КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
ГЕОГРАФІЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА КРАЇНОЗНАВСТВА ТА ТУРИЗМУ

ГІБРИДНІ ВІЙНИ ТА ЇХ ВПЛИВ НА СУЧАСНУ ГЕОПОЛІТИЧНУ ОБСТАНОВКУ У ЄВРОПІ

Кваліфікаційна робота магістра
за спеціальністю: 106 Географія
за освітньо-науковою програмою – Політична географія та геополітика
на здобуття освітнього ступеня: Магістр

Здобувачка денного відділення
Калюжна Катерина Романівна
Науковий керівник:
канд. геогр. наук, доц. Стафійчук В.І.

КИЇВ – 2025

ЗМІСТ

ВСТУП

Актуальність теми дослідження. У новітніх умовах глобального протистояння війна втратила ознаки класичної — із чіткими фронтами, формальним оголошенням, уніфікованою армією та зрозумілими цілями. Натомість сучасні конфлікти дедалі частіше набувають прихованих, багатошарових і водночас комплексних форм — політико-інформаційних, кібернетичних, економічних, дестабілізаційних. Усе це характеризує явище, відоме як гібридна війна. Його поява стала викликом не лише для безпекової політики окремих держав, а й для цілісної європейської геополітичної архітектури. Особливо це проявляється на тлі агресивної зовнішньої політики Російської Федерації, яка ще з 2014 року почала активно реалізовувати концепцію гібридного впливу на країни пострадянського простору, а згодом — і на весь європейський континент. Російсько-український конфлікт, що триває понад десятиліття, є концентрованим прикладом гібридної війни, яка включає в себе не лише бойові дії, а й кібератаки, інформаційні маніпуляції, економічний шантаж, дипломатичне нав’язування наративів та психологічний тиск на населення. Водночас європейські інституції — НАТО, ЄС, ОБСЄ — виявились змушеними адаптувати свої безпекові парадигми до умов, у яких відкритий напад часто підмінюється прихованим втручанням, а війна ведеться не гарматами, а через Wi-Fi, ефіри та фальшиві новини. Усе це зумовлює потребу в глибокому науковому аналізі явища гібридної війни, її наслідків і способів реагування на неї в умовах сучасної Європи.

Об'єкт дослідження. Гібридна війна як форма міждержавного протистояння в сучасному геополітичному контексті.

Предмет дослідження. Вплив гібридних воєн на геополітичну ситуацію в Європі, їхні складові та особливості реагування з боку окремих держав і міжнародних структур.

Мета дослідження. Системно проаналізувати гібридні війни як явище сучасної геополітики, дослідити їхні форми, етапи, механізми впливу, а також оцінити наслідки для безпекової структури Європи з урахуванням досвіду російсько-української війни.

Завдання дослідження:

1. Визначити поняття, генезу та теоретичні основи гібридної війни.
2. Виявити головні складові гібридного впливу (інформаційні, військові, політичні, економічні, кібернетичні).
3. Проаналізувати російсько-українську війну як приклад повномасштабної гібридної агресії.
4. Оцінити роль гібридних воєн у трансформації геополітичного простору Європи.
5. Вивчити реакцію Європейського Союзу, НАТО та ОБСЄ на нові типи загроз.
6. Дослідити інституційні та неформальні механізми протидії гібридним атакам у європейських державах.
7. Визначити потенціал використання досвіду України в контексті побудови європейської моделі стійкості.
8. Сформулювати загальні рекомендації щодо адаптації системи безпеки Європи до гібридних викликів.

Методологія дослідження. Аналіз побудований на застосуванні комплексу сучасних наукових підходів. Системний метод дозволив розглядати гібридну війну як міждисциплінарне явище, що одночасно функціонує у сфері політики, економіки, воєнної справи, інформації, культури та релігії. Геополітичний метод дав можливість інтерпретувати просторові зміни на мапі впливу гібридних акторів у Європі. Застосування кейс-стаді щодо конфлікту Росії проти України дало змогу глибоко реконструювати практику гібридної агресії. Усі методи працюють у взаємозв’язку, що дозволяє будувати комплексну аналітичну картину.

Наукова новизна. Робота пропонує комплексну типологізацію інструментів гібридної війни на основі європейського досвіду, вперше здійснює узагальнення

інституційних відповідей на гібридні виклики в розрізі регіональних блоків і демонструє Україну не лише як об’єкт агресії, а як учасника формування нової архітектури безпеки.

Практичне значення дослідження. Матеріали дипломної роботи мають практичну цінність для фахівців у сфері зовнішньої політики, безпеки, інформаційної аналітики, кіберзахисту та міжнародних відносин. Результати можуть бути використані в діяльності аналітичних центрів, державних структур, пов’язаних із розробкою стратегій кіберзахисту, інформаційної політики, збереження національного суверенітету. Крім того, напрацьовані положення, аналітичні моделі та класифікації можуть бути використані у викладанні дисциплін «міжнародні відносини», «геополітика», «сучасні конфлікти», «інформаційна безпека», «політологія міжнародної безпеки» у закладах вищої освіти, а також як база для модулів у системі підготовки держслужбовців, офіцерів ЗСУ, журналістів і фахівців із комунікацій.

Структура дипломної роботи. Робота складається з трьох розділів. У першому викладено теоретико-методологічні засади вивчення гібридної війни, зокрема еволюцію поняття, основні складові, існуючі наукові підходи. У другому розділі проаналізовано вплив гібридних війн на геополітичну конфігурацію Європи на прикладі ключового конфлікту — російсько-української війни. Третій розділ присвячено механізмам і стратегіям протидії гібридним загрозам з боку ЄС, НАТО, а також адаптації до них національних урядів. Завершальні висновки відображають загальні аналітичні результати й пропонують бачення майбутньої моделі європейської стійкості до багатовимірних конфліктів.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ГІБРИДНИХ ВІЙН

1.1 Гібридна війна як предмет дослідження в політичній географії

Розуміння війни у XXI столітті зазнало кардинального перегляду. Те, що ще кілька десятиліть тому вкладалося у класичне уявлення про конфлікти — зіткнення армій, контроль над територіями, окупація — нині набуває значно глибших, складніших форм. Однією з таких форм стала гібридна війна — явище, що впевнено вийшло за межі воєнного дискурсу і стало предметом міждисциплінарного аналізу. У політичній географії воно посіло особливе місце, оскільки прямо впливає на просторову структуру влади, кордони, національні ідентичності, інформаційний ландшафт і питання суверенітету.

Саме поняття "гібридна війна" стало масово використовуватися після 2014 року — у контексті вторгнення Росії в Україну. Але його інтелектуальні витоки — глибші. Ще у 2007 році Френк Хоффман окреслював перспективу появи конфліктів нового типу, де поєднуватимуться конвенційні та неконвенційні методи впливу, державні й недержавні актори, інформаційні кампанії, економічний тиск, диверсії, кібератаки, політичне втручання [14]. У цій складності полягає ключова характеристика гібридної війни: вона не має єдиного фронту, одного типу зброї чи чіткої лінії поділу між "ворогом" і "не ворогом".

Із точки зору політичної географії гібридна війна цікава тим, що трансформує класичні підходи до аналізу простору. Раніше аналітики зосереджувалися переважно на фізичних межах, геополітичному балансі сил, зоні контролю над певними територіями. Тепер фокус зміщується на контроль над віртуальними та ідеологічними просторами: інформаційними мережами, соціальними наративами, масовою свідомістю населення. Простір, в якому ведеться гібридна війна, не обов’язково фізично обмежений; це може бути медійна

сфера, ринок, освітнє середовище, релігійна спільнота — будь-який сегмент суспільства, де формуються і поширюються впливи.

У теоретичній площині дослідження гібридної війни виходить за межі лише військової науки або міжнародних відносин. Дедалі частіше воно охоплює і політичну географію, і безпекові студії, і соціологію, і комунікаційні науки. В академічному полі спостерігається стійкий консенсус щодо того, що гібридна війна — це передусім боротьба за домінування в системі значень, в інтерпретації подій, у визначенні того, що вважати правдою. Власне, у цьому контексті вкрай важливою є ідея «м'якого контролю над простором», який не потребує фізичного вторгнення — достатньо переформатувати уявлення населення про реальність [14]

Вивчаючи гібридну війну через призму політичної географії, не можна оминути питання просторової дифузії конфлікту. На відміну від традиційної війни, де об'єкти ураження зазвичай мають конкретні координати, у гібридному конфлікті цілі розпорошені. Вони можуть існувати паралельно у різних частинах світу: кампанія в соціальних мережах проти однієї держави здатна розгортатися з кількох континентів, фінансуватися з офшорних юрисдикцій і поширюватися мовою третьої країни [11].

Окрему увагу заслуговує зміна характеру державного суверенітету в умовах гібридних загроз. Геополітична карта, з якою працює політична географія, більше не відображає повного спектра впливів. Суверенітет, який раніше означав монополію на насильство на певній території, тепер має враховувати інформаційну та кіберсуверенність. Держава може зберігати контроль над фізичними кордонами, але бути повністю вразливою до зовнішніх впливів через інформаційні канали, маніпуляції в медіа, іноземні впливи на політичні процеси [8].

Значення концепції гібридної війни як дослідницької категорії також полягає в її інтерпретаційній багатовекторності. У полі наукової думки існують кілька конкуруючих підходів до визначення її сутності. Одні дослідники, зокрема Ю. Лисецький, О. Старовойтенко та Ю. Семенюк, наголошують на тому, що гібридна

війна — це насамперед конфлікт, де поєднуються методи класичної збройної боротьби з інструментами інформаційного, психологічного та економічного впливу [7]. Інші автори, такі як В. Жадько., П. Куляс, О. Харитоненко, розглядають гібридну війну крізь призму медіа та журналістики, акцентуючи увагу на її інформаційному ядрі та особливостях поширення дезінформації [11]

Паралельно з цим розвивається і критичний підхід, згідно з яким термін "гібридна війна" сам по собі є частиною пропагандистської конструкції. Один із яскравих прикладів — стаття Марка Ґалеотті про так звану "доктрину Герасимова", яка, як з'ясувалося, не є офіційною російською концепцією, а лише журналістською інтерпретацією [20]. Проте саме ця інтерпретація була широко підхоплена західними аналітиками й почала слугувати підґрунтям для формування безпекової риторики.

Ще одна особливість гібридної війни полягає в тому, що вона рідко має офіційно визнане оголошення. Така війна ведеться "у тіні", у сірій зоні - простором між миром і війною, де між собою конкурують державні і недержавні актори. Для розуміння операцій у сірій зоні збоку росії нижче продемонстровано картосхему (див. рис. 1.1). За даними CSIS російські операції охоплюють майже весь світ і відбуваються у формі шпигунства, військових провокацій, дезінформації, та втручання у політичний процес [18]

Вона не зупиняється у моменти формального перемир’я і не потребує класичних процедур капітуляції. Це особливо яскраво проявляється у випадку російсько-українського конфлікту, де етапи “мирного врегулювання” супроводжувалися активізацією інформаційних атак, саботажем, кібератаками та поширенням фейків [5].

У політичній географії важливо також враховувати просторову множинність гібридного впливу. Це стосується не тільки держав, що є безпосередніми об’єктами нападу, але й третіх країн, які мимоволі стають простором битви за інтерпретації. Наприклад, у країнах Балтії гібридна агресія РФ виявилася у формі

впливу на інформаційні простори російськомовного населення, політичного тиску, фінансування медіа-платформ, що поширювали прокремлівські меседжі [10].

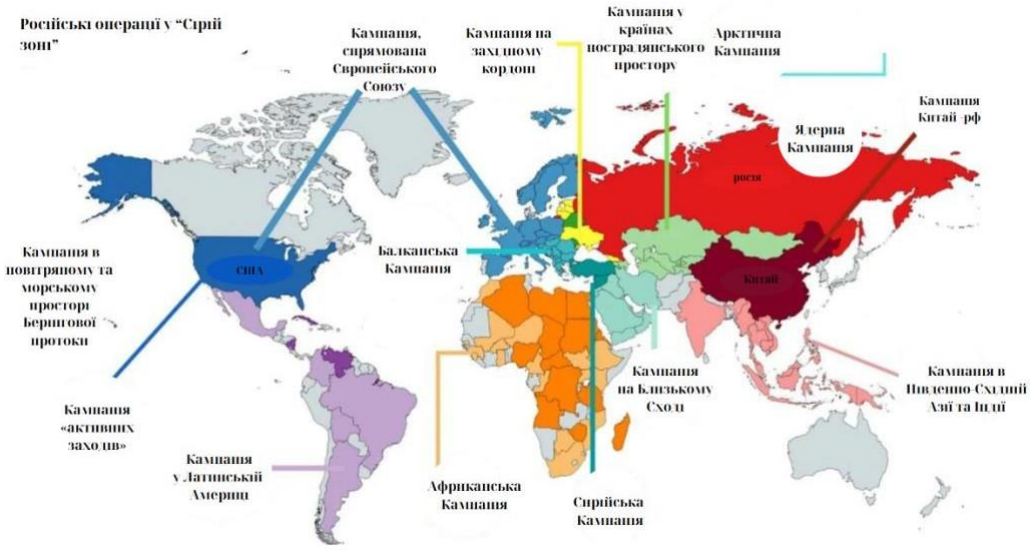

Рис 1.1. Картосхема російських гібридних операції у сірій зоні.

Джерело CSIS

Один із найкращих аналітичних підходів до структури гібридної війни пропонує Євген Магда, який виокремлює її складові через призму системного конфлікту, де поєднано інформаційні, воєнні, економічні та психологічні компоненти [12]. Він підкреслює, що гібридна війна завжди спрямована на дезорієнтацію, провокування внутрішньої дестабілізації та дискредитацію влади в очах громадян. Це дозволяє агресору досягати стратегічних цілей без повномасштабного вторгнення.

Цю думку розвиває також А. Рац у своєму дослідженні про російську гібридну війну в Україні, наголошуючи на цілеспрямованому послабленні здатності противника до опору не лише фізично, а й морально-психологічно [21]. Особливістю підходу А. Раца є акцент на інфільтрацію в політичні та суспільні структури: від фінансування «п'ятої колони» до поширення ідей фаталізму серед населення.

Інформаційний вимір гібридної війни окремо аналізується Володимиром Горбуліним, який вбачає у сучасних гібридних конфліктах боротьбу за інтерпретацію реальності. У його концепції мас-медіа постають не просто каналами поширення новин, а повноцінними полями бою, де вирішується, хто формує порядок денний [13]. Він також підкреслює роль алгоритмів соціальних мереж у «транспортуванні» маніпулятивного контенту.

На зміну традиційній концепції пропаганди приходить ідея «керованого хаосу», яку обґрунтовує Сергій Дацюк [17]. На його думку, гібридна агресія не обов'язково має на меті контроль, вона часто орієнтована на руйнування структур, що забезпечують стабільність у країні-жертві. Таким чином, політична географія стикається з явищем деструктивного впливу на соціальний простір: інституції розмиваються, суспільні орієнтири зникають, локальні ідентичності розчиняються у нав'язаному хаосі.

Зі свого боку, А. Хмель досліджує підхід Європейського Союзу до протидії гібридним загрозам, звертаючи увагу на нормативне закріплення принципу інформаційної безпеки як фундаментальної складової державного суверенітету [15]. У цьому контексті географічна категорія простору розширюється — не тільки фізична територія, а й віртуальний інформаційний простір потребує захисту як елемент державності.

Проблему методології дослідження гібридної війни також порушують В. Габчак [4], М. Гончаренко та М. Глух [8]. Габчак визначає гібридну війну як міждисциплінарну категорію, що поєднує методи політології, міжнародного права, соціології, безпекових студій. М. Гончаренко та М. Глух у свою чергу ж акцентують увагу на правовому аспекті: на їх думку, в міжнародному праві досі бракує чіткого визначення гібридної агресії, що створює ризики зловживань з боку держав-агресорів. У контексті політичної географії це відкриває питання про статус територій, окупованих без офіційного визнання — приклад Криму, частин Донбасу, Абхазії тощо.

Особливо глибоко просторову природу гібридної війни аналізують Ю. Лисецький, О. Старовойтенко та Д. Павленко. Вони пропонують схему, за якою гібридна агресія здійснюється по кількох осях: територіальній, інформаційній, політичній, демографічній [7]. Така мультиосність дозволяє розуміти війну як процес, що одночасно охоплює й впливає на фізичну територію, населення, структури влади й символічні конструкції — мови, наративи, образи минулого.

І. Цимбал, С. Панченко та А. Жовтун, аналізуючи інформаційно-психологічні аспекти гібридної війни, наголошують, що вона унікальна тим, що не тільки створює нові інформаційні конструкції, а й руйнує довіру до вже існуючих джерел знань. У цьому сенсі гібридна війна — це також війна проти інституцій: шкіл, університетів, медіа [16].

Окрему увагу варто звернути на аналіз зовнішньої політики Росії як інструменту гібридної експансії. Ці процеси детально досліджуються в роботі О. Білічака та А. Гуза [1], які показують, як через дипломатію, енергетичний шантаж і інформаційні атаки Росія створює нові форми впливу без прямого вторгнення.

На макрорівні наслідки гібридної агресії мають потенціал змінювати не лише політичний, а й географічний порядок. Так, анексія Криму та підтримка сепаратистів на Донбасі трансформували не лише адміністративну карту України, а й соціальну географію — мільйони внутрішньо переміщених осіб, нові осередки зростання, зміщення освітніх та релігійних центрів, перенесення бізнесу й державних установ [16].

Усе це — предмет політичної географії, що тепер має справу з реальністю, де війна не має лінії фронту, а зміни на карті відбуваються без формального оголошення війни. Таке нове середовище потребує переосмислення методів аналізу: індекси довіри, моніторинг медіа, аналіз інформаційних потоків та цифрової поведінки громадян доповнюють класичні інструменти роботи з територією.

Окремо слід зазначити, що гібридна війна — не лише конфлікт країн, а і взаємодія держави з недержавними суб'єктами. В цьому контексті працює теорія

про "війни четвертого покоління", які ведуться без оголошення, без фронтів, без чітких суб'єктів. Прикладом цього може бути діяльність проксі-структур у соціальних мережах, створених для впливу на громадську думку в інтересах іноземного уряду.

Окрема площина гібридної війни — це вплив на вибори. Такі впливи можуть змінювати результати голосувань шляхом дезінформації, маніпуляцій із цифровими платформами, поширення ворожих меседжів у ключові періоди електорального циклу. Це є безпосередньою загрозою не лише суверенітету, а й принципам демократичного устрою.

У відповідь на ці виклики країни НАТО розробили нову концепцію реагування. Вона не базується виключно на військовому стримуванні, як раніше. У статті «Hybrid Threats: NATO's Response» докладно описано, що союз адаптував свою політику до реалій, де атака в кіберпросторі чи кампанія дезінформації можуть спричинити такий самий ефект, як і обстріл [19]. НАТО визнає, що політична воля, інформаційна безпека та соціальна згуртованість — це ключові «просторові активи» країн-учасниць.

В Україні ці виклики набули гостроти ще з 2014 року. Аналізуючи український досвід, Н. Гординська і М. Майка зазначають, що з перших днів конфлікту Росія діяла на багатьох фронтах одночасно — від воєнного до ідеологічного, від дипломатичного до освітнього [9]. Ця мультивекторність породжує «гібридну картографію»: карту, яка не лише фіксує фізичні об'єкти, а й накладає шари впливу — інформаційного, економічного, політичного.

Серед українських дослідників, які зробили значний внесок у розуміння гібридної війни як географічного процесу, варто виокремити Миколу Білоусова. Він зосереджується на кіберкомпоненті, але виводить її в ширший контекст — як спосіб трансформації публічного простору, де людина вже не може безпечно споживати інформацію, адже будь-який канал може бути отруєний навмисною дезінформацією [2].

Ще один показовий кейс — досвід балтійських країн. Стаття на порталі "Борисфен Інтел" аналізує, як Естонія, Латвія й Литва створили комплексні системи протидії гібридній агресії, об'єднавши кіберзахист, мовну політику, медіаосвіту й інституційне будівництво [10]. Їхній приклад важливий тим, що гібридну війну не лише розпізнано, а й поставлено в основу державної політики, зокрема освітньої й регіональної.

Підсумовуючи сучасне бачення гібридної війни, важливо розуміти, що вона не має усталеного визначення, яке було б загальновизнаним у науковому середовищі. І саме ця багатозначність і складність пояснює її постійну актуальність у різних академічних сферах — від політичної географії до права, від комунікацій до економіки. Ключовою ознакою гібридної війни є системне поєднання засобів впливу, що виходять за межі традиційного бойового зіткнення: це інформаційна агресія, кібератаки, маніпуляції громадською думкою, тиск через економічні важелі, провокації на міжнародній арені [4].

Розмежування між війною й миром розмито, так само як і кордони між агресором і жертвою, між воєнними й цивільними суб’єктами, між внутрішньою кризою і зовнішнім втручанням. Ці межі — ключовий предмет зацікавлення політичної географії, оскільки вона працює не лише з простором як фізичною категорією, а з межами як символічними та політичними структурами.

Крім складових, пов’язаних із простором, не менш важливим є і питання термінологічної чіткості. Наприклад, Френк Хоффман запропонував поділити гібридну війну на три базові компоненти: воєнний, інформаційний та правовий, які комбінуються в залежності від цілей і контексту .

У цьому контексті важливо підкреслити й роль гуманітарних наук. Як зазначає Жадько в у вищезгаданому навчальному посібнику, спрямованому на журналістів, сучасна війна ведеться не лише у військових штабах, а й у редакціях, блогах, Telegram-каналах [11]. Це означає, що простір гібридної війни є не лише географічним або цифровим — він також є семіотичним: у ньому точиться боротьба за зміст, за правду, за право називати події своїми іменами.

Надзвичайно важливими є також трансформації в структурі міжнародних норм. Дослідники права, зокрема Гончаренко та Глух, вважають, що гібридна війна підриває здатність міжнародної спільноти реагувати оперативно, адже юридичні механізми часто не встигають адаптуватися до нових форм агресії [8]. Це виклик не лише для дипломатів і юристів, а й для аналітиків простору — адже розмивається навіть геополітичне уявлення про контроль, володіння і кордон.

Виключно на основі цієї системної критики народжується сучасна школа аналітики, яка відходить від наївного уявлення про «жорстку» війну як збройне протистояння. Наприклад, у статті Є. Магди «Гібридна війна: сутність та структура феномену.» [12] акцент робиться не на формальних структурах, а на діях, які здійснюються через посередників, наративи, економічні зв'язки. Згідно з цим підходом, політична географія має справу не з актами вторгнення, а з актами впливу, що мімікрують під звичайну зовнішню політику, гуманітарну допомогу або культурну дипломатію.

Саме тому сьогодні гібридна війна розглядається як нова форма глобального протистояння [3]. Вона не потребує декларацій, вона діє через те, що здається нормальним — торговельні угоди, гуманітарні програми, медіа, туризм, релігійні рухи, освіта. І це ставить перед політичною географією принципово нове завдання: навчитись читати карту не лише за фізичними показниками, а й за динамікою впливів, логікою взаємодій, системою координат, де важливішими стають не кордони, а сенси.

Отже, гібридна війна є складним явищем, яке об'єднує у собі мілітарні, інформаційні, економічні, правові й культурні елементи. Вона вимагає переосмислення понять суверенітету, безпеки, легітимності, простору та контролю. Для політичної географії це не просто ще один об'єкт дослідження — це виклик до перегляду самої дисципліни, її понять і методів. В умовах, коли війна точиться у словах, образах і символах, кожен географічний факт стає політичним, а кожен політичний жест — просторовим.

1.2 Гібридні війни як геополітичний інструмент сучасних держав

Гібридна війна — це не лише новітня форма ведення конфлікту, а й один із найефективніших інструментів впливу в арсеналі держав, які прагнуть реалізувати власні геополітичні інтереси, обходячи традиційні засоби міжнародної дипломатії. Її головна перевага — можливість досягнення стратегічної мети без відкритої ескалації, оголошення війни чи застосування регулярної армії. Саме тому сучасні авторитарні або ревізіоністські режими дедалі частіше звертаються до цього формату, намагаючись змінити баланс сил на міжнародній арені без порушення формальних міжнародно-правових норм [4].

Застосування гібридної війни як геополітичного інструменту ґрунтується на принципі асиметричної дії: сильна держава тисне на слабшу або дестабілізує регіон, не вступаючи у пряме збройне протистояння. Вигідність такої стратегії очевидна — вона дозволяє залишатися в зоні заперечення, маневрувати між юридичною відповідальністю і політичною вигодою, впливати через посередників або в обхід класичних міжнародних механізмів. У гібридній війні важливий не контроль над територією як таким, а вплив на ухвалення рішень, внутрішній порядок денний, ідентичність та орієнтири населення об’єкта впливу [3].

Російська Федерація стала найяскравішим прикладом держави, що системно і методично впроваджує гібридну війну як стрижневий елемент своєї зовнішньої політики. Цей підхід набув остаточної форми з початку 2010-х років, особливо після виступу Валерія Герасимова (начальника Генштабу РФ) у 2013 році, в якому було озвучено концепцію «нетрадиційних конфліктів», де «невійськові засоби досягають стратегічних цілей навіть ефективніше за збройні сили» [7]. Дані методи згадані нижче (див рис.1.2). Відтоді спостерігається системне впровадження в практику «гібридної доктрини», що поєднує військові, інформаційні, політичні, економічні та кіберметоди впливу на інші держави.

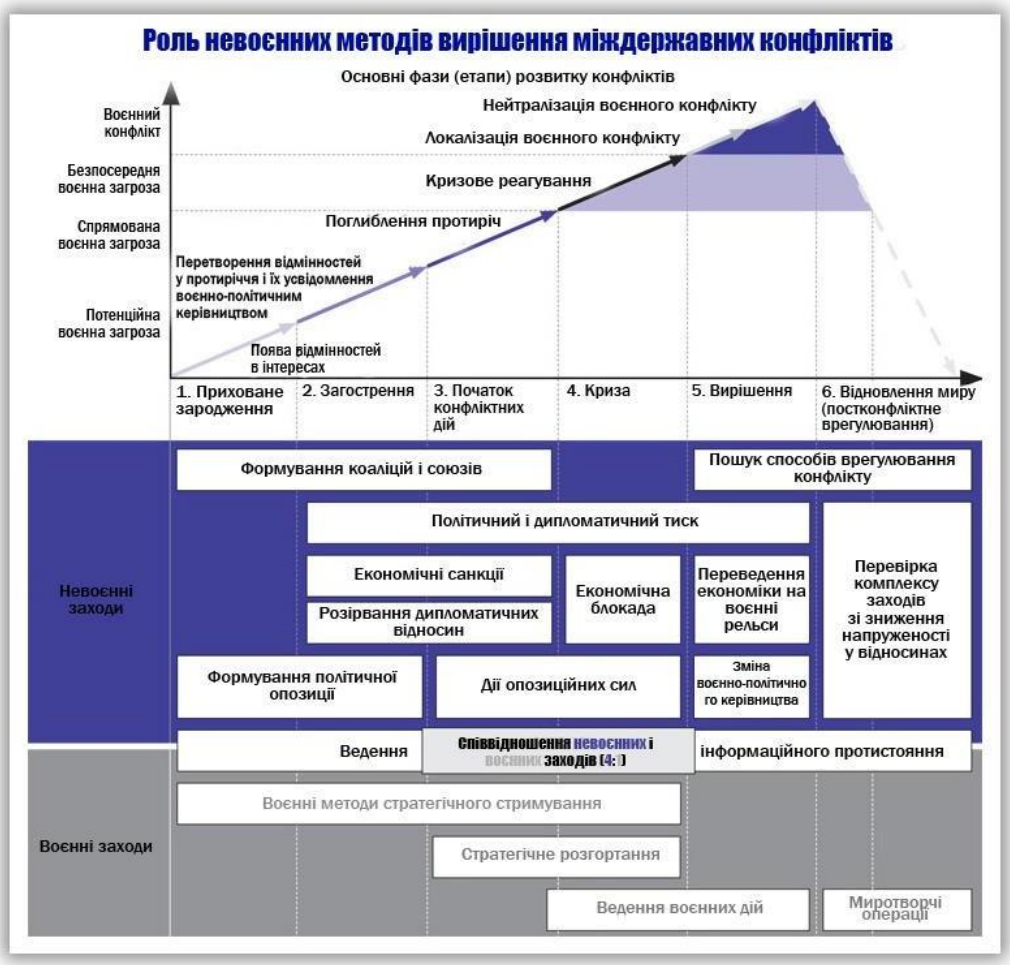

Рис. 1.2. Схема Герасимова, джерело: Ukrinform

Найбільш масштабним і тривалим прикладом такої політики стала агресія Росії проти України, що почалася у 2014 році. Анексія Криму, дестабілізація на Донбасі, спроби розколоти Україну зсередини через проросійські організації, інформаційні кампанії та втручання в економічну політику — все це елементи гібридної стратегії, що мала на меті не лише ослаблення української державності, а й демонтаж її західного геополітичного курсу [11].

Проте використання гібридної війни Росією не обмежується лише Україною. Подібні дії спостерігалися в Грузії (до та після війни 2008 року), Молдові (через підтримку Придністров'я), у країнах Балтії (через інформаційні операції, кібератаки, спроби дестабілізувати національні меншини), у Сирії (через

комбінацію військових дій, приватних армій, гуманітарних програм, медіа та економіки) [5].

Західні аналітичні центри, зокрема RAND Corporation, НАТО StratCom, Європейська служба зовнішніх дій, неодноразово вказували на те, що гібридна стратегія Росії спрямована на довгострокове руйнування єдності Європи, зниження довіри до трансатлантичних інституцій, блокування розширення НАТО та ЄС. Це відбувається через підтримку радикальних партій, дезінформаційні кампанії, кібердиверсії, фінансове втручання в виборчі процеси, розпалювання внутрішньоєвропейських конфліктів [4].

На цьому тлі в міжнародному середовищі почала зростати усвідомленість щодо потреби у стратегічній стійкості до гібридних загроз. Починаючи з 2016 року, НАТО і ЄС активно впроваджують програми, спрямовані на виявлення, нейтралізацію та превенцію гібридних атак: створено спеціальні відділи, започатковано освітні ініціативи, підписано угоди про співпрацю в сфері кібербезпеки, інформаційної гігієни, критичної інфраструктури [8].

Варто зазначити, що не лише авторитарні держави звертаються до гібридних інструментів. У певних обставинах навіть демократичні країни використовують ці методи, зокрема в умовах конкурентної геоекономіки або у відповідь на асиметричні загрози. Це піднімає питання етичної межі між легітимною зовнішньою політикою і гібридною агресією, а також ускладнює розмежування між безпековими заходами та наступальними стратегіями. Саме тому на міжнародному рівні досі не існує єдиної конвенції, яка б чітко визначала поняття «гібридна війна» та інструменти її ідентифікації [11].

Гібридна війна як інструмент зовнішньої політики не лише підриває стабільність окремих держав, але й змінює архітектуру глобальної безпеки. Після початку війни Росії проти України у 2014 році, а ще більше — після повномасштабного вторгнення у 2022-му, європейські країни були змушені радикально переглянути власні безпекові доктрини. Протидія гібридній агресії перестала бути теоретичною проблемою і стала питанням виживання —

насамперед у таких сферах, як кібербезпека, інформаційна стійкість, контроль над критичною інфраструктурою, енергетична незалежність і оборонна готовність [14].

Кожна держава обрала власну модель реагування, але спільним знаменником стало розуміння того, що класичні методи оборони більше не гарантують безпеки. Основною метою гібридного впливу є не військове знищення супротивника, а його ослаблення зсередини через втрату контролю над суспільними процесами та державними інституціями. Саме тому ключовим напрямом стало формування національної стійкості до мультивекторних загроз. Приклади реакції деяких європейських країн приведено у таблиці 1.1.

Таблиця 1.1

Реакції країн ЄС на гібридні загрози після 2014 року

Країна	Основні загрози	Реакція держави	Створені структури / політики
Естонія	Кібератаки, пропаганда	Кіберкомандування в ЗС, медіаосвіта в школах	Estonian Defence League, CCDCOE
Литва	Інформаційні операції	Боротьба з дезінформацією, заборона кремлівських каналів	Центр стратегічних комунікацій при МО
Польща	Енергетичний шантаж	Диверсифікація газопостачання, розвиток LNG-терміналів	Польська енергетична стратегія до 2040
Німеччина	Вплив на вибори, хакінг	Кібербезпека, підвищення прозорості виборчого процесу	BSI (Федеральне агентство кіберзахисту)
Фінляндія	Прикордонні провокації	Законодавча реформа, резервна армія, оборонне навчання	Всеохоплююча оборонна концепція

Джерело: складено на основі аналітики NATO StratCom та досліджень Центру безпекової політики (2022–2023)

Україна, безумовно, стала полігоном, на якому відпрацьовуються й моделюються основні сценарії гібридної агресії. Водночас її досвід — це унікальна база для вивчення ефективних (і неефективних) стратегій протидії. Після 2014 року було запроваджено низку реформ: від створення Центру протидії дезінформації при РНБО до повноцінної модернізації системи кіберзахисту та запуску освітніх ініціатив з інформаційної грамотності. Однак головним надбанням стало сформоване суспільне розуміння природи нової війни, яке стало запорукою масової мобілізації, волонтерського руху, цифрового супротиву [3]. У таблиці 1.2. наведено приклади основних інструментів гібридного впливу, які Росія використовувала в Європі за останнє десятиліття:

Таблиця 1. 2

Інструменти гібридного впливу РФ у країнах Європи (2014–2023)

Тип впливу	Країни / регіони застосування	Конкретні приклади
Енергетичний тиск	Україна, Молдова, Болгарія, Німеччина	Газовий шантаж, контроль над трубопроводами
Інформаційні атаки	Франція, Німеччина, Італія, Словаччина	Кампанії дезінформації під час виборів
Кібератаки	Естонія, Литва, Німеччина, Україна	Атаки на урядові сайти, критичну інфраструктуру
Підтримка партій	Італія, Австрія, Угорщина, Франція	Фінансування ультраправих та антиєвропейських сил
Проксі-групи	Балкани, Придністров’я, Донбас	Підтримка сепаратизму, приватні військові кампанії

Джерело: аналітика RAND Corporation, 2023

Наявність таких інструментів і варіативність їх застосування ще раз підтверджують: геополітична цінність гібридної війни полягає в її

універсальності. Вона дозволяє адаптувати методи під конкретну країну, її уразливості, політичний клімат, економічну залежність. При цьому міжнародна відповідальність мінімізується, оскільки навіть у разі виявлення факту втручання — суб'єктом часто виступають неофіційні або приватні структури, які юридично не пов'язані з державою-агресором.

Гібридні війни трансформували не лише безпекову політику окремих держав, а й геостратегічну логіку міжнародних відносин. У класичній геополітиці вплив визначався через територіальний контроль, військову присутність або економічне домінування. Проте гібридна війна продемонструвала нові підходи: вплив без присутності, руйнування без збройного втручання, панування через хаос.

У результаті цього спостерігається переорієнтація міжнародних гравців у бік інструментів, які раніше вважалися другорядними: інформаційна політика, цифрова дипломатія, психологічні операції, моделювання впливу на виборчий процес, дезінформаційні платформи. Все це набуло статусу повноцінного геополітичного ресурсу. Особливо активно до таких інструментів почали звертатися не лише традиційні глобальні гравці (США, Росія, Китай), а й середні держави з амбіціями регіонального лідерства (Туреччина, Іран, Саудівська Аравія, Ізраїль) [14].

Сполучені Штати Америки, зіткнувшись із хвилею зовнішнього втручання у президентські вибори 2016 року, кардинально оновили підходи до безпеки. У звітах Конгресу й розвідки офіційно визнано, що інструменти гібридної війни стали головною загрозою національній стабільності, випередивши навіть тероризм. Відтоді було впроваджено низку рішень — зокрема створено спеціальні центри моніторингу іноземного впливу, запущено законодавчі ініціативи щодо прозорості цифрової політичної реклами, посилено співпрацю з приватними платформами типу Facebook, Google, X (Twitter) [3].

У той же час Китай, як авторитарна держава з розгалуженим державним управлінням, ідеально адаптував інструменти гібридної війни під власну

глобальну стратегію. Відомий кейс — «діяльність інститутів Конфуція» у світі, що формально просувають китайську мову й культуру, але на практиці використовуються для впливу на освітню політику, академічну свободу, публічні дебати у десятках країн. Інформаційна експансія через мережі китайських державних медіа, кампанії зі скупівлі інфраструктурних об'єктів, просування наративу про «нероздільну відповідальність» в епоху COVID-19 — усе це стало частиною глобального гібридного впливу КНР [7].

Європейський Союз, попри довгий період фрагментації в питаннях безпеки, під тиском зовнішніх викликів — зокрема втручань у вибори, кібератак, енергетичних криз — також почав уніфікувати підходи до протидії гібридній загрозі. Зокрема у 2020–2023 роках активно працювали над Європейським актом про цифрові послуги, політикою боротьби з фейками, програмами кіберстійкості. Принципово важливо, що було визнано сам факт існування нових форм агресії, що потребують однаково серйозного ставлення, як і до конвенційних загроз [11].

У цьому контексті зросла роль інформаційних агентств як геополітичних інструментів. Російські канали RT, Sputnik, китайські CGTN або турецький TRT World виконують функцію м’якої, але цілеспрямованої ідеологічної експансії. Вони не лише поширюють певні версії подій, а й активно створюють альтернативну реальність для окремих країн або цілих регіонів, зокрема на Балканах, у Латинській Америці, у Франції, Італії та навіть США [9]. Для систематизації інформації щодо методів гібридного впливу вищезгаданих держав нижче додана таблиця 1.3.

Таблиця 1.3

Порівняльна характеристика гібридного впливу провідних геополітичних гравців

Держава	Основні напрямки впливу	Цілі використання гібридної стратегії
РФ	Інформаційні атаки, проксі-війни, кібератаки	Дестабілізація регіонів, знищення єдності ЄС та НАТО
США	Контрпропаганда, цифрова дипломатія	Захист демократії, стримування авторитарних режимів
Китай	Освітній і культурний вплив, фінансова експансія	Формування прихильної до КНР міжнародної думки, економічна залежність
Туреччина	Діаспорна політика, релігійний вплив	Посилення регіонального лідерства, вплив на Балкани
Іран	Медіа, проксі-мілітарні структури	Ідеологічне просування шиїзму, протидія США і Саудівській Аравії

Джерело: складено на основі матеріалів NATO StratCom, RAND Corporation, Foreign Affairs (2023)

Ці приклади підтверджують тезу про глобальний характер гібридної війни як геополітичного явища. Вона більше не є лише форматом локального протистояння — це інструмент великої політики, за допомогою якого формується вплив, змінюється політична динаміка, створюються передумови для нових альянсів або — навпаки — конфліктів.

Гібридні війни залишили глибокий слід у структурі міжнародної політики. Їхній вплив виявився настільки гнучким і проникаючим, що класичні інститути міжнародного правопорядку не завжди здатні адекватно реагувати на нові виклики. Одним із ключових наслідків стало розмиття меж між війною і миром, агресором і партнером, між внутрішніми процесами держави та зовнішніми

впливами. Цей ефект — фундаментальна трансформація політичної свідомості та архітектури міжнародної стабільності [14].

Сучасна система міжнародного права була створена з урахуванням чіткого поділу: суверенітет, територіальна цілісність, заборона збройної агресії, визнані інституції врегулювання спорів. Однак гібридна агресія функціонує поза цими рамками: вона не оголошується, не оформлюється як війна, а тому не активує формальні механізми захисту. Це дозволяє державам-агресорам зберігати образ легітимного учасника міжнародної спільноти, ведучи при цьому підривну діяльність проти інших [3].

Цей виклик породжує кризу довіри до традиційних багатосторонніх механізмів, таких як ООН, ОБСЄ або навіть Міжнародний суд. Навіть у випадку з Росією, яка здійснила анексію частини території суверенної держави — Української Республіки, — міжнародне реагування виявилося запізнілим, фрагментарним і переважно декларативним. Санкції та дипломатичні заяви не змогли змінити статус-кво, натомість Кремль скористався часом для посилення впливу в інших регіонах — Сирії, Центральній Африці, Південній Америці .

Окремим наслідком стала модернізація концепції «м’якої сили» (soft power). У гібридній війні навіть культурні, гуманітарні та академічні інструменти можуть бути використані для стратегічного тиску: фінансування освітніх програм, участь у конференціях, культурні центри, навіть книжкові переклади можуть служити каналами поширення вигідної ідеології. З боку Росії цей напрямок набув назви «русский мир», з боку Китаю — «м’яка синізація», з боку Ірану — релігійна експансія шиїзму. Усі ці вектори працюють на підрив альтернативних центрів впливу.

Особливо яскраво проявляється криза довіри в інформаційній сфері. Через масовані кампанії дезінформації, бот-мережі, спотворення фактів, псевдоаналітику, фейкові медіа — стало надзвичайно складно ідентифікувати джерело загрози. Традиційна модель журналістики, яка базувалася на правдивості та перевіреності, втратила монополію на вплив. Гібридна війна «розмила істину»

і створила паралельні інформаційні реальності, де громадянин країни-мішені часто не може відрізнити автентичний контент від спеціально сконструйованого [9].

Реакція демократичного світу на ці процеси лише формується. Серед найбільш дієвих стратегій — побудова національної стійкості: зміцнення освіти, розвиток критичного мислення, прозора комунікація між владою та суспільством, підтримка незалежної журналістики, виявлення й блокування ворожих наративів, цифрова безпека. У політиці — відмова від стратегічної наївності, посилення міжвідомчої координації, зміна підходів до дипломатії. У військовій сфері — поєднання класичної оборони з новими силами інформаційного і кіберреагування [4].

Паралельно активно розвивається нове поняття “колективної стійкості”. Якщо раніше безпека розумілася як захист окремої держави, то тепер дедалі більше організацій (НАТО, ЄС, GUAM, Ініціатива трьох морів) переходять до моделей, де загроза одному з членів автоматично стає загрозою для всіх. Цей підхід випливає з досвіду гібридної війни, яка зазвичай атакує найслабшу ланку, а не найближчого ворога [8].

Підсумовуючи, гібридна війна трансформувала світову політику в кількох аспектах:

- змінила уявлення про агресію;
- поставила під сумнів здатність класичних інституцій реагувати;
- надала нові інструменти впливу державам з меншим військовим потенціалом;
- привела до появи нової парадигми безпеки — моделі тотальної стійкості;
- створила необхідність нового міжнародного консенсусу щодо норм і принципів дій у сірій зоні конфлікту.

У таблиці 1.4. продемонстровано те, як гібридні війни змінили розуміння безпекового світопорядку.

Таблиця 1.4.

Гібридна війна та трансформація міжнародного порядку

Напрям зміни	Стан до 2014 року	Стан після 2014 року
Роль війни в політиці	Класична війна як крайній засіб	Гібридна війна як регулярний інструмент
Визначення агресора	Чітка суб'єктність і відповідальність	Розмитість, делегування атаки проксі-гравцям
Реакція міжнародних структур	Дипломатичні інструменти, санкції	Неоднозначна, сповільнена, не завжди ефективна
Геополітична стабільність	Підтримувана військовими альянсами	Залежна від кіберзахисту, інформаційної стійкості
Сприйняття загрози	Через армію, зброю, конфлікти	Через фейки, віруси, платформи, інфраструктуру

Джерело: авторська компіляція на основі даних NATO Review, European Commission, RAND, Українського центру стратегічних досліджень (2023)

У висновку варто зазначити: гібридна війна стала не винятком, а новим форматом глобальної конкуренції. Її ігнорування вже несе стратегічну поразку. Тому країни, які хочуть зберегти незалежність, стабільність і суверенітет, мають вбудовувати розуміння цієї загрози в кожен аспект своєї політики — від оборони до освіти, від енергетики до цифрової безпеки.

1.3. Методологія дослідження гібридних війн: основні підходи та моделі

Дослідження гібридних війн як специфічного феномена у міжнародних відносинах вимагає міждисциплінарного підходу. Зважаючи на складність і багаторівневість самого явища, яке охоплює одночасно воєнну, політичну, інформаційну, економічну, соціальну та кібернетичну сфери, жодна з класичних методологій у своїй ізольованій формі не дозволяє здійснити повноцінний аналітичний розгляд. Саме тому вивчення гібридних конфліктів ґрунтується на поєднанні кількох дослідницьких парадигм, серед яких важливе місце займають системний, конструктивістський, геополітичний, неореалістичний, компаративний і структурно-функціональний підходи.

Системний підхід дозволяє розглядати гібридну війну не як набір окремих інструментів чи проявів, а як цілісний процес, у якому взаємодіють політичні наративи, технології, військові дії, інституції, медіа, і навіть культурні коди. У межах цього підходу війна сприймається як відкрита система, що функціонує у змінному середовищі, пристосовується до умов, трансформується залежно від стійкості опонента. Саме ця здатність до трансформації — одна з ключових ознак гібридної війни, яка не має усталеної моделі, а постійно шукає найвразливіші точки у суспільстві супротивника. Системне бачення дає можливість не лише описати елементи гібридної агресії, а й моделювати сценарії розвитку конфлікту на основі логіки внутрішніх зрушень у цільовому середовищі.

Конструктивістська методологія фокусується на тому, як формуються смисли у просторі конфлікту. У випадку гібридної війни вирішальним чинником є не стільки сам факт атаки, скільки її інтерпретація. Інформаційні вкиди, маніпуляції, фейки, симуляція активності — все це діє лише тоді, коли аудиторія приймає певне уявлення про подію як істинне. Саме тому боротьба в межах гібридної війни ведеться за контроль над уявленням про реальність. У цій логіці дослідник має звертати увагу не лише на фактичні події, а на те, як вони

подаються, ким і з якою метою, у яких інформаційних ланцюгах поширюються, яку реакцію викликають. Конструктивізм виявляється особливо ефективним у випадках, коли гібридний вплив реалізується через культурні, мовні, релігійні чи історичні наративи, що глибоко вкорінені у суспільній свідомості.

Геополітичний підхід дозволяє інтерпретувати гібридну війну як засіб переділу сфер впливу у глобальному просторі. З його точки зору, застосування непрямих методів конфлікту — це стратегія сильного актора, який, не вступаючи у відкриту війну, здатен змінювати баланс сил на регіональному рівні. У випадку з Європою Росія виступає як гібридний геополітичний гравець, що використовує інструменти дестабілізації, аби відновити контроль над сусідніми державами та послабити консолідацію ЄС і НАТО. Геополітичне бачення дозволяє розглядати гібридну війну не лише як техніку впливу, а як просторову стратегію, в якій різні країни відіграють роль каналів тиску, буферних зон, транзитних коридорів або майданчиків для демонстрації сили.

У межах неореалістичного підходу гібридна війна розглядається як логічний інструмент державного самозбереження та просування національних інтересів у ситуації, коли пряме застосування сили стає недоцільним або занадто ризикованим. Держава, діючи як раціональний актор, використовує асиметричні засоби задля зниження вартості конфлікту і підвищення ймовірності досягнення бажаних цілей без прямої конфронтації. У цьому контексті особливо важливим є вивчення стратегії непрямого впливу, прихованих механізмів контролю, мережевого впливу через проксі-групи або незалежні платформи.

Компаративний підхід дозволяє аналізувати гібридні війни як типові й уніфіковані за структурою процеси, які мають певні константи незалежно від конкретного регіону. Порівнюючи приклади гібридних атак у різних країнах — від України до Литви, від Чорногорії до Німеччини — дослідник має змогу виділити повторювані патерни, виявити найбільш поширені методи впливу, оцінити ефективність різних моделей реагування. Порівняльний аналіз створює базу для формування універсальних підходів до побудови стійкості та мінімізації наслідків.

Структурно-функціональний підхід акцентує увагу на взаємодії між елементами гібридної агресії — військовими, інформаційними, політичними, дипломатичними, економічними. Він дозволяє побудувати логіку дії агресора, зрозуміти, як функціонує комплексний вплив, у якій послідовності застосовуються окремі інструменти, які з них є ключовими, а які допоміжними. Такий підхід особливо ефективний у дослідженні сценаріїв гібридних атак — він дозволяє розділити їх на фази, змоделювати алгоритм впровадження, передбачити потенційні варіанти подальших дій.

Застосування змішаних методів відкриває можливість створити багаторівневу дослідницьку модель, у якій враховуються як стратегічні чинники (цілі держави, геополітичні інтереси), так і тактичні аспекти (вибір часу атаки, цільова аудиторія, обрана платформа). Це особливо важливо при аналізі таких феноменів, як інформаційні операції, кібератаки, економічний тиск або електоральна дестабілізація.

Окрім теоретичних підходів, дослідження гібридних війн спирається на використання моделей. Серед них особливе значення мають моделі кібератаки, інфраструктурної вразливості, інформаційної ескалації, стратегічної поведінки проксі-структур, а також моделі оцінки впливу на суспільну довіру. Такі моделі дозволяють здійснювати емпіричний аналіз — наприклад, через симуляції інформаційних кампаній, аналіз бот-мереж, виявлення цифрових слідів маніпуляцій. У дослідженні часто застосовуються інструменти OSINT (open-source intelligence), аналіз соціальних графів, цифрова криміналістика, статистичне моделювання динаміки наративів. Вони є особливо актуальними в умовах, коли гібридна війна реалізується в цифровому просторі й має високий ступінь динаміки.

Отже, методологія дослідження гібридних війн у сучасній Європі — це поєднання класичних політичних парадигм і новітніх технологічних інструментів аналізу. Це дає змогу не лише описувати феномен, а й розуміти логіку його еволюції, прогнозувати нові форми, визначати зони ризику та формулювати

стратегії протидії. У наступних розділах ця методологічна база стане основою для аналізу конкретних кейсів, сценаріїв та інституційних реакцій на гібридні виклики в сучасній Європі.

Висновки до Розділу 1

Гібридні війни, як новий тип конфлікту, змінили уявлення про сучасну безпеку та потребують комплексних підходів для аналізу і реагування. Основними складовими гібридної війни є військові, інформаційні, економічні, політичні та кібернетичні методи, що застосовуються одночасно. Розвиток гібридних загроз вимагає від країн Європи перегляду традиційних моделей безпеки та інтеграції нових інструментів захисту. В Україні цей тип війни проявився через російську агресію, що стало уроком для інших країн Європи. Здатність до адаптації є ключовою для забезпечення стійкості та ефективності протидії гібридним атакам.

РОЗДІЛ 2. ГІБРИДНІ ВІЙНИ ТА ЇХНІЙ ВПЛИВ НА ГЕОПОЛІТИЧНИЙ ЛАНДШАФТ ЄВРОПИ

2.1 Історія війн у Європі та їхня трансформація

Європейський континент протягом останніх століть неодноразово був епіцентром масштабних воєн, які щоразу змінювали не лише політичні кордони, а й логіку самого сприйняття конфлікту. Від епохи Середньовіччя з її династичними війнами до тотальних світових протистоянь XX століття — війна залишалася інструментом сили, контролю, експансії. Проте початок XXI століття позначився появою нових форм насильства, які ззовні можуть виглядати як політична криза, економічний конфлікт або інформаційна кампанія, але за суттю — є продовженням воєнної логіки іншими засобами. Однією з таких форм стала гібридна війна, яка поступово витісняє класичну [14].

Щоби зрозуміти, як саме Європа прийшла до гібридного формату ведення війни, варто проаналізувати зміну характеру конфліктів упродовж останніх 500 років. У XVI–XVIII століттях війна трактувалась як інструмент династичного або імперського впливу. Її основою були регулярні армії, захоплення територій, облоги міст. Класичним прикладом є Тридцятилітня війна (1618–1648), яка завершилася Вестфальським миром — документом, що вперше закріпив принципи державного суверенітету й заклав підвалини сучасного міжнародного права [3].

У XIX столітті війна стала націоналізованою — її вело не лише військо, а й цілий народ. Французька революція і наполеонівські війни трансформували поняття конфлікту, додавши до нього ідеологічний компонент. Тепер війна була не лише про територію, а й про нав’язування ідей — саме це пізніше стане основою інформаційної складової гібридної агресії [7].

Перша і Друга світові війни стали піком тотальної війни — зі знищенням інфраструктури, масовою мобілізацією, геноцидом, використанням технологій. Війна перестала бути локальною — вона охопила всі сфери життя: економіку,

політику, інформацію, побут. Саме в цей період вперше виникають елементи, подібні до гібридних — наприклад, дезінформація, пропаганда, саботаж, дипломатичні пастки, політична інфільтрація [11].

Після 1945 року Європа опинилася в новому форматі — холодної війни, яка стала першим масштабним прикладом гібридного протистояння. Ідеологічний поділ між Заходом і Сходом породив унікальну систему конфлікту без відкритих боїв між головними гравцями. Війна велася через інформацію, шпигунство, економічний тиск, проксі-конфлікти в третіх країнах. Саме тут виникла модель, яка згодом стане фундаментом сучасної гібридної стратегії [9].

Особливу увагу заслуговують так звані «гарячі точки» холодної війни, які демонстрували, як великі держави реалізовували свої інтереси непрямими методами. Наприклад, підтримка радикальних груп у Латинській Америці, фінансування режимів у Африці, участь у війнах через проксі-сили в Азії — всі ці практики надалі трансформувались у шаблони гібридної агресії [6].

Розпад СРСР не припинив, а навпаки — активізував процес фрагментації безпекових підходів у Європі. Протягом 1990-х років виник новий тип конфліктів — локальні війни і міжетнічні зіткнення (Балкани, Кавказ, Придністров'я), у яких використовувались уже знайомі механізми: інформаційна маніпуляція, політичні лялькарі, економічна дестабілізація. Однак ці війни ще не мали чітко вираженого «гібридного» обрису — на той момент це був лише перехідний формат.

Переломним став 2014 рік. Анексія Криму росією і початок війни на Донбасі відкрили нову епоху гібридного конфлікту, де агресор поєднав військові, інформаційні, економічні, політичні та кіберінструменти. Усе це — без офіційного оголошення війни, без розпізнавальних знаків, із використанням місцевих колаборантів, фейкових медіа, псевдореферендумів, а також приватних військових структур. Цей випадок змінив парадигму — війна більше не виглядає як війна, а саме в цьому — її найбільша сила [11].

Після 2014 року вся європейська безпекова система була змушена адаптуватися. Було переглянуто стратегії НАТО, створено механізми

кібероборони, в ЄС розгорнуто програми медіаграмотності, запроваджено санкційні режими. Проте головне — у свідомості: європейці вперше за десятиліття зрозуміли, що війна поруч, і вона не виглядає як танки вулицями, вона — у фейсбуці, у платіжках за газ, у виборчих бюлетенях [6].

Війна як політичне явище завжди відображала рівень розвитку суспільства, його технологічну базу, систему міжнародних відносин і культуру. Європа, як центр політичної еволюції світу протягом кількох століть, дала не лише приклади найбільших воєн, а й моделі їх подолання — від Вестфальського миру до Хартії ООН. У цьому контексті гібридна війна не з'явилася на порожньому місці. Вона є продовженням процесу, де відкритий бій замінюється складною грою змістів, впливів і проксі-інструментів, а межі між війною і миром остаточно стираються.

Сьогоднішня ситуація в Європі є наслідком історичної трансформації підходів до насильства. Один із найбільш показових кейсів — Балкани 1990-х років. На перший погляд це — збройні конфлікти, що виникли внаслідок розпаду Югославії, однак при глибшому аналізі видно елементи класичної гібридної стратегії: розпалювання міжетнічної ворожнечі, дезінформаційні кампанії, залучення іноземних спецслужб, створення псевдополітичних утворень, економічна блокада та руйнування інституцій [14].

Не менш характерний приклад — війна в Грузії 2008 року. Росія активно використала інформаційну перевагу, зокрема через домінування у міжнародних ЗМІ в перші дні конфлікту. У той самий час на території самопроголошених утворень Південної Осетії й Абхазії діяли підконтрольні збройні формування, які формально не були частиною армії РФ, що дозволяло Кремлю уникати прямої юридичної відповідальності. Це — класичний елемент гібридної доктрини [3].

Після 2014 року кількість гібридних проявів у Європі стрімко зросла. У відповідь на ситуацію в Україні, Росія активізувала інформаційно-психологічні операції в країнах Балтії. Особлива увага приділялася російськомовному населенню в Естонії, Латвії та Литві. Через мовні та культурні зв'язки Кремль формував паралельний інформаційний простір — із власними медіа, історією,

термінами, героями. Результат — зниження довіри до місцевої влади, розмивання національної ідентичності, дестабілізація під час виборів [7].

Європейські країни поступово почали будувати системи виявлення гібридних загроз. Створено відповідні структури — зокрема у Фінляндії, Німеччині, Франції. У відповідь на втручання в кампанії Brexit і вибори у Франції (2016–2017), було впроваджено аналітичні центри та цифрові блоки при ЦВК, які моніторять медіаполе, виявляють аномалії трафіку, фейкові акаунти, синхронізовані інформаційні атаки. Йдеться вже не про військову протидію, а про еволюцію безпекового мислення, де обороняються не лише державні кордони, а й сенси, думки, довіра [11]. Для зручності ключові зміни у розумінні війни протягом історії наведені у таблиці 2.1.

Таблиця 2.1

Етапи трансформації війни в Європі

Період	Характер війни	Мета	Інструменти
XVI–XVIII ст.	Династична, імперська	Територія	Армії, облоги, дипломатія
XIX ст.	Національна, ідеологічна	Політична модель	Мобілізація, пропаганда
XX ст. (1914–1945)	Тотальна, світова	Виживання, домінування	Авіація, танки, пропаганда
Холодна війна	Ідеологічна, проксі	Глобальний вплив	Шпигунство, війни через союзників
1990-ті – початок 2000-х	Локальні війни, дезінтеграція	Контроль над регіонами	Етнічний розкол, підтримка сепаратизму
Після 2014 року	Гібридна війна	Дестабілізація, хаос	Інформація, кібератаки, проксі-сили

Джерело: складено за матеріалами [4, 11]

Особливу роль у цій трансформації відіграє технологічний чинник. З розвитком інтернету, соціальних мереж, цифрових платформ гібридна війна отримала глобальний масштаб. Кіберпростір став полем бою, де можна вразити ворога швидше, дешевше і без ризику відповідальності. Один фейковий ролик, одна фальшива новина — і реальний ефект на політичні процеси. Такий формат було застосовано, зокрема, в Італії, Угорщині, Іспанії, де зафіксовано зовнішній вплив на виборчі кампанії [8].

Зміна характеру війни в Європі — не просто результат еволюції технологій чи політичних інтересів. Це — глибока трансформація самого поняття безпеки, яке впродовж останніх десятиліть перейшло від концепту "захисту кордонів" до "захисту цілісності державного устрою в умовах невидимого тиску". У класичних війнах XX століття було зрозуміло, де ворог, хто командує, коли оголошено війну, коли вона закінчилася. У гібридному світі ці ознаки стерті: атака може виглядати як економічна криза, фейкова інформація, цифровий збій або політична кампанія [14].

Після 2014 року, коли Росія розпочала гібридну агресію проти України, саме Європа стала лабораторією, де експериментували з новими формами тиску. Від вторгнення в інформаційний простір до втручання у вибори — всі ці явища засвідчили, що гібридна війна — це війна за управління процесами, а не за території. Її мета — зробити державу вразливою, слабкою, розколотою зсередини настільки, щоби зовнішній контроль не потребував танків [3].

Один із ключових аспектів трансформації війни — вплив на суспільну довіру. Гібридна війна спрямована не лише на уряд, армію чи парламент, а передусім на громадянина. Знищення довіри до інституцій, поширення ідей зради, дискредитація сил оборони, уявлення про безсилля держави — усе це формує середовище, у якому стає неможливим ефективне управління. Тому у відповідь на гібридну загрозу країни змушені формувати не лише армії, а й національну психологічну стійкість [7].

Це добре розуміють у країнах Балтії. Після вторгнення РФ в Україну, Литва, Латвія та Естонія зосередились на розбудові цілісної моделі оборони, що включає:

- освітні програми з медіаграмотності у школах;
- держпідтримку незалежних ЗМІ;
- оперативні аналітичні центри;
- резервні формування територіальної оборони;
- інтеграцію цифрових платформ у систему реагування [4].

Водночас у країнах Західної Європи домінує інша стратегія: створення стійких демократичних інститутів, які самі по собі є бар'єром для гібридного проникнення. Підвищення прозорості виборчих процесів, обмеження політичної реклами ззовні, цифрова ідентифікація громадян, боротьба з бот-мережами — все це є новими формами оборони, які раніше не асоціювались з терміном "війна", але тепер — це її передова [9].

Цей процес чітко виявляється через порівняльний аналіз підходів країн до гібридної загрози, який показано у таблиці 2.2

Таблиця 2.2

Порівняльна реакція держав Європи на гібридну трансформацію конфліктів

Країна	Основний вектор реагування	Приклади реалізованих стратегій
Литва	Оборона інформаційного простору	Закон про заборону ворожих каналів, державне фінансування аналітичних центрів
Естонія	Кібербезпека	NATO CCDCOE, національні кіберманеври
Німеччина	Захист демократії та прозорості	Центр кібербезпеки BSI, індексація політичного контенту

Франція	Моніторинг іноземного втручання	Аналітичні звіти про втручання у вибори, судові процеси проти дезінформації
Україна	Всеосяжна оборона та інформаційна протидія	Центр протидії дезінформації, «Дія», мобільна оборона

Джерело: аналітична компіляція на основі [8], 11]

Отже, головним висновком трансформації воєн у Європі є те, що гібридний конфлікт — не заміна війни, а її еволюція. Він дозволяє впливати на інститути, суспільства, економіки, залишаючись у зоні формального миру. Саме ця особливість — дія без оголошення — є найбільшою проблемою для сучасної системи безпеки.

Цей тип війни руйнує основи міжнародного правопорядку, тому потребує нової нормативної бази, яка враховувала б проксі-сили, цифрові атаки, інформаційні вторгнення. Європа, яка пережила десятки війн, тепер має сформулювати власну відповідь на нові загрози, у яких стріляють не гармати, а медіа, код і наративи.

2.2 Російсько-українська війна як головний приклад гібридного конфлікту в Європі

Російсько-українська війна, що розпочалася у 2014 році з анексії Криму та перейшла у відкриту фазу з масштабним вторгненням у 2022-му, є найяскравішим прикладом гібридного конфлікту не лише в Європі, а й у світі. Її особливість полягає в тому, що Росія поєднала традиційні військові засоби із масштабною інформаційною, політичною, економічною та кібернетичною агресією, при цьому намагаючись формально заперечити свою участь у ключових етапах ескалації [14].

Цей конфлікт не обмежується лінією фронту — він розгортається у медіа, соцмережах, системі постачання енергоносіїв, дипломатичних процесах, навіть у школах, церквах і платформах таксі. Саме така багатовекторність робить війну

гібридною: жодна сфера суспільного життя не залишається поза зоною ураження. Відповідно, й захист має охоплювати не лише армію, а й державне управління, цифрові платформи, культуру, освіту, соціальні мережі, бізнес [3].

У період 2014–2015 років Росія діяла згідно з логікою «гібридного заперечення»: анексію Криму було реалізовано силами без розпізнавальних знаків, через так званих «ввічливих людей», яких формально не можна було ідентифікувати як армію РФ. Одночасно було запущено потужну інформаційну кампанію, метою якої було сформувати наративи про «історичну справедливість», «захист російськомовного населення», «фашистський переворот у Києві» [7].

На сході України в цей час розгорталася модель «керованого хаосу»: РФ підтримувала сепаратистські рухи зброєю, фінансуванням, логістикою та управлінськими кадрами, але на рівні міжнародної дипломатії заперечувала будь-яку участь. При цьому активно використовувались місцеві проксі-групи, криміналітет, вплив через місцевих політиків, а також інструменти психологічного тиску — викрадення, катування, поширення страху [11].

Водночас у тилу Росія реалізовувала масовані інформаційні операції, спрямовані як на українське, так і на міжнародне суспільство. Через RT, Sputnik, соціальні мережі, а також проросійські ресурси в Україні поширювались фейки, змонтовані відео, вигадані події. Основна мета — зруйнувати образ України як жертви, змусити сумніватися в легітимності її влади, представити війну як «громадянський конфлікт» [9].

Паралельно здійснювався економічний тиск. Росія зупиняла поставки газу, обмежувала транзит, створювала перешкоди для експорту українських товарів. Була спроба дестабілізувати курс гривні, вивести капітали з українських банків. Економіка ставала полем бою, де удари наносилися через санкції, енергетику, бізнес-залежності. Особливий ефект мала диверсифікація ризиків через кримінальні структури — блокування вугілля, тиск на металургію, втручання у фінансову систему [4].

Війна також набирала нових форм у кіберпросторі. Починаючи з 2014 року, Україна зазнала сотень кібератак на урядові сайти, енергетичні компанії, залізницю, банки. У 2015 році вперше в історії було здійснено кібератаку на енергосистему, яка залишила сотні тисяч українців без світла — результат діяльності російських хакерських груп APT28 та Sandworm. Усе це — без фізичної присутності ворога, але з реальними наслідками [8].

Наступні етапи війни лише посилили гібридний ефект. У 2019–2021 роках, за офіційними звітами СБУ, зафіксовано значне збільшення психологічних операцій, спрямованих на підрив довіри до ЗСУ, мобілізаційного ресурсу, дискредитацію командування, формування втоми від війни серед населення. Ці кампанії часто поширювались через анонімні Telegram-канали, фейкові ЗМІ, бот-мережі, які видавали себе за «незалежні джерела» [8].

Ці процеси отримали максимальне загострення у 2022 році. Повномасштабне вторгнення, попри свою брутальність, супроводжувалось усіма гібридними компонентами: поширення паніки, заклики до капітуляції, фейки про «здачу міст», спроби сформувати паралельні адміністрації на окупованих територіях. Структури типу «комендатур» створювались з використанням місцевих кадрів, накачувались пропагандою, супроводжувались медійною імітацією стабільності [6].

Розуміння гібридної сутності російсько-української війни вимагає детального аналізу конкретних інструментів, які використовуються не лише проти України, а й проти всієї Європи. Цей конфлікт став практичною моделлю гібридного впливу — від інформаційного та психологічного тиску до роботи із культурними кодами, релігією, мовою та історією.

Одним із ключових елементів є маніпуляція історичною пам’яттю. Через медіа, освітні матеріали, заяви офіційних осіб і навіть кіно Росія нав’язує наративи про «єдиний народ», «спільне коріння», «нелегітимність української ідентичності». Цей компонент не є новим, але в умовах війни він став

інформаційною зброєю, мета якої — підважити право України на окреме існування [14].

У релігійному контексті використовується інструмент розколу та політичного тиску через церковні структури. Московський патріархат активно транслює проросійські ідеї, просуває ворожу до української державності риторику, підтримує окупаційні адміністрації. У такий спосіб створюється духовний простір війни, де церква замість миру стає інструментом зовнішньої агресії. Це породжує глибокі суспільні суперечності, а водночас легалізує окупаційні наративи [3].

Окрема сфера — інформаційно-психологічні спецоперації. У 2022–2023 роках особливо активізувались кампанії, спрямовані на:

- дискредитацію ЗСУ;
- підрив довіри до волонтерських ініціатив;
- стимулювання паніки під час ракетних обстрілів;
- просування зрадницьких наративів через блогерів і підставні медіа;
- створення фейкових документів і листів нібито від офіційних осіб.

Ці дії ретельно плануються — і часто виглядають переконливо для неспеціаліста. Саме тому з 2022 року в Україні запрацював Центр протидії дезінформації при РНБО, який фіксує, перевіряє і спростовує фейки, аналізує інформаційні атаки, а також виводить на «світло» бот-мережі й Telegram-канали, керовані з росії [7]. Щоб показати масштаб і системність гібридних інструментів, наведемо таблицю 2.3.

Таблиця 2.3.

Сфери реалізації гібридної стратегії РФ в Україні (2014–2023)

Сфера	Конкретні прояви	Наслідки для України
Військова	Наявність ПВК, диверсійні групи, без ідентифікації	Підрив довіри до збройної безпеки
Інформаційна	Фейки, ІПСО, дезінформація	Дестабілізація, паніка, розкол суспільства
Енергетична	Газовий тиск, блокада вугілля, атаки на ТЕС	Енергетична нестабільність
Релігійна	Використання РПЦ як політичного інструменту	Поширення антидержавної ідеології
Культурна	Переписування історії, цензура в ОРДЛО	Дегуманізація української ідентичності
Кіберпростір	Атаки на держсервіси, зломи, віруси	Параліч інфраструктури, крадіжки даних

Джерело: складено на основі [7,11]

Російська гібридна стратегія в Україні також тісно пов’язана з використанням міжнародного середовища. Через дипломатичні канали, агентів впливу, проросійські партії та аналітичні центри Кремль системно формує негативне уявлення про Україну на Заході, просуває тези про «непрацюючу демократію», «зовнішнє управління», «русофобію», «утиски меншин». Ці наративи знаходять ґрунт у частині західного суспільства, що погано розуміє контекст і може бути схильне до спрощених версій подій [4].

Ще одна важлива площина — вплив на тимчасово окуповані території. Тут гібридна стратегія поєднує фізичний тиск (затримання, депортації, фільтрації) з інформаційною обробкою (телебачення, листівки, соціальні виплати, культурна ізоляція). Усе це створює ілюзію «нормального життя» під окупацією, що, у свою чергу, підриває національну єдність. Головна мета — нав’язати людям нову ідентичність і перешкодити реінтеграції [8].

Окрему загрозу становлять спроби дискредитації міжнародної підтримки України. оосія запускає фейки про «втому Заходу», «нецільове використання допомоги», «розкрадання зброї» тощо. Це спрямовано на демобілізацію західної аудиторії, зниження довіри до Києва, провокування внутрішніх суперечок у західних суспільствах [11].

Реакція України на гібридну агресію росії стала не лише спробою оборони, а й прикладом поступового формування нової моделі національної стійкості, в якій класичні інструменти безпеки поєднуються з громадянським спротивом, цифровою трансформацією, дипломатичною активністю та культурним відродженням. Україна в умовах постійного зовнішнього тиску змогла побудувати горизонтальну модель спротиву, яка стала унікальною на європейському просторі [14].

Ця модель складається з кількох фундаментальних опор:

1. Від самого початку конфлікту основою опору стали не інститути, а громадяни. Волонтерський рух, самоорганізація, територіальна оборона — все це не лише компенсувало слабкість держави на перших етапах, але й створило соціальний імунітет до дезінформації та психологічного тиску. Довіра до ЗСУ, армії, медиків, волонтерів суттєво переважає довіру до політичних структур — це новий феномен гібридної епохи, коли обороноздатність вимірюється не лише кількістю танків, а й глибиною самоорганізації [3].
2. Україна активно впровадила цифрові інструменти — від «Дії» до кібероборони. Під час війни з’явився цифровий рекрутинг, мобільні трекери тривог, платформи для перевірки новин, бази для розпізнавання фейкових акаунтів. Створено механізми швидкого виявлення інформаційних атак, у тому числі через аналітику Telegram-мереж, інтеграцію OSINT, аналітику даних з відкритих джерел. Усе це суттєво ускладнює реалізацію російських гібридних операцій [7].

3. Попри складні умови, в Україні створено цілу низку нових інституцій, орієнтованих на виявлення та нейтралізацію гібридних загроз:

- Центр протидії дезінформації при РНБО;
- департамент кібербезпеки в СБУ;
- національні групи реагування на кібератаки;
- інформаційні підрозділи в Міноборони;
- центр стратегічних комунікацій при уряді [11].

Європейські країни, спостерігаючи за масштабом та багатовекторністю гібридної війни проти України, почали масово переглядати власні системи безпеки. Якщо до 2014 року Європа переважно орієнтувалася на класичні загрози, то тепер створюються багатофункціональні моделі безпеки, що включають аналітику медіаполя, моніторинг бот-мереж, захист енергетичних мереж, боротьбу з фейками таблиця 2.4

Таблиця 2.4.

Реакції західних партнерів на гібридну фазу війни в Україні (2022–2023)

Країна / інституція	Реалізовані ініціативи	Напрямок дії
Європейський Союз	Стратегія протидії дезінформації, East StratCom	Інформаційна безпека
НАТО	Створення Оперативної групи зі стратегічних комунікацій	Кібертаборона, боротьба з пропагандою
Польща	Програми з підвищення кіберграмотності, резервні війська	Цивільна мобілізація
Литва	Блокування кремлівських медіа, реформи у сфері освіти	Психологічна стійкість
Німеччина	Медіареформа, підтримка незалежної журналістики	Демократична протидія дестабілізації

Джерело: авторська компіляція на основі [4], 9]

Гібридна війна також змінила дипломатичний ландшафт. Україна змогла перетворити себе на центр глобального аналітичного інтересу, де обговорюються моделі безпеки нового покоління. Вперше за десятиліття у міжнародних дискусіях домінують не лише військові, а й інформаційні, кібернетичні, культурні аспекти. Український досвід розглядається як основа для формування Європейської доктрини гібридної стійкості [11].

Цей досвід має кілька унікальних особливостей:

- Швидка адаптація інституцій до умов повномасштабної війни;
- Готовність суспільства до мобілізації у всіх сенсах — від фізичного до цифрового;
- Система самоідентифікації на основі відторгнення ворога, а не ідеологічного конструкта;
- Гнучкість у співпраці з міжнародними партнерами та використанні новітніх технологій.

Однак, навіть попри значні успіхи, Україна залишається в зоні підвищеної вразливості. Гібридна війна — це постійний процес, який не завершується разом із боями на фронті. І після перемоги потрібно буде зберігати системність, продовжувати зміцнення наративів, перевірку інформаційних каналів, посилення інституцій.

У підсумку, російсько-українська війна продемонструвала, що гібридна агресія — це не сукупність хаотичних інструментів, а системна стратегія. І Україна — держава, яка не лише зупинила цю стратегію, а й перетворилася на платформу для формування європейських відповідей на гібридну загрозу.

2.3 Гібридні війни як виклик для безпекової архітектури Європи (НАТО, ЄС, ОБСЄ)

Поява гібридних форм агресії в XXI столітті стала серйозним викликом для традиційної безпекової архітектури Європи. Інституції, створені в епоху після Другої світової війни — насамперед НАТО, Європейський Союз і ОБСЄ — формувалися з урахуванням передусім традиційних загроз, які включали військову агресію, порушення кордонів і дипломатичні кризи. Водночас гібридна війна діє за зовсім іншими правилами: вона не вимагає перетину державних рубежів, може бути реалізована без єдиного пострілу, а її наслідки — не менш руйнівні, ніж у класичних конфліктах [14].

НАТО, як головний військово-політичний союз Заходу, опинилося перед необхідністю переосмислення принципу колективної оборони. Стаття 5 Вашингтонського договору передбачає реагування на збройну агресію, однак не дає чіткої відповіді щодо кібернападів, дезінформації або диверсій, здійснених через приватні структури. Саме після гібридної атаки на Естонію у 2007 році (масовані кіберудари по державних сервісах) в Альянсі вперше прозвучала думка про необхідність перегляду стратегій реагування на нові типи загроз [3].

У 2016 році НАТО офіційно визнало кіберпростір полем воєнних дій. Це стало важливим кроком у напрямку адаптації. Було створено Центр з кіберзахисту у Таллінні (CCDCOE), розпочато серії навчань з виявлення гібридної агресії, зміцнено співпрацю з приватним сектором у сфері кібербезпеки. Однак водночас залишаються значні прогалини у процедурній частині — наприклад, не всі країни-члени визнають однаково високий рівень загроз від фейків чи інформаційних операцій [8].

Європейський Союз також не мав чітких механізмів реагування на гібридну агресію до початку 2010-х. Однак із початком війни в Україні ситуація змінилась. У 2015 році була створена група East StratCom Task Force, основне завдання якої — виявлення, документування та спростування дезінформації, спрямованої проти

ЄС. На її базі з'явився один із найпотужніших у світі відкритих ресурсів — EUvsDisinfo — що щотижня оновлює базу російських фейків [11].

У 2020–2023 роках ЄС реалізував низку стратегій, серед яких:

- Європейський акт про цифрові послуги (Digital Services Act);
- Програма зміцнення кіберстійкості;
- Спільна стратегія боротьби з дезінформацією;
- Платформа перевірки достовірності новин для ЗМІ;
- Створення цифрових центрів у країнах-партнерах (у тому числі в Україні, Грузії, Молдові) [9].

ОБСЄ, з іншого боку, виявилася менш готовою до гібридних викликів. Основні інструменти цієї організації — спостереження, перемовини, посередництво — ефективні лише за наявності визнаних сторін конфлікту. У гібридній війні ж агресор часто заперечує свою участь, а конфлікт видається внутрішнім. Наприклад, на Донбасі Росія роками представлялась "спостерігачем", попри очевидну військову, фінансову і політичну участь. ОБСЄ не змогла виробити дієвих механізмів примусу до правди — її місія працювала формально, без повноважень і реального впливу [4].

Ця слабкість класичних структур сприяла створенню паралельних ініціатив, зокрема:

- Центр стратегічних комунікацій НАТО (Riga StratCom);
- Платформа Hybrid CoE у Гельсінкі;
- Платформа протидії гібридним загрозам при Єврокомісії;
- Центри OSINT-аналізу в національних спецслужбах.

Усі ці організації є відповіддю на нову логіку війни, в якій інформація — це зброя, а дестабілізація — мета. У другій частині підпункту буде докладно розглянуто взаємодію між структурами ЄС, НАТО і національними урядами, з аналізом конкретних кейсів успішної або неефективної протидії гібридній агресії.

Після початку гібридної агресії росії проти України міжнародні безпекові структури, зокрема НАТО та Європейський Союз, опинилися в ситуації, коли

наявні нормативні та організаційні рамки перестали відповідати реальному характеру загроз. Упродовж десятиліть ці інституції формувалися навколо поняття відкритої військової агресії — збройного нападу, порушення державних кордонів, окупації або загрози збройним насильством. Проте у нових умовах війна розгортається в інформаційному полі, в кіберпросторі, в економічних каналах, у дипломатичних маніпуляціях. Саме тому європейські уряди почали будувати альтернативні системи реагування, які дозволяють швидко виявляти, аналізувати й знешкоджувати прояви гібридного впливу навіть без формального початку війни.

Показовим прикладом такої трансформації стала стратегія Литви, яка у 2016–2023 роках створила цілісну вертикаль реагування на інформаційні атаки. Починаючи з регіональних офісів інформаційного моніторингу, які отримують дані зі шкільної освіти, медіа та соціальних мереж, і завершуючи урядовими центрами аналізу загроз, країна вибудувала модель, де громадянське суспільство не лише інформується, а й включається у процес протидії. Литовські державні органи не обмежились реагуванням, а взяли курс на напереджувальне стримування — йдеться про освітні ініціативи, інтервальні навчання, тренінги для держслужбовців, аналіз цифрових джерел впливу. Аналогічний досвід реалізовували й інші країни Балтії, які, маючи історичну пам’ять про радянське домінування, швидше за інших усвідомили небезпеку російського реваншизму в нових формах.

Німеччина після 2016 року, особливо в контексті виборів і спроб російського втручання в політичний процес, почала модернізувати систему кіберзахисту. Було створено незалежний Центр кібербезпеки (BSI), розширено повноваження відомств внутрішніх справ і спецслужб у сфері боротьби з дезінформацією. Водночас у цій країні тривалий час домінувала концепція ліберальної інформаційної відкритості, яка ускладнювала регулювання інформаційного поля. Тому підхід Німеччини до протидії гібридним загрозам тривалий час базувався не на забороні контенту, а на прозорості джерел фінансування, підвищенні

медіаграмотності й публічному аналізі загроз. Це створює ситуацію, коли безпековий ефект залежить не від адміністративного тиску, а від рівня критичного мислення у суспільстві.

Важливо зазначити, що гібридна війна — це не лише інструмент слабших держав проти сильніших. У сучасному світі вона стає полем боротьби між рівними — коли суперництво відбувається не в площині кількості військ чи озброєнь, а у здатності розхитувати суспільну єдність супротивника. Саме це пояснює, чому Росія не зупинилася лише на Україні, а активно впливала на внутрішньополітичні процеси в Італії, Франції, Іспанії, Чехії, Угорщині. Створення фейкових новин, підтримка маргінальних партій, фінансування ультраправих рухів, легалізація проросійської позиції через медіа — усе це стало стандартною тактикою, яку в Європі дедалі частіше сприймають як елемент гібридної агресії, а не лише як прояв свободи слова.

НАТО як військовий альянс довго утримувався від прямого втручання у справи, пов’язані з інформаційною безпекою або кіберпростором. Однак із часом стало очевидно, що невійськові інструменти можуть дестабілізувати країни-члени так само, як танки чи ракети. Саме тому у 2019 році на рівні альянсу було ухвалено рішення про те, що гібридна атака може вважатися підставою для активації Статті 5 — якщо її наслідки можна прирівняти до збройного нападу. Це стало першим кроком до розширення парадигми безпеки, де оборона не обмежується фізичним протистоянням, а передбачає цілісне бачення впливу — від дезінформації до шантажу енергетичними ресурсами.

Особливу роль у новій моделі реагування відіграють держави Північної Європи — зокрема Швеція, Норвегія, Данія. Вони розробили власні стратегії цифрової стійкості, які базуються на концепціях прозорості, міжсекторального моніторингу, а також швидкої комунікації з населенням. Замість заборон і блокувань ці держави обирають формат оперативного інформування — коли у відповідь на фейк влада не мовчить, а дає вичерпне пояснення. Це дозволяє утримувати довіру без обмеження свобод і створювати стійкий імунітет до

маніпуляцій. Такий підхід вважається одним із найбільш адаптивних у довгостроковій перспективі.

Криза довіри до ОБСЄ як платформи розв'язання конфліктів у гібридну епоху зумовлена тим, що організація не має ані власних сил стримування, ані механізмів для роботи з проксі-утвореннями. Коли сторони конфлікту не визнають одна одну, коли агресор заперечує свою присутність, коли бойові дії здійснюються через формально незалежні групи — традиційна дипломатія виявляється безсилою. Саме тому ОБСЄ на Донбасі роками фіксувала порушення, але не могла жодним чином вплинути на ситуацію. Це поставило питання про ефективність спостереження як інструменту, якщо немає важелів впливу або санкційного ресурсу.

На цьому тлі окремі країни почали формувати власні регіональні платформи. Так з'явилися ідеї про створення "гібридної ініціативи" на базі Східного партнерства, окремих проєктів у межах ініціативи "Тримор'я", а також пропозиції щодо об'єднання зусиль країн Чорноморського регіону у сфері протидії дезінформації та економічному тиску. Усе це вказує на те, що універсальні інститути більше не сприймаються як достатні, і що гібридна війна потребує гнучких, спеціалізованих структур.

Завершальний етап осмислення ролі гібридних загроз у європейському безпековому просторі пов'язаний із появою абсолютно нової парадигми безпеки — не оборонної, а проактивної, мережевої, інтегрованої у всі рівні державного і громадського управління. Якщо раніше безпека сприймалась як щось зовнішнє щодо громадянина — щит, який має виставити держава, то в умовах гібридного конфлікту кожен елемент соціуму стає і вразливим місцем, і потенційною оборонною точкою. Школа, місцеве самоврядування, освітній курс в університеті, новинний заголовок, мем у соцмережі — все це може бути або мішенню, або захистом, залежно від того, наскільки держава сформувала внутрішню стійкість.

Європейські країни, пройшовши фазу шоку після початку агресії проти України, поступово почали формувати свої системи раннього попередження про

гібридні ризики. Але що принципово нове — це рівень координації між державами, який раніше не був притаманний континенту. В умовах, коли гібридна війна може торкнутись будь-якої країни в Європі незалежно від її геополітичної активності, держави почали обмінюватися даними про інформаційні атаки, координувати інформаційні кампанії, створювати спільні центри моніторингу. Зокрема, у 2022–2023 роках запрацювали спільні ініціативи між Балтійськими країнами, Польщею та Україною, які об'єднали зусилля у сфері стратегічних комунікацій, кіберзахисту та протидії пропаганді.

На рівні Європейського Союзу значний прогрес показала інтеграція медіаполітики в контексті безпеки. Публічна комунікація політиків, оцінка дій росії, пояснення санкційної політики — усе це стало предметом окремої аналітики. З'явились спеціальні підрозділи у структурах ЄС, які займаються лише аналізом інформаційних загроз. Саме на основі цієї аналітики ухвалювались рішення про заборону трансляції російських медіа, блокування сайтів, обмеження платформ типу RT, Sputnik і створення чорних списків дезінформаторів. Причому ці рішення більше не сприймаються як обмеження свободи слова — натомість розглядаються як захист інфраструктури правди, без якої неможливо забезпечити ні вибори, ні демократичні процеси.

Водночас у Європі стало очевидним, що гібридна війна — це не окрема загроза, а матриця, яка лягає на всі інші виклики. Енергетика, міграція, екологія, національні меншини, економічна криза — всі ці теми можуть бути використані гібридно. І це вже не теоретичний сценарій, а реальність. Спроби росії впливати через енергетичні важелі, наприклад, використання газу як засобу політичного тиску, чи маніпуляції щодо мігрантів через Білорусь, або кампанії проти LGBTQ+ у Східній Європі — це вже не просто пропаганда, а механізми делегітимації європейського політичного устрою.

Ще одним результатом гібридної агресії стало розуміння необхідності виходу за межі вузької компетенції класичних безпекових інституцій. Тепер у сферу безпеки входять і Міністерства освіти, і цифрової трансформації, і культури.

У цьому сенсі війна більше не є справою лише військових. Саме тому нова архітектура безпеки формується як горизонтальна — не ієрархічна, а мережево розподілена. Це дозволяє швидко локалізовувати загрози, не чекаючи централізованої реакції. Наприклад, інформаційна атака в Угорщині тепер може бути проаналізована в Польщі за кілька годин, а база бот-мереж із Латвії — використана в Іспанії.

Гібридна війна стала також точкою розриву між класичною дипломатією та публічною безпековою політикою. Якщо раніше міжнародні організації мали справу з державами, тепер доводиться працювати з мережами — приватними акторами, медіа, організаціями, які можуть мати вплив, не будучи частиною жодної офіційної структури. Це змінило характер перемовин, що тепер включають у себе і медійний компонент, і аналітичний супровід, і цифровий захист. Операційне поле стало значно ширшим, і нові безпекові доктрини ЄС це прямо відображають.

На цьому тлі значно зріс інтерес до досвіду України. Саме вона стала тестовим полігоном, на якому випробовуються гібридні сценарії, і водночас — джерелом реальних інструментів протидії. Українські центри OSINT, волонтерські платформи, технологічні ініціативи з верифікації інформації, цифрова оборона критичної інфраструктури — все це інтегрується у навчальні програми та аналітичні напрацювання в європейських столицях. Не випадково багато європейських експертів називають Київ не лише фронтом, а штабом нової епохи безпеки.

На завершення варто наголосити: гібридна війна змінила саме розуміння сили в міжнародній політиці. Сила тепер вимірюється не лише боєздатністю, а й здатністю суспільства чинити опір впливу, адаптуватися до нових форм загрози, підтримувати свою модель правди, свої інституції, свою ідентичність. Гібридна війна — це війна за реальність, за уявлення про себе, про світ, про ворога і про союзника. У цій війні перемагає той, хто здатен відновлювати сенси швидше, ніж їх руйнують. Європа, яка пережила історії тиранії, геноциду й диктатур, має всі

шанси стати простором нової безпеки — безпаперової, швидкої, гнучкої, людяної. Але це потребує розуміння, що війна більше не починається з танка. Вона починається з фрази. І не завжди російською.

Висновки до Розділу 2

Російсько-українська війна є яскравим прикладом гібридної агресії, яка поєднує військові та невоєнні методи впливу. Війна на сході України та анексія Криму показали, як ефективно застосовуються інформаційні, економічні та політичні інструменти для досягнення геополітичних цілей. Україна змушена була не тільки захищати свою територію, а й формувати нові стратегії безпеки для боротьби з гібридними загрозами. Досвід України є важливим уроком для європейських країн щодо необхідності адаптації до нових форм агресії. Однак, незважаючи на певні успіхи, проблеми протидії гібридним загрозам залишаються актуальними для Європи.

РОЗДІЛ 3. СТРАТЕГІЯ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ У ЄВРОПІ

3.1. Політика ЄС і НАТО щодо боротьби з гібридними війнами

Після 2014 року, коли стало очевидним, що Росія веде повномасштабну гібридну кампанію проти України та паралельно здійснює вплив на держави Європейського Союзу, відбувся помітний зсув у сприйнятті характеру безпекових загроз у Європі. Традиційна структура оборони, розрахована на відкриту збройну агресію, виявилась недостатньою в умовах, коли атака не супроводжується офіційним оголошенням війни, не має чіткої фронтальної лінії й реалізується засобами інформації, кіберпростору, енергетики та внутрішньополітичної дестабілізації. Як НАТО, так і ЄС були змушені у короткі терміни переглянути свої концепції реагування на конфлікти та почати формування нового типу політики — комплексної, проактивної, адаптивної до гібридного середовища.

На рівні Європейського Союзу перші системні кроки в напрямі протидії гібридним загрозам були зроблені у 2015 році зі створенням спеціальної групи — East StratCom Task Force. Вона була покликана відслідковувати, документувати та аналізувати дезінформаційні кампанії, спрямовані проти ЄС, з особливим акцентом на країни Східного партнерства, включно з Україною. На базі цієї структури почала функціонувати платформа EUvsDisinfo, яка стала важливим інструментом збору доказів та реакцій на інформаційні атаки.

Уже на наступному етапі було розроблено ширшу стратегічну рамку: з’явилась Спільна рамка щодо боротьби з гібридними загрозами (Joint Framework on Countering Hybrid Threats), ухвалена у 2016 році. Цей документ сформулював базові пріоритети: підвищення ситуаційної обізнаності, нарощування потенціалу стійкості держав-членів, зміцнення відповідних інституцій, забезпечення оперативного реагування. Було наголошено на необхідності інтеграції дій цивільного та військового секторів, покращення обміну даними між державами, підготовки до кризових сценаріїв та проведення навчань, зокрема спільно з НАТО.

Значним кроком стало посилення взаємодії між ЄС та НАТО. Обидві організації підписали у 2016 році спільну декларацію про намір тісніше координувати свої дії у сфері безпеки, особливо у протидії кіберзагрозам, дезінформації та нестандартним загрозам. У подальшому цей формат було розширено, і з'явився окремий Пункт 6 у списку спільних пріоритетів співпраці — він безпосередньо стосувався протидії гібридній війні. У результаті НАТО і ЄС почали регулярно проводити спільні навчання, створили канали швидкої комунікації у разі гібридних атак, почали формувати єдині сценарії реагування [9].

Паралельно з інституційними рішеннями зростала увага до цифрової безпеки. У 2020–2022 роках ЄС ухвалив кілька важливих нормативно-правових актів: Регламент про кібербезпеку, Європейський акт про цифрові послуги (Digital Services Act), а також Європейський акт про цифрове управління. Ці документи ввели суворіші правила щодо прозорості онлайн-платформ, відповідальності за поширення дезінформації, обов'язку верифікації джерел і боротьби з бот-мережами. Така активність пов'язана не лише з війною проти України, але й зі спробами впливу на вибори у Франції, Німеччині, Іспанії та країнах Балтії [11].

На окрему увагу заслуговує створення центру Hybrid CoE — Центру з вивчення гібридних загроз, який функціонує у Гельсінкі. Він не є частиною жодної міжнародної організації, однак має статус аналітичного хабу, що об'єднує країни-члени НАТО та ЄС. Його завдання — вивчення практик гібридного впливу, розробка аналітичних моделей, тестування реакцій, організація спільних навчань та вироблення рекомендацій для урядів [4].

Паралельно НАТО адаптувало свою стратегічну концепцію. У 2010-х роках Альянс ще розглядав конфлікти переважно у військовій площині. Але після нападів на Естонію (2007), гібридної агресії проти України (2014), численних прикладів втручання у політичне життя західних держав, було вирішено офіційно визнати кіберпростір як повноцінну зону військових дій. У 2016 році на саміті у Варшаві ця позиція була закріплена. Водночас було оголошено, що у випадку

гібридної атаки, яка матиме значний вплив, НАТО може застосувати Статтю 5 Вашингтонського договору про колективну оборону [3].

Цей крок став визначальним у формуванні нової безпекової філософії: якщо раніше Альянс реагував лише на збройну агресію, то тепер визнається, що дезінформація, кібератака або енергетичний шантаж можуть становити загрозу такого ж рівня. На практиці це означає створення багаторівневої системи реагування, у якій цивільні, військові, розвідувальні та технологічні інституції працюють у тісній координації.

Політика НАТО, спрямована на протидію гібридним загрозам, отримала практичне наповнення через створення спеціальних аналітичних і командних структур. До них, зокрема, належить Оперативна група зі стратегічних комунікацій (Strategic Communications Centre of Excellence), що базується в Ризі. Її завдання — відстеження ворожих інформаційних кампаній, аналіз структури впливу, підготовка військових і цивільних фахівців до роботи в умовах інформаційного тиску [9]. Такі центри не обмежуються аналітикою: вони беруть участь у моделюванні сценаріїв, організовують навчання, розробляють алгоритми реагування на ситуації, коли, наприклад, країна-член піддається кіберзагрозам або підривній пропаганді.

У процесі активізації російської агресії проти України після 2022 року НАТО посилило комунікацію з партнерами, особливо з Україною, Фінляндією, Швецією та країнами Східного флангу. Підвищено обмін розвідувальними даними, вдосконалено протоколи реагування на неідентифіковані дії у прикордонних районах, активізовано функціонування Центру кібероперацій у Монсі. Саме там зосереджено координацію дій у разі загрози атаки на цифрову інфраструктуру країн-членів, у тому числі — критичної: енергосистем, транспортних мереж, систем урядового зв’язку.

Особливе місце в антикризовій стратегії посідає моделювання гібридних загроз. Такі навчання, як CMX (Crisis Management Exercise), організовуються НАТО регулярно й охоплюють ситуації з інфофейками, атаками на виборчі

системи, маніпуляціями через соцмережі, кібершантажем тощо. За участі країн ЄС ці навчання імітують реальні гібридні сценарії, спрямовані на виявлення слабких місць у комунікаційних ланцюгах, перевірку протоколів, оцінку дій урядів і командного складу [3].

На практиці ці заходи знайшли своє застосування у низці криз. У випадку з атакою на критичну інфраструктуру Литви в 2022 році — блокування морських портів шляхом кібератак і дезінформаційної кампанії — було швидко введено в дію комунікаційний план стратегічної відповіді. Поширено правдиву інформацію, заблоковано джерела фейків, нейтралізовано вплив через координовану взаємодію між урядом, операторами зв'язку та місією ЄС. Подібну модель у 2023 році застосовувала Польща, коли на території країни зафіксували хвилю фейкових повідомлень про теракти, які мали спричинити паніку в прикордонних районах [4].

У контексті України та російської гібридної агресії, особливо після 2022 року, обидві структури — ЄС і НАТО — посилили координацію допомоги. Йдеться не лише про поставки озброєння, а про навчання з кіберзахисту, фінансування Центру протидії дезінформації при РНБО, розширення співпраці з українськими ІТ-фахівцями. НАТО також надав доступ до аналітичних інструментів, які дозволяють відстежувати поведінку бот-мереж і каналів впливу, що працюють з території РФ або Білорусі. ЄС, своєю чергою, ініціював запуск механізмів швидкого реагування на інфоатаки, які можуть стосуватися України, включаючи автоматизовану верифікацію новин і консультаційно-аналітичну підтримку СБУ [7].

Попри такі зрушення, лишається низка труднощів. По-перше, країни-члени НАТО і ЄС мають різний рівень обізнаності й чутливості до гібридних загроз. Якщо Литва, Польща, Естонія або Чехія добре усвідомлюють характер гібридної агресії, то в Італії, Австрії чи Іспанії іноді фіксується недостатня готовність визнати, що інформаційна кампанія може бути формою воєнної дії. По-друге, дезінформаційні кампанії часто спираються на внутрішні проблеми країн —

корупцію, соціальну нерівність, мовні суперечки — і саме тому вимагають від урядів не лише зовнішньої, а й внутрішньої стійкості. По-третє, формально ЄС і НАТО — це дві різні структури, які діють за окремими мандатами. І попри зростаючу взаємодію, подекуди спостерігається дублювання функцій або суперечливі підходи до однакових ситуацій.

Однак ключовим досягненням стало розуміння того, що гібридна агресія вимагає не лише реакції, а постійної готовності, аналітики, попередження. Саме тому в Європі формується нова доктрина стійкості — не як реакції на напад, а як політики завчасного виявлення і знешкодження механізмів впливу. У фінальній частині цього підпункту буде розглянуто поточні виклики та шляхи вдосконалення вже наявної європейської безпекової стратегії з урахуванням досвіду України.

Значним викликом для ЄС та НАТО залишається асиметрія між країнами-членами у здатності протидіяти гібридним загрозам. У державах Центральної та Східної Європи, які мають безпосередній історичний досвід російського втручання, спостерігається вища чутливість до небезпек такого типу, краще налагоджені механізми кризового реагування, вища мобілізаційна готовність суспільства. Натомість у Західній Європі подекуди зберігається сприйняття гібридної війни як вторинної загрози, не здатної спричинити безпосередню дестабілізацію. Це створює складнощі при виробленні єдиної політики, особливо в частині санкцій, обмеження доступу до ресурсів та визначення джерел загроз.

Ще одним проблемним елементом є різний рівень цифрової грамотності та культури споживання інформації у населення країн-членів. Саме через цю нерівномірність маніпулятивні наративи поширюються швидше у певних соціальних сегментах або регіонах. Дезінформація має змогу вкорінюватися в аудиторії через брак критичного аналізу, недовіру до офіційних джерел, нерозвиненість державних каналів комунікації. Як наслідок, навіть найсучасніші технічні системи захисту можуть виявитися неефективними без активної участі громадян у формуванні інформаційної стійкості.

Проте на рівні стратегічного планування відбувається зрушення: європейські безпекові концепції дедалі частіше передбачають побудову систем стійкості не лише через інституційні засоби, а через залучення громадських організацій, освіти, приватного сектору. Наприклад, у країнах Балтії реалізуються програми медіаосвіти для школярів і студентів, курси для держслужбовців із виявлення фейків, проєкти спільного реагування між державою та незалежними фактчекерами. У межах НАТО започатковано ініціативу з підтримки нових технологічних розробок, які дозволяють аналізувати великі масиви даних з метою виявлення прихованих впливів — таких як скоординовані мережі ботів, фінансування псевдоаналітичних платформ або медіа з непрозорою структурою власності.

Важливо також, що і ЄС, і НАТО на рівні політичних заяв дедалі частіше апелюють до концепції "стратегічної автономії" у сфері безпеки. Йдеться не лише про спроможність реагувати без залучення США чи інших зовнішніх сил, а про здатність формувати цілісну політику захисту від внутрішніх і зовнішніх загроз без посередництва. У цьому контексті особливу увагу приділяють розробці єдиного європейського підходу до захисту інформаційного простору — створення механізмів, що дозволятимуть виявляти ворожий вплив на всій території ЄС одночасно, з подальшим ухваленням скоординованих рішень.

Досвід України в умовах гібридної агресії Росії починає сприйматися у європейських столицях не лише як елемент боротьби за незалежність, а як джерело практичних рішень. Саме тому Україна дедалі активніше інтегрується в аналітичні платформи НАТО, отримує підтримку для розвитку центрів кіберзахисту, долучається до обміну даними щодо дезінформаційних кампаній. З'являється концепція "forward resilience" — тобто зміцнення стійкості не лише всередині ЄС, а й у країнах-партнерах, що перебувають на передовій боротьби з гібридними загрозами. Україна стає одним із головних майданчиків для реалізації такої концепції.

Отже, політика ЄС і НАТО щодо боротьби з гібридними війнами пройшла складний еволюційний шлях — від заперечення самої можливості такого типу конфлікту до формування багаторівневої системи реагування. В основі цієї політики лежить визнання, що сучасна війна не обов'язково супроводжується стрілянинӧю, але може нести не менше руйнівні наслідки через вплив на інституції, ідентичність, довіру громадян до власної держави. Ключем до протидії визнано поєднання оперативного реагування, аналітичної підготовки, цифрової безпеки та медіаграмотності. Водночас, ця стратегія потребує постійного оновлення, адаптації до нових умов, врахування досвіду держав, що вже перебувають у гібридному конфлікті.

Європейська безпекова політика вже ніколи не буде такою, якою вона була до 2014 року. В умовах, коли війна більше не починається з артобстрілів, а з наративу в соціальних мережах, а перемога вимірюється не лише територією, а й стійкістю системи до деструктивного впливу, ЄС і НАТО змушені будувати нову архітектуру. Її формування ще триває, але вже очевидно: саме гібридні загрози стали каталізатором створення Європи як безпекової спільноти нового типу — гнучкої, проактивної, технологічно підготовленої, здатної захищати не лише кордони, а й інформацію, реальність, правду.

3.2. Досвід України у протидії гібридній агресії: уроки для європейських країн

Після початку російської гібридної агресії у 2014 році Україна стала головним полем випробування новітніх форм конфлікту. Йдеться не лише про військове протистояння, а про ситуацію, в якій одночасно діють десятки каналів впливу — від пропаганди й фейків до кібератак, шантажу через газ, втручання у внутрішню політику, інфільтрацію в інформаційні середовища. Усі ці складові не просто ускладнили традиційне реагування, а вимагали від українського суспільства, держави, бізнесу, армії та медіа нових форм самоорганізації. Саме тому досвід України вважається унікальним для всієї Європи: він демонструє,

яким чином держава без повноцінних ресурсів Альянсу чи структур ЄС змогла вибудувати адаптивну модель спротиву гібридним загрозам.

Перші кроки України у відповідь на гібридну війну були радше інстинктивними, ніж системними. На початковому етапі відсутність чітких механізмів оцінки інформаційної загрози, недостатній рівень цифрової підготовки, фрагментованість державного управління та вразливість до фейків створювали високий ступінь дестабілізації. Проте вже у 2015–2016 роках було сформовано нову логіку реагування. Вона базувалась не стільки на формальних структурах, скільки на горизонтальній самоорганізації — саме це стало ознакою українського способу протидії. Волонтерські ініціативи, ІТ-ком'юніті, аналітичні платформи, незалежні фактчекери, освітні кампанії — усі вони разом почали будувати стійкість ізнизу. Така модель протистоїть не лише атакам, а й загальному атмосферному фону, який прагне посіяти розгубленість, зневіру, дезорієнтацію.

Починаючи з 2014 року, після окупації Криму та розгортання бойових дій на Донбасі, українське суспільство виявилося в умовах масштабної гібридної агресії, яка охоплювала всі ключові сфери життя: військову, політичну, інформаційну, економічну, соціальну, культурну й релігійну. Відмінною рисою цієї агресії була її неоголошеність і багатошаровість: водночас відбувалася анексія територій, кампанія дезінформації в українських і міжнародних медіа, блокування постачання енергоносіїв, підтримка антидержавних рухів та організацій, спроби делегітимізації нової влади та вплив на політичні процеси через підконтрольні медіа й агентів впливу.

Офіційне усвідомлення гібридної загрози на рівні української державної політики почалося у 2015 році, коли вперше було зафіксовано системну роботу російських структур із розхитування ситуації всередині країни, використання інформаційного тиску на громадську думку, маніпуляцій щодо українських Збройних сил, запуску дезінформаційних кампаній через соцмережі та проросійські медіа [15]. Однією з перших відповідей стала концептуальна зміна ролі громадянського суспільства — від традиційно споживацької до мобілізованої,

активної. Саме добровольчі об’єднання, волонтерські ініціативи, ІТ-групи стали першими, хто почав документувати інформаційні атаки, ідентифікувати ворожі кампанії, створювати мережі цифрового моніторингу.

Важливим елементом цієї протидії стало заснування в Україні незалежних проєктів OSINT (Open Source Intelligence), зокрема InformNapalm, Molfar, Texty.org.ua та StopFake. Вони не просто розвінчували фейки — вони створювали методологію перевірки інформації, яка пізніше була інтегрована в аналітичну практику західних країн [7], [11]. StopFake, зокрема, вже у 2014 році започаткував регулярний моніторинг російських дезінформаційних наративів у медіа, соцмережах і навіть у політичних висловлюваннях окремих європейських лідерів, які транслювали кремлівську риторику.

Наступним кроком стало створення державних структур, здатних реагувати на гібридні загрози на інституційному рівні. У 2021 році при РНБО України було створено Центр протидії дезінформації — перший державний орган, що спеціалізується виключно на виявленні, аналізі та нейтралізації інформаційно-психологічних операцій, які мають ознаки гібридного впливу [7]. У його функції входить виявлення фейків, координація комунікацій між органами державної влади, налагодження співпраці з фактчекерами та навчання державних службовців правилам поведінки в умовах ІПСО.

У сфері кібербезпеки Україна ще до повномасштабного вторгнення у 2022 році почала активно вибудовувати національну систему захисту критичної інфраструктури. Створено Державну службу спеціального зв’язку та захисту інформації, НЦУКЗ (Національний центр управління кібербезпекою), що відповідають за відслідковування та відбиття атак на енергетичні об’єкти, медичні системи, транспортну інфраструктуру, банківський сектор. Український кіберфронт, що виник у перші дні вторгнення — об’єднання незалежних ІТ-фахівців, хактивістів, волонтерів — став реальним чинником протидії. Їхні дії призвели до масового знеструмлення серверів окупантів, перехоплення

пропагандистських повідомлень, блокування каналів взаємодії між колаборантами [16].

Інформаційна сфера стала одним з основних полів бою. Російські кампанії були націлені не лише на внутрішню дестабілізацію України, а й на вплив на європейську й американську аудиторії. Україна у відповідь застосувала комплекс дій: від оперативного спростування фейків до створення ефективної цифрової комунікації. Офіційні акаунти Президента України, Генштабу, МЗС, Мінцифри, РНБО у Twitter, Facebook, Telegram стали не лише каналами інформування, а й засобом стратегічної комунікації — у реальному часі, без посередників. Саме ця прозорість дозволила Україні стати джерелом довіри в інформаційній війні. Ключовим стало не лише говорити правду, а й робити це швидше, ніж супротивник встигне нав'язати свій наратив [5].

Окрім оперативної комунікації, український уряд реалізував довгострокові стратегії цифрового спротиву. Особливу роль тут відіграє Міністерство цифрової трансформації, яке з початку повномасштабної фази війни координує заходи зі збереження роботи державних сервісів, забезпечення кіберзахисту даних та підтримки цифрової грамотності населення. Програма «Дія.Цифрова освіта» трансформувалася з платформи про базові навички в центр системної протидії дезінформації. Окремі навчальні модулі були присвячені виявленню фейкових новин, алгоритмам поведінки в умовах інформаційної атаки, правилам цифрової гігієни. Цей підхід отримав схвальні відгуки від європейських партнерів та став базою для адаптації схожих ініціатив у країнах Балтії [16].

Унікальною рисою українського досвіду стало поєднання державної, волонтерської та IT-ініціатив. Саме горизонтальні мережі, які швидко мобілізуються в кризові моменти, виявилися ефективнішими за жорстко централізовані структури. Це стосується як роботи на інформаційному фронті, так і в сфері аналітики. Так, спільнота OSINT-дослідників (наприклад, Bellingcat, InformNapalm, Molfar, DeepState) працює паралельно з державними розвідками,

забезпечуючи швидке підтвердження подій, ідентифікацію військової техніки супротивника, геолокацію злочинів, викриття фальсифікацій [7], [11].

Особливої уваги заслуговує формування національної моделі інформаційної стійкості. На відміну від багатьох країн ЄС, Україна не лише ідентифікувала загрозу, а й розробила власну логіку реагування, яка передбачає:
– виявлення ворожого наративу ще до того, як він стане вірусним;
– оперативну реакцію через державні та незалежні інформаційні канали;
– залучення авторитетних експертів, журналістів, волонтерів для поширення спростувань;
– подальший моніторинг інформаційного сліду й адаптацію меседжів.
Цей механізм реалізується через постійний обмін інформацією між Центром протидії дезінформації, СБУ, РНБО, Мінцифри, а також журналістськими колективами, що мають репутацію надійних джерел [5], [9].

Важливим аспектом є те, що у ході гібридної війни Україна не обмежилася обороною — вона ініціювала активні інформаційні операції, спрямовані на нейтралізацію ворожої пропаганди у міжнародному середовищі. Це відбувалося через регулярні брифінги, взаємодію з міжнародними медіа, запуск англомовного контенту, залучення лідерів думок та світових культурних діячів. Держава створила нову форму дипломатії — цифрову, яка дозволила комунікувати напряму з аудиторією західних країн, минаючи офіційні канали. Так, інформаційна кампанія «#ArmUkraineNow», яка стартувала у березні 2022 року, охопила понад 100 мільйонів користувачів у соцмережах і стала прикладом ефективного громадянського тиску на уряди європейських країн [4].

Значний внесок у боротьбу з гібридною агресією зробили українські правозахисні та журналістські розслідувальні ініціативи. Зокрема, організації «Інститут масової інформації», «Інтерньюз-Україна», «Лабораторія цифрової безпеки» розробляли інструкції, алгоритми реагування, надавали експертні консультації ЗМІ, проводили тренінги для журналістів щодо безпечної роботи в умовах війни та маніпулятивного тиску. Цей досвід уже сьогодні інтегрується у

навчальні програми європейських університетів, аналітичних центрів, шкіл журналістики. Так, курси на базі Центральноєвропейського університету (CEU) у Відні та Ризької школи журналістики містять модулі, розроблені на основі українських кейсів 2014–2023 років [11].

Українська модель спротиву довела ефективність у реальних умовах багаторічної гібридної атаки, і це стало причиною активної інтеграції України до західних безпекових систем. Україна вже бере участь у програмах НАТО з кіберстійкості, регулярно обмінюється досвідом з країнами Балтії, Польщею, Чехією, а її аналітичні напрацювання використовуються у формуванні відповідей на гібридні виклики в інших регіонах Європи — зокрема, у випадках впливу на вибори, інформаційного тиску на нацменшини, спроб розхитати довіру до демократичних інститутів.

З огляду на вищезгадане, український досвід є джерелом практичних рішень у кількох площинах:

– формування швидкої реакції на ІПСО;

– організація цифрового самозахисту громадян;

– налагодження горизонтальної моделі протидії гібридному впливу;

– інтеграція держави, суспільства та ІТ-спільноти в єдиний механізм;

– стратегічна комунікація з міжнародною аудиторією на основі прозорості й довіри.

Досвід, який Україна сформувала протягом десятиліття протистояння гібридній агресії, набуває особливої цінності в умовах, коли аналогічні форми тиску дедалі частіше застосовуються й проти держав-членів Європейського Союзу та Північноатлантичного альянсу. У багатьох із них вже фіксувались спроби втручання у виборчі кампанії, поширення дезінформаційних наративів, політичне фінансування проксі-партій, активність інформаційних агентів, атак на цифрову інфраструктуру. Водночас, система реагування в цих країнах досі залишається орієнтованою переважно на класичні моделі загроз — із чіткими джерелами, з ідентифікованим ворогом і традиційною логікою оборони.

Україна, діючи в умовах постійного тиску, розробила модель, яка може бути адаптована до специфіки інших держав. Ідеться про багаторівневу побудову інформаційної стійкості, де поряд із державними механізмами активно діють недержавні гравці, які не є об'єктами політичного впливу, але мають довіру суспільства і фахову спроможність реагувати швидше, ніж бюрократичні інституції. Ця швидкість і гнучкість стали одним із ключових факторів ефективності.

Країни ЄС почали переймати окремі елементи цієї моделі. У Литві, Латвії та Естонії запроваджено громадські платформи верифікації інформації, які тісно співпрацюють з офіційними структурами, однак залишаються незалежними від них у прийнятті рішень. У Польщі впроваджено навчальні модулі для держслужбовців, базовані на досвіді українських програм із розпізнавання ІПСО. У Німеччині та Франції після 2022 року розпочато переосмислення підходу до прозорості інформації — з визнанням того, що демократичне суспільство може бути вразливим до агресії не через нестачу інституцій, а через надлишок довіри до інформаційного середовища.

Окремим внеском України стало переосмислення ролі цифрових технологій. У країнах Європи існує тенденція до концентрації таких функцій у межах окремих відомств, натомість український досвід демонструє ефективність горизонтальних структур, де ініціатива йде від низу до верху. Це забезпечує швидку реакцію, креативність, адаптацію до змін. Українські ІТ-фахівці, працюючи часто у статусі волонтерів, стали рушієм цифрового спротиву, розробили десятки сервісів і механізмів виявлення загроз, аналізу джерел тиску, нейтралізації дезінформації. У країнах ЄС і НАТО вже обговорюється створення аналогічних структур — цифрових добровольчих платформ, які будуть діяти в координації з урядами, але на умовах відкритості й прозорості.

Ще один напрям, який викликає зацікавленість у європейських партнерів — це комунікаційна стратегія України на міжнародному рівні. Україна змогла сформувати нову модель дипломатії — публічної, заснованої не лише на зустрічах

і заявах, а на прямій взаємодії з аудиторією іноземних країн. Офіційні канали влади стали не просто інформаторами, а учасниками глобального медіаполя. Такий підхід уможливлює оперативне формування позиції, випереджувальну реакцію на ворожі наративи та швидке пояснення складних рішень. У кількох країнах НАТО вже створено аналогічні центри, які аналізують український кейс і впроваджують його принципи в свою інформаційну політику [3], [11].

Для Європи головним уроком є не лише необхідність підвищення технічної спроможності. Український досвід вказує на важливість довіри — між громадянами та державою, між експертним середовищем і силовими структурами, між журналістами та держслужбовцями. Там, де ця довіра існує, навіть потужна дезінформаційна атака не призводить до паніки чи розпаду суспільної злагоди. У європейському контексті це означає, що боротьба з гібридними загрозами має охоплювати не лише безпековий, а й етичний, освітній, комунікаційний рівень.

У результаті, українська практика вже сьогодні трансформує політику ЄС і НАТО. Ряд елементів української стійкості включено у стратегічні документи Альянсу, а концепція forward resilience — тобто зміцнення країн-партнерів на зовнішньому контурі — фактично виникла з українського контексту. Крім того, Україна є одним із небагатьох прикладів, коли країна, яка зазнає постійної агресії, не лише не розпалася, а стала активним суб’єктом формування нової безпекової парадигми в Європі.

3.3. Інструменти захисту від інформаційної війни та кіберзагроз

Коли війна перестає бути виключно справою фронту, лінія оборони зміщується у зовсім інші простори — в голови людей, у цифрову інфраструктуру, в соціальні мережі, в персональні пристрої. Те, що ще десять років тому розглядалося як периферія безпеки, сьогодні є її центром. У сучасних умовах будь-яка держава, яка ігнорує захист інформаційного простору та вразливість цифрової системи, залишає відкритими двері для впливу, навіть якщо її армія готова до війни. Саме тому і Європейський Союз, і НАТО протягом останніх років почали

системно будувати новий рівень захисту — той, який не замикається у військових казармах, а охоплює інфраструктуру міст, роботу медіа, державні портали, освітні платформи й навіть звичні способи комунікації в месенджерах.

Реакція на інформаційні загрози починається з усвідомлення їхнього масштабу. У період з 2016 по 2023 роки зафіксовано сотні спроб впливу на вибори, державну політику, громадську думку в європейських країнах — і практично всі вони мали спільну рису: були замасковані під внутрішні процеси. Це робить інформаційну атаку складною для виявлення. Саме тому у ЄС сформовано мережу центрів раннього попередження, зокрема EU Hybrid Fusion Cell, що працює під егідою Інституції зовнішньої дії ЄС. Завдання цієї структури — не чекати моменту, коли кампанія вийде на поверхню, а ідентифікувати тренди на етапі формування — через аналіз новин, соціальних мереж, відкритих джерел.

Ще один приклад нової логіки дій — програма Digital Services Act, яка набрала чинності у 2023 році. Вперше на рівні законодавства найбільші цифрові платформи зобов'язані виявляти та припиняти поширення дезінформації. Раніше подібні ініціативи існували лише у вигляді саморегуляції, але сьогодні держави переходять до прямої відповідальності: якщо Facebook, YouTube чи TikTok не реагують на очевидні маніпуляції, їх очікують санкції. Це сигнал не лише для компаній, а й для суспільства: інформація — це не просто вільна думка, а частина безпеки [11].

У сфері кібербезпеки одним з головних елементів стало створення Європейського агентства з кібербезпеки (ENISA), яке координує дії країн ЄС, надає методичні рекомендації, проводить регулярні навчання й аналізує нові загрози. Після кібератак на системи охорони здоров'я в Ірландії, банківську інфраструктуру Італії, транспортні компанії Франції, стало зрозуміло, що критична інфраструктура більше не захищена самою лише фізичною безпекою. Напади відбуваються без жодного попередження, залишаючи після себе збій систем, викрадені дані, фінансові втрати. Саме тому держави змушені були

переглянути підхід до захисту. Сьогодні кібербезпека — це не окремий відділ у міністерстві, а горизонтальна функція, присутня в усіх секторах управління [4].

Один із помітних зрушень у підходах до інформаційної безпеки в Європі — активне залучення неурядових організацій та незалежних аналітичних центрів. Національні уряди визнають, що традиційна вертикаль реагування часто запізнюється або ж не встигає адаптуватися до швидкості, з якою працюють інформаційні кампанії. Саме тому почали з'являтися партнерські програми між міністерствами та незалежними фактчекінговими платформами. У Франції, Німеччині, Литві та Фінляндії такі проєкти отримують пряме фінансування, але зберігають контентну автономію. Це дозволяє зберігати довіру до джерел, уникати звинувачень у цензурі та одночасно створювати швидкий і надійний механізм протидії фейкам.

Крім того, держави почали працювати з платформами ще до того, як контент стане вірусним. У межах Центру боротьби з гібридними загрозами у Гельсінкі (Hybrid CoE), який працює на стику ЄС та НАТО, створено систему попереднього аналізу інформаційних викидів, що базується на машинному виявленні змін у мовленні бот-мереж, аномалій у взаємодії акаунтів та повторюваних патернів викиду однотипних повідомлень [4].

На рівні НАТО ситуація з кібербезпекою отримала ще більш централізовану структуру. У Штаб-квартирі Альянсу у Брюсселі діє Центр координації кібероперацій, який відповідає за реагування у разі кібератаки проти будь-якої країни-члена. Згідно з рішенням саміту 2021 року, масштабна кібератака, що призводить до серйозних наслідків для інфраструктури, може бути підставою для застосування Статті 5 — тобто розглядатися як збройна агресія. Це означає зміну розуміння самої суті безпеки: не обов'язково запускати ракети, достатньо знищити зв'язок, фінансову систему, електропостачання — і країна опиняється в умовах паралічу [3].

Європейські держави почали активно модернізувати критичну інфраструктуру з урахуванням кіберризиків. Зміни торкнулись банків, залізниці,

авіаперевезень, енергетики, медицини. Усе більше об'єктів під'єднують до систем раннього сповіщення про аномалії — не лише фізичні, а й цифрові. У Німеччині працює система цифрового аналізу «SINA», у Литві — комплекс із виявлення впливу на громадську думку через Telegram-канали. В Україні, ще до 2022 року, були створені прототипи подібних систем, які у ході повномасштабної агресії стали основою координації між Мінцифрою, СБУ, Центром протидії дезінформації та громадськими ініціативами [8].

Одним з найвиразніших прикладів взаємодії держави, цифрового сектору й аналітичного середовища стала платформа EU DisinfoLab, яка на постійній основі документує інформаційні кампанії, координовані або підтримувані державними та недержавними структурами, пов'язаними з Росією. Саме завдяки їхнім дослідженням вдалося викрити десятки псевдоаналітичних ресурсів, які мали вигляд авторитетних західних ЗМІ, але фактично виконували функції впливу на громадську думку в Європі. У 2019–2022 роках за їх участі виявлено мережу з понад 250 сайтів, які маскувались під місцеві медіа й поширювали однотипні меседжі — від дискредитації України до підриву довіри до європейських урядів.

Окрему увагу варто приділити платформі EUvsDisinfo — це не просто сайт зі спростуваннями. Це аналітична база даних, у якій зафіксовано понад 14 тисяч прикладів дезінформації, їх джерела, аудиторії, структура подачі, а також методи протидії. Платформа інтегрується в навчальні програми, використовується журналістами, науковцями, дипломатами. Її головна мета — не просто спростовувати, а пояснювати, як побудована атака, якими є механізми її поширення, чому вона виявилась ефективною чи ні. Це переходить від реакції до профілактики.

У сфері кібербезпеки європейські держави поступово переходять до моделі симетричної й асиметричної відповіді. Симетрична — це захист власних систем, модернізація ПЗ, побудова резервних каналів зв'язку, створення національних центрів кіберзахисту. Асиметрична — це можливість атакувати відповідно до міжнародного права, паралізувати мережі, які стали джерелом загрози. Тут постає

складне питання: що вважати виправданою відповіддю, а що — ескалацією. У рамках ЄС нині триває розробка «кибердоктрини», яка має встановити юридичні межі й правила гри у кіберпросторі.

Досвід України у цій галузі особливо цінується. Після 2022 року Україна стала фактично живою лабораторією для відпрацювання моделей кібероборони. Ще у 2020 році в Україні був створений Національний центр резервного управління у сфері кіберзахисту (НЦУКЗ), який став ключовим координаційним майданчиком між військовими, розвідкою, Мінцифрою, приватними розробниками. В умовах масованих атак — зокрема на «Дію», банківську систему, логістику, зв'язок — саме цей центр забезпечив безперервність основних сервісів. Досвід його роботи вже вивчається в Естонії та Чехії — країнах, які свідомо готуються до сценаріїв кіберконфліктів [7], [11].

Що ж до практичних уроків — одним із них є важливість не лише наявності технологій, а й людей, які ними керують. У багатьох випадках українські фахівці, які до 2022 року працювали у приватному секторі, самостійно організовувались у кіберволонтерські групи, створювали засоби виявлення атак, виводили з ладу інформаційні ресурси агресора. Ці люди не мали державного мандату, але мали довіру, досвід і технічну компетенцію. Такі горизонтальні ініціативи стали прикладом для держав ЄС — не як тимчасовий захід, а як модель довгострокової мобілізації цифрового ресурсу у кризовий час.

Європейські країни, аналізуючи власну вразливість до гібридних впливів, визнають, що ключ до ефективного захисту не стільки в кількості технічних ресурсів, скільки в логіці взаємодії. Система, де міністерства, спецслужби, ІТ-спільнота, журналісти, освітяни та місцеві адміністрації працюють паралельно — рано чи пізно зазнає збою. Система, в якій ці гравці діють спільно, постійно обмінюючись даними, методами й баченням — створює реальну стійкість. Саме таку модель почала будувати Україна, і саме такий підхід сьогодні поступово впроваджують у країнах Балтії, Польщі, Чехії, Швеції.

Практика останніх років свідчить: будь-яка держава, що ігнорує цифровий фронт, стає вразливою. Не обов'язково бути у стані війни — достатньо мати відкриту політичну дискусію, вибори, чутливі теми — і це вже буде точкою входу. Тому сучасна європейська безпека будується не лише на танках і радарах, а на серверних центрах, механізмах моніторингу, цифровій гігієні, здатності розрізняти факт і маніпуляцію.

Досвід України — унікальний. Це приклад того, як країна, не маючи формальних гарантій безпеки від НАТО, без повноправного членства в ЄС, самостійно, за участі суспільства і фахової спільноти, побудувала систему, що витримала атаки безпрецедентного масштабу. Її елементи вже починають інтегруватися в європейські рішення — як зразок не «допомоги біднішому», а співпраці на рівних. Це співпраця тих, хто вже пройшов через гібридну агресію, з тими, хто до неї лише готується.

Цифрова і інформаційна безпека більше не є другорядним розділом стратегії — вона стає одним із її наріжних каменів. Коли війна ведеться через екрани, дані і наративи, саме ті, хто навчився захищатися мовою фактів, швидкістю реакції та чесною комунікацією — мають перевагу. І в цьому сенсі український досвід формує нову якість європейської безпеки.

3.4. Перспективи адаптації Європи до нових форм гібридних загроз

Упродовж останнього десятиліття стало зрозуміло: система європейської безпеки більше не може функціонувати у межах логіки, сформованої після Холодної війни. Той підхід, який передбачав, що загроза має чітке джерело, зафіксовану точку початку та завершення, більше не відповідає характеру сучасних викликів. Гібридні загрози порушують цю логіку. Вони починаються без офіційного сигналу, розгортаються паралельно в різних середовищах, часто залишаються невидимими до моменту, коли наслідки стають незворотними.

Європа вже не перебуває у фазі обговорення гібридної війни як гіпотетичного сценарію. Це реальність, із якою стикаються уряди, суспільства,

приватний сектор, освітні системи. Ситуації втручання у вибори, маніпуляції у медіа, спроби дестабілізації через цифрову інфраструктуру чи тиск на національні меншини — все це фіксується не у країнах «на кордоні», а в самісінькому центрі Європейського Союзу. Така динаміка вимагає не лише тактичної відповіді, а й довготривалої стратегії адаптації.

Перші кроки вже зроблено. Ідеться про зміну уявлень про межі між війною й миром, про формування законодавства, яке визнає дезінформацію не як свободу слова, а як інструмент підриву демократичних систем. Проте попереду значно складніше завдання — переосмислення архітектури самої європейської політики безпеки. Ця архітектура має бути здатною працювати не з одним джерелом загрози, а з множинними — часто паралельними, не завжди ідентифікованими, часом внутрішніми за формою.

Для того, щоб протистояти гібридним викликам, європейська система безпеки має вийти за рамки оборонних міністерств і силових структур. Це більше не сфера виключно військових або розвідників. Інформаційні атаки вимагають залучення фахівців з цифрових технологій, комунікацій, психології, соціології, освіти. Кібератаки — компетентного IT-сектора, бізнесу, технічної аналітики. Економічний тиск чи деструктивна дипломатія — синхронної роботи урядів, фінансових інституцій, міжнародних правників.

Усе це означає зміну уявлення про саме поняття «безпекова спроможність». Йдеться не лише про готовність реагувати, а про здатність вчасно розпізнати слабке місце, передбачити точку тиску, зафіксувати зміну у медіаповедінці чи соціальному тоні. І в цьому полягає головний виклик: адаптація передбачає не оборону як реакцію, а бачення наперед. Це означає, що держава має навчитися бачити середовище не в моменті, а в динаміці. Визначати не просто фейк, а його джерело, логіку розповсюдження, мету й цільову аудиторію.

Змінюється і розуміння стійкості. Сьогодні вона вже не зводиться до фізичної безпеки чи наявності ресурсів. Йдеться про інформаційну гігієну, цифрову автономність, прозору взаємодію між владою та суспільством. Там, де є

довіра, дезінформація не проростає. Там, де є навички перевірки інформації — вона не перетворюється на масову паніку. Там, де є незалежна журналістика — ворожа кампанія втрачає основу.

Саме тому, з-поміж технічних інструментів захисту, дедалі важливішими стають речі немеханічні: освіта, критичне мислення, комунікаційна культура. У країнах, які першими зіткнулися з гібридною агресією — як Литва, Естонія, Україна — ці сфери почали активно інтегрувати в безпекові стратегії. Медійна грамотність — більше не факультатив у школі, а компонент державної політики. Громадські ініціативи, що займаються фактчекінгом, отримують державне фінансування не як ЗМІ, а як частина системи безпеки. Це вже не журналістика — це превенція.

Коли європейські суспільства почали усвідомлювати, що об'єктами атак стають не лише уряди чи інфраструктура, а самі принципи відкритості, свободи слова, плюралізму — виникла необхідність шукати баланс між безпекою і демократичністю. Саме це сьогодні стає одним із найтонших місць у процесі адаптації до гібридних загроз: як захистити себе, не зруйнувавши при цьому те, що й становить суть європейського суспільного договору.

Рішення не може бути універсальним. У деяких країнах обирають модель жорсткого регулювання контенту, в інших — роблять ставку на саморегуляцію та освіту. Але загальна тенденція помітна: зростає роль незалежних медіа, фактчекінгових платформ, освітніх програм для журналістів, аналітиків, державних службовців. Це вже не про свободу висловлювань, це — про стійкість суспільства до маніпуляцій.

І тут український досвід знову набуває особливого значення. У ситуації, коли країна перебуває у стані повномасштабної війни, зберегти доступ до альтернативних думок, відкрите обговорення й комунікаційну прозорість — це не менш важливо, ніж захистити об'єкти критичної інфраструктури. Саме ці практики сьогодні вивчають і адаптують партнери з країн ЄС. Не для того, щоб копіювати, а щоб зрозуміти, як за умов надзвичайного тиску можливо не тільки не

скотитися в ізоляцію, а навпаки — зберегти орієнтацію на відкритість як інструмент сили.

Зміни мають відбуватись і на рівні інституційної логіки. Структури ЄС та НАТО, які традиційно були зорієнтовані на міждержавні ризики, поступово змінюються — у бік більш тісної співпраці з локальними урядами, громадянським сектором, освітніми середовищами. Центри, що вивчають гібридні загрози, сьогодні тісно взаємодіють з університетами, IT-інкубаторами, дослідницькими мережами. Це — не розширення бюрократії, а спроба підготувати інфраструктуру майбутнього: гнучку, чутливу, компетентну.

Досвід останніх років свідчить: адаптація до гібридних загроз — це не про побудову ще однієї фортифікації чи розширення повноважень окремого відомства. Йдеться про зміну самої логіки функціонування держави в умовах інформаційно-контрольованого середовища. Коли основним ресурсом стає довіра, ключовим інструментом — вчасна комунікація, а головною загрозою — не завжди зброя, а тиша, дезінформація чи технологічна несправність.

Показовим прикладом таких змін є стратегія цифрової стійкості, яку впроваджують Фінляндія, Естонія, Литва. Вона передбачає не лише технічне зміцнення інфраструктури, а й створення умов для того, щоб громадяни могли самостійно ідентифікувати загрози, приймати зважені рішення, не піддаватись тиску через соціальні мережі чи інформаційний шум. Усе це реалізується через системну медіаосвіту, довіру до державних ресурсів, прозорість процедур та обов’язковий обмін інформацією між секторами.

На рівні Європейського Союзу ці ініціативи починають набувати форми стратегічних документів. Прийнято «Digital Europe Programme», який фінансує розвиток нових інструментів у сфері цифрової безпеки, алгоритмів боротьби з дезінформацією, програм навчання для спеціалістів. З боку НАТО — постійне оновлення кібердоктрини, інтеграція досвіду партнерів, зокрема України, до навчальних програм і симуляцій криз. Це вже не декларації, а конкретна робота над архітектурою адаптації.

Питання майбутнього — не коли буде наступна атака, а чи встигне система її ідентифікувати до того, як вона досягне цілі. І тут немає універсального рецепту. Кожна країна має знайти свій баланс між контролем і свободою, між відкритістю й захищеністю. Але без розуміння, що світ змінився — а з ним і сам характер загроз — неможливо побудувати жодну ефективну модель. Гібридна агресія — це не епізод. Це нова норма, до якої не просто потрібно звикнути, а до якої варто підготуватись.

Український досвід стає в цьому сенсі не лише джерелом рішень, а точкою відліку. Країна, яка з 2014 року живе під постійним тиском багаторівневої агресії, вчить не як оборонятися, а як жити, розвиватися і змінюватися в умовах війни нового типу. Цей урок сьогодні поступово засвоює Європа — не теоретично, а практично. І, схоже, це вже не тенденція, а стратегія.

Висновки до розділу 3

Політика ЄС та НАТО щодо боротьби з гібридними загрозами зазнала змін після початку російсько-української війни, сприяючи розвитку нових механізмів реагування на такі загрози. Зокрема, ЄС посилив свої інструменти інформаційної безпеки та кіберзахисту, а НАТО — механізми колективної оборони в умовах гібридних атак. Однак європейські країни ще мають вирішити низку проблем, зокрема щодо інтеграції кіберзахисту в систему колективної оборони. Адаптація до гібридних загроз вимагає більшої політичної волі та співпраці між країнами-членами ЄС і НАТО. Важливою складовою є підвищення стійкості країн до нових форм агресії, а також розвиток механізмів обміну інформацією та колективної оборони.

ВИСНОВКИ

Проведене дослідження гібридних війн та їхнього впливу на сучасну геополітичну обстановку в Європі, зокрема на прикладі російсько-українського конфлікту, дозволило зробити кілька важливих висновків. Гібридна війна, як форма агресії, поєднує в собі військові, інформаційні, економічні, політичні та кібернетичні методи впливу, що значно ускладнює процес реагування на неї як з боку держав, так і міжнародних організацій. Російсько-українська війна, розпочата в 2014 році, стала яскравим прикладом застосування гібридної стратегії, де агресор використовує низку різноманітних інструментів для досягнення своїх геополітичних цілей без формального оголошення війни. Це створює серйозні проблеми для національних систем безпеки країн Європи, оскільки традиційні методи протистояння, що ґрунтуються на класичних формах військової агресії, не можуть забезпечити ефективний захист від новітніх загроз.

Досвід України в протидії гібридним загрозам є надзвичайно важливим для європейських країн, оскільки Україна, стикаючись із повномасштабною агресією з боку росії, змушена була розвивати нові підходи до забезпечення національної безпеки. Це включало створення спеціалізованих органів для боротьби з дезінформацією, розвиток кіберзахисту, а також зміцнення міжнародної кооперації, зокрема з країнами НАТО та ЄС. Однак, незважаючи на значні зусилля, протидія гібридним загрозам залишається складним і тривалим процесом, оскільки ефективна боротьба з такими загрозами потребує не лише технологічних інструментів, але й політичної волі, єдності між державами та готовності до швидкої адаптації до нових реалій. НАТО та Європейський Союз після початку війни в Україні змушені були переглянути свої стратегії безпеки, впроваджуючи нові політики щодо протидії гібридним загрозам. Це включало створення спільних механізмів для боротьби з інформаційними атаками, розвиток кіберзахисту, а також зміцнення енергетичної безпеки. Проте цей процес потребує додаткових зусиль з боку ЄС та НАТО для посилення інтеграції між військовими та

цивільними інструментами протидії, а також для вироблення чітких критеріїв і правових рамок, які дозволяють швидко і ефективно реагувати на гібридні загрози.

Необхідно зазначити, що для протидії гібридним загрозам важлива не лише військова, а й економічна, інформаційна та політична стабільність. Європейські країни мають значно посилити свої внутрішні механізми безпеки та розробити спільні політики для реагування на кібератаки, інформаційну пропаганду та інші форми невоєнного втручання. Окрім того, необхідно посилювати міжнародну співпрацю та підтримку країн, що перебувають під загрозою гібридних атак, таких як Україна, щоб забезпечити стабільність і безпеку в Європі в умовах нових викликів.

Отже, уроки, отримані з досвіду України, є важливими для всієї Європи. Вони вказують на необхідність гнучкості, здатності швидко адаптуватися до нових реалій і використовувати нові форми співпраці для протидії гібридним загрозам. Європейські країни повинні враховувати цей досвід у своєму підході до безпеки, що дозволить зберегти стабільність і мир на континенті, а також зміцнити єдність між державами-членами ЄС і НАТО.

Результати проведеного дослідження можуть бути застосовані не лише як частина теоретичного осмислення. Вони мають безпосередню практичну цінність — як для фахівців із безпеки, міжнародників, аналітиків, державних службовців, так і для викладачів та освітян. Зміст аналізованих підходів, структур, інструментів, моделей реагування може бути використаний у підготовці освітніх курсів з міжнародної безпеки, політичної географії, інформаційної гігієни, кібербезпеки. Український досвід, уособлений у прикладах цифрової мобілізації, інформаційної самозахисту, швидкої комунікації, може стати основою практичних модулів, воркшопів, тренінгів.

Крім того, матеріали цієї дипломної роботи можуть бути застосовані для розробки методичних підходів у середовищі шкіл і університетів — особливо у контексті формування критичного мислення у студентської молоді. Це особливо актуально у країнах, що межують із потенційно агресивними режимами або мають

високий рівень вразливості до інформаційного впливу. Також ці напрацювання можуть слугувати вихідною базою для оновлення програм безпекового навчання у системі підготовки публічних службовців — як на національному, так і регіональному рівнях.

Гібридна війна не завершується перемогою в бою чи завершенням військової кампанії. Вона триває в інформаційному середовищі, в соціальних мережах, у ставленні громадян до подій, у внутрішньому дискурсі, у роботі з травмами, у пам'яті про конфлікт. Саме тому її вивчення — не лише завдання аналітиків. Це — завдання освітян, журналістів, цифрових інженерів, медиків, істориків, громадських активістів. Робота над цією темою має не просто дослідницький характер, а безпосередню етичну відповідальність. Тільки через глибоке розуміння механізмів гібридної агресії, через здатність розпізнати її форми та наслідки можна будувати політику, яка не є реакцією, а є випередженням.

Підсумовуючи, можна сказати, що гібридні війни не тільки змінили правила міжнародної гри — вони змусили змінитися саме уявлення про безпеку. І ця зміна триває. Європа вже вийшла за межі теоретичних дискусій, Україна — вже давно поза фазою спостереження. І обидві сторони мають, чим поділитися одна з одною. Власне, ця робота — спроба зафіксувати цей діалог і надати йому структури, яку можна використовувати — в аналізі, у викладанні, в управлінні, в розумінні реальності, в якій ми всі живемо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Білічак О., Гуз А. Гібридна війна як інструмент зовнішньої політики російської федерації: український вимір (1991 – 2023). *Східноєвропейський історичний вісник*. 2024. № 30. С. 162–178. URL: https://doi.org/10.24919/2519-058x.30.299897 (дата звернення: 21.04.2025).
2. Білоусов М., Алєйник В. Російська гібридна війна: загрози і кібервиклики для європейської інформаційної безпеки. *Науковий журнал «Регіональні студії»*. 2023. № 33. С. 119–125.
3. Буряченко О. Гібридна війна як нова форма глобального протистояння. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2024. № 2(74). С. 24–31. URL: https://doi.org/10.32689/2523-4625-2024-2(74)-3 (дата звернення: 21.04.2025).
4. Габчак В. «Гібридна війна»: поняття та сутність. *Вісник Прикарпатського університету.Політологія / ДОСЛІДЖЕННЯ МОЛОДИХ НАУКОВЦІВ*. 2018. Т. 1, № 12. С. 257–260. URL: https://journals.pnu.edu.ua/index.php/politics/article/view/4246/4819.
5. Гетьманчук М. П. «Гібридна війна» росії проти україни: інформаційний аспект. *Військово-науковий вісник*. 2017. № 27. С. 296–307. URL: https://doi.org/10.33577/2313-5603.27.2017.296-307 (дата звернення: 21.04.2025).
6. Гібридна війна: in verbo et in praxi. : монографія / ред. Р. Додоова. Вінниця : Нілан-ЛТД, 2017. 412 с. URL: https://jmonographs.donnu.edu.ua/article/view/3781.

7. Гібридні війни. компоненти та особливості / Ю. Лиснецький та ін. *Публічне управління у сфері державної безпеки та охорони громадського порядку*. 2021. № 4. С. 63–70. URL: https://doi.org/10.32838/TNU-2663-6468/2021.5/11.
8. Глух М. В., Гончаренко М. В. Сутнісне розуміння та природа поняття «гібридна війна» в сучасній доктрині міжнародного права. *Ірпінський юридичний часопис*. 2024. № 1(14). С. 197–205. URL: https://doi.org/10.33244/2617-4154-1(14)-2024-197-205 (дата звернення: 21.04.2025).
9. Городинська Н., Майка М. Гібридна війна як форма глобального протистояння. м. Тернопіль, 18–19 квіт. 2024 р. Терпопілб, 2024. С. 68–70. URL: https://elartu.tntu.edu.ua/handle/lib/44776?utm_source=chatgpt.com.
10. Досвід країн Балтії щодо протидії агресії зі сторони Російської Федерації. *Аналітичний центр Борисфен Інтел*. URL: https://bintel.com.ua/uk/article/opyt-baltii (дата звернення: 21.04.2025).
11. Кол. авт. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навч. посіб. / ред. В. Жадько ; упоряд.: О. Харитоненко, Ю. Полтавець. Київ : НПУ ім. М. П. Драгоман., 2018. 356 с. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi72/0052980.pdf.
12. Магда Є. Гібридна війна: сутність та структура феномену. *Міжнародні відносини Серія "Політичні науки"*. 2014. № 4. URL: https://www.academia.edu/42584031/ГІБРИДНА_ВІЙНА_СУТНІСТЬ_ТА_СТРУКТУРА_ФЕНОМЕНУ?utm_source=chatgpt.com.
13. Світова гібридна війна: український фронт : монографія / ред. В. Горбулін. Київ : Нац. ін-т стратег. дослідж., 2017. 496 с.

URL: https://shron1.chtyvo.org.ua/Horbulin_Volodymyr/Svitova_hibrydna_viina_ukrainskyi_front.pdf?PHPSESSID=0oaa3afcv46ntvbcca4j1qcn84 .

14. Уздєнова Ю. Гібридна війна: сутність, складові та ключові поняття. *Вчені записки ТНУ імені В.І. Вернадського. Серія: публічне управління та адміністрування*. 2024. Т. 35(74), № 4. С. 172–179. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2024/4_2024/28.pdf.
15. Хмель А. Боротьба із гібридними загрозами в ЄС (за нормативно-правовою базою Європейського Союзу). *Acta de historia & politica: saeculum XXI*. 2022. № 03. С. 91–101. URL: https://doi.org/10.26693/ahpsxxi2021-2022.03.091 (дата звернення: 21.04.2025).
16. Цимбал І., Панченко С., Жовтун А. Інформаційна складова гібридної війни. *Науковий часопис НПУ імені М. П. драгоманова*. 2016. № 19. С. 185–189. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/27495/Tsymbal_Panchenko_Zhovtyn.pdf?sequence=1&isAllowed=y.
17. Що таке теорія "керованого хаосу" і як їй протидіяти? - рецепт від Сергія Дацюка. *Останні новини України та світу.- головні новини дня - UAinfo*. URL: https://uainfo.org/blognews/1438683712-shcho-take-teoriya-kerovanogo-haosu-i-yak-yiy-protidiyati---retsept.html (дата звернення: 21.04.2025).
18. Cordesman A. H. Chronology of possible russian gray area and hybrid warfare operations : report. 2020. 45 p. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200702_Burke_Chair_Russian_Chronology.pdf.

19. Countering hybrid threats. *NATO*. URL: https://www.nato.int/cps/en/natolive/topics_156338.htm (date of access: 21.04.2025).
20. Galeotti M. The mythical ‘Gerasimov Doctrine’ and the language of threat. *Critical studies on security*. 2018. Vol. 7, no. 2. P. 157–161. URL: https://doi.org/10.1080/21624887.2018.1441623 (date of access: 21.04.2025).
21. Russia's hybrid war in ukraine: breaking the enemy's ability to resist. Ulkopoliittinen Instituutti, 2015.