «гібридна війна» та визначив її як поєднання симетричних і асиметричних форм ведення бойових дій із використанням державних і недержавних акторів[67]. Філіп Карбер у своїй праці «Уроки гібридної війни Росії в Україні» розглянув практичні

прояви гібридних методів на прикладі російської агресії проти України, зокрема поєднання військових операцій, інформаційного тиску, кібератак та енергетичного шантажу[84]. Важливе місце займають і праці українських дослідників, передусім Валентина Горбуліна «Гібридна війна: сутність, структура, особливості», який запропонував системний підхід до аналізу гібридної агресії як цілісного процесу, де військові, інформаційні, економічні та політичні інструменти діють у взаємозв'язку[6]. Горбулін наголошує, що головна мета гібридної війни полягає не стільки у фізичному знищенні противника, скільки у підриві його стійкості. Також слід згадати й роботу Андрія Клименка «Морський вимір гібридної війни», де розкрито морський аспект гібридної агресії, зокрема захоплення та мілітаризацію Криму, блокування морських шляхів і використання морського простору для політичного тиску[14].

Підводячи підсумок, слід сказати, що дослідження феномену гібридної війни потребує комплексного, багатовимірного підходу. Нормативно-правові та стратегічні документи, аналітичні звіти міжнародних організацій, наукові та експертні праці, а також медіа-джерела й дані соціальних мереж дозволяють поєднати правовий, військово-стратегічний, політичний і комунікаційний аспекти гібридного протистояння. Такий підхід забезпечує розуміння не лише природи та механізмів гібридних загроз, а й їхніх наслідків для міжнародної безпеки, прав людини та інформаційного простору. Використання широкого спектра джерел дає можливість відтворити динаміку інформаційних кампаній, оцінити роль цифрових технологій у сучасних конфліктах і виявити закономірності координації дій державних та недержавних акторів. У цілому, багатовимірний аналіз джерельної бази дозволяє формувати науково обґрунтовані висновки щодо ефективних стратегій протидії гібридним загрозам та адаптації міжнародного права і національної політики до викликів XXI століття.

1.3. Методологічні засади дослідження

Методологічна основа дослідження ґрунтується на поєднанні системного, міждисциплінарного підходів та порівняльно-аналітичних методів, що дозволяють комплексно охопити феномен гібридної війни як багатовимірне політичне, інформаційне та воєнно-комунікаційне явище. Враховуючи складність і поліструктурність об’єкта, трансформації методів гібридної агресії Російської Федерації проти України у 2014–2025 роках, дослідження спирається на поєднання якісних і кількісних методів аналізу, що забезпечують об’єктивність і репрезентативність висновків.

У роботі використано системний підхід, який дозволяє розглядати гібридну агресію, у межах якої взаємодіють військові, політичні, економічні, інформаційні та психологічні компоненти. Це дало змогу визначити внутрішні зв’язки між елементами гібридного впливу, від інформаційно-психологічних операцій до енергетичного шантажу та простежити логіку їх трансформації протягом 2014–2025 років.

Історико-порівняльний аналіз було використано для виявлення еволюційних змін у стратегіях гібридної війни РФ. Порівняння періоду після анексії Криму та Донбасу у 2014 році з початком повномасштабного вторгнення 2022 року. Такий метод дозволив визначити зміни в тактиках, співвідношення військових і невійськових засобів, а також роль нових технологій кібероперацій, deepfake і штучного інтелекту у сучасних інформаційних кампаніях.

Метод контент аналізу, був спрямований на дослідження інформаційного виміру гібридної війни. Аналіз медіаповідомлень, матеріалів міжнародних аналітичних центрів, офіційних заяв, соціальних мереж та інформаційних кампаній дозволив простежити зміну наративів, тем і форматів інформаційно-психологічних операцій РФ. Цей метод був ключовим

при вивченні процесів дезінформації, функціонування координації інформаційних атак.

Також було використано індуктивно-дедуктивний методологічний прийом, який сприяв формуванню узагальнених висновків на основі емпіричних спостережень. Дедуктивна логіка дозволила перевірити гіпотези щодо закономірностей розвитку російського гібридного інструментарію та його впливу на міжнародну безпеку. Метод структурно-функціонального аналізу дав змогу визначити роль окремих елементів гібридного впливу (проксі-сил, кібератак, енергетичного тиску, інформаційних кампаній) у загальній стратегії агресора та їхню взаємодію у межах єдиної системи. Крім того, застосовано метод аналізу документів, а саме вивчення нормативно-правових актів, стратегій національної безпеки, військових доктрин РФ і міжнародних звітів, що забезпечило емпіричну базу для дослідження. Залучення міждисциплінарного підходу дозволило інтегрувати знання з галузей міжнародних відносин, політології, інформаційних технологій і комунікаційних студій.

У сукупності використані методи дали змогу побудувати комплексну картину трансформації гібридних загроз, виявити їхні закономірності, інструменти реалізації та наслідки для державної й міжнародної безпеки України. Такий методологічний підхід забезпечує системність, наукову обґрунтованість і практичну цінність отриманих результатів.

РОЗДІЛ 2
СТАНОВЛЕННЯ ОСНОВНИХ МЕТОДІВ ГІБРИДНОЇ ВІЙНИ РФ ПРОТИ УКРАЇНИ

2.1. Гібридизація політичного та економічного тиску

Гібридні війни у сучасному міжнародному середовищі нерідко охоплюють енергетичний вимір, що прямо пов’язаний із методами економічного та політичного тиску. Тоді, коли ресурси, такі як газ чи нафта, перетворюються на інструменти тиску не лише на Україну, а й на весь колективний Захід. Даний розділ охоплює основні витоки становлення методів гібридної агресії РФ проти України та початок латентної форми агресії з 2014 по 2022 рік.

Одним із найпомітніших прикладів використання енергетики як засобу впливу є політика Російської Федерації, яка системно застосовувала природний газ як інструмент шантажу щодо України та Європейського Союзу. Після розпаду Радянського Союзу Російська Федерація розпочала активне використання енергетичного чинника як засобу реалізації своїх зовнішньополітичних цілей. Україна, яка залишалася значною мірою залежною від російських енергоносіїв, мала для Кремля стратегічне значення у контексті прагнення відновити вплив на пострадянському просторі. У першій половині 1990-х років українська держава не володіла розвинутими механізмами переходу на альтернативні джерела енергоресурсів, що давало змогу Росії ефективно використовувати постачання газу та нафти як політичний важіль тиску. Показовим у цьому контексті є інцидент березня 1995 року, коли російська компанія «Газпром» звинуватила Україну у несплаті за постачання природного газу та пригрозила припиненням його експорту[42]. У якості «вирішення» конфлікту російська сторона запропонувала Києву передати частину прав на управління українською

газотранспортною системою. Втім, український уряд відмовився від такої пропозиції, що призвело до подальшого загострення двосторонніх відносин. Водночас Україна намагалася використовувати своє транзитне становище як важливий аргумент у переговорах і фактор досягнення компромісів з Москвою.

Газова агресія з боку Росії розпочалася задовго до повномасштабного вторгнення 2022 року й набула чітких форм під час так званих «газових криз» 2006 та 2009 років, коли російська сторона припиняла транзит блакитного палива через територію України. Така тактика мала на меті покарання держав, що прагнули зменшити залежність від російського впливу [78]. Європейський інститут з питань безпеки охарактеризував події 2006 і 2009 років як «тривожний сигнал» для європейської енергетичної політики, що виявив критичну вразливість ЄС до зовнішнього енергетичного тиску [54]. Ці кризи фактично стали поворотним моментом у ставленні Європейського Союзу до енергетичного партнерства з Росією. Під час конференції у Вільнюсі 2006 року, у питанні енергетичних відносин з РФ, вперше по відношенню РФ було офіційно вжито термін «енергетична зброя». Тодішній віце-президент США Дік Чейні наголосив, що Росія використовує нафту й газ як засіб шантажу, маніпулюючи обсягами постачання та прагнучи встановити монополію на транспортні маршрути енергоресурсів [54]. Відтоді компанія «Газпром» почала сприйматися міжнародною спільнотою не як комерційний суб’єкт, а як інструмент Кремля для реалізації геополітичних цілей.

Після анексії Криму у 2014 році енергетичний вимір гібридної війни Росії проти України та Заходу набув системного характеру. Москва почала активно використовувати контроль над поставками газу як засіб політичного економічного тиску. У 2014–2015 роках «Газпром» неодноразово обмежував постачання палива до України, вимагаючи підвищення цін і відмови від закупівель з Європи[79]. У 2014 році Росія знову вдалася до енергетичного шантажу, підвищивши ціну на газ до 485 доларів США за тисячу

кубометрів[122]. Це призвело до чергового раунду напружених переговорів між Києвом і Москвою. У відповідь Україна активізувала політику диверсифікації енергетичних ресурсів, розпочала розбудову власної енергетичної інфраструктури та розвиток альтернативних джерел постачання, що поступово зменшувало її залежність від російських енергоносіїв.

У 2016 році Росія оголосила про плани повністю припинити транзит через українську газотранспортну систему після завершення контракту у 2019 році, що супроводжувалося політичним тиском на європейських споживачів і спробами реалізувати обхідні маршрути [79]. Паралельно Кремль просував проєкти «Турецький потік» і «Північний потік-2», які мали стратегічну мету зменшити роль України як транзитної держави та посилити енергетичну залежність Європейського Союзу від російського газу.

У 2018 році російська сторона штучно зменшувала обсяги постачання до країн Центральної Європи, створюючи дефіцит і зростання цін на ринку, що збігалося з політичними подіями в Україні, зокрема підготовкою до виборів [30]. Європейська комісія кваліфікувала такі дії як маніпуляцію ринком та порушення принципів добросовісної конкуренції. У 2021 році Росія повторила цю тактику, скоротивши транзит через українську територію та не заповнюючи свої підземні газові сховища у Німеччині та Австрії [29]. Ці кроки призвели до рекордного зростання цін на енергоносії напередодні зими та мали на меті змусити Європейський Союз якнайшвидше погодити запуск «Північного потоку-2». Таким чином упродовж 2014–2022 років Росія послідовно застосовувала енергетичну зброю як інструмент гібридного тиску, поєднуючи економічні, політичні та інформаційні методи впливу для досягнення стратегічних цілей. Тобто, як можна побачити з попереднього аналізу, енергетична залежність від Російської Федерації є одним із найсерйозніших ризиків для безпеки Європейського Союзу. У відповідь на агресію проти України ЄС ухвалив рішення про повну відмову від імпорту російського газу до 2027 року[45]. Такий крок став стратегічним зрушенням

у європейській енергетичній політиці та завдав значних економічних збитків російській стороні. За даними фінансових звітів, «Газпром» втратив понад 7 мільярдів доларів США, а видобуток газу скоротився майже на чверть.

Як було згадано раніше, до 2022 року Російська Федерація послідовно використовувала енергетичну залежність Європи як інструмент політичного впливу, прагнучи через шантаж домогтися добудови проєкту «Північного потоку-2» і зберегти своє домінування на європейському ринку газу. Проте європейська спільнота, після початку повномасштабного вторгнення РФ на територію України, розпочала активні кроки щодо диверсифікації джерел постачання та розвитку відновлюваної енергетики. Запустивши нові проєкти у межах Євросоюзу, а саме ініціатива з підвищення енергетичної незалежності ЄС (RePowerEU) та проект по підтримці агрополітики ЄС (AgricultureEU). Ця політика стала потужним ударом по російській енергетичній стратегії, адже перетворила колишню перевагу Кремля на стратегічну вразливість. Попри структурні зміни у сфері енергетики, Росія залишалася небезпечним чинником на європейських енергоринках. Її спроби монополізувати поставки природного газу тривалий час створювали ризики дестабілізації енергопостачання в Європі. Основною передумовою цієї ситуації стала політика ЄС, орієнтована на поступовий перехід до екологічно чистих джерел енергії. Через скорочення видобутку вугілля, опір розвитку атомної енергетики та зменшення власного видобутку газу європейські країни були змушені покладатися на дешевий імпорт з Росії, що посилювало їхню вразливість до політичного шантажу.

З початком повномасштабної війни у 2022 році Росія перейшла до відкритого застосування військових методів енергетичного тиску. Масовані ракетні удари та атаки безпілотників по об’єктах критичної інфраструктури мали на меті дестабілізувати енергетичну систему України та спричинити гуманітарну кризу. Попри значні втрати, завдяки міжнародній підтримці, оперативному відновленню об’єктів і посиленню системи протиповітряної оборони українська енергосистема зберегла стабільність. Унаслідок цих дій,

лише за листопад 2024 року, було пошкоджено або зруйновано 25 теплових електростанцій, 7 гідроелектростанцій та 2 об’єкти відновлюваної енергетики. Крім того, понад 100 ударів припало на мережі передачі та розподілу електроенергії [32].

Підводячи підсумок слід сказати, як це видно з попереднього аналізу, Російська Федерація використовує природний газ і нафту як інструмент політичного та економічного тиску Ця практика проявлялася ще з 1990-х років, посилилася під час «газових криз» 2006 та 2009 років, а після анексії Криму у 2014 році набула системного характеру. Росія обмежувала постачання газу, підвищувала ціни, просувала проєкти «Північний потік-2» і «Турецький потік», намагаючись зменшити роль України як транзитної держави та посилити енергетичну залежність ЄС. У відповідь Європейський Союз реалізує політику диверсифікації джерел постачання та розвитку відновлюваної енергетики, що значно зменшує стратегічну перевагу РФ у регіоні. Крім енергетичного тиску, Кремль активно застосовує політичні та інформаційні методи впливу. В Україні з початку 2000-х років російські спецслужби втручалися у вибори, підтримуючи проросійських кандидатів. Аналогічні практики спостерігаються в інших країнах Центрально-Східної Європи, зокрема в Румунії під час президентських виборів 2024–2025 років, а також у США в 2016 році. Метою цих дій є не лише підтримка проросійських сил, а й підрив довіри громадян до демократичних процедур, посилення внутрішніх розколів і дестабілізація політичних систем. Таким чином, Російська Федерація використовує комплексний підхід у гібридних війнах, поєднуючи економічний, політичний та інформаційний тиск для досягнення стратегічних цілей, а країни-об’єкти впливу змушені застосовувати механізми диверсифікації та протидії для збереження своєї безпеки й стабільності

2.2. Використання проксі-сил та маріонеткових режимів у гібридній агресії

Проксі-сили та маріонеткові режими стали одними з ключових інструментів гібридної агресії Російської Федерації проти України, почалося це в період після анексії Криму у 2014 році та початку збройного конфлікту на сході України. Використання таких форм впливу відповідає концепту російської стратегічної думки, закріпленій у «Воєнній доктрині РФ» (2014), «Доктрині інформаційної безпеки РФ» (2016) та низці інших нормативних документів, що передбачають можливість застосування непрямих методів досягнення політичних та стратегічних цілей без формального оголошення війни [5].Така стратегія дозволяє Кремлю створювати ситуації нестабільності у сусідніх державах, легітимізувати власні військові дії та мінімізувати ризики прямого міжнародного засудження. З 2014 року, РФ використовувала практику використання «зелених чоловічків» і «ополченців» у Криму та на Донбасі.

Проксі-сили в рамках гібридної війни виступають як проміжний механізм впливу, який включає підтримку місцевих озброєних формувань, фінансове забезпечення, підготовку кадрів та координацію політичних та військових дій через приховані канали. Першими такими силами, стали так звані «зелені чоловічки», використані путінським режимом на території Криму у 2014 році[13]. 20 лютого 2014 року Росія розпочала окупацію Криму, того ж дня на півострові з'явилися вантажівки без номерних знаків і озброєні військові без розпізнавальних знаків, яких називали «зеленими чоловічками». 26 лютого 2014 року біля будівлі Верховної Ради Автономної Республіки Крим відбулися дві масштабні акції з протилежними політичними позиціями[13]. Проукраїнський мітинг, організований Меджлісом кримськотатарського народу, рухом «Євромайдан Крим» та іншими громадськими організаціями, об’єднав близько 10 тисяч учасників, які висловлювали підтримку територіальній цілісності України та протестували

проти можливого втручання Росії у справи півострова [107]. Одночасно відбувся проросійський мітинг, у якому взяли участь приблизно 700 осіб. Його ініціювала партія «Руська єдність», учасники якої вимагали проведення референдуму щодо відокремлення Криму від України[107].27 лютого «зелені чоловічки», здійснили операцію із захоплення ключових адміністративних будівель у Сімферополі, а саме Ради міністрів Автономної Республіки Крим. Після захоплення над спорудами було піднято російський прапор. За даними українських офіційних джерел, у цій операції брали участь розвідувально-диверсійні групи 45-го окремого полку спеціального призначення Повітрянодесантних військ РФ[27]. Того ж дня, під контролем озброєних російських військових, кримський парламент оголосив про намір провести так званий «референдум» щодо приєднання Криму до Російської Федерації [26]. Ця подія стала переломним моментом у реалізації російського плану анексії півострова. Упродовж наступних днів використовувані РФ проксі-сили, «зелені чоловічки», зайняли всі військові стратегічні об'єкти на всій території Криму.

Щодо заяв президента РФ Володимира Путіна щодо питання поширення «зелених чоловічків на півострові», то він неодрозово заявляв «нас там немає», а також наголошував, що на півострові замість збройних сил РФ, знаходяться «загони самооборони», що складаються із небайдужих українців-патріотів РФ [19]. Також було заявлено, що контингент даних загонів самооборони складають близько 22 тис. осіб, які під час анексії Криму відібрала зброю у українських збройних сил, що були на півострові на початку окупації його [19]. На той час Росія неодноразово відмовлялася визнавати свою причетність до цих подій, заявляючи, що ці озброєні люди не є російськими військовими. Однак через 44 дні після окупації Криму та проведення фейкового референдуму «про статус Криму» Москва зрештою визнала «зелені чоловічки» – це російські солдати.

Продовжуючи огляд парадигми використання проксі сил на території Криму, слід згадати й про питання використання тактики «живих щитів».

Дослідження, презентоване Українською Гельсінською Спілкою з прав людини, Представництвом Президента України в Автономній Республіці Крим, Прокуратурою АРК та Регіональним центром прав людини (РЦПЛ), отримало назву «Окупація Криму: без знаків, без імен, ховаючись за спинами цивільних» [106]. Воно детально аналізує заборонені методи ведення війни, які Російська Федерація застосовувала під час окупації Криму в 2014 році. Основна увага в дослідженні приділяється тактикам, що суперечать міжнародним гуманітарним нормам. Одним з головних аспектів під час окупації Криму було використання так званих «живих щитів», тобто, примусове залучення цивільного населення для захисту військових об'єктів та підрозділів РФ на території півострову [106].Слід зазначити, що дана тактика прямо порушує основні принципи міжнародного права, зокрема Женевські конвенції, які забороняють використання цивільних осіб в якості щитів у воєнних діях [106]. Дослідження також вказує на відсутність розпізнавальних знаків у російських військових підрозділах, що здійснювали захоплення Криму, а також на тактику маскування російських військ під цивільних осіб або представників місцевих правоохоронних органів для створення ілюзії «легітимності» дій. Також слід згадати й про незаконне використання емблем, форм та уніформи українських силових структур, зокрема ВМС та тодішньої міліції [106]. Такі дії створювали плутанину і дозволяли «зеленім чоловічкам» маскувати свої операції під захоплення українських об'єктів. Олександра Дворецька, кримчанка, що пережила ці події, згадує, як вона стала свідком ситуації на вокзалі, коли міліція спочатку давала одну інформацію, а потім з'являлися люди з російським акцентом, які все заперечували[10]. Відповідно до висновків, наведених у дослідженні Гельсінської групи, так звані «зелені чоловічки» представляли собою військовослужбовців Російської Федерації, одягнених у форму без розпізнавальних знаків, що дозволяло Москві заперечувати свою безпосередню участь у захопленні Криму. У ході операції російська сторона також активно застосовувала тактики, які передбачали використання

цивільного населення для блокування українських військових частин, що створювало додаткові труднощі для оборони та мінімізувало можливість відкритого спротиву. Крім того, Росія вдалася до дезінформаційних і маніпулятивних дій, спрямованих на введення українських військових в оману та нейтралізацію їхніх дій. Поєднання прихованого військового втручання, інформаційного впливу та ефекту раптовості забезпечило швидке встановлення контролю над територією півострова.

Продовжуючи огляд питання використання «зеленими чоловічками», цивільного населення, під час окупації Криму, слід згадати й про реакцію міжнародної спільноти на це. Згідно зі статтею 8 Римського статуту Міжнародного кримінального суду, використання "живих щитів" слід кваліфікувати як воєнний злочин [71]. Це порушення також закріплене в статті 28 IV Женевської конвенції, статті 51 Додаткового протоколу до Женевських конвенцій і нормі 97 звичаєвого міжнародного гуманітарного права. Крім того, умисне використання цивільних осіб для прикриття військових операцій порушує зобов'язання щодо застосування всіх можливих заходів обережності для розрізнення цивільних та військових об'єктів [77].

У лютому 2019 року до Міжнародного кримінального суду було подано нове повідомлення, що стосувалося використання Росією цивільного населення як «живих щитів» під час захоплення об'єктів на території Криму в 2014 році[11]. Це повідомлення було підготовлено Українською Гельсінською спілкою з прав людини (УГСПЛ), Регіональним центром прав людини (РЦПЛ) і прокуратурою АР Крим. Як було згадано раніше, російські військові (тоді ще «зелені чоловічки»), використовували цивільних як живі щити, перебуваючи за їхніми спинами в момент захоплення воєнних об’єктів на території півострову. Цивільне населення, яке становило цей «живий щит», включало кілька категорій людей: кримчан, які мали як проросійські, так і проукраїнські погляди; цивільних осіб, переміщених з Росії; представників казачества та так званої «Кримської самооборони»[66]. До того ж, серед учасників були й інші особи, зокрема сербські четники, які

брали участь у захопленнях[67]. Згідно з результатами дослідження Української Гельсінської спілки з прав людини (УГСПЛ), у процесі окупації Криму російські сили застосовували тактику залучення цивільного населення як «живого щита» під час захоплення українських військових об’єктів. Зафіксовано, що таким способом було захоплено щонайменше десять об’єктів Збройних сил України, до чого було залучено понад тисячу цивільних осіб. Одним із найяскравіших прикладів є штурм військово-морської бази в селищі Новоозерне, де у блокуванні брали участь понад триста осіб, серед яких були чоловіки, жінки, підлітки та люди похилого віку [67].

У межах російської інформаційно-психологічної операції, спрямованої на легітимізацію окупації Криму, ключовим інструментом стала поява терміну «ввічливі люди» — евфемізму, який запровадив проросійський блогер Борис Рожин. Цим визначенням позначалися озброєні військові без розпізнавальних знаків. Використання цього образу мало чітко пропагандистський характер, адже воно покликане нейтралізувати сприйняття російських сил як агресорів і створити ілюзію їхньої «миротворчої місії» та «захисту населення Криму». Згідно з повідомленнями Служби безпеки України, Борис Рожин, який діяв під псевдонімом Colonel Cassad, є одним із головних інформаційних рупорів Кремля[24]. Він розпочав активну діяльність ще під час анексії Криму, перебуваючи тоді на півострові як фрилансер, а згодом очолив окупаційне інтернет-видання «Голос Севастополя», що поширювало дезінформацію та фейки про події в Україні. Термін «ввічливі люди» («зелені чоловічки», «іхтамнєти») став популярним мемом, що використовувався для позначення російських військових, які були одягнені у військову форму без знаків розрізнення і захоплювали стратегічні об'єкти на території українського Криму під час його анексії Росією в 2014 році[1]. Спочатку Росія заперечувала участь своїх військ у захопленні Криму, і цей термін активно використовувався російськими ЗМІ для маскування факту вторгнення. Термін «ввічливі люди» швидко увійшов у вжиток в

російських ЗМІ в кінці лютого на початку березня 2014 року, коли стратегічні об'єкти в Криму були захоплені людьми в камуфляжній формі без розпізнавальних знаків. Однак 17 квітня 2014 року президент РФ Володимир Путін публічно визнав, що «ввічливими людьми» були саме російські військові [18].

Після початку збройного конфлікту на сході України у 2014 році Російська Федерація активно застосувала проксі-сили також і для захоплення територій Донецької та Луганської областей. Основу цих сил становили нібито місцеві збройні формування, яких в російській пропаганді прозвали «ополченцями» (так зване «народне ополчення Донбасу»). На початкових етапах гібридного протистояння, в Донецьку та Луганську були сформовані групи з цих ополченців, що згодом ввійшла до «Армії Новоросії». «Місцеві ополченці» виконували низку завдань від блокування українських військових частин та контролю ключових об’єктів інфраструктури до підтримки діяльності адміністративних органів та забезпечення безпеки під час проведення «референдумів» щодо створення бананових республік ДНР та ЛНР. Однією з ключових тактик цих проксі сил, було маскування особового складу. «Ополченці» (замасковані російські військові) діяли під виглядом цивільних осіб, використовували одяг без розпізнавальних знаків та використовували форму і символіку українських силових структур.

У березні 2014 року члени так званих «народних дружин» під керівництвом Олександра Захарченка діяли як місцеві формування, що на початковому етапі нібито підтримували правопорядок і навіть протистояли радикальнішим групам «Народного ополчення Донбасу» (НОД). Водночас і ті, і інші сповідували антиукраїнські позиції[33]. Якщо представники колишніх «регіоналів» та пов’язаних із ними структур виступали за федералізацію й розширення автономії в межах України, то НОД орієнтувалося на відокремлення регіону та підтримувало деструктивні заклики до захоплення адміністративних споруд і дестабілізації ситуації. У квітні 2014 року діяльність «Народного ополчення Донбасу» стала більш

організованою. Його учасники долучилися до операцій із захоплення адміністративних будівель у Слов'янську та Краматорську спільно з озброєним формуванням під командуванням Ігоря Гіркіна (Стрєлков), який прибув з території Російської Федерації[128]. Після захоплення об'єктів стратегічного значення було зведено барикади та блокпости, що символізувало початок фактичного встановлення контролю над частиною Донбасу поза межами українського урядування. Перші серйозні збройні сутички між незаконними формуваннями та підрозділами Збройних сил України сталися 15 квітня 2014 року в районі Краматорська[69]. Наступного дня бойовики здійснили спробу штурму військової частини у Маріуполі. 22 квітня під Слов'янськом вони відкрили вогонь по українському військовому літаку. До кінця травня тривали локальні бої, штурми військових об'єктів і напади на авіацію, зокрема, 25 квітня ополченці збили гелікоптер Мі-8, а 2 травня українські сили провели масштабну антитерористичну операцію зі звільнення Слов'янська та Краматорська, під час якої було знищено щонайменше три українські гелікоптери[69].У Маріуполі бойові дії також супроводжувалися захопленням адміністративних будівель, зокрема міської ради. 16 квітня відбулася спроба штурму місцевої військової частини, а в ніч із 6 на 7 травня неподалік Мангуша сталася збройна сутичка між бойовиками «Народного ополчення Донбасу» та підрозділом добровольчого батальйону «Азов»[69].

Аналіз застосування Російською Федерацією проксі-сил та формування маріонеткових режимів свідчить, що цей інструментарій став фундаментальною складовою гібридної агресії проти України. Починаючи з окупації Криму у 2014 році, Росія системно використовувала нелегальні збройні формування, без розпізнавальних знаків та контрольовані «народні ополчення» для досягнення своїх політичних і воєнних цілей без офіційного оголошення війни. Тактика «зелених чоловічків» у Криму, а згодом створення груп «ополченців» на Донбасі стали зразком класичної моделі проксі-війни, що поєднує військові, політичні та інформаційно-психологічні

елементи. Використання таких сил дозволило Кремлю запровадити контроль над окупованими територіями, легітимізувати власну агресію через створення ілюзії «внутрішнього конфлікту» та уникнути прямої відповідальності на міжнародному рівні. Одночасно це сприяло дестабілізації України зсередини, підриву її обороноздатності й політичної цілісності. У Криму це проявилося у поєднанні військових і пропагандистських дій, зокрема в поширенні образу «ввічливих людей» як миротворців, тоді як насправді йшлося про спецпідрозділи Збройних сил РФ. На Донбасі проксі-механізм еволюціонував у більш масштабну форму, а саме формування квазідержавних структур «ДНР» і «ЛНР», які де-факто перебували під російським військово-політичним контролем.

Застосування Росією проксі-сил супроводжувалося системними порушеннями міжнародного гуманітарного права, використанням цивільних осіб як «живих щитів», незаконним захопленням об’єктів, дезінформацією та пропагандою. Це підтверджується документами Української Гельсінської спілки з прав людини, звітами міжнародних правозахисних організацій і розслідуваннями Міжнародного кримінального суду. Таким чином, досвід 2014 року демонструє, що стратегія проксі-впливу є системним і свідомо інтегрованим елементом російської гібридної війни. Вона забезпечує Москві гнучкість, можливість маневрування між відкритими й прихованими формами агресії та створює умови для подальшої ескалації конфлікту під виглядом «внутрішнього протистояння». Ця модель, відпрацьована на прикладі Криму й Донбасу, надалі стала універсальним інструментом російської зовнішньої політики, спрямованої на підрив суверенітету сусідніх держав.

2.3. Інформаційно-психологічні операції як ключовий елемент гібридної війни

Упродовж останніх років інформаційно-психологічні операції РФ проти України набули системного характеру й проявляються в низці взаємопов'язаних тактик, що мають як стратегічні, так і тактичні цілі. Однією з таких тактик є просування «миротворчих» наративів, у межах яких прокремлівські медіа та координаційні мережі наполегливо поширюють меседжі про нібито відкинуті «реальні» мирні ініціативи Україною або про те, що лише Росія пропонує «справжній» мир. Мета цієї кампанії полягає в підриві довіри до українського керівництва, загостренні внутрішніх розколів і створенні умов для міжнародної легітимації позицій агресора; документування таких кампаній міститься в звітах «ЄС проти дезінформації» (EUvsDisinfo) та «Лабораторії цифрової криміналістики» (DFRLab).

ІПСО виступають одним із центральних інструментів сучасної гібридної війни, що поєднує традиційні військові дії з комплексом економічних, політичних та соціально-психологічних методів впливу. Сутність ІПСО полягає у цілеспрямованому використанні інформаційного простору для формування певних уявлень, переконань і поведінки цільових аудиторій, зокрема громадян, політичних еліт і міжнародної спільноти.У контексті гібридної агресії проти України його роль стає особливо помітною. Російська Федерація активно застосовує широкий спектр інструментів, що включають масовану пропаганду через соціальні мережі, маніпуляції традиційними медіа, поширення фейкової інформації, створення координаційних мереж бот-акаунтів, а також організацію кампаній із дискредитації політичних інститутів і керівництва країни. Такі дії спрямовані на підрив довіри до державних структур, деморалізацію населення, а також легітимізацію власних політичних і військових дій на міжнародній арені.

Інформаційно-психологічні операції є центральним елементом сучасної гібридної війни та спрямовані на маніпулювання суспільною свідомістю, послаблення внутрішньої єдності держави-жертви та вплив на міжнародну аудиторію. Гоффман, один із засновників поняття «гібридна війна», визначає її як тип військової стратегії, що поєднує традиційні засоби ведення бойових

дій із нетрадиційними методами, такими як дії парамілітарних формувань, економічний тиск, санкції та поширення пропаганди і фейкових новин, що впливають на моральний стан противника[67]. Такий комплексний підхід дозволяє агресору одночасно атакувати військові, економічні та психологічні аспекти функціонування держави. З погляду Гоффмана, ІПСО не є суто допоміжним засобом; вони формують центральний елемент гібридної стратегії, оскільки дозволяють агресору одночасно впливати на політичні, соціальні та психологічні аспекти функціонування держави-жертви. Інформаційно-психологічні операції охоплюють створення та поширення дезінформації, маніпуляції медійними наративами, використання цифрових платформ і соціальних мереж для координованих кампаній, а також масові інформаційні хвилі, спрямовані на делегітимацію влади, підірвання довіри до інститутів і стимулювання внутрішньополітичних конфліктів. Гоффман також підкреслює, що ІПСО у гібридній війні діють на перетині кількох рівнів: стратегічного, операційного та тактичного. На стратегічному рівні вони спрямовані на формування міжнародної думки та вплив на політику держав-партнерів[67]. Стоуелл підкреслює, що гібридна війна реалізується як «нелінійна війна», у якій психологічні, економічні, політичні та кібернетичні методи взаємодіють для створення системного тиску на державу-жертву[113].

Використання інформаційних кампаній у цифровому середовищі, координація бот-мереж та маніпуляції у соціальних медіа дозволяють формувати потрібні наративи, делегітимізувати владу та посилювати внутрішньополітичні протиріччя. Особливо ефективними у сучасній гібридній війні є цифрові платформи та соціальні мережі. Використання координації бот-мереж, автоматизованих акаунтів і «тролінгових фабрик» дозволяє створювати масові інформаційні хвилі, які формують потрібні наративи, поширюють дезінформацію та делегітимізують органи влади. Такий підхід дає змогу агресору одночасно впливати на національну політику, суспільну думку й міжнародне сприйняття конфлікту, поєднуючи фізичний тиск з психологічним та інформаційним впливом. Стоуелл також

підкреслює, що нелінійний характер гібридної війни полягає в тому, що агресор не обмежується прямим військовим тиском, а створює комплексний ефект через інтегроване використання різних сфер впливу. Це включає економічний шантаж, кібератаки, інформаційні маніпуляції та дипломатичні дії, які в сукупності підривають стабільність держави-жертви та змінюють поведінку її ключових інститутів і суспільства загалом. Таким чином, інформаційно-психологічні операції стають стратегічним інструментом, що дозволяє реалізувати цілі гібридної війни у багатофакторному та багаторівневому форматі [113].

Слід також зазначити, що поширення інформаційних технологій разом із зростаючим впливом соціальних мереж полегшило проведення ІПСО. За останні роки спостерігається масове використання фейкових відео й зображень, а також генеративних технологій, зокрема deepfake. Створення синтетичного контенту використовується для моделювання паніки, фальшивих свідчень масової мобілізації або «карательних» дій з боку українських сил, що має на меті деморалізацію населення і провокацію соціальної напруги. Аналітичні матеріали DFRLab разом зі сповіщеннями українських органів вказують на систематичне застосування таких технологій в інформаційних кампаніях[111].Координовані бот-мережі й боти в месенджерах, зокрема в Telegram, формують ще одну важливу складову ІПСО [111]. Через скоординовані масові розсилки та повторювані повідомлення про локальні проблеми створюється враження «масової думки».

Важливим напрямом гібридних операцій є цілеспрямоване використання мобільних мереж і мобільних месенджерів для маніпулювання цивільним населенням. У практиці такої операції фігурують щонайменше три техніко-операційні моделі, а саме масові SMS-розсилки й push-повідомлення, що імітують офіційні повідомлення органів влади або рятувальних служб; автоматичні дзвінки із записаними повідомленнями; розсилка в популярних месенджерах (Telegram, Signal, Viber) та підроблені акаунти, які дублюють

SMS-кампанії. До прикладу в квітні 2024 року жителі Харкова отримували фейкові повідомлення й повідомлення від імені ДСНС і місцевої влади з вимогою терміново евакуюватися через нібито загрозу оточення[108].Також дослідження DFRLab і OpenMinds виявили мережу тисяч автоматизованих акаунтів у Telegram (3 634 акаунти), які впродовж січня 2024, квітня 2025, що публікували сотні тисяч коментарів і повідомлень, спрямованих на мешканців тимчасово окупованих територій (ТОТ). Ці боти адаптували меседжі під локальні проблеми, а саме відсутність води чи світла, поширюючи наратив того, що в цьому винний «київський режим Зеленського», а не кремлівські загарбники [41].

У жовтні 2023 року, українські користувачі отримали повідомлення від провайдера «Ланет», в якому стверджувалося, що вони нібито мешкають «в Одеській області Росії», а діяльність провайдера «переходить під контроль РФ» [21]. Насправді, провайдер не здійснює свою діяльність у межах Одеської області, що свідчить про штучний характер розсилки і спрямованість її на дезінформацію та деморалізацію населення. Також, 26 жовтня 2023 року користувачі українці отримали SMS-повідомлення із закликами «злити» інформацію про Збройні Сили України[22]. За даними Служби Безпеки України та Центра стратегічних комунікацій та інформаційної безпеки, ця розсилка походила з РФ і є елементом інформаційно-психологічної операції. Тобто, метою ворога виступає не лише розповсюдження дезінформації, а залучення користувачів до співпраці з ними через «зливання даних».

Переходячи до огляду політичних завдань ІПСО, слід розглянути також кейси втручання РФ у вибори в США, України та Румунії. Кремль активно використовує дезінформацію, хакерські атаки, кампанії у соціальних мережах і фінансування радикальних політичних рухів для впливу на результати виборів. Ці дії мають на меті не лише підтримати проросійських кандидатів, а й підірвати довіру громадян до демократичних процедур як таких. В Україні такі спроби зафіксовано неодноразово. Російські спецслужби втручалися у

виборчі кампанії ще з початку 2000-х років, підтримуючи проросійські політичні сили та кандидатів, які відстоювали ідею «нейтралітету» України й виступали проти інтеграції до Європейського Союзу та НАТО. У 2004 році під час президентських виборів Кремль відкрито підтримував Віктора Януковича, а російські політтехнологи, серед яких Глєб Павловський і Сергій Марков, координували його виборчу кампанію[59]. Після Революції Гідності 2014 року Росія змінила тактику, роблячи ставку на інформаційні операції в соцмережах. Через бот-мережі та фейкові акаунти в X (Twitter), Facebook і TikTok вона поширювала наративипро «нелегітимність» української влади, «зовнішнє управління» державою, а також дискредитувала військове керівництво під час виборів 2014 та 2019 років [59].

В Румунії також зафіксовано спроби зовнішнього втручання у виборчі процеси, коли проросійські боти через соціальні мережі підтримували ультраправого кандидата, що виступав проти членства Румунії в НАТО. Під час президентських виборів 2024-2025 років кандидат Калін Джорджеску, відомий своїми проросійськими поглядами, отримав несподівано сильну підтримку у першому турі, і румунська розвідка заявила про координацію онлайн-кампанії через TikTok та інші платформи, яка мала «характерним чином» ознаки російського впливу [90].

Підводячи підсумок слід сказати, внаслідок проведеного аналізу, було визначено основні засоби гібридної агресії РФ проти України з 2014 році. Як це видно з розділу, практика застосування енергетичної складової гібридної війни проявлялася ще з 1990-х років, посилилася під час «газових криз» 2006 та 2009 років, а після анексії Криму у 2014 році набула системного характеру. Головною ознакою даного періоду було збереження та заперечення прямої участі, а саме, агресор подавав військові дії як громадянський конфлікт, економічний тиск як комерційні суперечки, а інформаційну війну як думку громадськості та незалежних засовів масової інформації.

Росія обмежувала постачання газу, підвищувала ціни, просувала проєкти «Північний потік-2» і «Турецький потік», намагаючись зменшити

роль України як транзитної держави та посилити енергетичну залежність ЄС. У відповідь Європейський Союз реалізує політику диверсифікації джерел постачання та розвитку відновлюваної енергетики, що значно зменшує стратегічну перевагу РФ у регіоні. Крім енергетичного тиску, Кремль активно застосовує політичні та інформаційні методи впливу. В Україні з початку 2000-х років російські спецслужби втручалися у вибори, підтримуючи проросійських кандидатів. Аналогічні практики спостерігаються в інших країнах Центрально-Східної Європи, зокрема в Румунії під час президентських виборів 2024–2025 років, а також у США в 2016 році. Метою цих дій є не лише підтримка проросійських сил, а й підрив довіри громадян до демократичних процедур, посилення внутрішніх розколів і дестабілізація політичних систем. Таким чином, Російська Федерація використовує комплексний підхід у гібридних війнах, поєднуючи економічний, політичний та інформаційний тиск для досягнення стратегічних цілей, а країни-об'єкти впливу змушені застосовувати механізми диверсифікації та протидії для збереження своєї безпеки й стабільності.

Аналіз застосування Російською Федерацією проксі-сил і формування маріонеткових режимів демонструє системний характер гібридної агресії проти України. Використання «зелених чоловічків» у Криму та «ополченців» на Донбасі забезпечило створення ілюзії внутрішнього конфлікту, що дозволило Росії тимчасово уникати прямої міжнародної відповідальності та легітимізувати власні дії шляхом маніпулятивних наративів. Залучення невизнаних збройних формувань, застосування дезінформації, використання цивільного населення як «живих щитів» і маскування військової присутності стали ключовими елементами цієї стратегії. Такий інструментарій не лише сприяв швидкому встановленню контролю над окупованими територіями, а й створив передумови для подальшої ескалації конфлікту, підриву українського суверенітету та дестабілізації політичного простору держави. Досвід 2014 року засвідчив, що проксі-механізми є невід'ємною складовою російської зовнішньої політики, інтегрованою в її військово-політичне планування та

спрямованою на досягнення стратегічних цілей шляхом поєднання прихованих і відкритих форм впливу.

Огляд використання інформаційно-психологічних операцій Російської Федерації проти України сформували цілісну систему гібридного впливу, у якій поєднуються стратегічні, операційні та тактичні інструменти. Їхня сутність полягає у перманентному використанні інформаційного простору для формування вигідних агресору наративів, делегітимізації української влади, підриву суспільної довіри та створення передумов для політичної дестабілізації. У цьому контексті «миротворчі» меседжі, дезінформаційні кампанії, цифрові маніпуляції, бот-мережі, фейкові повідомлення в месенджерах і SMS-розсилки виступають взаємодоповнюваними елементами єдиної операційної структури, що націлена на вплив як на внутрішню аудиторію, так і на міжнародну спільноту. Масштабність і технологічність цих дій демонструють, що ІПСО перетворилися на ключовий компонент гібридної стратегії РФ, який дозволяє агресору здійснювати тиск одночасно в інформаційній, політичній, соціальній та психологічній площинах. Такий підхід робить інформаційну сферу одним з основних театрів протистояння та підтверджує необхідність для України послідовно зміцнювати інституційну стійкість, удосконалювати механізми кібер- й інформаційної безпеки та розвивати медіаграмотність населення як ключову умову протидії сучасним формам гібридної агресії.

РОЗДІЛ 3
ТРАНСФОРМАЦІЯ РОСІЙСЬКИХ ГІБРИДНИХ ЗАСОБІВ ВПЛИВУ: ВІД ЛАТЕНТНОЇ ДО ВІДКРИТОЇ ФОРМ АГРЕСІЇ

3.1. Гібридні кібероперації РФ проти України

Починаючи з 2014 року, Україна перебуває під постійним тиском російських кібератак, які стали невід'ємною частиною ширшої гібридної агресії. Кібератаки використовуються як інструмент політичного, інформаційного та військово-технічного впливу, спрямований на дестабілізацію державних інституцій, створення паніки серед населення, порушення функціонування критичної інфраструктури та дискредитацію української влади. Згідно з аналітичними оцінками, наведеними у виданні Politico, щомісяця проти України здійснюються тисячі атак різної інтенсивності, що фактично робить український кіберпростір своєрідною «пісочницею» для випробування нових форм кіберзброї, тактик та інструментів, які згодом можуть бути використані й проти інших держав[70].

У березні 2022 року президент США Джо Байден офіційно попередив про можливість масштабного розширення російських кібератак на західні компанії та державні установи, підкресливши, що потенційна загроза стосується не лише військових і державних структур, а й приватного сектору, фінансових установ та критичної інфраструктури. Він закликав американський бізнес активізувати заходи щодо зміцнення власної кібероборони, включно з аудитом IT-систем, впровадженням багатофакторної аутентифікації, регулярним оновленням програмного забезпечення та підвищенням обізнаності персоналу про фішингові та соціально-інженерні атаки[127]. Це рішення стало сигналом для глобального бізнес-середовища про необхідність посилення кіберстійкості у відповідь на загострення гібридної війни.

На цьому тлі Європейський Союз активізував свої зусилля щодо підтримки кіберстійкості України, враховуючи значний ризик поширення російської кіберактивності на країни-сусіди та партнерів. Як це видно із табл. 3.1, у рамках цієї політики було створено спеціальні програми технічної допомоги, які включали надання сучасних систем виявлення і реагування на кіберзагрози, розгортання платформ моніторингу мережевої активності та навчання українських фахівців із кібербезпеки. Запровадження механізмів обміну експертами між державами-членами ЄС і Україною дозволило не лише передавати технічні знання, але й сприяти координації реагування на загрози в реальному часі, підвищуючи ефективність національної системи кіберзахисту. Крім того, фінансування від ЄС забезпечило розвиток українських систем раннього виявлення кібератак, що є критично важливим для запобігання масштабним інцидентам та мінімізації негативного впливу на державні сервіси і критичну інфраструктуру.

Таблиця 3.1. Проєкти ЄС з питань кіберзахисту України

Назва проєкту	**Рік запуску**	**Основні завдання**	**Ефективність**
DigitalEuropeProgramme (2021-2027)	2021 (згодом включено Україну у 2025)	Надати Україні доступ до фінансування розвитку цифрових технологій, кібербезпеки, інфраструктури, навичок [121]	Модернізовано 10 державних реєстрів та масштабовано систему «Трембіта». Впроваджено електронний підпис, сумісний зі стандартами

			ЄС.
EU Cyber security Reserve	2025 (угода з Україною)	Забезпечити оперативну експертну підтримку України у випадку масштабних кібератак (сертифіковані фахівці ЄС) [119]	Приєднання України до резерву дає право на оперативну підтримку від сертифікованих експертів ЄС для захисту, стримування та швидкого відновлення систем.
StrengtheningCyber Security in Ukraine	2022	Захист баз даних і мереж уряду України, забезпечення конфіденційності, цілісності, доступності даних [51]	Програма займається підтримкою урядової програми «Дія».
EU4DigitalUA	2022	Підтримка цифрової трансформації України, включно із кібербезпекою, реєстрами,	В межах програми передбачене фінансування цифрових технологій, кібербезпеки,

		державними IT-сервісами[28]	навичок, інфраструктури тощо. Реальна ефективність залежатиме від того, як саме Україна скористається цим доступом реалізації проєктів, співробітництва з ЄС

Водночас ЄС посилив власну нормативно-правову базу у сфері кібербезпеки, насамперед шляхом прийняття Директиви NIS2, яка встановлює більш жорсткі вимоги до захисту критичної інфраструктури держав-членів, у тому числі до енергетичного сектору, телекомунікацій, транспорту та фінансових установ[43]. Директива передбачає обов'язкове запровадження систем управління ризиками, планів реагування на інциденти та регулярного звітування про кіберінциденти, що підвищує рівень колективної кіберстійкості ЄС і дозволяє координувати дії з іншими партнерами, зокрема Україною. Такий комплексний підхід, який поєднує технічну допомогу, обмін експертними знаннями та нормативне регулювання, демонструє інтегровану стратегію західних держав у протидії кіберагресії Російської Федерації та підкреслює важливість міжнародної кооперації у сфері кібербезпеки.

Найбільш інтенсивна хвиля кібератівності спостерігалася напередодні та у перші тижні повномасштабного вторгнення 24 лютого 2022 року. Тоді

фіксувалися спроби масових фішингових атак, блокування урядових сайтів, зламів медіа-ресурсів та спотворення інформаційного простору через поширення дезінформації. Проте, на відміну від очікувань західних аналітиків, кібератаки не призвели до паралічу українських систем управління, енергетичних мереж чи комунікацій. Масштабна спроба вивести з ладу енергомережу, здійснена у квітні 2022 року, була успішно відбита фахівцями з кібербезпеки [70]. Це засвідчило значне підвищення рівня кіберзахисту України порівняно з подіями 2015–2017 років, коли хакерські угруповання, пов'язані з РФ, зуміли тимчасово вивести з ладу частину енергосистеми та банківського сектору [70].

Перші масовані кібератаки проти України зафіксовано навесні 2014 року. У період анексії Криму було здійснено втручання в комунікаційні системи урядових структур, зокрема атаковано мережі Верховної Ради, Міністерства закордонних справ та енергетичних компаній. За даними експертів з кібербезпеки, у цей період активно використовувалися шкідливі програми типу Snake (або Uroburos), пов'язані з групою російських хакерів Turla, яка діє під контролем ФСБ [34]. Мета цих операцій полягала у зборі чутливої інформації, перехопленні комунікацій і підриві можливостей українських державних органів координувати дії у кризових умовах. У грудні 2015 року відбулася одна з найвідоміших атак на українську енергетичну систему, унаслідок якої близько 230 тисяч споживачів залишилися без електропостачання [130]. Використання шкідливого програмного забезпечення BlackEnergy та KillDisk, яке дозволило дистанційно вимкнути енергомережі, стало першим у світі задокументованим випадком кібератаки, що спричинила реальні фізичні наслідки [130]. У 2016–2017 роках подібні методи повторювалися, кульмінацією чого стала атака NotPetya, яка паралізувала роботу державних органів, банків, медіа та підприємств, завдавши Україні та світовій економіці збитків на понад 10 мільярдів доларів [103].

У 2016 році Україна зазнавала інтенсивних кіберзагроз, що проявлялися у масових атаках на державні інформаційні ресурси. Президент України Петро Порошенко повідомляв, що за період двох місяців було виявлено понад шість тисяч планованих кібератак, спрямованих на п’ять ключових державних установ та тридцять один інформаційний ресурс державного значення[17]. Це свідчить про системний характер кіберактивності та високий рівень координації атак, які, за оцінками українського керівництва, мали зв’язок із Російською Федерацією [17].Застосовані методи включали спроби доступу до інформаційних систем, фішингові атаки, а також дестабілізаційні впливи на функціонування державних сервісів. Зафіксована активність демонструє прагнення зловмисників не лише отримати технічний контроль над ресурсами, але й впливати на функціонування державних структур та інформаційну безпеку країни в цілому.

Упродовж 2022–2025 років Україна зазнала низки масштабних кібератак, які стали складовою гібридного протистояння національної безпеки. Згідно з інфографікою видання Слово і Діло, кількість зафіксованих інцидентів, зросла з приблизно 2,2 тисяч у 2022 році до 2,5 тисяч у 2023 році, а вже у 2024 році перевищила 4,3 тисячі[22]. Зокрема, 14 січня 2022 року російські хакери атакували близько 70 державних сайтів (включно з порталами Дія, сайтами Кабінет Міністрів України, Міністерство охорони здоров’я України, Міністерство освіти і науки України) [22].Напередодні вторгнення було зафіксовано серію атак типу wiper, шкідливих програм, що знищують дані на комп’ютерах державних структур. Однією з таких стала програма HermeticWiper, яка атакувала українські урядові мережі 23 лютого 2022 року, синхронізовано з початком ракетних обстрілів [105]. Паралельно тривали атаки на системи супутникового зв’язку Viasat, що тимчасово порушили комунікацію між військовими та цивільними користувачами у Європі [105].

Україна, своєю чергою, змогла значно підвищити рівень кіберстійкості. Завдяки співпраці з ЄС, США та НАТО було створено комплексну систему

реагування на інциденти, посилено координацію між державними структурами, приватними компаніями та волонтерами кіберспільноти. Організації на кшталт CERT-UA та IT ArmyofUkraine стали важливими елементами оборони цифрового простору, протидіючи як атакам на інфраструктуру, так і інформаційним кампаніям.

З проведеного аналізу можна зробити кілька ключових висновків. По-перше, починаючи з 2014 року, кібератаки стали системним інструментом гібридної агресії Російської Федерації проти України, спрямованим на дестабілізацію державних інституцій, порушення функціонування критичної інфраструктури, збір чутливої інформації та дискредитацію української влади. По-друге, масштаб та складність атак поступово зростали: від локальних втручань у 2014 році та атак на енергетичну систему у 2015–2017 роках до масованих кібератак перед і під час повномасштабного вторгнення 2022 року, включно з використанням wiper-програм та атак на комунікаційні системи. По-третє, міжнародна підтримка, зокрема від США, ЄС та НАТО, зіграла ключову роль у підвищенні кіберстійкості України. Запровадження комплексних систем раннього виявлення загроз, обміну експертними знаннями, технічної допомоги та нормативного регулювання (наприклад, Директива NIS2 в ЄС) дозволило значно посилити захист критичної інфраструктури та державних ресурсів. По-четверте, успішна протидія атакам у 2022–2025 роках засвідчує ефективність інтегрованого підходу, який поєднує державні інституції, приватний сектор та волонтерські кіберспільноти (CERT-UA, IT ArmyofUkraine). Це підтверджує, що сучасна кібероборона потребує комплексної, багаторівневої координації та постійного вдосконалення стратегій захисту цифрового простору. Загалом, досвід України демонструє, що кібератаки є невід’ємною складовою сучасної гібридної війни, і їх протидія потребує як технічних, так і політичних, міжнародно-координаційних рішень.

3.2. Відкрита інформаційна війна: нові форми маніпуляцій, deepfake та ШІ

У сучасному світі використання технології deepfake та ШІ, стають одним з найбільш потужних інструментів маніпулювання інформацією, особливо у контексті ведення інформаційної війни[35].Історично маніпулювання інформацією було складним і трудомістким процесом, який вимагав значних ресурсів, що обмежувало його застосування переважно лідерам різних країн та спецслужб. З розвитком цифрових технологій цей процес поширення дезінформації серед великих мас населення стало легшим. Поява програмних засобів для редагування фото- і відеоконтенту, таких як Photoshop, а також соціальних мереж, серед яких Тік Ток, X (Твіттер), YouTube, Facebook, Instagram, а також систем штучного інтелекту, зокрема мовних моделей нового покоління, зробила маніпулювання інформацією масовим явищем[37]. Технології, які раніше вимагали значних фінансових і технічних зусиль, стали доступними практично кожному користувачеві, а швидкість поширення спотвореного контенту зросла.

Поява нових програм для створення фото та відео контенту стала новою фазою гібридної інформаційної війни. Розвиток нейронних мереж дозволив користувачам таких програм створювати високо реалістичні дипфейки, які майже неможливо відрізнити від не правди. Це породило нові ризики для інформаційного простору, оскільки межа між правдою та фальсифікацією стала розмитою. Водночас ті самі технології використовуються для розроблення інструментів, здатних ідентифікувати та викривати ці цифрові підробки. Тобто використання ШІ для створення фото та відео контенту, поєднує у собі як потенціал створення дезінформації, так і засоби для її виявлення, що підкреслює його амбівалентну природу. Початково технології генеративного штучного інтелекту, застосовувалися з метою покращення якості зображень, автоматизації перекладів, персоналізації рекомендацій та підтримки голосових асистентів. Проте з

розвитком машинного навчання ці інструменти перетворилися на потужний засіб створення контенту. Впровадження перщої ШІ мережі «GenerativeAdversarialNetworks» у 2014 році стало революційним кроком, адже вони надали можливість створювати фотореалістичні зображення, які людське око практично не здатне відрізнити від справжніх [61]. Подальша еволюція штучного інтелекту призвела до появи програм, що можуть синтезувати людські голоси, створювати музику, відео та інші типи мультимедійного контенту, тим самим відкриваючи як нові можливості для творчості, так і загрози для інформаційної безпеки. Серед яких є OpenAI, Grok, GeminiAI, а також моделі перетворення тексту у відео Sora.

Дипфейки та інший штучно згенерований контент стали новими формами міфотворення та дезінформації у цифрову добу. Якщо раніше маніпуляції з текстом були порівняно простими, то сьогодні до цього додаються складні мультимедійні технології, що створюють ілюзію достовірності. Автоматизовані чат-боти, керовані мовними моделями, здатні генерувати фейкові новини, використовуючи стилістику відомих медіа або публічних осіб, що робить їх особливо переконливими, до прикладу використання чатygpt американськими генералами Трампа [118].

Технологія deepfakeє відносно новим досягненням у сфері штучного інтелекту, що дає змогу створювати відеозаписи подій, які фактично ніколи не відбувалися [115]. Її потенціал робить цю технологію особливо придатною для використання у процесах поширення дезінформації, маніпулятивних наративів у соціальних мережах і цифровому медіа середовищі загалом. Крім того, deepfake розглядаються як ефективний інструмент у контексті кібервійни та гібридних інформаційних операцій. Маніпулювання відео контентом за допомогою технологій штучного інтелекту передбачає поєднання автентичних і синтетичних елементів, що забезпечує високий рівень реалістичності та переконливості таких матеріалів.

Війна в Україні, зокрема, стала чудовим прикладом того, як фальшиві медіа-матеріали можуть використовуватися для психологічного тиску,

поширення дезінформації та маніпулювання громадською думкою. Deepfakeє матеріалами, що створені за допомогою технології штучного інтелекту для імітації реальних осіб і подій, здатні змінювати реальність на рівні сприйняття масовою аудиторією. Термін «Deepfake» вперше був придуманий наприкінці 2017 року однойменним користувачем Reddit [36]. Цей користувач створив простір на сайті новин та агрегації в Інтернеті, де вони ділилися відео, в яких використовувалася технологія обміну обличчями з відкритим вихідним кодомGoogle. З тих пір цей термін розширився, включивши в себе «синтетичні медіа-додатки», які існували до появи сторінки на Reddit, і нові творіння, такі як StyleGAN, що дозволяє створювати й реалістичні фото матеріали людей, яких не існує.

Однак існує багато плутанини навколо терміну deepfake. Оскільки використання цього терміну стало універсальним описом усього: від найсучасніших відео, створених штучним інтелектом, до будь-якого зображення, яке здається потенційно шахрайським. Основним інгредієнтом deepfake є машинне навчання, яке дозволило виробляти їх набагато швидше за нижчих витрат. Щоб зробити deepfake-відео з кимось, автор спочатку тренує нейронну мережу на багатогодинних реальних відеоматеріалах людини, щоб дати їй реалістичне «розуміння» того, як вона виглядає з різних ракурсів і при різному освітленні. Потім вони поєднували навчену мережу з технікою комп'ютерної графіки, щоб накласти копію людини на іншого актора [126].

Особливо небезпечними є випадки, коли deepfake використовуються в політиці або для маніпулювання суспільною думкою у умовах війни. Створення фальшивих відео з високопосадовцями країн, як-от один із перших deepfake 2017 року Барака Обами [39].Одним із найбільш відомих прикладів використання цієї технології стало відео, в якому президент України Володимир Зеленський нібито закликає українців здатися Росії, скласти зброю і припинити опір, ще у 2022 році [91]. Згідно з видання УНІАН, на взламаному ефірі телеканалу Україна 24 президент України

Володимир Зеленський виголошував наступні слова: «…Любі Українці! Шановні захисники! Бути президентом виявилося не так вже й легко. Я змушений ухвалювати складні рішення. Спочатку я вирішив повернути Донбас. Настав час глянути у вічі. Не вийшло. Стало тільки гірше. Значно гірше Більше нема ніякого завтра. Принаймні в мене. І тепер я ухвалив рішення попрощатися з вами. Я раджу вам скласти зброю і повернутися до своїх сімей. На цій війні не варто помирати. Я раджу вам жити, і я збираюся зробити те саме…» [3]. Відео мало кілька очевидних ознак підробки, таких як піксельовані деталі, незвичайна форма голови та незвичайний голос, однак воно все одно було поширене через соціальні мережі, зокрема через російськомовні платформи, як-от Telegram та VK, а згодом потрапило на Facebook, Instagram та Тік Ток. Це відео, хоча й не надто майстерно створене, все ж встигло викликати обурення серед частини україномовної аудиторії, що підтверджує, як навіть погано виконаний відеоматеріал може поширювати паніку і дезінформацію. Також, російським хакерам вдалося транслювати це відео через телеканал «Україна 24», закликали українців припинити бойові дії та здати зброю. Також було ретрансльовано інформацію, що Зеленський нібито втік з Києва [38].Згідно з експертами, відео було класичним прикладом застосування deepfake для політичної маніпуляції [38]. Головна проблема полягала в тому, що воно було створено без достатньо високої якості, тому було очевидно, що це підробка, навіть якщо відео можна було б сприймати як реальне для тих, хто не має досвіду в аналізі подібних матеріалів. Але через технічні дефекти, такі як неприродна форма голови, деформація очей і змінений голос, для фахівців було очевидно, що це маніпуляція. Відео мало виражені артефакти, які були результатом недостатньо точного використання технологій для генерації 3D-об'єктів і синтезу голосу. Це показує, що навіть погано виконаний deepfake може мати велику силу в контексті війни, коли інформація швидко поширюється і викликає паніку або недовіру серед населення. Крім того, існують й інші більш складні діп фейки, які можуть бути набагато важче виявити, особливо коли вони створюються з

високоякісною графікою та використанням сучасних методів штучного інтелекту.

Також український Центр стратегічних комунікацій попередив, що російська влада цілком може використовувати deepfake, щоб переконати українців здаватися. Щодо інших платформ, одразу ж наступного дня 17 березня 2022 р. відео з Meta (Facebook, Instagram) та YouTube були видалені [57]. У треді в Twitter глава політики безпеки Meta Натаніель Глейхер заявив, що компанія «швидко розглянула та видалила» deepfake за порушення своєї політики проти маніпульованих ЗМІ, що вводять в оману[97]. Як зауважує експертка, авторка книги «Діпфейки», Ніна Шик, в випадку відео з Зеленським було легко виявити, але в майбутньому такі фейки можуть бути набагато складнішими і складніше піддаються виявленню [7]. Вона також звертає увагу на те, що платформи концентруються на найбільш очевидних випадках, але часто ігнорують інші форми дезінформації, які можуть бути набагато більш ефективними і небезпечними. Вона підкреслює, що навіть погано зроблені фейки можуть суттєво підірвати довіру до реальних новин і автентичних медіа.

Підводячи підсумок слід сказати, що розвиток технологій штучного інтелекту та генеративних нейронних мереж суттєво трансформував інформаційний простір і створив нові виклики для національної безпеки. Deepfake та інший синтетичний контент стали потужними інструментами маніпулювання громадською думкою, здатними створювати ілюзію достовірності подій, які насправді не відбувалися. Ці технології поєднують у собі як можливості для творчості та автоматизації створення контенту, так і потенціал для дезінформації, психологічного тиску та політичних маніпуляцій. Війна в Україні наочно продемонструвала, що навіть погано виконані deepfake можуть мати значний ефект, впливати на сприйняття аудиторії та підривати довіру до офіційних джерел інформації. При цьому розвиток інструментів для виявлення такого контенту є критично важливим для протидії інформаційним загрозам. Ефективна боротьба з дезінформацією

потребує комплексного підходу, що поєднує технологічні засоби, медіаграмотність населення та активну роботу платформ соціальних мереж у виявленні та блокуванні маніпулятивного контенту.

3.3. Розширення гібридного впливу: енергетичний, продовольчий, міграційний шантаж

Після початку повномасштабної агресії проти України, Російська Федерація істотно розширила спектр своїх гібридних інструментів. Зачіпаючи вже нові парадигми, а саме енергетику, торгівлю продовольством і міграційний шантаж. У межах сучасної гібридної війни така стратегія спрямована не лише на підрив стійкості України, але й на дестабілізацію регіональної та глобальної безпеки. Енергетичний тиск залишається одним із ключових інструментів гібридного впливу Російської Федерації. Ще до 2022 року Москва систематично використовувала свої енергетичні ресурси як засіб політичного тиску на країни Європейського Союзу, зокрема шляхом обмеження постачання природного газу у періоди кризових ситуацій або під час переговорних процесів[65]. Особливе значення у цій стратегії мав газопровід «Північний потік 1», через який Росія здійснювала постачання до ключових європейських споживачів, зокрема Німеччини та Угорщини.

У випадку Угорщини енергетичний шантаж набув особливої політичної форми, адже уряд прем’єр-міністра Віктора Орбана неодноразово підкреслював важливість енергетичного союзу Угорщини та РФ. Відмовляючись приєднуватися до деяких санкцій ЄС проти Росії та демонструючи готовність продовжувати імпорт газу за прямими домовленостями з Москвою. Залежність Угорщини від російських поставок була суттєвою, адже у 2024 році вона імпортувала приблизно 80-85 % свого природного газу та 80 % нафти саме з Росії[50].Угорщина виявляла готовність продовжувати імпорт газу за прямими домовленостями з Москвою (через Gazprom) навіть тоді, коли решта країн ЄС збільшували диверсифікацію

джерел енергії. Зокрема, видання Balkan Insight повідомляє, що Угорщина уклала новий довгостроковий контракт із Gazprom — збільшила річний обсяг поставок до понад 6,7 млрд м³ газу, всупереч тенденції ЄС зменшувати залежність від російських джерел. Москва, у свою чергу, використовувала ці домовленості як механізм тиску на Орбана, стимулюючи його опозицію до європейської координації та посилюючи внутрішньополітичні дебати щодо підтримки України [73].

Ще одним інструментом впливу, через енергетичний шантаж, стало зменшення обсягів експорту газу, ключові маршрути постачання були призупинені, а ціни на газ та електроенергію на європейських ринках підвищувалися штучно, що створювало економічну турбулентність і посилювало внутрішньополітичні дискусії в країнах ЄС щодо підтримки України. Через такі дії Москва прагнула не лише поглибити енергетичну залежність окремих держав, а й стимулювати політичне розколювання Європи, використовуючи аргументи про економічні втрати та зростання цін на енергоносії. Як зазначає Європейська комісія у звіті 2023 року, енергетичний шантаж Москви став «невід'ємною частиною стратегії гібридного тиску», спрямованої на підрив єдності європейських держав [104] Вибухи на газопроводах «Північний потік» у 2022 році стали символом енергетичної вразливості Європи та показали, що критична інфраструктура може бути об'єктом гібридних атак. У цьому контексті Росія прагнула не лише підвищити енергетичну залежність окремих країн, але й стимулювати внутрішньополітичні дебати в ЄС щодо підтримки України, використовуючи аргументи економічних втрат і зростання цін на енергоносії. Як зазначає Європейська комісія у звіті 2023 року, енергетичний шантаж Москви виявився «невід'ємною частиною стратегії гібридного тиску», спрямованої на підрив єдності європейських держав [104].

Другим важливим напрямом гібридного тиску стала маніпуляція глобальною продовольчою безпекою. Після початку повномасштабного вторгнення, Росія свідомо використовує продовольство як геополітичну

зброю. Блокування армією РФ українських портів на Чорному морі у 2022–2023 роках призвело до різкого скорочення експорту зерна з України, яка до війни забезпечувала близько 10 % світового експорту пшениці, 15 % кукурудзи та понад 40 % соняшникової олії[58]. За даними Продовольчої та сільськогосподарської організації ООН, обмеження морського експорту спричинило істотне зростання цін на продовольство у світі, зокрема в країнах Африки, Близького Сходу та Південної Азії [123]. Згідно з оцінками Світової продовольчої програми, понад 47 млн людей опинилися на межі голоду внаслідок скорочення українських поставок [117]. Таким чином, воєнна блокада портів стала не лише інструментом тиску на Київ, але й фактором дестабілізації міжнародного порядку. Підписання у липні 2022 року та подальше систематичне зривання Росією «зернової угоди» є ще одним прикладом продовольчого шантажу. Угода, підписана за посередництва ООН і Туреччини, дозволила частково відновити експорт українського зерна, але Москва неодноразово порушувала її умови, обстрілюючи порти Одеси та Чорноморська[123]. Коли у липні 2023 року Росія офіційно вийшла з угоди, вона супроводила цей крок кампанією дезінформації, звинувачуючи Захід у нібито «перешкоджанні постачанню зерна до найбідніших країн» [80]. У дійсності ж понад 70 % вантажів за угодою надходило саме до держав Африки та Азії, які найбільше страждали від дефіциту [80].На стратегічному рівні Росія прагне продемонструвати власну незамінність у світових агропродовольчих ланцюгах, позиціонуючи себе як «гаранта стабільності» на ринку зерна. Кремль активно просуває меседж, що «санкції Заходу провокують голод» у Глобальному Півдні, перекладаючи відповідальність за кризу на ЄС і США. У серпні 2023 року, під час саміту «Росія – Африка» у Санкт-Петербурзі, Путін оголосив про «безоплатні поставки зерна» до шести африканських держав крок, який мав не стільки економічний, скільки пропагандистський характер [85].

Продовжуючи огляд питання продовольчої безпеки, проросійські медіа систематично поширюють дезінформацію про «розкрадання зерна»

українською владою або про те, що «зерно з України потрапляє лише до Європи». У соціальних мережах ідеї «несправедливого розподілу ресурсів» активно використовуються для стимулювання антизахідних настроїв у країнах, де продовольча безпека має критичне значення [98]. Аналітики НАТО відзначають, що такі меседжі допомагають Москві перенаправляти фокус уваги від власних агресивних дій до уявної провини Заходу, створюючи ілюзію, ніби Росія бореться за «справедливий світовий порядок»[98].Також Кремль використовує контроль над добривами, аміаком та іншими агроресурсами як важіль тиску. Обмеження експорту добрив у 2022 році призвело до підвищення цін на агропродукцію у світі, а також до збільшення собівартості виробництва в країнах, що розвиваються[53]. Таким чином, Москва отримує додаткові важелі впливу, стимулюючи залежність окремих держав від своїх ресурсів і пропонуючи «пільгові умови» лише тим, хто демонструє лояльність.

Не менш значущим інструментом у гібридній стратегії Кремля є використання міграційних потоків як засобу політичного тиску. Вперше дана стратегія була використана під час подій 2021 року на білорусько-польському та білорусько-литовському кордонах. Режим Олександра Лукашенка, за підтримки Москви, організовано завозив мігрантів із країн Близького Сходу, а саме з Іраку, Сирії, Афганістану, Лівану, Йорданії. Громадяни цих країн користуючись послугами мінських туристичних агентств, які діяли під прикриттям «візових турів» до ЄС, тисячі осіб були вивезені до кордонів Європейського Союзу, де їх використовували як «живий таран» проти прикордонних служб Польщі та Литви[53]. Ця криза мала не лише гуманітарний, а й інформаційно-психологічний вимір: російські та білоруські пропагандистські медіа активно транслювали кадри зіткнень, створюючи враження жорстокості й нелюдяності європейських урядів.

Після початку повномасштабного вторгнення Росії в Україну у лютому 2022 року, масштаби гібридного міграційного шантажу істотно розширилися. Кремль посилив інформаційні та психологічні операції, спрямовані на

дискредитацію політики ЄС у сфері міграції, експлуатуючи контраст між прихильним ставленням до українських біженців та обмеженням доступу для мігрантів з Близького Сходу й Африки [98]. Пропагандистські наративи наголошували на «подвійних стандартах» Заходу, формуючи у свідомості аудиторії в країнах Глобального Півдня уявлення про Європу як «лицемірну цивілізацію», яка поділяє біженців на «гідних» і «негідних» допомоги [98].У межах інформаційних кампаній російські медіа та анонімні мережі в соціальних платформах (Telegram, X, TikTok) систематично поширюють фейки та маніпуляції щодо масштабів міграційної кризи, розпалюючи ксенофобські настрої ЄС. Наприклад, навесні 2023 року мережа проросійських акаунтів поширювала твердження про нібито «привілейоване становище українських переселенців» у Польщі та Чехії, що спричинило хвилю протестів і зростання антиукраїнських коментарів у соціальних мережах [48]. Такі меседжі часто поєднуються з такими аргументами як, «українці отримують наші робочі місця», «ЄС витрачає гроші на чужу війну», що посилює політичний популізм і підігріває недовіру до урядів, які підтримують Київ[48].

Підсумовуючи аналіз підрозділів, можна зробити висновок, що сучасна гібридна війна проти України є комплексним та багатовимірним явищем, яке поєднує кібероперації, інформаційні маніпуляції та економічно-політичний тиск. З 2014 року російські кібератаки стали системним інструментом агресії, спрямованим на дестабілізацію державних інституцій, порушення роботи критичної інфраструктури та дискредитацію влади. Масштаби та складність таких атак з часом зростали, від локальних втручань у комунікаційні системи до масованих кібератак перед і під час повномасштабного вторгнення 2022 року, включно з використанням wiper-програм та атак на системи супутникового зв’язку. Також початок повномасштабного вторгнення можна вважати як період певного переломного моменту, після якого гібридна агресія набула ознак відкритих форм. Провал «блискавичної війни» змусив РФ адаптувати наявні методи та застосовувати нові.

Аналіз гібридних кібероперацій РФ проти України виявив їхню радикальну трансформацію. Якщо до 2022 року кібератаки як-от Not Petya були епізодичними та формально не пов'язаними з діями російської держави, то після початку повномасштабного вторгнення вони стали невід'ємною складовою військових операцій. Синхронізація кібератак з ракетними ударами по енергетичній інфраструктурі України восени-взимку 2022-2023 років засвідчила перетворення кіберпростору на повноцінний фронт бойових дій. Щоденні атаки на критичну інфраструктуру, державні реєстри, фінансову систему та телекомунікації демонструють, що кібервійська РФ діє як інтегрована складова Збройних Сил, а не як окремі хакерські угруповання.

Водночас розвиток технологій штучного інтелекту та генеративних нейронних мереж призвів до появи нових форм інформаційної війни, зокрема deepfake та автоматизованих систем генерації мультимедійного контенту. Такі технології дозволяють створювати високо реалістичні фальшиві відео та аудіоматеріали, що значно ускладнює розпізнавання дезінформації та підвищує ризик маніпуляції громадською думкою. Досвід України показав, що навіть відносно низькоякісні deepfake можуть спричиняти психологічний тиск, поширювати паніку та підривати довіру до офіційних джерел інформації. Одночасно розвиток інструментів для виявлення таких матеріалів є критично важливим, а ефективна протидія вимагає поєднання технологічних рішень, медіаграмотності населення та активної роботи соціальних платформ у блокуванні маніпулятивного контенту.

Особливого значення набула глобалізація гібридного впливу через енергетичний, продовольчий та міграційний шантаж. Тут найбільш яскраво проявляється різниця між двома формами гібридної війни. Якщо економічний тиск 2014-2022 років був спрямований переважно на Україну та окремі країни ЄС і подавався як "комерційні суперечки", то після 2022 року він трансформувався у глобальну геополітичну зброю. Блокада українського зернового експорту створила загрозу голоду в Африці та Азії, припинення постачання газу до Європи та диверсія на "Північних потоках" мали на меті

зламати санкційну єдність Західного альянсу, а штучно спровокована міграційна криза на кордонах ЄС використовувалася для дестабілізації європейських суспільств. Географія впливу розширилася від регіональної до глобальної, а мета змінилася з примусу України до капітуляції на розкол міжнародної підтримки українського опору. Міграційний тиск використовується через організацію масових потоків мігрантів до кордонів ЄС та поширення дезінформації щодо «подвійних стандартів» у політиці прийому біженців, що створює соціально-політичну напруженість і стимулює антизахідні настрої.

Загалом, досвід України демонструє, що сучасні гібридні загрози є взаємопов'язаними, багаторівневими та постійно еволюціонують, охоплюючи кіберпростір, інформаційний, економічний та соціальний виміри. Протидія таким загрозам потребує комплексного підходу, який поєднує національні та міжнародні зусилля, державні та приватні інституції, технічні засоби захисту та підвищення обізнаності населення. Ефективна стратегія гібридної безпеки передбачає постійне вдосконалення систем раннього виявлення, обмін досвідом із міжнародними партнерами, координацію дій між різними суб'єктами безпеки та активну протидію інформаційним і психологічним операціям. Таким чином, досвід України є наочним прикладом того, як сучасна держава може протистояти комплексним загрозам гібридного характеру, забезпечуючи стійкість критичної інфраструктури, захист інформаційного простору та збереження довіри громадян навіть у умовах широкомасштабної агресії.

РОЗДІЛ 4
МЕХАНІЗМИ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ: УКРАЇНСЬКИЙ ДОСВІД ТА МІЖНАРОДНА СПІВПРАЦЯ

4.1. Формування української системи протидії гібридним загрозам

У сучасних міжнародних відносинах поняття гібридної війни посідає центральне місце в дослідженні і плануванні державної та наддержавної безпеки та оборони. Воно відображає тенденцію до ускладнення форм збройного та незбройного протистояння у XXI ст., у якому межі між традиційними воєнними діями, інформаційними впливами, економічним тиском і політичним маніпулюванням поступово розмиваються. Гібридні загрози поєднують у собі широкий спектр методів – від дезінформації та кібератак до використання енергетичних і дипломатичних інструментів. Це унеможливлює їх ефективне нейтралізування конвенційними воєнними засобами. Йдеться не лише про створення оборонних механізмів, а й про розбудову стійких політичних інститутів, інформаційної безпеки, національної єдності та ефективної взаємодії з міжнародними партнерами.

Для держав, яким на заваді потенційні конвенційні воєнні загрози, питання формування системи протидії гібридним загрозам також набуває стратегічного значення. Україна постала перед необхідністю вироблення власної моделі реагування на комплексні загрози, які поєднують військові, економічні, інформаційні та соціально-політичні елементи, у тому числі механізми координації між державними і недержавними структурами. У цьому контексті ключовим постає питання: чи змогла Україна за часів незалежності сформувати ефективну систему протидії гібридним загрозам?

Формування української системи протидії гібридним загрозам неможливо розглядати без урахування загального стану національної безпеки у період становлення незалежної держави. З 1991 р. Україна зосередила зусилля на побудові інституцій політичного управління та оборонної системи,

орієнтуючись переважно на традиційні форми безпекових викликів. У цей час питання інформаційної, кібернетичної чи енергетичної безпеки не розглядалися як складові національної безпеки в їх сучасному розумінні. Така ситуація зумовлювалася як обмеженими ресурсами, так і відсутністю усвідомлення комплексного характеру нових загроз у політичному та науковому середовищі. У 1990-х роках безпекова політика України формувалася під впливом «постбіполярного» міжнародного порядку, у межах якого пріоритет надавався питанням ядерного роззброєння (згідно інтересам останнього «полюса» у міжнародному порядку – Сполучених Штатів Америки), а також питанню збереження контролю над колишнім радянським озброєнням та при цьому збереженні суверенітету і територіальної цілісності. Аналіз тодішнього законодавства констатує, що норми щодо зовнішньої й інформаційної безпеки 1990-х рр. ще не інтегрували методи протидії гібридним атакам. Проте, описуючи «стратегічні питання протидії загрозам суспільству та державі», Концепція національної безпеки України, схвалена Постановою Верховної Ради України у 1997 р., в цілому, охоплювала вектори, які нині розуміються як основні зовнішні й внутрішні гібридні загрози у політичній, економічній, соціальній, воєнній, науковій, екологічній сферах. Концепція не торкалася питань інформаційної безпеки та не мала статусу закону, тому на кінець 1990-х рр. ще неможливо говорити про сформованість в Україні законодавчої основи для системи протидії гібридним загрозам [86, с. 7–8].

Тобто, станом на 1990-ті рр., у законодавчому полі формування системи захисту від гібридних загроз мало фрагментарний характер: окремі стратегічні та секторні документи почали враховувати зміни в характері загроз, але комплексного підходу не було виокремлено. Державна політика протидії гібридним загрозам та забезпечення економічної безпеки України тільки набирала системного характеру [4, с. 36–43].

У перші роки 2000-х років Україна перебувала в процесі консолідації своєї зовнішньої політики та безпекового курсу, що разом із слабкою

інституційною базою складало фон для побудови системи протидії гібридним загрозам. Політична еліта більш-менш узгоджено підтримувала курс на європейську та євроатлантичну інтеграцію, зокрема вступ до програми НАТО «Партнерство заради миру», що підвищувало міжнародну взаємодію в царині безпеки [112, с. 2–9]. Протягом цього періоду відбувалося законодавче та стратегічне оформлення системи національної безпеки: зокрема, у 2003 році ухвалено Закон «Про основи національної безпеки України», який вперше відкрито декларував курс на членство в НАТО [88]. Внутрішні проблеми України початку 2000-х рр. (корупція, залежність від російських енергетичних постачань, слабка модернізація оборонного сектору) залишали значні «вузькі місця» у безпековій архітектурі, що зазначалося навіть у проектних документах стратегічної безпеки 2015 р. [44].Крім того, був проголошений курс на реформу Збройних СилУкраїни, цивільного контролю над ними, подальшу модернізацію оборонно-безпекового сектору [125]. Проте саме гібридний аспект загроз, із його поєднанням інформаційного, економічного, політичного впливу з елементами військового, ще системно не враховувався в стратегіях та механізмах реагування на загрози безпеці Україні.

На економічному і інформаційному фронтах Україна 1990–2000-х рр. стикалася з активною залежністю від РФ: енергоносії, ринки, фінансові зв’язки – усе це створювало можливості впливу ззовні. Фактично, РФ втілилася до проєктування і розроблення економічних проблем через економічне протистояння з переходом в економічну (торгову) війну та протидію зв’язкам країни-жертви із сусідніми країнами та країнами-партнерами. Саме такі залежності становили основу для майбутніх гібридних операцій проти України [24, с. 191]. Вплив на міжнародні відносини, санкції та інші методи економічного тиску і досі використовуються для забезпечення підтримки російських інтересів у регіоні. Через так званий «газовий шантаж» та ймовірний підкуп частини європейських політиків російська пропаганда може поширювати серед європейців свої наративи та пропаганду [2, с. 23].

Подібно небезпечними залишалися виклики у сфері інформаційного простору. Вони виникали з точки зору створення єдиного інформаційного простору, формування національної ідентичності та суспільної стійкості. Ці аспекти розглядають як невід'ємні частини протидії гібридним загрозам [96, с. 17].

Водночас міжнародна співпраця в царині безпеки і оборони зростала, але залишалася фрагментарною й більше концентрувалася на класичних аспектах (військово-технічна допомога, участь у міжнародних місіях) ніж на цілісному протидії гібридним впливам. Наприклад, влада України регулярно долучалася до програм НАТО, до зовнішньополітичних ініціатив ЄС, але координація між державними структурами, недержавним сектором і громадянським суспільством не мала чіткої системності [112, p. 3]. Таким чином, період ранніх 2000-х років слугує своєрідним «пробним» етапом: з одного боку, визначилися стратегічні пріоритети, з іншого – відставали практика і механізми реагування на нові види загроз. В цілому, як зазначають численні українські та європейські дослідники, саме у передвоєнний період (до 2014 р.) система протидії гібридним загрозам залишалася недостатньо сформованою: відсутня була чітка національна стратегія, слабка координація між державними органами, недосконала взаємодія з армією, спецслужбами та громадським сектором. Колектив авторів аналітичного звіту 2018 р. «Hybrid Threats to Ukraine and Public Security. The EU and Eastern Partnership Experience», підготовленого для органів ЄС, влучно зазначив, що Україна була не підготовлена до зовнішніх загроз, особливо гібридних, а державний механізм безпеки мав «прогалини, які перешкоджали відновленню суверенітету і забезпечення безпеки суспільства» [76, с. 30–51].

Російсько-українська війна, починаючи з 2014 р., кваліфікується дослідниками як міжнародний збройний конфлікт (фактично не оголошена війна). Порівнюючи з іншими прикладами в міжнародних відносинах, ця війна підпадає фактично під кожен критерій ведення гібридних воєн. У ході війни застосовувалися локальні проксі (іррегулярні військові формування),

економічний вплив, ведення активної пропагандистської діяльності з поширенням величезної кількості фальшивих новин (зокрема, і через проплачені іноземні мас-медіа). Також до уваги «союзники» агресора, які умовно належать до табору партнерів України, членів ЄС і НАТО, але фактично саботують українську сторону війни [24, с. 190]. Звичайно, гібридна війна включає і безпосередньо пряме військове втручання із застосуванням усіх наявних в арсеналі країни-агресора засобів та сил, при чому навіть на оголошеного «повномасштабного» вторгнення у 2022 р. на Донбасі у 2014–2021 рр. використовувалися новітні засоби зброї ВСРФ: моделі «Панцир-С1», «Буратіно», «Т-90А», «Свєт-КУ» та інші.

У період 2014–2021 рр. українська система протидії гібридним загрозам почала формуватися активніше, що зумовлювалося зовнішньою агресією та необхідністю швидкої адаптації. Після окупації та відкритої анексії Криму РФ та початку збройного конфлікту на Донбасі держава звернула увагу на нові форми загроз – інформаційні, кібернетичні, економічні. Так, на засіданні Рада національної безпеки і оборони України 17 листопада 2014 р. під час зустрічі з Північноатлантичний альянс було підкреслено необхідність спільної відповіді на «гібридну війну» [116].У 2015 р. затверджено Стратегія національної безпеки України, яка вперше прямо згадувала про гібридну агресію як одну з форм загроз [99, с. 103]. У сфері кібербезпеки були створені нові інституції: наприклад, Центр кіберзахисту при Служба безпеки України та були затверджені відповідні стратегічні плани [76, с. 67–68]. Законодавча база почала заповнювати прогалини – аналіз показує, що українське законодавство в цей період стало більш чітко враховувати комплексні загрози, включно з гібридними. Реформи у сфері національної безпеки та оборони, проведені за президентства п’ятого Президента України Петра Порошенка (2014–2019 рр.), мали суттєве позитивне значення для формування української системи протидії гібридним загрозам. Вони сприяли консолідації оборонно-безпекового сектору, впровадженню цивільного контролю над Збройними Силами, модернізації озброєння та створенню нових структур,

здатних реагувати на комплексні загрози. Особливу увагу було приділено розвитку інформаційної та кібербезпеки, інтеграції українських інституцій у міжнародні механізми співпраці з НАТО та ЄС, а також підвищенню оперативної здатності державних органів і громадянського суспільства до взаємодії у кризових ситуаціях. Ці кроки заклали фундамент для подальшої трансформації системи безпеки, дозволивши Україні ефективніше реагувати на гібридні виклики та адаптуватися до динамічного характеру загроз.

Разом з тим, активна політична боротьба та впровадження політики децентралізації створили певні виклики для реалізації реформ у сфері безпеки: розпорошеність повноважень між центральною та місцевою владою, уповільнення координації між різними відомствами та затримки у фінансуванні та ресурсному забезпеченні нових інституцій обмежували ефективність впровадження окремих ініціатив, частково стримуючи повну інтеграцію інструментів протидії гібридним загрозам. Практика захисту від гібридних загроз у 2014–2021 рр. залишалася недостатньо координованою: нові підрозділи та документи були створені, але їхня взаємодія, а також взаємодія державного сектору з громадянським суспільством і міжнародними партнерами ще не набула системного характеру. Інформаційна компонента стала одним із пріоритетів: держава та недержавні актори активізували протидію дезінформації та ворожим наративам. Наприклад, аналіз вказує на те, що український уряд у співпраці з волонтерами й громадянськими ініціативами забезпечив більш скоординовану відповідь на інформаційні атаки [31]. Економічна і фінансова безпека також зазнали змін: були вжиті заходи для зміцнення фінансової стійкості держави перед загрозами економічного тиску [69, с. 61–68].

Отже, період 2014–2021 рр. можна розглядати як етап активного становлення української системи протидії гібридним загрозам – із запуском ключових інституцій, створенням стратегічних документів, посиленням інформаційної та кібернетичної безпеки. Проте залишалися виклики в

координації, ресурсному забезпеченні, законодавчому наповненні та повній інтеграції інструментів реагування.

У 2022 р., після повномасштабного вторгнення Україна, система протидії гібридним загрозам в державі зазнала радикального прискорення. Кризова ситуація стала каталізатором для інтеграції інструментів інформаційної, кібернетичної та економічної безпеки в єдину модель реагування. Національний звіт «Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз» (2022) відзначає, що концепція національної стійкості стала ключовою для переосмислення ролі держави, громадянського суспільства і міжнародних партнерів у протидії гібридним ризикам [16, с. 18, 52].Законотворчі та інституційні зміни також відбулися у 2022–2025 рр. були запущені програми, заходи й міжнародні партнерства, орієнтовані на гібридні загрози, зокрема посилення співпраці з ЄС та іншими союзниками [120].У міжнародній площині Україна стало активним учасником партнерських ініціатив із протидії гібридним загрозам. Зокрема, у сфері обміну досвідом, навчання, розвитку спільних стандартів із ЄС та НАТО-партнерами [102].Разом з тим, незважаючи на динамічні зміни, залишилися суттєві виклики. Інституційна координація між державними структурами, громадським сектором та міжнародними партнерами досі потребує вдосконалення. Законодавча база, хоча і стала більш адаптованою до гібридних загроз, все ще зазнає труднощів із імплементацією на практиці.

У сфері кібербезпеки та інформаційної війни українська влада та громадянські ініціативи оперативно формували нові формати: наприклад, діяльність волонтерських цифрових батальйонів, посилення захисту критичної інфраструктури та інформаційна мобілізація суспільства [111]. Ще одним результативним напрямом у цьому контексті стало оперативне реагування на посилені російські кампанії в кіберпросторі та інформаційному полі, які скеровані не лише проти України, але й проти країн-партнерів. Зростання значення колективної гібридної стійкості очевидне станом на

2024 р., безпекова стратегія України і союзників описується як боротьба «рою бджіл проти мамонта» [82].

Відповідно, період 2022–2025 рр. можна охарактеризувати як етап глибокої трансформації української системи протидії гібридним загрозам. Україна рухалась від моделі реакції до більш проактивної, орієнтованої на стійкість і міжнародну координацію. Проте, цей процес ще не завершено: перед країною досі стоять завдання щодо повної інтеграції інструментів, вдосконалення оперативних механізмів і забезпечення законодавчого, інституційного та, врешті, й ресурсного фундаменту для довготривалої протидії у формі чіткої оборони гібридним загрозам.

Аналіз етапів становлення української системи протидії гібридним загрозам дає змогу зробити низку узагальнюючих висновків, які відображають складний і поступовий характер цього процесу. Україна, як держава, що відновила незалежність у нових геополітичних умовах, формувала свою систему безпеки в умовах обмежених ресурсів, інституційної несталості та невизначеності міжнародного середовища. Це призвело до того, що формування дієвої системи протидії гібридним загрозам відбувалося нерівномірно, еволюційно та значною мірою реактивно.

У 1990-х – на початку 2000-х років відсутність усвідомлення феномену гібридної війни як комплексної форми впливу зумовила орієнтацію державної політики безпеки переважно на класичні воєнні та політичні ризики. Українські стратегічні документи цього часу не враховували інформаційно-психологічних, економічних чи кіберзагроз, що робило державу вразливою до нетрадиційних методів впливу. Лише окремі фрагменти концепцій і законодавчих актів торкалися питань, які сьогодні відносяться до складових гібридної безпеки. Такий стан речей пояснювався не лише браком наукового осмислення проблеми, а й значною залежністю України від Російської Федерації у сфері енергетики, торгівлі та інформаційного простору. Тому ще до 2014 року було закладено низку структурних слабких місць в українській безпеці, які в подальшому стали об’єктом зовнішнього впливу.

Події 2014 року стали вододілом у формуванні системи національної протидії гібридним загрозам. Зовнішня агресія Росії примусила державу переглянути підходи до безпеки й почати розробку нового покоління стратегічних документів, які вперше закріпили поняття гібридної агресії на рівні державної політики. З'явилися спеціалізовані структури, зміцнилася інформаційна безпека, активізувалися міжнародні партнерства з ЄС і НАТО, а також розпочалося формування кіберзахисної інфраструктури. У цей період українська система переходила від стану «реакції на події» до спроб створення сталих інституційних механізмів попередження й нейтралізації гібридних впливів. Проте її ефективність залишалася обмеженою через фрагментарність рішень, нестачу ресурсів і недосконаліть координації між відомствами в умовах зростання політичної боротьбі всередині країни.

Період після 2022 року став етапом найглибшої трансформації системи безпеки України. Повномасштабна війна актуалізувала необхідність комплексного підходу до гібридних загроз, що включає поєднання військових, інформаційних, кібернетичних, економічних і дипломатичних інструментів. Україна перейшла від моделі реагування до концепції національної стійкості, яка базується на інтеграції зусиль держави, суспільства та міжнародних партнерів. Було розширено законодавчу базу, створено нові інституції, сформовано системи стратегічних комунікацій і кіберзахисту. Водночас, навіть за умов швидкого розвитку, наявні виклики зберігаються у сферах міжвідомчої координації, стратегічного планування, кадрової підготовки й ефективного використання міжнародної допомоги.

Отже, відповідаючи на поставлене питання, чи змогла Україна за часів незалежності сформувати ефективну систему протидії гібридним загрозам, слід зазначити, що така система сформувалася частково і досі перебуває у стані динамічного становлення. Україна створила основу для багаторівневої моделі національної безпеки, здатної виявляти й реагувати на гібридні загрози, однак її ефективність залишається нерівномірною. Вона значною

мірою залежить від зовнішньої підтримки, оперативності внутрішніх реформ і спроможності інтегрувати усі складові безпеки в єдину архітектуру.

Таким чином, можна констатувати, що Україна зробила суттєвий крок у напрямі створення системи протидії гібридним загрозам і перетворюється на один із ключових центрів застосуванні та здобуття практичного досвіду у цій сфері в європейському просторі. Проте остаточне оформлення й стабілізація цієї системи вимагатимуть часу, комплексного вдосконалення інституційних механізмів і подальшої інтеграції у євроатлантичну безпекову систему, цілком можливо – вже зі здобутим українським досвідом.

4.2. Міжнародні механізми координації у протидії гібридній агресії

У XXI столітті міжнародна безпекова система зіткнулася з якісно новим типом викликів, який не вписується у класичні рамки ведення війни. Гібридна агресія, стала ключовим інструментом держав, що прагнуть досягти політичних або військових цілей без прямого оголошення війни, використовуючи комбінацію військових, економічних, кібернетичних, інформаційних та дипломатичних засобів. Саме Російська Федерація, починаючи з 2014 року, продемонструвала ефективність таких методів проти України, країн Європейського Союзу, США та держав-членів НАТО. Особливість гібридної агресії полягає у розмитті меж між внутрішніми та зовнішніми загрозами з використанням так званих «незаконних методів ведення війни» (як-от використання проксі сил на території України). Цей багатовимірний характер загроз вимагає розвинених міжнародних механізмів координації, які забезпечують спільну відповідь на кібернапади, втручання у вибори, диверсії проти енергетичної інфраструктури та напади на країни використовуючи проксі сили безпосередньо.

Після початку російської агресії проти України у 2014 році Європейський Союз визнав гібридні загрози одним із пріоритетів своєї спільної зовнішньої та безпекової політики. Вперше поняття гібридні загрози,

було чітко закріплено у «Спільній рамковій стратегії ЄС із протидії гібридним загрозам», де визначено базові напрями дій, зокрема виявлення загроз, посилення стійкості, координація між інституціями та стратегічна комунікація [53; 54]. Цей документ заклав основи системного підходу, що передбачає інтеграцію політики безпеки, дипломатії та інформаційних технологій для мінімізації ризиків від зовнішніх гібридних впливів.Для забезпечення оперативної взаємодії між державами-членами та центральними інституціями у 2016 році було створено Hybrid Fusion Cell у складі Європейської служби зовнішніх дій (EEAS)[49]. Головним завданням цього центру є інтеграція та аналіз інформації, що надходить з розвідувальних служб держав-членів, дипломатичних представництв, а також від спеціалізованих агенцій, з метою виявлення потенційних гібридних атак. Особливу увагу приділено кампаніям дезінформації, втручанню у виборчі процеси, економічному тиску, включаючи енергетичну залежність, та кібератакам на критичну інфраструктуру. Також, у 2015 році було запущено Європейську групу стратегічних комунікацій «EastStratComTaskForce», яка керує платформою EUvsDisinfo [55]. Ця платформа фіксує, аналізує та спростовує випадки дезінформації, що походять переважно з Російської Федерації, зокрема у медіа та соціальних мережах. Лише у 2022–2023 роках платформа задокументувала понад 15 тисяч випадків антиєвропейських та антиукраїнських наративів, охоплюючи теми енергетичної безпеки, нібито порушень прав людини в Україні через діяльність ТЦК, а також дискредитації української влади.

Гібридна війна, як наголошується в аналітичних звітах Європейської ради з міжнародних відносин (ECFR), потребує не лише військової відповіді, а передусім політичної та інституційної узгодженості, здатності виявляти вразливості у політичних системах, інформаційному просторі та економічних структурах [40].Європейські країни дедалі частіше стикаються з поєднанням кібератак, кампаній дезінформації, тиску на енергетичний сектор і втручання у виборчі процеси. Особливо ситуація з гібридним втручанням з боку

Кремля, збільшилися після почтку повномасштабного вторгнення, коли РФ на пряму намагається впливати, як це було згадано раніше, на енергетичну незалежність ЄС, а також вибори в країнах. Для протидії таким викликам формується концепція «стійкої Європи» (ResilientEurope), що базується на чотирьох основних напрямах: розбудові національних систем безпеки, покращенні стратегічної комунікації, посиленні кіберзахисту та формуванні колективних механізмів реагування[40]. Після виборів в США 2016 року, коли РФ на пряму намагалися вплинути на вибори в Штатах, для боротьби з гібридними впливами, був створений Європейський центр з протидії гібридним загрозам (HybridCoE)[52]. Центр функціонує як майданчик для обміну досвідом між країнами ЄС і НАТО, розробки спільних навчань, тестування сценаріїв гібридних атак і розробки стратегій щодо відновлення стійкості суспільства після інформаційних або кібероперацій. Участь у роботі центру беруть понад тридцять держав, що дозволяє поєднати ресурси та аналітичний потенціал у межах єдиного євроатлантичного простору. Ключовим елементом протидії гібридним загрозам є підвищення інформаційної безпеки та зміцнення довіри між державними інститутами і громадянами[52].

Переходячи до НАТО, то альянс розглядає гібридні загрози як комплексні та багатогранні виклики, що поєднують традиційні військові дії із нетрадиційними методами впливу, включно з кібероперацією, дезінформацією, економічним тиском і політичним маніпулюванням[76]. Для протидії таким загрозам, відповідно до дослідження «Протидія гібридним загрозам: Кроки до вдосконалення співпраці між ЄС і НАТО», альянс розробив системний підхід, який базується на трьох взаємопов'язаних рівнях: стратегічному, оперативному та тактичному. На стратегічному рівні НАТО формує політичні рамки, визначає пріоритети реагування та координує дії держав-членів, щоб забезпечити спільну готовність до протидії гібридним загрозам. Важливим елементом цієї роботи є створення механізмів обміну інформацією та аналітичної підтримки, що дозволяє своєчасно

ідентифікувати потенційні загрози та оцінювати їхній вплив на безпеку Альянсу. На оперативному рівні ключовим завданням НАТО є підвищення здатності держав-членів швидко реагувати на кризові ситуації, пов'язані з гібридними операціями. Це включає проведення навчань і тренінгів, спрямованих на відпрацювання сценаріїв кібератак, інформаційних кампаній та інших форм непрямого впливу, а також розробку оперативних процедур для координації дій між цивільними та військовими структурами. Альянс активно підтримує створення «Центрів передового досвіду» та аналітичних підрозділів, які спеціалізуються на вивченні тактик гібридної агресії, моделюванні можливих сценаріїв та розробці рекомендацій для підвищення національної стійкості[76].На тактичному рівні НАТО здійснює практичні заходи з протидії конкретним формам гібридної агресії, включно з кіберзахистом критично важливої інфраструктури, боротьбою з дезінформаційними кампаніями та підвищенням кіберграмотності населення. Окрім цього, НАТО підтримує партнерські країни у підвищенні їхніх спроможностей захищати власні комунікаційні мережі, фінансові системи та урядові структури від гібридних загроз, що забезпечує більш високий рівень колективної безпеки. Важливим аспектом протидії гібридній війні є також правове та нормативне забезпечення, яке визначає рамки дозволених дій та процедури взаємодії між державами-членами. НАТО сприяє створенню стандартів, що регламентують обмін інформацією, захист критичних об'єктів та реагування на кібератаки, забезпечуючи при цьому дотримання міжнародного права та прав людини. Таким чином, протидія гібридним загрозам у рамках НАТО є багаторівневою і комплексною стратегією, що поєднує політичні, військові, технічні та правові інструменти для забезпечення колективної безпеки та стійкості Альянсу перед сучасними викликами[76].

Отже, аналіз діяльності Європейського Союзу та НАТО у сфері протидії гібридним загрозам свідчить про формування цілісної багаторівневої системи безпеки, яка поєднує аналітичні, інституційні,

інформаційні та правові інструменти реагування. Європейський Союз сконцентрував свої зусилля переважно на розбудові механізмів стратегічної стійкості, від створення HybridFusionCell для аналітичної координації до запуску програм EastStratComTaskForce та HybridCoE, які формують основу європейської інформаційної та кібербезпеки. Ці ініціативи спрямовані на виявлення гібридних атак, протидію дезінформації, посилення міждержавної співпраці та підвищення обізнаності суспільства щодо методів інформаційного впливу.

НАТО, своєю чергою, розвиває більш комплексний і багаторівневий підхід, який охоплює стратегічний, оперативний і тактичний виміри. Альянс зосереджується на забезпеченні колективної готовності держав-членів до реагування на гібридні виклики, вдосконаленні стандартів кіберзахисту, розробці спільних сценаріїв навчань та зміцненні партнерських зв'язків із країнами, які перебувають поза межами НАТО. Спільною рисою підходів ЄС і НАТО є визнання того, що гібридна війна має насамперед політичний характер, а отже, ефективна відповідь на неї потребує не лише військових рішень, а й розвитку демократичних інститутів, зміцнення інформаційного простору. Таким чином, протидія гібридній агресії у сучасних умовах є не лише завданням окремих держав, а спільною відповідальністю всього євроатлантичного простору.

Аналіз міжнародної та української практики протидії гібридним загрозам свідчить, що сучасна гібридна війна є багатовимірним явищем, яке поєднує військові, інформаційні, кібернетичні, економічні та політичні засоби впливу. Досвід України після 2014 року демонструє ефективність гібридної агресії РФ у поєднанні традиційних і новітніх методів, а трансформація цих засобів під час повномасштабного вторгнення 2022 року підкреслює потребу у швидкій адаптації захисних механізмів. Міжнародні інституції, зокрема ЄС та НАТО, формують системний багаторівневий підхід до протидії гібридним загрозам, який поєднує стратегічну координацію, аналітичну підтримку та практичні заходи на оперативному і тактичному

рівнях. Україна активно інтегрується в ці механізми, використовуючи можливості обміну інформацією, участі у навчаннях та розвитку національної кібер- та інформаційної безпеки.

Спільною рисою міжнародних та національних стратегій є визнання політичного та інституційного характеру гібридної агресії, що підкреслює необхідність комплексного підходу: від розвитку демократичних інститутів і підвищення стійкості суспільства до застосування новітніх технологій для виявлення і нейтралізації загроз. Отже, ефективна протидія гібридним викликам у сучасних умовах є не лише завданням окремих держав, а спільною відповідальністю України та її євроатлантичних партнерів.

4.3. Рекомендації щодо вдосконалення системи протидії гібридним загрозам

Досвід останніх років, зокрема анексія Криму, збройний конфлікт на сході України, початок повномасштабного вторгнення та активізація інформаційних кампаній противника в цифровому середовищі, продемонстрував, що ефективна безпека потребує не лише зміцнення оборонного потенціалу, а й комплексного підходу, який охоплює всі аспекти функціонування держави. Водночас ключовим елементом гібридної стратегії противника є не стільки застосування великого набору методів, скільки пошук «слабкої ланки» у внутрішній системі держави. Вплив на таку вразливість дає можливість агресору суттєво послабити або навіть паралізувати здатність країни чинити опір.

У цьому контексті, для запровадження ефективної боротьби проти російської гібридної війни проти України, стратегічне значення набуває розвиток системи протидії таким загрозам, здатної своєчасно виявляти ризики, забезпечувати координацію між різними органами влади, залучати міжнародних партнерів, а також адаптуватися до швидко змінного характеру загроз. Вдосконалення такої системи вимагає узгоджених і багаторівневих

заходів, що поєднують правові, організаційні, технологічні та освітні інструменти, формуючи комплексну стратегію захисту національних інтересів та зміцнення довіри громадян до державних інститутів.

Ключовою умовою ефективної протидії гібридним загрозам є зміцнення внутрішньої стійкості суспільства через системну боротьбу з корупцією як критичною вразливістю національної безпеки. Сучасний досвід переконливо демонструє, що корупція перетворюється на стратегічний інструмент дестабілізації, який ворог активно експлуатує для підриву довіри до державних інституцій, поглиблення суспільних розколів та послаблення обороноздатності. Для мінімізації цих ризиків необхідно запровадити жорсткі механізми притягнення до відповідальності посадових осіб за корупційні правопорушення, особливо в оборонному та безпековому секторах, забезпечити реальну незалежність антикорупційних органів та прозорість державних закупівель, а також посилити громадський контроль за діяльністю влади. Лише через викорінення системної корупції можна позбавити противника можливості використовувати внутрішні вразливості держави для досягнення своїх стратегічних цілей та створити міцний фундамент національної ідентичності, здатної протистояти багатовимірним гібридним викликам.

Одним із головних напрямів розвитку є підвищення ефективності міжвідомчої координації та управління ресурсами, що передбачає створення інтегрованої платформи обміну інформацією між центральними органами влади, місцевими адміністраціями, спеціальними службами та громадянськими структурами. Така система дозволяє своєчасно виявляти загрози, відстежувати їхній розвиток і оперативно приймати стратегічні рішення, забезпечуючи єдність дій на всіх рівнях управління. Не менш важливим є посилення законодавчої та нормативної бази, яка регламентує механізми протидії гібридним впливам, забезпечує правові рамки для взаємодії державних органів та міжнародних партнерів і водночас гарантує дотримання принципів прав людини та міжнародного права. У цьому

контексті пріоритетом є адаптація національних законів до стандартів ЄС і НАТО, що створює передумови для ефективної інтеграції України у євроатлантичний простір безпеки та спрощує координацію у спільних гібридних операціях. Особлива увага має приділятися розвитку інформаційної та кібербезпеки, що включає не лише захист критичної інфраструктури, урядових комунікаційних мереж і фінансових систем, а й підвищення цифрової грамотності населення, створення аналітичних центрів моніторингу дезінформації та оперативного реагування на інформаційні кампанії противника.

Також слід приділити подальшій інтеграції України в євроатлантичні безпекові структури. Покращення українських стандартів безпеки з принципами НАТО та ЄС, участь у програмах Partnership Interoperability Initiative, Resilience Concept, а також у діяльності HybridCoE та Cyber Diplomacy Tool box, сприятиме не лише зміцненню обороноздатності, а й підвищенню міжнародної довіри до України як до надійного партнера у сфері колективної безпеки. Впровадження таких практик дозволить створити спільну архітектуру реагування на гібридні загрози, що базуватиметься на обміні інформацією, спільних оцінках ризиків і координації політичних рішень.

Узагальнюючи зміст наведеного матеріалу, можна дійти висновку, що формування української системи протидії гібридним загрозам було тривалим, нерівномірним і значною мірою реактивним процесом, зумовленим історичними, політичними та геополітичними обставинами. Від моменту проголошення незалежності Україна стикалася з обмеженими інституційними можливостями та недостатнім розумінням багатовимірного характеру сучасних загроз. У 1990-х – на початку 2000-х років безпекова політика залишалася переважно зорієнтованою на традиційні воєнні та політичні ризики, а енергетична, інформаційна та економічна залежність від Російської Федерації створила передумови для подальших гібридних впливів. Переломним моментом стали події 2014 року, коли Україна фактично вперше

зіткнулася з масштабною гібридною агресією, що змусило державу переглянути підходи до національної безпеки, створити нові інституції, закріпити поняття гібридної війни в стратегічних документах, активізувати співпрацю з Європейським Союзом і НАТО та сформувати засади для кіберзахисту й інформаційної стійкості. Попри ці кроки, система залишалася фрагментарною, недостатньо централізованою і часто залежною від політичної кон'юнктури. Повномасштабне вторгнення 2022 року стало каталізатором глибоких трансформацій, прискоривши формування моделі національної стійкості, яка передбачає інтеграцію військових, інформаційних, кібернетичних, дипломатичних та економічних інструментів. Сучасна Україна дедалі активніше залучається до міжнародних механізмів координації, взаємного обміну даними та спільного планування гібридної безпеки, що робить її практичним полігоном для вироблення євроатлантичних підходів у цій сфері. Водночас ефективність національної системи протидії гібридним загрозам все ще обмежується недосконалою міжвідомчою взаємодією, потребою у подальшій модернізації законодавчої бази, кадровими викликами та залежністю від міжнародної підтримки. Незважаючи на значний прогрес, система перебуває у процесі становлення та вимагає поглиблення координації, укріплення інституційної спроможності та комплексного розвитку інструментів раннього виявлення, стримування й нейтралізації гібридних впливів. Україна не лише рухається до створення повноцінної й ефективної моделі протидії гібридним загрозам, а й набуває унікального досвіду, який може стати важливою складовою євроатлантичної архітектури безпеки.

ВИСНОВКИ

Проведене дослідження трансформації методів гібридної агресії Російської Федерації проти України у 2014–2025 роках дало змогу комплексно реалізувати поставлену мету й повною мірою виконати завдання, визначені у вступі. Аналіз теоретико-концептуальних підходів засвідчив, що феномен гібридної війни у сучасній науковій думці розглядається як системна, багатовимірна форма конфлікту, що інтегрує військові, політичні, інформаційні, економічні, енергетичні та психологічні інструменти впливу. Узагальнення положень світових і українських дослідників дало змогу уточнити сутність гібридної агресії та визначити її як процес, спрямований передусім на підрив стійкості держави-жертви та маніпулювання суспільною свідомістю. Аналіз джерельної бази та методологічних засад забезпечив комплексність і міждисциплінарність підходу до викладеної проблематики. Робота спиралася на поєднання нормативно-правових документів, міжнародних стратегій, матеріалів НАТО, ЄС та HybridCoE, аналітичних звітів, медіаджерел і наукових досліджень, що дозволило простежити еволюцію гібридних методів РФ у широкому політичному й інформаційному контексті.

Серед основних передумов гібридної агресії є сприйняття Росією українських євроінтеграційних прагнень як загрози. Європейський та євроатлантичний вибір України, що оформився після Революції Гідності 2013-2014 років, російське керівництво інтерпретувало як екзистенційну загрозу власній авторитарній моделі та геополітичним амбіціям. Водночас розвиток інформаційних технологій, соціальних мереж та кіберпростору надали агресору принципово нові інструменти впливу, які дозволяли досягати стратегічних цілей без масштабного застосування конвенційних збройних сил. Асиметрія потенціалів між Росією та Україною, поєднана з відносною слабкістю міжнародно-правових механізмів протидії гібридним загрозам,

створила сприятливе середовище для реалізації російської стратегії поетапного підриву української державності.

У ході дослідження було визначено, що в період 2014–2021 років Росія застосовувала комплексний набір гібридних інструментів, який включав політичний і економічний тиск, енергетичні маніпуляції, діяльність проксі-сил та маріонеткових утворень на Донбасі, а також масштабні інформаційно-психологічні операції. Ці методи дозволяли агресору уникати прямого міжнародного осуду, здійснювати прихований вплив на внутрішню політику України та створювати умови для подальшої ескалації конфлікту.

З початком повномасштабного вторгнення гібридна агресія РФ зазнала трансформації. Відбулося не стільки розширення інструментарію, скільки зміна його інтенсивності, пріоритетів та форм застосування. Гібридний тиск поєднався з відкритими воєнними діями, утворивши комбінований формат війни, у якому зросла роль кібератак, енергетичного й продовольчого шантажу, маніпуляцій у міжнародному інформаційному просторі, а також технологій deepfake та штучного інтелекту. Новітні технології дали змогу РФ проводити швидкі, адресні та важковиявні інформаційні операції, спрямовані як на внутрішню аудиторію України, так і на міжнародну спільноту. Особливе значення в умовах повномасштабної агресії набули інформаційно-психологічні операції, які стали центральним компонентом російської стратегії. Координовані дезінформаційні кампанії, робота бот-мереж та створення штучних інформаційних хвиль продемонстрували системність російського впливу та його тісну прив’язаність до ключових політичних подій. Дослідження українських механізмів протидії показало, що з 2014 року система національної стійкості пройшла шлях від реактивної моделі до стратегічно орієнтованої структури, яка включає розвиток кіберзахисту, зміцнення інформаційної безпеки, формування інституцій стратегічних комунікацій та підготовку до комплексного реагування на гібридні загрози. Важливою складовою цього процесу стала міжнародна співпраця з НАТО, ЄС та спеціалізованими центрами протидії гібридним загрозам, що

забезпечило впровадження передових практик, посилення координації та збільшення можливостей України у сфері безпеки.

Наслідки трансформації методів гібридної війни мають багатовимірний характер і виходять далеко за межі українсько-російського конфлікту, фундаментально змінивши архітектуру глобальної безпеки, прискоривши технологічні та геополітичні трансформації та виявивши критичні вразливості сучасної міжнародної системи. Для України наслідки є екзистенційними — масштабні людські втрати, руйнування інфраструктури та міграція мільйонів громадян поєднуються з безпрецедентною консолідацією суспільства, модернізацією збройних сил та перетворенням країни на глобального експерта з питань протидії гібридній агресії. На міжнародному рівні конфлікт виявив критичні недоліки існуючої системи міжнародного права у протидії гібридним загрозам.

Формування рекомендацій щодо вдосконалення системи протидії стало логічним підсумком проведеного аналізу. Вони охоплюють напрями зміцнення міжвідомчої взаємодії, підвищення ефективності стратегічних комунікацій, модернізації кіберзахисту, удосконалення законодавчої бази та розширення міжнародної координації. Узагальнений досвід підтверджує, що лише системний підхід, заснований на синергії державних інституцій, суспільства та міжнародних партнерів, здатен забезпечити стійкість перед гібридними викликами XXI століття.

У підсумку встановлено, що гібридна війна Росії проти України є тривалим, багатофазовим і технологічно динамічним процесом, спрямованим на підрив української державності та дестабілізацію європейської безпеки. Її еволюція у 2014–2025 роках свідчить про здатність агресора гнучко адаптувати тактику відповідно до змін міжнародного середовища та розвитку цифрових технологій. Водночас розвиток української системи протидії та міжнародної підтримки демонструє, що Україна поступово вибудовує ефективну модель національної стійкості, яка стає важливою складовою сучасної євроатлантичної архітектури безпеки.

СПИСОК ДЖЕРЕЛ І ЛІТЕРАТУРИ

1. Аэропорты Симферополя и Севастополя захвачены вооруженными людьми. *Politnavigator*. URL: https://web.archive.org/web/20251107135834/https://www.politnavigator.net/aehroport-simferopolya-zakhvachen-vooruzhennymi-lyudmi.html (дата звернення: 02.10.2025).

2. Бартош Н. В. Актуальні питання удосконалення реалізації державної інформаційної політики України в умовах гібридної війни. *Публічне урядування*. 2021. № 3 (28). С. 17–24.

3. В ефірі «Україна 24» показали фейкове повідомлення Зеленського про «капітуляцію», президент його спростував. *UNIAN*. URL: https://www.unian.ua/society/v-efiri-ukrajina-24-pokazali-feykove-povidomlennya-zelenskogo-pro-kapitulyaciyu-prezident-yogo-sprostuvav-novini-ukrajini-11746198.html (дата звернення: 05.08.2025).

4. Васильців Т., Лупак Р., Волошин В. Стратегічні імперативи державної політики протидії гібридним загрозам і забезпечення економічної безпеки України. *Економіка України*. 2021. № 64. С. 32–51. DOI: 10.15407/economyukr.2021.02.032.

5. Военная доктрина Российской Федерации: утверждена Президентом РФ 25 декабря 2014 г. URL: https://web.archive.org/web/20251007142739/http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf (дата звернення: 02.09.2025).

6. Горбулін В. П. Гібридна війна: сутність, структура, особливості. Київ: НІСД, 2017. 320 с.

7. Діпфейки президентів, які використовуються в російсько-українській війні. *BBC*. URL: https://www.bbc.com/news/technology-60780142 (дата звернення: 02.08.2025).

8. Додаткові протоколи до Женевських конвенцій від 8 червня 1977 року. Протокол I та Протокол II. *ICRC*. URL: https://www.icrc.org/uk/doc/resources/documents/misc/additional-protocols-1977.htm (дата звернення: 01.08.2025).

9. Доктрина информационной безопасности Российской Федерации: Указ Президента РФ від 5 грудня 2016 р. № 646. URL: https://web.archive.org/web/20251109180553/http://kremlin.ru/acts/bank/41460 (дата звернення: 02.10.2025).

10. Дослідження «Окупація Криму: без знаків, без імен, ховаючись за спинами цивільних». URL: https://web.archive.org/web/20200131145841/https://helsinki.org.ua/publications/doslidzhennia-okupatsiia-krymu-bez-znakiv-bez-imen-khovaiuchys-za-spynamy-tsyvil-nykh/ (дата звернення: 15.09.2025).

11. Женевські конвенції про захист жертв війни від 12 серпня 1949 року. *Ombudsman.gov.ua*. URL: https://ombudsman.gov.ua/uk/zhenevski-konvenciyi-pro-zahist-zhertv-vijni-1949-roku (дата звернення: 02.08.2025).

12. «За спинами жінок і дітей»: використання РФ цивільного населення як «живих щитів» під час окупації Криму. *Helsinki.org.ua*. URL: https://web.archive.org/web/20200131145747/https://helsinki.org.ua/articles/za-spynamy-zhinok-i-ditej-vykorystannya-rf-tsyvilnoho-naselennya-yak-zhyvyh-schytiv-pid-chas-okupatsiji-krymu/ (дата звернення: 02.08.2025).

13. «Зелені чоловічки» в Криму: з чого все почалося і чим закінчилося (відео). URL: https://umoloda.kyiv.ua/number/0/196/130858/ (дата звернення: 02.09.2025).

14. Клименко А. Морський вимір гібридної війни. Київ: Black Sea Institute of Strategic Studies, 2020. 112 с.

15. Мартинова В. В. Особливості російської концепції гібридної війни та її практичного втілення. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*. 2025. Вип. 17, т. 1. С. 44–48. URL: https://jvestnik-sss.donnu.edu.ua/article/view/17288.

16. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь / ред. кол.: С. І. Пирожков та ін. Київ: ІПіЕНД ім. Кураса НАН України, 2022. 552 с.

17. Перепелиця Г. М. Гібридна війна Росії проти України: воєнно-політичний аналіз і стратегічні наслідки. Київ: НІСД, 2015. 520 с.

18. Порошенко: Держструктури зазнали 6,5 тис. кібератак, до деяких причетна РФ. *Ukrinform*. URL: https://www.ukrinform.ua/rubric-polytics/2148600-porosenko-derzstrukturi-zaznali-65-tisaci-kiberatak-do-deakih-pricetna-rf.html (дата звернення: 01.10.2025).

19. Путін вперше визнав, що «зелені чоловічки» — його військові. *Українська правда*. URL: https://www.pravda.com.ua/news/2014/04/17/7022770/ (дата звернення: 01.10.2025).

20. Путін: в Криму діють не війська РФ, а «загони самооборони». *Espreso.tv*. URL: https://web.archive.org/web/20140419190403/http://espreso.tv/new/2014/03/04/putin_v_krymu_diyut_ne_viyska_rf_a_zahony_samooborony_yaki_zabraly_zbroyu_v_ukrayinciv (дата звернення: 03.10.2025).

21. Росія намагається узаконити примусову мобілізацію на окупованих територіях. *Glavcom.ua*. URL: https://glavcom.ua/country/incidents/rosija-namahajetsja-uzakoniti-primusovu-mobilizatsiju-na-okupovanikh-teritorijakh-1086160.html (дата звернення: 02.11.2025).

22. Російські хакери розповсюджують фейкові СМС про Одесу. *Odessa.life*. URL: https://odessa-life.od.ua/uk/news-uk/rosijski-hakery-rozpovsyudzhuyut-cherez-sms-bezgluzdyj-fejk-pro-odesu (дата звернення: 02.11.2025).

23. Росіяни розсилають фейкові SMS із закликами «зливати» інформацію про ЗСУ. *KP.ua*. URL: https://kp.ua/ua/politics/a678655-rosijani-rozsilajut-fejkovi-sms-iz-zaklikami-zlivati-informatsiju-pro-zsu (дата звернення: 02.11.2025).

24. Савлюк М. Гібридна війна в Україні: сучасні підходи. *Вісник Прикарпатського університету. Політологія*. 2024. Вип. 17. С. 187–197. DOI: 10.32782/2312-1815/2024-17-23.

25. СБУ повідомила про підозру блогеру, який придумав словосполучення «ввічливі люди». *RBC.ua*. URL: https://www.rbc.ua/rus/news/sbu-povidomila-pidozru-blogeru-kiy-pridumav-1717425991.html (дата звернення: 12.09.2025).

26. Хакерські атаки на Україну. *Слово і Діло*. URL: https://www.slovoidilo.ua/2025/03/24/infografika/bezpeka/najmasshtabnishi-kiberataky-ukrayinu (дата звернення: 12.10.2025).

27. 11-та річниця незаконного «референдуму» у Криму. *Espreso.tv*. URL: https://espreso.tv/suspilstvo-richnitsya-z-dnya-provedennya-nezakonnogo-referendumu-v-krimu (дата звернення: 12.10.2025).

28. 27 лютого 2014 року — захоплення адміністративних будівель у Сімферополі. *PPU.gov.ua*. URL: https://ppu.gov.ua/press-center/27-liutoho-2014-rotsi-zakhoplennia-rosiyskymy-spetspryznachentsiamy-administratyvnykh-budivel-v-simferopoli (дата звернення: 12.09.2025).

29. Actions on the ground: EU projects reacting to help Ukraine in the face of Russian aggression. *Euneighbourseast*. URL:

https://euneighbourseast.eu/standwithukraine/euprojects (дата звернення: 03.09.2025).

30. Anti trust: Commission Opens Formal Investigation into Gazprom's Business Practices. *EC.europa.eu*. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_15_4828 (дата звернення: 02.11.2025).

31. Atlantic Council. The Kremlin's Gas Games in Europe: How Russia Manipulates Energy for Geopolitical Gain. URL: https://www.atlanticcouncil.org (дата звернення: 02.11.2025).

32. Beznosiuk M. Russian hybrid warfare: Ukraine's success offers lessons for Europe. *Atlantic Council*. 5 June 2025. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/russian-hybrid-warfare-europe-should-study-ukraines-unique-experience/ (дата звернення: 05.10.2025).

33. Bilichak O., Huz A. Hybrid war as an tool of foreign policy of the Russian Federation: the Ukrainian dimension (1991–2023). *East European Historical Bulletin.* 2024. № 30. P. 162–178.

34. Conflict in Ukraine: A timeline. *UK Parliament Research Briefings*. URL: https://researchbriefings.files.parliament.uk/documents/CBP-9476/CBP-9476.pdf (дата звернення: 06.10.2025).

35. Crimea – The Russian Cyber Strategy to Hit Ukraine. *Infosec Institute*. URL: https://www.infosecinstitute.com/resources/threat-intelligence/crimea-russian-cyber-strategy-hit-ukraine (дата звернення: 06.10.2025).

36. Deepfake presidents used in Russia-Ukraine war. *BBC*. URL: https://www.bbc.com/news/technology-60780142 (дата звернення: 05.09.2025).

37. Deepfakes, explained. *Mitsloan.mit.edu*. URL: https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained (дата звернення: 11.10.2025).

38. Deepfakes, Misinformation, and Disinformation in the Era of Frontier AI. *arXiv*. URL: https://arxiv.org/pdf/2311.17394 (дата звернення: 11.10.2025).

39. Deepfake video of Zelenskyy could be 'tip of the iceberg'. *NPR*. URL: https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia (дата звернення: 06.10.2025).

40. Deepfake: Fake Obama Video Calling Trump Dipshit Is a Disturbing Trend. *BusinessInsider*. URL: https://www.businessinsider.com/obama-deepfake-video-insulting-trump-2018-4 (дата звернення: 07.10.2025).

41. Defending Europe's Resilience: Hybrid Threats and the Future of European Security. *ECFR Policy Brief*. URL: https://ecfr.eu/publication/defending-europes-resilience-hybrid-threats/ (дата звернення: 07.11.2025).

42. Digital occupation: Pro-Russian bot networks target Ukraine's occupied territories on Telegram. *Atlantic Council*. URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/report-russian-bot-networks-occupied-ukraine (дата звернення: 02.10.2025).

43. Dilemmas of Interdependence. *Problems of Post-Communism*. Library and Archives Canada. URL: https://www.collectionscanada.gc.ca/obj/s4/f2/dsk2/mq22786.pdf (дата звернення: 09.10.2025).

44. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for cybersecurity (NIS2). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng (дата звернення: 02.11.2025).

45. National Security Strategy of Ukraine. Draft. 2015. URL: https://niss.gov.ua/sites/default/files/2015-01/Draft_strategy.pdf (дата звернення: 05.10.2025).

46. Energy as a Weapon: Call Russia's Bluff and Stem Ukraine's Corruption. *ICDS*. URL: https://icds.ee/en/energy-as-a-weapon-call-russias-bluff-and-stem-ukraines-corruption/ (дата звернення: 09.10.2025).

47. European Commission & High Representative. The EU's Cybersecurity Strategy for the Digital Decade. Brussels, 2022. JOIN(2020) 18 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0018 (дата звернення: 11.10.2025).

48. European Commission. Joint Framework on Countering Hybrid Threats: a European Union response. Brussels, 2016. COM(2016) 410 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018 (дата звернення: 11.10.2025).

49. EU DisinfoLab. The impact of Russian disinformation on migration narratives in Europe. Brussels, 2023. URL: https://www.disinfo.eu/publications/the-impact-of-russian-disinformation-on-migration-narratives-in-europe (дата звернення: 06.10.2025).

50. EU Hybrid Fusion Cell. *EEAS*. URL: https://www.eeas.europa.eu/eeas/eu-hybrid-fusion-cell_en (дата звернення: 06.10.2025).

51. EU needs to rethink Russian sanctions to cut energy costs — Hungary's Orban. *Reuters*. URL: https://www.reuters.com/world/europe/eu-needs-rethink-russian-sanctions-cut-energy-costs-hungarys-orban-says-2024-11-15 (дата звернення: 01.09.2025).

52. EU Support to Strengthening Cyber Security in Ukraine. *EGA*. URL: https://ega.ee/project/strengthening-cyber-security-in-ukraine (дата звернення: 01.10.2025).

53. European Centre of Excellence for Countering Hybrid Threats. Annual Report 2023. Helsinki: HybridCoE. URL: https://www.hybridcoe.fi/publications/ (дата звернення: 16.10.2025).

54. European Commission. Impact of Russia's sanctions on global food and fertiliser markets. Brussels, 2023. 27 p.

55. European Union Institute for Security Studies. The EU and the 2006 and 2009 Gas Crises: Lessons for Energy Security. URL: https://www.iss.europa.eu (дата звернення: 17.10.2025).

56. EUvsDisinfo. EUvsDisinfo Annual Review 2023: Disinformation Dynamics in the Context of Russia’s War against Ukraine. Brussels: EEAS, 2023. 54 p.

57. Everyone's favourite Hillary Clinton quote. *Reddit*. URL: https://www.reddit.com/r/PoliticalCompassMemes/comments/155qygk/everyones_favourite_hillary_clinton_quote/ (дата звернення: 20.10.2025).

58. Facebook видалив дипфейк із президентом Зеленським — це суперечить політиці соцмережі. *NV*. URL: https://techno.nv.ua/ukr/it-industry/facebook-vidaliv-dipfeyk-iz-prezidentom-ukrajini-zelenskim-ce-superechit-politici-socmerezhi-50225783.html (дата звернення: 21.10.2025).

59. Food and Agriculture Organization of the United Nations. FAO scales up efforts to save upcoming harvest, ensure export of vital grains. Rome, *fao.org* URL: https://www.fao.org/newsroom/detail/ukraine-fao-scales-up-efforts-to-save-upcoming-harvest-ensure-export-of-vital-grains/en (дата звернення: 17.10.2025)

60. Foreign interference in Ukraine's election. Atlantic Council. URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/foreign-interference-in-ukraine-s-election/ (дата звернення: 17.10.2025).

61. Hoffman F. G. Hybrid Warfare and Challenges. Potomac Institute for Policy Studies, 2007. 25 p.

62. Goodfellow I., Pouget-Abadie J., Mirza M., Xu B., Warde-Farley D., Ozair S., Courville A., Bengio Y. Generative Adversarial Networks. *Communications of the ACM*. Vol. 63. Issue 11. P. 139 – 144. URL: https://doi.org/10.1145/3422622

63. Governance: A 'whole-of-society' approach. United Nations iLibrary. URL: https://www.un-ilibrary.org/content/books/9789210026208c021 (дата звернення: 17.10.2025).

64. Helsinki Commission. Human Rights in Occupied Crimea: 2014–2023 Reports. Washington, D.C.: CSCE, 2023. 112 p.

65. Henderson J., Mitrova T. Russia's Strategy in European Gas Markets. Oxford Institute for Energy Studies, 2020. URL: https://www.oxfordenergy.org/publications/russias-strategy-in-european-gas-markets (дата звернення: 17.10.2025).

66. "Hiding Behind Women and Children": Civilians Used by Russia as Human Shields During Occupation of Crimea. URL: https://old.helsinki.org.ua/en/articles/hiding-behind-women-and-children-civilians-used-by-russia-as-human-shields-during-occupation-of-crimea (дата звернення: 17.10.2025).

67. Hoffman F. Hybrid War and Challenges. Washington, D.C.: Potomac Institute for Policy Studies. 25 p.

68. Horbulin V. The World Hybrid War: Ukrainian Forefront: monograph. Kharkiv: Folio, 2017. 158 p.

69. How did Russia's military aggression against Ukraine begin: Donbas. *War.ukraine.ua*. URL: https://war.ukraine.ua/russia-s-invasion-timeline/how-is-

russia-communicating-about-the-2014-invasion-of-ukraine (дата звернення: 14.10.2025).

70. How Ukraine became a test bed for cyber weaponry. *Politico.eu*. URL: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks (дата звернення: 14.10.2025).

71. Human Rights and International Security. Washington, D.C. (дата звернення: 14.10.2025).

72. Human Shields. Guide-humanitarian-law.org. URL: https://guide-humanitarian-law.org/content/article/3/human-shields (дата звернення: 14.10.2025).

73. Hungary Turns Itself into Hub for Russian Gas. BalkanInsight. URL: https://balkaninsight.com/2024/12/11/hungary-turns-itself-into-hub-for-russian-gas (дата звернення: 14.10.2025).

74. HybridCoE Strategic Analysis Reports 2021–2024. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2024. 78 p.

75. Hybrid threats to Ukraine and public security. The EU and Eastern Partnership Experience. Kyiv: Centre for Global Studies “Strategy XXI”, 2018. 106 с.

76. Hybrid threats: searching for a definition. Clingendael.org. URL: https://www.clingendael.org/pub/2021/countering-hybrid-threats/2-hybrid-threats-searching-for-a-definition (дата звернення: 14.10.2025).

77. International Committee of the Red Cross. International Review of the Red Cross, No. 872: The prohibition of using human shields in international humanitarian law. URL: https://international-review.icrc.org/sites/default/files/irrc-872.pdf

78. International Centre for Defence and Security. Energy as a Weapon: Call Russia’s Bluff and Stem Ukraine’s Corruption. URL: https://icds.ee/en/energy-as-a-weapon-call-russias-bluff-and-stem-ukraines-corruption/ (дата звернення: 14.10.2025).

79. Investopedia. Wheat prices jump after Russia pulls out of deal allowing grain shipments from Ukraine. URL: https://www.investopedia.com/russia-pulls-out-of-deal-allowing-grain-shipments-from-ukraine-7561824 (дата звернення: 14.10.2025).

80. Kaldor M. New and Old Wars: Organized Violence in a Global Era. 3rd ed. Stanford: Stanford University Press, 2012. 272 с.

81. Kalenský J., Osadchuk R. Hybrid CoE Research Report 11: How Ukraine Fights Russian Disinformation: Beehive vs Mammoth. URL: https://www.hybridcoe.fi/publications/hybrid-coe-research-report-11-how-ukraine-fights-russian-disinformation-beehive-vs-mammoth/ (дата звернення: 14.10.2025).

82. Karber F. Lessons of Russian Hybrid War in Ukraine. Atlantic Council, 2015. 42 p.

83. Kennan D. F. The Sources of Soviet Conduct. *Foreign Affairs*. 1947. Vol. 25, № 4. P. 566–582.

84. Kortunov S. Russia announces free grain deliveries to six African countries. URL: https://web.archive.org/web/20251108201702/https://russiancouncil.ru/en/analytics-and-comments/analytics/russia-announces-free-grain-deliveries-to-six-african-countries/ (дата звернення: 12.10.2025).

85. Kresin O. Counteracting Hybrid Threats in Ukrainian Legislation. *Foreign Trade: Economics, Finance, Law.* 2022. № 120 (1), P. 4–17. DOI: 10.31617/zt.knute.2022(120)01.

86. Kuchmii O., Frolova O. The Use of Social Media as a Tool of Modern Hybrid Warfare, 2023. DOI: https://doi.org/10.26693/ahpsxxi2023.si.093.

87. Kuzio T. The Long and Arduous Road: Ukraine Updates Its National Security Strategy. RUSI, 2020. URL: https://surl.lt/ztaqaf (дата звернення: 12.10.2025).

88. Liddell Hart B. H. Strategy. Praeger, 1954. 366 p.

89. Likely Kremlin-Backed Election Interference Against Romania Threatens Bucharest's Continued Support for Ukraine and NATO. Understandingwar.org. URL: https://understandingwar.org/backgrounder/likely-kremlin-backed-election-interference-against-romania-threatens-bucharests (дата звернення: 12.10.2025).

90. Thalen M. X.com. URL: https://x.com/MikaelThalen/status/1504123674516885507 (дата звернення: 12.10.2025).

91. Murray W., Mansur P. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge: Cambridge University Press, 2012. 364 p.

92. National Resilience of Ukraine: Hybrid Threats Challenge Response and Prevention Strategy: national report / eds. Pyrozhkov S. I. et al. Kyiv: Kuras Institute of Political and Ethnic Studies, 2022. 552 p.

93. NATO. Military Concept for Countering Hybrid Warfare (MC 0641). Brussels: NATO, 2015. 16 p.

94. NATO. Wales Summit Declaration. 5 September 2014. URL: https://www.nato.int/cps/en/natohq/official_texts_112964.htm (дата звернення: 12.10.2025).

95. NATO. Warsaw Summit Communiqué. 9 July 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (дата звернення: 12.10.2025).

96. Gleicher N. X.com. URL: https://x.com/ngleicher/status/1504186935291506693 (дата звернення: 01.10.2025).

97. NATO StratCom Centre of Excellence. Russian Influence Campaigns: Disinformation, Propaganda and the Use of Social Media. Riga, 2023. 48 p.

98. Nauka i Pravookhorona: Legal and Organizational Support of Law Enforcement Activities: monograph. Lviv: Liha-Pres, 2019. 308 p.

99. OPK. Herasimov's Hybrid Warfare. URL: https://surl.li/fkufyx (дата звернення: 12.10.2025).

100. Osadchuk R., Adam I., Gigitashvili G., Furbish M. How Inauthentic Accounts Exploit Telegram Comments to Spread Anti-Ukrainian Narratives. Atlantic Council. URL: https://dfrlab.org/2024/12/18/inauthentic-telegram-accounts-ukraine/ (дата звернення: 25.10.2025).

101. Participation in the Final International Workshop "Resilience to Hybrid Threat Challenges". Erasmusplus.org.ua. URL: https://erasmusplus.org.ua/en/news/participation-in-the-final-international-workshop-resilience-to-hybrid-threat-challenges-based-on-the-results-of-the-erasmus-cbhe-warn-project-07-11-2024-online (дата звернення: 27.10.2025).

102. Petya cyber-attack: Global damage and Ukraine impact. BBC News. URL: https://www.bbc.com/news/technology-40442578 (дата звернення: 23.10.2025).

103. European Parliament. Report on the Proposal for a Regulation on Phasing Out Russian Natural Gas Imports. URL: https://www.europarl.europa.eu/doceo/document/A-10-2025-0195_EN.html (дата звернення: 23.10.2025).

104. Cyber attack on satellite provider Viasat hits Europe. Reuters, 4 Mar. 2022. URL: https://www.reuters.com/technology/cyberattack-satellite-provider-viasat-hits-europe-2022-03-04/ (дата звернення: 28.11.2025).

105. Russia used "little green men" in Crimea. URL: https://web.archive.org/web/20200131145731/https://helsinki.org.ua/articles/rf-pid-chas-okupatsii-krymu-vykorystovuvala-zhyvi-shchyty-zelenykh-cholovichkiv-ta-zastosovuvala-virolomstvo-doslidzhennia/ (дата звернення: 28.11.2025).

106. Russian propaganda myths about Crimea. Ukrainer.net. URL: https://www.ukrainer.net/en/propaganda-myths-crimea (дата звернення: 28.10.2025).

107. Russia vs Ukraine: the biggest war of the fake news era. Reuters. URL: https://www.reuters.com/world/europe/russia-vs-ukraine-biggest-war-fake-news-era-2024-07-31 (дата звернення: 20.10.2025).

108. Russian–Ukrainian cyber warfare. Mr.kuchewar.com. URL: https://mr.kuchewar.com/russian-ukrainian-cyberwarfare (дата звернення: 27.10.2025).

109. Soesanto S. Ukraine's Counter-Hybrid Campaigns in Cyberspace. HCSS, 2023. URL: https://docs.clingendael.org/sites/docs/files/2023-11/ukraine_counter-hybrid_campaigns_in_cyberspace.pdf (дата звернення: 27.10.2025).

110. State Information Policy in the Sphere of the European and Euro-Atlantic Integration. National Security & Defence, 2008, № 1 (95), pp. 2–29.

111. Stowell J. Hybrid Warfare: Nonlinear Strategies and Psychological Operations. New York: Routledge, 2019. 256 p.

112. Svetoka S. Social Media as a Tool of Hybrid Warfare. URL: https://stratcomcoe.org/publications/social-media-as-a-tool-of-hybrid-warfare/177 (дата звернення: 25.10.2025).

113. The Liar's Dividend: The Impact of Deepfakes and Fake News on Trust in Political Discourse. Ideas.repec.org. URL: https://ideas.repec.org/p/osf/socarx/x43ph.html (дата звернення: 23.10.2025).

114. The need for a joint response to a threat of the hybrid war. RNBO. URL: https://www.rnbo.gov.ua/en/Diialnist/1874.html (дата звернення: 16.10.2025).

115. How the War in Ukraine Is Driving a Global Food Crisis. Time, 2022. URL: https://time.com/6166810/ukraine-global-food-crisis/ (дата звернення: 14.10.2025).

116. Top US Army General Says He's Letting ChatGPT Make Military Decisions. Futurism.com. URL: https://futurism.com/future-society/general-taylor-korea-chatgpt (дата звернення: 05.10.2025).

117. Ukraine to receive EU cyber support in event of attacks. Eufordigital.eu. URL: https://eufordigital.eu/ukraine-to-receive-eu-cyber-support-in-event-of-attacks (дата звернення: 05.11.2025).

118. Ukraine and the EU deepen partnership to counter hybrid threats. RNBO. URL: https://www.rnbo.gov.ua/en/Diialnist/7306.html (дата звернення: 05.10.2025).

119. Ukraine Gains Access to the EU Cybersecurity Reserve. Digitalstate.gov.ua. URL: https://digitalstate.gov.ua/news/govtech/ukraine-gains-access-to-the-eu-cybersecurity-reserve-operational-support-in-the-event-of-large-scale-attacks (дата звернення: 05.09.2025).

120. Ukraine must pay its gas bill – Russia declares Ukraine must pay its gas bill or be cut off. DW.com. URL: https://www.dw.com/en/russia-declares-ukraine-must-pay-its-gas-bill-or-be-cut-off/a-17630657 (дата звернення: 13.09.2025).

121. United Nations. Security Council briefing on the impact of the Ukraine conflict on global food security. URL: https://press.un.org/en/2022/sc14894.doc.htm (дата звернення: 14.09.2025).

122. United Nations. New deal to resume grain exports through Ukrainian ports. URL: https://press.un.org/en/2022/sc14990.doc.htm (дата звернення: 14.09.2025).

123. VoxUkraine Team. White Book of Reforms 2025. Chapter 16. Reforms of the Armed Forces of Ukraine. URL: https://voxukraine.org/en/white-book-of-reforms-2025-chapter-16-reforms-of-the-armed-forces-of-ukraine (дата звернення: 13.09.2025).

124. What Are Deepfakes and How Are They Created? IEEE Spectrum. URL: https://spectrum.ieee.org/what-is-deepfake (дата звернення: 13.11.2025).

125. White House. Statement by President Biden on Our Nation's Cybersecurity. URL: https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity (дата звернення: 16.10.2025).

126. Why the Donbas War Was Never “Civil”. Sceeus.se. URL: https://sceeus.se/en/publications/why-the-donbas-war-was-never-civil (дата звернення: 13.10.2025).

127. Ximera. Herasimov’s Doctrine. Ximera.com.ua, 2022. URL: https://ximera.com.ua/2022/10/gerasimov-doctrine/ (дата звернення: 20.10.2025).

128. Zetter K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Wired.com. URL: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (дата звернення: 20.10.2025).