МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ
Кафедра політології та публічного управління

На правах рукопису

КАНЕВСЬКА ЛІЛІЯ ЮРІЇВНА

ГІБРИДНА ВІЙНА: ТЕОРЕТИЧНІ ОСНОВИ ТА ПРАКТИЧНІ ПРОЯВИ В СУЧАСНИХ КОНФЛІКТАХ

Спеціальність: 052 «Політологія»
Освітньо-професійна програма: «Політологія та державне управління»
Робота на здобуття освітнього ступеня «Бакалавр»

Науковий керівник:
КУЗЬМУК ОЛЬГА МИКОЛАЇВНА,
кандидат соціологічних наук,
доцент

РЕКОМЕНДОВАНО ДО ЗАХИСТУ
Протокол №
засідання кафедри політології та
публічного управління
від 2025 р.
Завідувач кафедри
проф. Бусленко В. В.

ЛУЦЬК – 2025

АНОТАЦІЯ

Каневська Лілія Юріївна. Гібридна війна: теоретичні основи та практичні прояви в сучасних конфліктах. – Кваліфікаційна наукова праця на правах рукопису.

Робота на здобуття освітнього ступеня «Бакалавр». Спеціальність: 052 «Політологія». Освітньо-професійна програма: «Політологія та державне управління». – Волинський національний університет імені Лесі Українки, Луцьк, 2025.

У **Вступі** розкрито актуальність обраної теми, визначено її мету і завдання, об’єкт і предмет дослідження, а також методологічну базу та наукову новизну отриманих результатів. Загальний обсяг роботи складає з 50 сторінок.

Метою бакалаврської роботи є комплексний аналіз теоретичних основ гібридної війни та особливості її практичного застосування в сучасних міжнародних конфліктах.

Об'єктом дослідження є сучасні міжнародні конфлікти та протистояння між державами.

Предметом дослідження виступають теоретичні основи та практичні прояви гібридної війни як особливої форми міжнародного конфлікту.

У *Розділі 1 «Теоретичні основи гібридної війни»* визначено поняття, основні компоненти та особливості гібридної війни, простежено історичний розвиток концепції, а також розкрито її місце в еволюції сучасних форм конфліктів.

У *Розділі 2 «Типологія гібридних конфліктів»* здійснено класифікацію гібридних конфліктів за різними критеріями, розглянуто приклади їх успішної та неуспішної реалізації, а також проаналізовано взаємодію традиційних і нетрадиційних методів ведення війни.

У Розділі 3 «Вплив гібридної війни на міжнародні відносини» проаналізовано трансформацію міждержавної взаємодії під впливом гібридних

загроз, окреслено основні безпекові виклики для держав та розглянуто роль міжнародних організацій у реагуванні на них.

У *Висновках* підсумовано результати дослідження, зроблено акценти на ключових ознаках гібридної війни, її загрозах для міжнародної безпеки та окреслено перспективи протидії цим викликам.

Ключові слова: гібридна війна, гібридні конфлікти, безпека, міжнародні відносини, інформаційна війна, стратегія, нетрадиційні методи, міжнародні організації, збройний конфлікт.

ЗМІСТ

Стор.

ВСТУП 5
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ГІБРИДНОЇ ВІЙНИ 7
1.1. Поняття гібридної війни: визначення та особливості 7
1.2. Основні компоненти гібридної війни 9
1.3. Історичний розвиток концепції гібридної війни 12
1.4. Гібридна війна в контексті нових форм конфліктів 17
РОЗДІЛ 2. ТИПОЛОГІЯ ГІБРИДНИХ КОНФЛІКТІВ 20
2.1. Класифікація гібридних війн: за учасниками, за інструментами, за географічним охопленням 20
2.2. Приклади успішних і неуспішних гібридних конфліктів 23
2.3. Взаємодія традиційних і нетрадиційних методів ведення війни 27
РОЗДІЛ 3. ВПЛИВ ГІБРИДНОЇ ВІЙНИ НА МІЖНАРОДНІ ВІДНОСИНИ 31
3.1. Взаємодія держав у контексті гібридних війн 31
3.2. Безпекові виклики та стратегічні наслідки для держав 35
3.3. Роль міжнародних організацій у протистоянні гібридним загрозам 40
ВИСНОВКИ 45
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 48

ВСТУП

Актуальність теми дослідження обумовлена тим, що в сучасному світі характер військових конфліктів суттєво змінився. Традиційні форми протистояння поступаються місцем більш складним і комплексним формам конфліктів, які отримали назву «гібридні війни». Ці конфлікти поєднують у собі військові та невійськові методи протистояння, використовують інформаційні, економічні, дипломатичні та інші інструменти впливу. Особливої актуальності дослідження гібридних війн набуває в контексті зростання міжнародної напруженості та появи нових форм протистояння між державами.

Мета дослідження полягає у комплексному аналізі теоретичних основ гібридної війни та особливостей її практичного застосування в сучасних міжнародних конфліктах.

Для досягнення поставленої мети визначено такі завдання дослідження:

- проаналізувати поняття та особливості гібридної війни;
- дослідити основні компоненти гібридної війни та їх взаємозв'язок;
- простежити історичний розвиток концепції гібридної війни;
- визначити типологію гібридних конфліктів;
- проаналізувати успішні та неуспішні приклади гібридних конфліктів;
- дослідити взаємодію традиційних і нетрадиційних методів ведення війни;
- розглянути вплив гібридних війн на міжнародні відносини;
- проаналізувати роль міжнародних організацій у протистоянні гібридним загрозам.

Об'єктом дослідження є сучасні міжнародні конфлікти та протистояння між державами.

Предметом дослідження виступають теоретичні основи та практичні прояви гібридної війни як особливої форми міжнародного конфлікту.

Методологічну основу дослідження складає комплекс загальнонаукових та спеціальних методів. Серед використаних методів: системний підхід (для аналізу гібридної війни як цілісного явища), історичний метод (при дослідженні

еволюції концепції гібридної війни), порівняльний аналіз (при вивченні різних типів гібридних конфліктів), структурно-функціональний аналіз (при дослідженні компонентів гібридної війни), case-study (при аналізі конкретних прикладів гібридних конфліктів).

Інформаційну базу дослідження становлять наукові праці вітчизняних та зарубіжних дослідників з проблематики гібридних війн, міжнародних конфліктів та безпеки, аналітичні матеріали міжнародних організацій, документи та звіти військових відомств різних країн, матеріали наукових конференцій та семінарів з питань гібридних загроз, публікації в спеціалізованих виданнях з військової справи та міжнародних відносин.

Практичне значення отриманих результатів полягає в можливості їх використання для розробки стратегій протидії гібридним загрозам, вдосконалення систем національної безпеки, а також у навчальному процесі при викладанні дисциплін, пов'язаних з міжнародною безпекою та сучасними конфліктами. Теоретичні узагальнення та практичні рекомендації, представлені в роботі, можуть бути корисними для фахівців у сфері національної безпеки, військових експертів, дипломатів та політичних аналітиків.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ГІБРИДНОЇ ВІЙНИ

1.1. Поняття гібридної війни: визначення та особливості

У сучасному світі війни стали набагато складнішими, ніж раніше. Гібридна війна - це особливий вид протистояння, де противники використовують не тільки звичайну військову силу, але й багато інших способів боротьби одночасно. Це як велика головоломка, де кожен елемент важливий і впливає на загальну картину. Наприклад, замість того, щоб просто воювати на полі бою, країна-агресор також намагається заплутати людей через інтернет, створює економічні проблеми для противника, поширює неправдиву інформацію та намагається посварити людей між собою [3] (рис. 1.1)

Рис. 1.1. Особливості гібридної війни

Головна особливість гібридної війни полягає в тому, що вона розмиває межі між війною і миром. Часто буває важко зрозуміти, чи знаходиться країна у стані війни, чи ні. Наприклад, якщо одна країна атакує комп'ютерні системи іншої країни або намагається вплинути на її економіку через різні обмеження - це вже можна вважати елементами гібридної війни, хоча формально війна може бути не оголошена. Це робить гібридну війну особливо небезпечною, адже противник може завдавати шкоди, залишаючись ніби в тіні.

У гібридній війні дуже важливу роль відіграє інформаційна складова. Країна-агресор часто намагається створити свою версію подій і переконати в ній якомога більше людей. Для цього використовуються соціальні мережі, телебачення, радіо та інші засоби масової інформації. Мета такої інформаційної атаки - заплутати людей, посіяти сумніви та недовіру, створити розкол у суспільстві. Це може бути навіть небезпечніше, ніж звичайні військові дії, адже такі інформаційні атаки можуть тривати роками і змінювати думки та переконання цілих поколінь [12].

Економічна складова гібридної війни теж відіграє важливу роль. Країна-агресор може використовувати різні економічні інструменти: від прямих санкцій до складних фінансових схем. Наприклад, можуть створюватися перешкоди для торгівлі, блокуватися важливі економічні проекти, здійснюватися тиск на бізнес. Метою є послаблення економіки противника, створення проблем для простих людей, щоб викликати невдоволення та протести.

Важливою особливістю гібридної війни є те, що вона часто ведеться не напряму, а через різних посередників. Це можуть бути підтримувані агресором групи всередині країни-жертви, різні організації, які діють в інтересах агресора, або навіть найманці. Така стратегія дозволяє країні-агресору заперечувати свою участь у конфлікті і уникати прямої відповідальності за свої дії.

У гібридній війні також активно використовуються новітні технології. Це можуть бути кібератаки на важливі об'єкти інфраструктури, втручання в роботу комп'ютерних систем, крадіжка важливої інформації. Технології дозволяють завдавати серйозної шкоди противнику, не перетинаючи фізично його кордонів.

Наприклад, одна успішна кібератака може паралізувати роботу важливих державних установ або навіть порушити електропостачання цілих регіонів.

Особливу увагу в гібридній війні приділяють впливу на свідомість людей. Агресор намагається змінити спосіб мислення населення країни-жертви, посіяти сумніви в правильності дій власного уряду, створити атмосферу недовіри та страху. Для цього використовуються різні психологічні прийоми, маніпуляції з інформацією, створення фальшивих новин та поширення чуток. Метою є послаблення волі до опору та створення сприятливих умов для досягнення цілей агресора [2].

Ще однією важливою особливістю гібридної війни є її довготривалий характер. На відміну від звичайної війни, яка має чіткий початок і кінець, гібридна війна може тривати роками або навіть десятиліттями. Вона може то загострюватися, то затихати, але постійно залишається присутньою у різних формах. Це вимагає від країни-жертви постійної готовності до протидії різним загрозам та великої витривалості.

Гібридна війна також характеризується тим, що вона ведеться одночасно на багатьох рівнях - від міжнародного до локального. На міжнародному рівні агресор може намагатися ізолювати країну-жертву, послабити її позиції у світовій спільноті, завадити отриманню допомоги від союзників. На локальному рівні можуть створюватися конфлікти між різними групами населення, розпалюватися протиріччя, підтримуватися радикальні рухи.

1.2. Основні компоненти гібридної війни

Гібридна війна є складним та багатовимірним явищем, що включає цілу низку взаємопов'язаних компонентів. Кожен з цих компонентів може діяти як самостійно, так і в поєднанні з іншими, створюючи потужний комплексний вплив на країну-жертву. На рисунку 1.2 представлено основні складові частини гібридної війни, які охоплюють військову, інформаційну, економічну, соціальну та інші сфери. Розуміння цих компонентів та особливостей їхньої взаємодії має

вирішальне значення для створення ефективної системи протидії гібридним загрозам. Глибокий аналіз кожної складової дозволяє краще усвідомити механізми дії гібридної війни та оцінити реальні масштаби небезпеки, яку вона становить для сучасних держав.

Рис. 1.2. Компоненти гібридної війни

Військова складова залишається однією з найважливіших частин гібридної війни, хоча вона може проявлятися не так явно, як у традиційних конфліктах. Вона включає використання регулярних військових підрозділів, але часто в замаскованому вигляді, без розпізнавальних знаків. Також можуть використовуватися різні воєнізовані групи, приватні військові компанії та місцеві збройні формування, які підтримуються країною-агресором. Важливою особливістю є те, що військові дії можуть вестися приховано, з уникненням відкритих масштабних зіткнень. Замість цього перевага надається невеликим операціям, діям спеціальних підрозділів та створенню постійної напруги на певних територіях [14].

Інформаційна складова є чи не найпотужнішим інструментом у гібридній війні. Вона охоплює широкий спектр дій, спрямованих на формування потрібної агресору громадської думки та підрив довіри до влади у країні-жертві. Сюди входить поширення неправдивої інформації через засоби масової інформації та соціальні мережі, створення фальшивих новин, які важко відрізнити від правдивих, маніпулювання історичними фактами та створення альтернативних версій подій. Важливим елементом є також робота з різними групами населення через соціальні мережі, форуми та месенджери, де поширюються потрібні агресору наративи та створюються групи підтримки його позиції [9].

Економічна складова гібридної війни спрямована на підрив економічної стабільності країни-жертви. Вона може включати різні форми економічного тиску: від прямих торговельних обмежень до складних фінансових операцій, спрямованих на дестабілізацію національної валюти чи банківської системи. Агресор може використовувати свій контроль над важливими ресурсами (наприклад, енергоносіями) як інструмент тиску, створювати перешкоди для міжнародної торгівлі, намагатися ізолювати країну-жертву від світових ринків. Також можуть застосовуватися методи економічного саботажу через підконтрольні компанії та створення штучних економічних проблем.

Кібернетична складова стає все більш важливою у сучасній гібридній війні. Вона включає різноманітні атаки на комп'ютерні системи та мережі країни-жертви, спроби отримати доступ до секретної інформації, порушення роботи важливих інфраструктурних об'єктів через кібератаки. Особливу небезпеку становлять атаки на системи управління критичною інфраструктурою - електростанціями, водопостачанням, транспортними системами. Також важливим елементом є збір розвідувальної інформації через кіберпростір та створення можливостей для майбутніх атак [15].

Соціально-психологічна складова спрямована на розкол суспільства та створення атмосфери недовіри і страху. Агресор намагається використати існуючі в суспільстві протиріччя - соціальні, етнічні, релігійні, мовні - для створення конфліктів між різними групами населення. Важливим елементом є

підтримка радикальних рухів та організацій, які можуть дестабілізувати ситуацію зсередини. Також застосовуються методи психологічного тиску через поширення чуток, створення атмосфери невпевненості у майбутньому, підрив довіри до державних інституті [7].

Дипломатична складова гібридної війни передбачає дії на міжнародній арені, спрямовані на ізоляцію країни-жертви та послаблення її позицій у світовій спільноті. Це може включати створення негативного іміджу країни на міжнародній арені, блокування її ініціатив у міжнародних організаціях, перешкоджання отриманню міжнародної допомоги та підтримки. Агресор також може намагатися створити коаліції держав, які підтримують його позицію, або принаймні залишаються нейтральними у конфлікті.

Культурно-ідеологічна складова спрямована на підрив національної ідентичності та системи цінностей країни-жертви. Це може відбуватися через нав'язування альтернативних версій історії, применшення значення національної культури та традицій, просування ідей про штучність державності чи культурної самобутності країни-жертви. Важливим елементом є також спроби впливу на освітню систему, культурні установи та засоби формування суспільної свідомості [20].

Організаційна складова гібридної війни включає створення та підтримку різноманітних структур, які діють в інтересах агресора на території країни-жертви. Це можуть бути громадські організації, політичні рухи, аналітичні центри, засоби масової інформації, які формально є незалежними, але фактично працюють на просування інтересів агресора. Важливим елементом є також створення мереж впливу через підкуп чи шантаж представників влади, бізнесу та громадських діячів.

1.3. Історичний розвиток концепції гібридної війни

Гібридна війна як особливий вид протистояння має глибоке історичне коріння, хоча сам термін з'явився відносно нещодавно. На рисунку 1.3

відображено основні історичні етапи розвитку та становлення концепції гібридної війни. Цей еволюційний шлях охоплює період від стародавніх часів, коли військові стратеги вже розуміли важливість поєднання різних методів ведення війни, до сучасної епохи, де гібридна війна набула нових форм завдяки технологічному прогресу та глобалізації. Кожен історичний період додавав нові елементи до розуміння гібридної війни, збагачував її методи та інструменти. Особливо важливим є простеження того, як традиційні методи ведення війни поступово доповнювалися новими формами протистояння - економічними, інформаційними, психологічними, що врешті сформувало сучасне розуміння гібридної війни як комплексного явища [10].

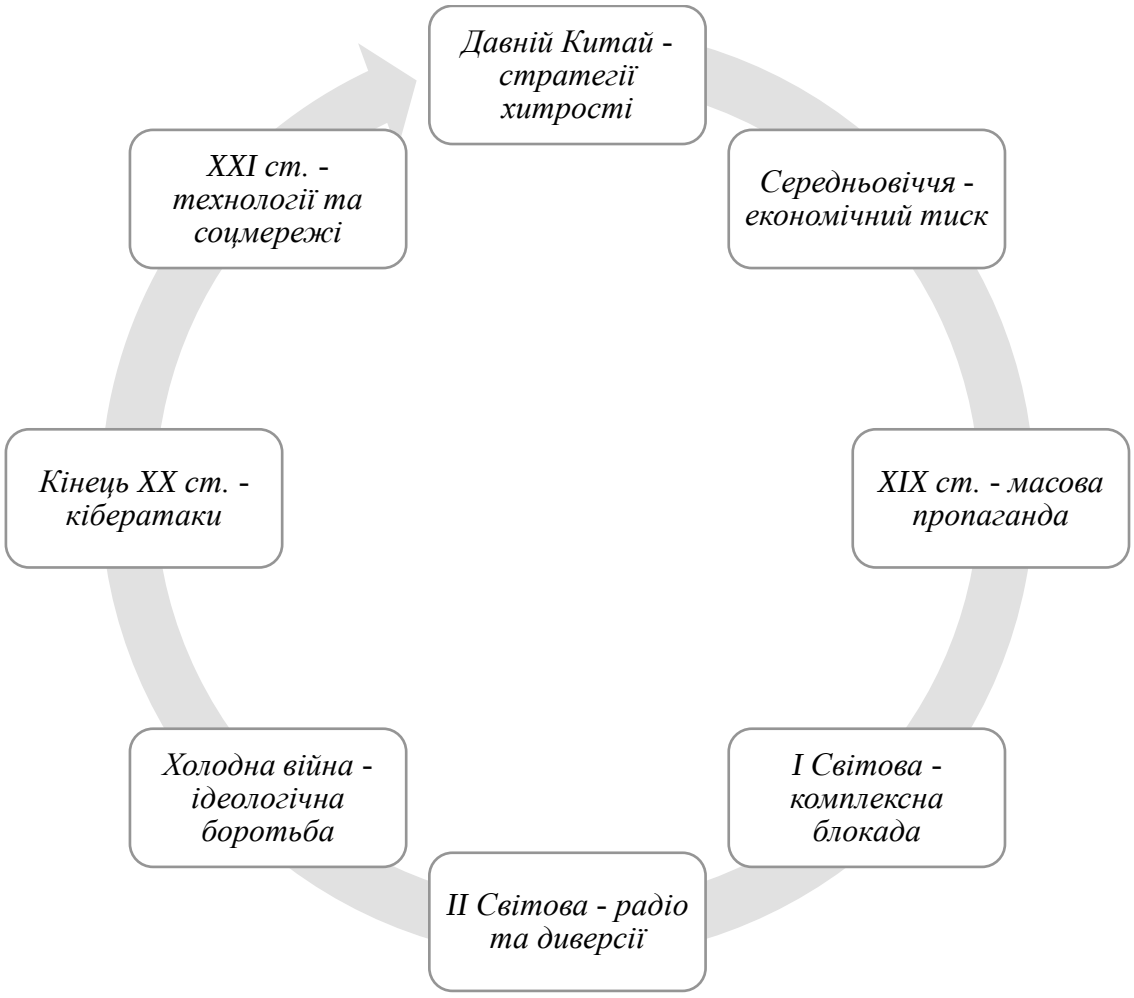

Рис. 1.3. Історичний розвиток гібридної війни

Хоча сам термін «гібридна війна» з'явився відносно нещодавно, методи, які ми зараз називаємо гібридними, використовувалися ще в давні часи. У

стародавньому Китаї, наприклад, відомий військовий стратег Сунь-Цзи вже писав про важливість використання не лише військової сили, але й хитрості, дезінформації та психологічного впливу на противника. Він наголошував, що найкраща перемога - це та, якої можна досягти без прямого бойового зіткнення. Ці ідеї можна вважати першими кроками до розуміння того, що ми сьогодні називаємо гібридною війною [19].

У середні віки методи ведення війни стали ще більш різноманітними. Правителі активно використовували економічний тиск, релігійні протиріччя та династичні зв'язки для досягнення своїх цілей. Наприклад, венеціанські купці могли блокувати торгові шляхи своїх конкурентів, що часто було ефективнішим за військові дії. Також широко застосовувалися методи підриву влади противника зсередини через підкуп знаті, поширення чуток та створення внутрішніх конфліктів. Ці методи можна вважати ранніми формами економічної та інформаційної складових гібридної війни [4].

Період після Французької революції та війн Наполеона показав світу нову важливу істину про війни. Раніше генерали думали лише про солдатів, гармати та фортеці, але тепер стало зрозуміло, що думки та настрої звичайних людей можуть змінити весь хід війни. Влада різних країн почала приділяти велику увагу тому, що думають прості громадяни про війну та політику. Вони зрозуміли, що якщо люди підтримують війну - армія буде сильнішою, а якщо не підтримують - навіть найкраща армія може програти. Тому почали активно використовувати газети та листівки, щоб впливати на думки людей. У газетах писали про перемоги своєї армії та про слабкість ворога, розповідали історії про героїв та зрадників. Листівки розкидали на території противника, щоб посіяти сумніви та страх серед його населення. Це був перший раз в історії, коли інформація та пропаганда стали такою ж важливою зброєю, як гармати та багнети. Так почався новий етап у веденні війн, де боротьба за думки людей стала не менш важливою, ніж бої на полях битв.

Перша світова війна відкрила нову сторінку у способах ведення війни, коли країни почали воювати не тільки зброєю, але й всіма можливими методами

впливу. Окрім звичайних боїв з використанням гвинтівок та гармат, держави почали перекривати одна одній торговельні шляхи, блокувати порти кораблями, щоб ворог не міг отримувати важливі товари та продовольство. Вони створили спеціальні відділи, які займалися збором секретної інформації про промисловість та військові плани противника. Через газети та нове на той час радіо поширювали новини та історії, які мали переконати людей у правильності війни або змусити їх сумніватися у своїй владі. Особливо цікавим був новий підхід до роботи з національними меншинами - країни намагалися переконати різні народи, які жили на території ворога, повстати проти своєї держави. Всі ці нові методи виявилися дуже дієвими, і після війни їх продовжили вдосконалювати та розвивати, що згодом привело до появи того, що ми зараз називаємо гібридною війною [21].

Друга світова війна значно розширила арсенал методів ведення війни, вийшовши далеко за межі звичайних бойових дій. Радіо стало потужним інструментом впливу - тепер країни могли напряму говорити з населенням ворога, передаючи свої повідомлення прямо в їхні домівки, незважаючи на заборони влади. Війна велась не тільки на фронті, але й в економіці - країни намагалися зруйнувати промисловість одна одної, перекривали торгові шляхи, заморожували банківські рахунки. На території ворога діяли спеціальні групи, які влаштовували диверсії - підривали мости, залізниці, заводи. Важливу роль відігравали партизани та підпільні організації, які створювали постійні проблеми в тилу ворога - атакували невеликі групи солдатів, знищували склади з припасами, збирали важливу інформацію. Всі ці методи разом створювали величезний тиск на країну-противника, змушуючи її витрачати ресурси не тільки на армію, але й на боротьбу з внутрішніми проблемами та захист своєї економіки.

Період холодної війни між США та СРСР став справжньою лабораторією для розвитку нових методів протистояння без прямого військового зіткнення. Хоча ці дві наддержави майже не воювали напряму, вони постійно змагалися за вплив у світі всіма можливими способами. Вони використовували економічні санкції, забороняючи торгівлю важливими товарами та технологіями, щоб

послабити одна одну. Через радіо, газети та телебачення вони вели постійну інформаційну боротьбу, намагаючись довести перевагу свого способу життя - капіталізму чи комунізму. Обидві країни витрачали величезні кошти на створення нової зброї, постійно намагаючись перевершити одна одну. В різних країнах світу вони таємно підтримували різні політичні групи та повстанців, які могли допомогти поширити їхній вплив. Також вони створили величезні шпигунські мережі для збору секретної інформації. Всі ці методи, розроблені під час холодної війни, стали основою для сучасних гібридних конфліктів, де країни намагаються досягти своїх цілей, не починаючи відкритої війни [17].

Кінець XX століття повністю змінив методи ведення гібридної війни завдяки новим технологіям та глобалізації. Поява телебачення, а потім і інтернету дала країнам можливість миттєво поширювати інформацію на весь світ. Якщо раніше для впливу на думки людей потрібні були роки, то тепер це можна зробити за кілька днів через соціальні мережі та новинні сайти. Світова економіка стала настільки взаємопов'язаною, що економічні санкції почали діяти набагато сильніше - якщо великі країни відмовляються торгувати з кимось або забороняють використовувати свою банківську систему, це може серйозно нашкодити економіці цілої держави. З'явилася можливість атакувати важливі системи противника через інтернет - зламувати електростанції, транспортні системи, банки, лікарні. Всі ці нові інструменти об'єдналися в сучасне розуміння гібридної війни, де перемагає не той, хто має більше танків, а той, хто може ефективніше використовувати всі доступні методи впливу - від економічних санкцій до кібератак [13].

На початку XXI століття концепція гібридної війни остаточно оформилася як цілісна теорія. Досвід різних конфліктів показав, що успіху можна досягти лише при комплексному використанні різних методів впливу: військових, економічних, інформаційних, кібернетичних та інших. Особливо важливим стало розуміння ролі інформаційного простору та соціальних мереж у сучасних конфліктах. Саме вони часто стають головним полем битви в гібридній війні.

Сучасний етап розвитку концепції гібридної війни характеризується все більшим зростанням ролі технологічних факторів. Штучний інтелект, великі дані, соціальні мережі та інші сучасні технології створюють нові можливості для ведення гібридної війни. При цьому важливо розуміти, що технології не замінюють традиційні методи, а доповнюють їх, створюючи нові комбінації та можливості для впливу на противника.

1.4. Гібридна війна в контексті нових форм конфліктів

У сучасному світі конфлікти стали набагато складнішими та багатовимірнішими, ніж раніше. Гібридна війна є частиною цієї нової реальності, де межі між різними формами протистояння стають все більш розмитими. На відміну від традиційних війн, де все було досить зрозуміло - є два противники, які відкрито воюють між собою, сучасні конфлікти часто відбуваються у "сірій зоні", де важко визначити, хто є справжнім агресором, і навіть чи відбувається війна взагалі. Гібридна війна особливо добре вписується в цю картину, оскільки вона дозволяє вести активні ворожі дії, при цьому формально не перетинаючи межу відкритої війни.

У контексті нових форм конфліктів гібридна війна тісно пов'язана з поняттям "війни нового покоління". Ці конфлікти характеризуються тим, що в них використовується весь спектр можливих засобів впливу на противника - від традиційної військової сили до найсучасніших інформаційних технологій. При цьому важливою особливістю є те, що різні методи впливу використовуються не послідовно, а одночасно, створюючи складний комплексний тиск на противника. Наприклад, економічні санкції можуть поєднуватися з кібератаками, інформаційними кампаніями та діями спеціальних підрозділів, причому все це відбувається одночасно і за єдиним планом [6].

Особливе місце в сучасних конфліктах займає інформаційне протистояння, яке часто стає головним полем битви. У цьому контексті гібридна війна виявляється особливо ефективною, оскільки вона дозволяє створювати та

поширювати різні версії реальності, маніпулювати громадською думкою та впливати на прийняття рішень противником. Сучасні технології, особливо соціальні мережі та інтернет-медіа, надають для цього небачені раніше можливості. За допомогою правильно організованої інформаційної кампанії можна досягти цілей, які раніше вимагали би застосування значної військової сили.

Важливою особливістю сучасних конфліктів є те, що вони часто відбуваються в міському середовищі та серед цивільного населення. Гібридна війна добре пристосована і до цих умов, оскільки вона дозволяє вести бойові дії "малої інтенсивності", використовувати цивільну інфраструктуру та залучати місцеве населення до конфлікту. При цьому агресор може заперечувати свою причетність до подій, списуючи все на внутрішні протиріччя та громадянський конфлікт [14].

У сучасних конфліктах все більшу роль відіграють недержавні учасники - приватні військові компанії, терористичні організації, кримінальні угруповання, громадські рухи. Гібридна війна активно використовує цих учасників, часто перетворюючи їх на інструменти досягнення своїх цілей. Це дозволяє країні-агресору діяти через посередників, уникаючи прямої відповідальності за свої дії та створюючи видимість "природного" розвитку подій.

Економічна складова сучасних конфліктів також набуває нових форм. В умовах глобалізованої економіки фінансові інструменти, торговельні обмеження та економічні санкції можуть бути не менш ефективними, ніж військова сила. Гібридна війна вміло поєднує економічний тиск з іншими формами впливу, створюючи комплексні проблеми для противника. При цьому економічні заходи можуть бути спрямовані не тільки проти держави в цілому, але і проти окремих галузей, компаній або навіть конкретних осіб.

Технологічний розвиток створює нові можливості для ведення конфліктів. Кібератаки, використання штучного інтелекту, безпілотних систем та інших новітніх технологій стають важливою частиною сучасного протистояння. Гібридна війна активно включає ці елементи у свій арсенал, створюючи нові

комбінації традиційних та високотехнологічних методів впливу. При цьому важливо розуміти, що технології не просто додаються до старих методів, а створюють принципово нові можливості для ведення конфлікту.

Особливістю сучасних конфліктів є також те, що вони часто ведуться не за територію чи ресурси, а за вплив на свідомість людей, за право формувати їхнє світосприйняття та цінності. У цьому контексті гібридна війна виявляється особливо ефективною, оскільки вона дозволяє впливати на різні аспекти життя суспільства - від політичних переконань до культурних орієнтирів. При цьому такий вплив може бути досить тривалим і мати наслідки, які будуть відчуватися протягом багатьох років.

Важливою рисою сучасних конфліктів є їхній асиметричний характер, коли противники мають різні можливості та використовують різні методи боротьби. Гібридна війна добре підходить для таких умов, оскільки дозволяє слабшій стороні ефективно протистояти сильнішому противнику, використовуючи його вразливі місця та уникаючи прямого зіткнення. При цьому сильніша сторона може опинитися в складній ситуації, оскільки її традиційні переваги можуть виявитися неефективними проти гібридних методів ведення війни [3].

РОЗДІЛ 2. ТИПОЛОГІЯ ГІБРИДНИХ КОНФЛІКТІВ

2.1. Класифікація гібридних війн: за учасниками, за інструментами, за географічним охопленням

Гібридні війни - це складне явище, яке може проявлятися по-різному, тому для кращого розуміння їх потрібно класифікувати за певними ознаками. Це як велика головоломка, де кожен елемент має своє місце. Розуміння цих різних типів допомагає краще підготуватися до можливих загроз та розробити ефективні методи захисту. Це особливо важливо в сучасному світі, де гібридні війни стають все більш поширеним явищем (рис. 2.1).

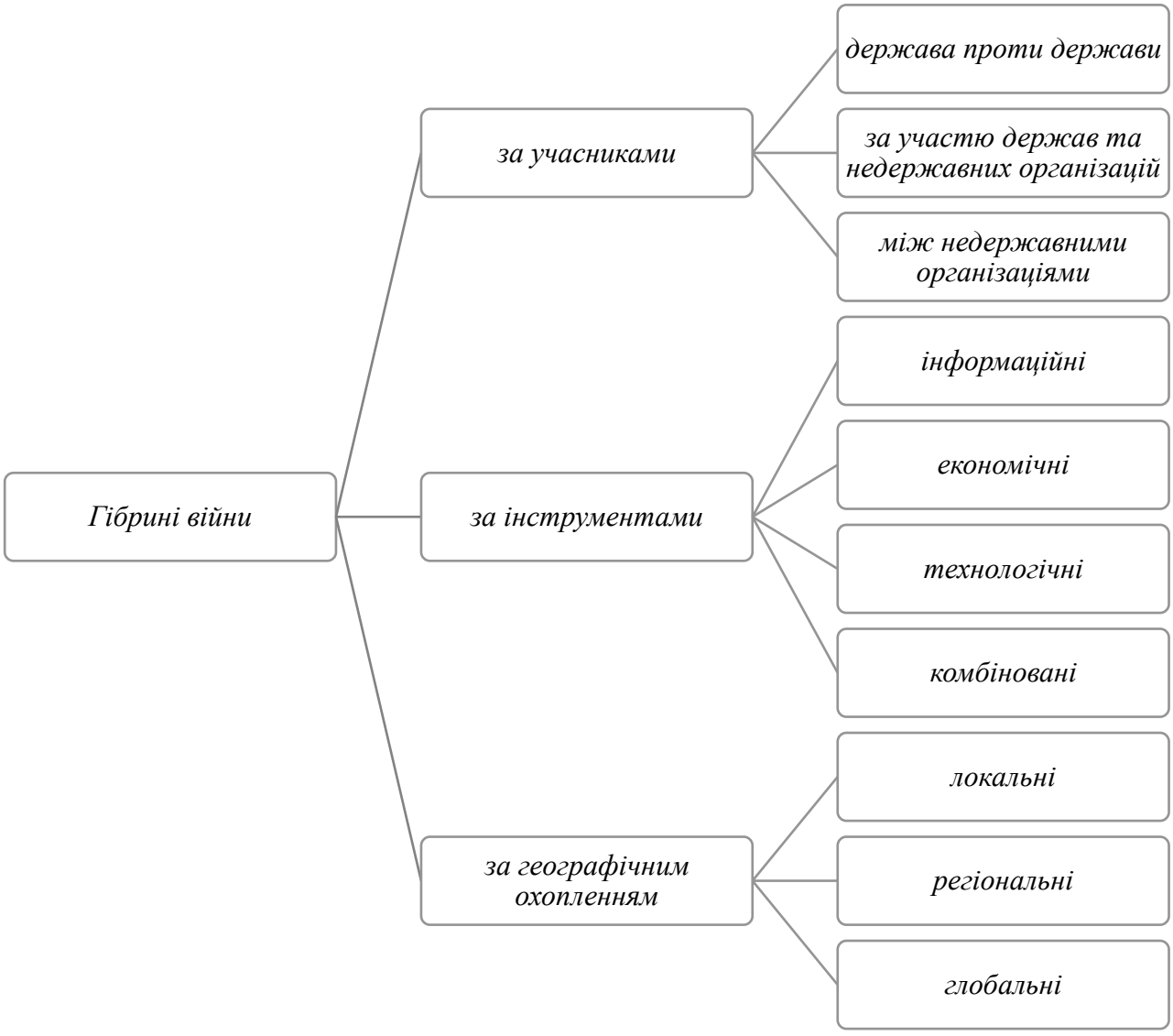

Рис. 2.1. Класифікація гібридних війн

За учасниками гібридні війни можна поділити на кілька основних типів. Перший тип - це коли одна держава веде гібридну війну проти іншої держави. В такому випадку країна-агресор використовує різні способи тиску: і економічний, і інформаційний, і військовий. Наприклад, вона може накладати торгові обмеження, поширювати неправдиву інформацію через інтернет та телебачення, а також підтримувати різні збройні групи на території противника. Другий тип - це коли в гібридній війні беруть участь не тільки держави, але й різні організації, компанії чи навіть окремі впливові особи. Такі конфлікти часто стають дуже заплутаними, бо буває важко зрозуміти, хто насправді стоїть за тими чи іншими діями. Також є випадки, коли гібридну війну ведуть недержавні організації - наприклад, великі міжнародні злочинні угруповання чи терористичні організації, які мають достатньо ресурсів для такої діяльності [9].

Якщо говорити про інструменти ведення гібридної війни, то тут теж можна виділити кілька основних груп. До першої належать війни, де головним інструментом є інформаційний вплив. У таких конфліктах основна боротьба відбувається в інтернеті, соціальних мережах та засобах масової інформації. Агресор намагається змінити думку людей, посіяти недовіру до влади, створити розкол у суспільстві. Для цього використовуються фейкові новини, маніпуляції з інформацією, створення груп у соціальних мережах, які поширюють потрібні агресору ідеї. Друга група - це конфлікти, де головну роль відіграє економічний тиск. Тут використовуються різні економічні обмеження, блокування торгівлі, створення проблем для бізнесу, спроби обвалити національну валюту. Мета такої війни – створити економічні проблеми в країні, щоб викликати невдоволення населення і тим самим досягти своїх цілей.

Є також гібридні війни, де основний акцент робиться на технологічній складовій. В таких конфліктах активно використовуються кібератаки на важливі об'єкти інфраструктури, втручання в роботу комп'ютерних систем, крадіжка важливої інформації. Особливо небезпечними є атаки на системи управління електростанціями, водопостачанням, транспортом. Одна успішна кібератака може паралізувати роботу цілого міста чи навіть регіону. Ще один тип - це

гібридні війни, де поєднуються військові дії з іншими методами впливу. В таких конфліктах можуть діяти невеликі збройні групи, які створюють постійну напругу, але при цьому активно використовуються й інші методи – від економічного тиску до інформаційних атак.

За географічним охопленням гібридні війни теж можна розділити на кілька типів. Локальні конфлікти відбуваються на відносно невеликій території, часто в межах одного регіону. Але навіть такі локальні конфлікти можуть мати серйозний вплив на ситуацію в цілій країні. Регіональні гібридні війни охоплюють територію кількох країн або цілого регіону. В таких конфліктах часто переплітаються інтереси різних держав, що робить їх особливо складними для вирішення. Глобальні гібридні війни - це конфлікти, які впливають на ситуацію в багатьох країнах світу. Такі війни часто пов'язані з протистоянням великих держав або боротьбою за вплив у важливих регіонах світу.

Важливо розуміти, що в реальності більшість гібридних війн не можна чітко віднести до якогось одного типу. Не можна просто сказати: «Це тільки інформаційна війна» або «Це лише економічний тиск». Насправді все набагато складніше - як у грі, де правила постійно змінюються. Наприклад, спочатку конфлікт може бути схожий на маленьку пожежу в одному місці, але потім він раптом поширюється на сусідні території, як вогонь у сухому лісі. Або спершу країна-агресор може тільки поширювати фейкові новини та пропаганду, а потім раптом починає використовувати економічний тиск, кібератаки чи навіть військові дії. Саме ця здатність змінюватися і пристосовуватися робить гібридні війни такими небезпечними - це як боротися з тінню, яка постійно змінює форму. Коли ви думаєте, що знайшли спосіб захиститися від одного виду атаки, противник вже використовує інший підхід, і вам доводиться придумувати нові методи захисту [20].

Окремо варто звернути увагу на те, як сучасні технології змінили обличчя гібридних війн, перетворивши їх на щось схоже на комп'ютерну гру, але з реальними наслідками. Сьогодні, щоб атакувати іншу країну, не потрібно відправляти танки чи літаки – достатньо мати команду хакерів та медіа-фахівців

із комп'ютерами та доступом до інтернету. Через Facebook, Instagram чи TikTok можна запускати фейкові новини, які швидко поширюються по всьому світу, як вірус. За допомогою сучасних банківських технологій можна створювати проблеми в економіці іншої країни, просто натискаючи кнопки на клавіатурі – це як перекривати воду в крані, але тільки з грошима. Найцікавіше те, що всі ці атаки можна проводити сидячи в офісі за тисячі кілометрів від цілі, ніби граючи в стратегічну відеогру. Саме тому багато країн обирають такий спосіб ведення війни – він дешевший за звичайну війну, менш ризикований, але при цьому може бути дуже ефективним. Це як боксер, який перемагає не силою ударів, а спритністю та розумною тактикою [18].

Розуміння різних типів гібридних війн має величезне значення для створення надійної системи захисту держави. Коли країна чітко розуміє всі можливі способи атаки – через інформаційний простір, економічні важелі, кібератаки чи інші методи – вона може розробити справді ефективні методи протидії. У сучасному світі гібридні війни стають все більш поширеним явищем, і кількість країн, які використовують такі методи, постійно зростає. Тому кожна держава повинна бути готова одночасно захищатися від різних типів загроз: від атак на критичну інфраструктуру, від поширення дезінформації, від економічного тиску та інших методів впливу. Лише глибоке розуміння всіх можливих видів загроз дозволяє створити комплексну систему захисту, яка зможе вчасно виявляти та нейтралізувати спроби гібридного втручання. В умовах сучасних міжнародних відносин це стає критично важливим для збереження національної безпеки будь-якої країни [12].

2.2. Приклади успішних і неуспішних гібридних конфліктів

Щоб краще зрозуміти, як працюють гібридні війни, варто подивитися на реальні приклади таких конфліктів з історії. Це як вивчати історії хвороб у медицині - на конкретних випадках легше побачити, що працює, а що ні. В різні часи країни використовували різні підходи до гібридної війни - деякі досягли

своїх цілей, інші зазнали невдачі. Цікаво, що один і той самий конфлікт може вважатися успішним з точки зору однієї сторони і провальним - з точки зору іншої. Все залежить від того, які цілі ставила перед собою кожна сторона. Наприклад, якщо країна хотіла просто послабити противника - це одне, а якщо прагнула повністю його підкорити - зовсім інше. Аналіз таких прикладів допомагає зрозуміти, які фактори найбільше впливають на результат гібридної війни і як краще протистояти таким загрозам (табл. 2.1).

Таблиця 2.1

Приклади гібридних конфліктів

Конфлікт	Статус	Методи	Результат
Наполеонівські війни	Успішний	Військові дії + політична пропаганда + економічний тиск + поширення ідей революції	Значний вплив на Європу, довготривалі реформи залишились
Холодна війна (США-СРСР)	Змішаний	Економічна допомога + культурний вплив + підтримка політичних рухів + перевороти	Часткові успіхи обох сторін, завершення через економічне виснаження СРСР
Італія Муссоліні	Неуспішний	Військова сила + пропаганда + економічний тиск	Повна невдача через переоцінку можливостей та погану координацію
Іран на Близькому Сході	Успішний	Підтримка політичних груп + інформаційна політика + економічна співпраця + культурний вплив	Значне розширення впливу в регіоні попри санкції

Одним із класичних прикладів успішної гібридної війни можна вважати дії Наполеона під час його європейських кампаній. Він вміло поєднував військові дії з політичною пропагандою та економічним тиском. Наполеон не просто завойовував території - він створював складну систему впливу, яка включала поширення ідей Французької революції, встановлення нових законів та адміністративних систем, зміну економічних відносин. Важливу роль відігравала його пропаганда, яка представляла французьку армію як визволительку народів Європи від старих монархічних режимів. Це допомагало знаходити підтримку серед місцевого населення та створювати лояльні до Франції уряди на завойованих територіях. Успіх цієї стратегії був настільки значним, що навіть

після поразки Наполеона багато його реформ та ідей залишилися в європейських країнах.

Цікавим прикладом гібридної війни, яка мала змішані результати, можна вважати холодну війну між США та СРСР. З одного боку, обидві сторони досягли певних успіхів у просуванні своїх інтересів та ідеологій у різних частинах світу. Вони використовували широкий спектр інструментів: від економічної допомоги та культурного впливу до підтримки різних політичних рухів та навіть організації переворотів. США успішно створили мережу союзників та військових баз по всьому світу, розвинули потужну систему міжнародної торгівлі та фінансів. СРСР, у свою чергу, зміг поширити свій вплив на значну частину світу, створивши систему соціалістичних держав та рухів. Проте в кінцевому підсумку жодна зі сторін не змогла досягти повної перемоги традиційними військовими засобами, і конфлікт завершився через економічне виснаження однієї зі сторін [17].

Прикладом неуспішної гібридної війни можна вважати спроби Італії під керівництвом Муссоліні створити нову Римську імперію. Незважаючи на використання різних інструментів впливу – від військової сили до пропаганди та економічного тиску - Італія не змогла досягти своїх цілей. Причиною цього була недооцінка супротивників, переоцінка власних можливостей та невміння ефективно координувати різні елементи гібридної війни. Пропаганда виявилася неефективною, економічні ресурси були обмеженими, а військові дії часто були невдалими. Це показує, що просто використання різних інструментів гібридної війни не гарантує успіху - важливо вміти правильно їх поєднувати та враховувати реальні можливості та обмеження.

У більш недавній історії можна побачити, як Іран майстерно веде гібридну війну на Близькому Сході, щоб збільшити свій вплив у регіоні. Замість того, щоб відкрито воювати з сильнішими країнами, Іран діє хитріше - як досвідчений гравець у шахи, який не робить прямих атак, а поступово посилює свої позиції на дошці. Вони підтримують різні групи в сусідніх країнах, надаючи їм гроші, зброю та навчання - це як мати своїх представників у кожній важливій точці

регіону. Водночас Іран активно працює над своїм іміджем через засоби масової інформації, розвиває торгівлю з сусідами та поширює свою культуру – музику, фільми, традиції. Це схоже на те, як велика компанія розширює свій бізнес: не захоплюючи конкурентів силою, а створюючи мережу партнерів та прихильників. І хоча інші країни намагаються стримувати Іран через санкції та інші обмеження, така розумна стратегія дозволяє їм успішно збільшувати свій вплив у регіоні, ніби вода, що знаходить щілини навіть у найміцнішій греблі.

Важливо також розглянути приклади гібридних конфліктів, які відбуваються в інформаційному просторі. Показовим є приклад інформаційного протистояння навколо виборів у різних країнах, де активно використовуються соціальні мережі, фейкові новини та інші інструменти впливу на громадську думку. Успішність таких кампаній часто залежить від готовності суспільства протистояти інформаційним маніпуляціям та від наявності ефективних систем захисту інформаційного простору. У деяких випадках такі кампанії досягали своїх цілей, суттєво впливаючи на результати виборів, в інших – зустрічали ефективну протидію та зазнавали невдачі [15].

Аналізуючи ці приклади гібридних конфліктів, можна зрозуміти головні складові успіху в такій війні. Найперше – це вміння правильно оцінити свої можливості, як у грі в шахи, де потрібно знати силу кожної своєї фігури. Важливо розуміти, які ресурси є в наявності: скільки людей, техніки, грошей можна використати. Також треба добре вивчити слабкі місця противника – це як знайти тріщини в стіні замку. При цьому всі елементи війни – військові операції, інформаційні атаки, економічний тиск – мають працювати разом, як добре налагоджений механізм годинника, де кожна шестерня крутиться в потрібному напрямку.

Аналізуючи далі, бачимо, що успіх залежить від здатності швидко змінювати свою стратегію, коли ситуація цього вимагає. Це як вода, яка завжди знаходить новий шлях, коли старий заблоковано. Не можна триматися за план, який вже не працює – треба вміти придумувати нові рішення. І дуже важливо розуміти, як на конфлікт реагують інші країни світу. Їхня позиція може сильно

вплинути на результат, як реакція глядачів та суддів у спортивному матчі. Тому перемога в гібридній війні залежить від вміння бачити повну картину, враховувати всі фактори і швидко реагувати на зміни, ніби досвідчений диригент, який керує складним оркестром.

Досвід різних гібридних конфліктів також показує, що успіх часто залежить від здатності створити ефективну комбінацію різних інструментів впливу. Наприклад, економічний тиск стає більш ефективним, якщо він супроводжується правильно організованою інформаційною кампанією. А військові дії можуть дати кращий результат, якщо вони підкріплені дипломатичними зусиллями та роботою з місцевим населенням. При цьому важливо розуміти, що копіювання успішних стратегій з інших конфліктів не гарантує успіху – кожна ситуація унікальна і вимагає власного підходу.

2.3. Взаємодія традиційних і нетрадиційних методів ведення війни

У сучасних війнах успіх залежить від того, наскільки вміло країна може поєднувати старі та нові методи ведення бою. Це як у кулінарії - традиційні рецепти можна покращити новими інгредієнтами, але базові принципи приготування залишаються важливими. З одного боку, класичні військові методи (як танки, артилерія, піхота) нікуди не зникли і залишаються важливою частиною будь-якого конфлікту. З іншого - з'явилося багато нових способів вести війну: кібератаки, інформаційні операції в соціальних мережах, економічний тиск. Найбільшого успіху досягають ті, хто вміє «змішувати» ці підходи - наприклад, поєднувати військову операцію з потужною інформаційною кампанією в інтернеті або координувати кібератаки з традиційними військовими діями. Це робить сучасні конфлікти набагато складнішими, але й відкриває нові можливості для тих, хто вміє грамотно використовувати всі доступні інструменти (табл. 2.2).

Таблиця 2.2

Методи ведення сучасної війни та їх взаємодія

Категорія	Приклади	Характеристики	Роль у конфлікті
Традиційні методи	Звичайні збройні сили, військова техніка, класичні операції	Прямі військові дії з використанням армії та техніки	Забезпечують реальну військову силу та можливість прямого впливу
Нетрадиційні методи	Інформаційні операції, кібератаки, економічний тиск, соціальні мережі	Приховані, часто не сприймаються як військові дії	Створюють умови для успіху традиційних методів, послаблюють противника
Технологічні елементи	Дрони, системи зв'язку, комп'ютерні системи управління	Поєднують традиційні та нетрадиційні методи	Підвищують ефективність обох типів методів, створюють нові можливості
Взаємодія методів	Інформаційні кампанії + військові дії, кібератаки + традиційні операції	Комплексний вплив, взаємне підсилення методів	Створює синергетичний ефект, підвищує загальну ефективність

Традиційні методи ведення війни включають у себе використання звичайних збройних сил, військової техніки, проведення класичних військових операцій. Це все те, що люди зазвичай уявляють, коли думають про війну: танки, літаки, артилерія, піхота. Такі методи залишаються важливими, адже в кінцевому підсумку саме можливість застосувати військову силу часто стає вирішальним фактором у конфлікті. Проте у сучасному світі традиційні військові дії рідко використовуються самі по собі – зазвичай вони є частиною більш складної стратегії, де військова сила поєднується з іншими методами впливу. Наприклад, військові операції можуть проводитися одночасно з потужною інформаційною кампанією, яка формує потрібне сприйняття цих дій у суспільстві [14].

Нетрадиційні методи ведення війни стають все більш різноманітними та впливовими. До них належать інформаційні операції, кібератаки, економічний тиск, використання соціальних мереж для впливу на громадську думку, створення підставних організацій та рухів, які діють в інтересах агресора. Особливістю цих методів є те, що вони часто не сприймаються суспільством як

військові дії. Наприклад, якщо країна стає жертвою потужної кібератаки, яка паралізує роботу важливих об'єктів інфраструктури, багатьом людям може бути складно зрозуміти, що це насправді є актом війни. Так само, коли через соціальні мережі поширюється неправдива інформація, яка має на меті посварити різні групи населення, це може здаватися просто частиною звичайних інформаційних процесів, а не елементом військової стратегії.

Взаємодія традиційних і нетрадиційних методів може відбуватися по-різному. Іноді нетрадиційні методи використовуються для підготовки до традиційних військових дій. Наприклад, перед початком військової операції може проводитися потужна інформаційна кампанія, яка має на меті дезорієнтувати противника та послабити його здатність до опору. Також можуть проводитися кібератаки на системи управління та зв'язку, щоб ускладнити координацію дій противника. В інших випадках традиційні військові дії можуть використовуватися як прикриття для застосування нетрадиційних методів. Наприклад, загроза військового вторгнення може використовуватися для посилення економічного та політичного тиску на країну [20].

Особливу роль у взаємодії різних методів ведення війни відіграють сучасні технології. Вони дозволяють створювати нові комбінації традиційних і нетрадиційних методів, підвищуючи їхню ефективність. Наприклад, використання дронів та інших безпілотних систем дозволяє проводити військові операції з мінімальним ризиком для власних сил, а сучасні системи зв'язку та управління дозволяють краще координувати різні елементи гібридної війни. При цьому важливо розуміти, що технології можуть як допомагати, так і створювати нові вразливості. Наприклад, залежність від складних комп'ютерних систем робить військові сили більш ефективними, але одночасно створює ризик того, що ці системи можуть бути атаковані противником.

Важливим аспектом взаємодії традиційних і нетрадиційних методів є їхній вплив на суспільство. Традиційні військові дії зазвичай викликають чітку реакцію – люди розуміють, що відбувається війна, і відповідно реагують. Натомість нетрадиційні методи можуть діяти приховано, поступово змінюючи

думки та настрої людей, не викликаючи явного спротиву. Це робить такі методи особливо небезпечними, адже суспільство може не помічати, що стає об'єктом ворожого впливу. Тому дуже важливо розуміти, як різні методи ведення війни взаємодіють між собою та як вони впливають на суспільство.

Цікавим аспектом взаємодії різних методів ведення війни є те, як вони можуть підсилювати або послаблювати один одного. Наприклад, успішні військові дії можуть зробити більш ефективною інформаційну кампанію, створюючи враження непереможності та змушуючи людей повірити в пропаганду агресора. З іншого боку, невдалі спроби використання традиційної військової сили можуть звести нанівець усі зусилля в інформаційній та економічній сферах. Тому дуже важливо правильно оцінювати, які методи і в якій послідовності краще використовувати в конкретній ситуації [6].

У сучасних конфліктах все частіше можна спостерігати, як традиційні та нетрадиційні методи ведення війни переплітаються настільки тісно, що їх стає важко розділити. Наприклад, сучасна військова операція може включати в себе одночасно і класичні бойові дії, і кібератаки, і інформаційні операції, і економічний тиск. При цьому всі ці елементи працюють як єдиний механізм, підсилюючи один одного та створюючи комплексний вплив на противника. Це вимагає нового підходу до планування та проведення військових операцій, де потрібно враховувати всі можливі способи впливу та їхню взаємодію.

РОЗДІЛ 3. ВПЛИВ ГІБРИДНОЇ ВІЙНИ НА МІЖНАРОДНІ ВІДНОСИНИ

3.1. Взаємодія держав у контексті гібридних війн

Світ міжнародних відносин став набагато складнішим через появу гібридних війн. Якщо раніше все було просто і зрозуміло - країни або відкрито воювали, або мирно спілкувалися через дипломатів, то зараз ситуація змінилася докорінно. Уявіть собі дві країни, які публічно потискають одна одній руки, підписують угоди про співпрацю та говорять про дружбу, але за лаштунками одна з них проводить кібератаки на важливі об'єкти іншої, поширює дезінформацію в соціальних мережах або таємно підтримує групи, які створюють проблеми для свого «партнера». Це як гра в шахи, де частина фігур схована під столом - ніколи не знаєш, який насправді наступний хід зробить твій суперник. Така прихована ворожість робить міжнародні відносини дуже непередбачуваними і змушує країни бути постійно напоготові, навіть коли все здається мирним і спокійним (табл. 3.1).

Таблиця 3.1

Взаємодія держав у контексті гібридних війн

Аспект взаємодії	Характеристика
Характер відносин	Непрозорі та складні відносини між державами, де офіційна дружба може поєднуватися з прихованою ворожістю
Механізми співпраці	Традиційні механізми часто неефективні, потреба в нових форматах співробітництва для протидії гібридним загрозам
Роль малих держав	Зростання впливу малих та середніх країн завдяки новим технологіям та методам ведення гібридної війни
Економічний фактор	Складне балансування між економічною співпрацею та протистоянням в умовах гібридної війни
Коаліції та союзи	Потреба у формуванні нових, більш гнучких форматів міжнародних союзів для протидії гібридним загрозам
Технологічний вплив	Постійна необхідність адаптації до нових технологій та створення механізмів контролю їх військового використання

У контексті гібридних війн відносини між державами стали дуже непрозорими. Часто буває важко зрозуміти, хто насправді є другом, а хто –

противником. Наприклад, одна країна може публічно заявляти про дружбу та співпрацю з іншою, але при цьому таємно підтримувати групи, які створюють проблеми для цієї країни, або проводити кібератаки на її важливі об'єкти. Така подвійна гра робить міжнародні відносини дуже складними та непередбачуваними. Країнам стає все важче довіряти одна одній, бо вони ніколи не можуть бути впевнені в справжніх намірах своїх партнерів.

Особливо цікаво спостерігати, як змінюються традиційні механізми міжнародної співпраці в умовах гібридних війн. Міжнародні організації, договори та угоди часто виявляються неефективними, бо вони були створені для регулювання традиційних конфліктів. Наприклад, якщо одна країна проводить потужну інформаційну кампанію проти іншої через соціальні мережі, дуже складно довести, що це саме державна політика, а не просто активність звичайних користувачів інтернету. Так само складно притягнути країну до відповідальності за кібератаки, бо часто неможливо однозначно довести, хто стоїть за цими атаками.

В умовах гібридних війн держави змушені створювати нові форми співпраці та захисту своїх інтересів. Наприклад, країни починають об'єднуватися для спільної протидії інформаційним атакам, створюють системи раннього виявлення та попередження про кібератаки, розробляють спільні правила поведінки в інформаційному просторі. Також з'являються нові формати міжнародної співпраці, спрямовані на протидію гібридним загрозам. Це можуть бути спільні центри вивчення та аналізу гібридних загроз, програми обміну досвідом та інформацією, спільні навчання з протидії різним видам гібридних атак [9].

Цікавим аспектом взаємодії держав у контексті гібридних війн є те, як змінюється роль малих та середніх країн. Якщо в минулому такі країни переважно виступали пасивними об'єктами міжнародної політики, що проводилася великими державами, то в умовах гібридного протистояння ситуація докорінно змінилася. Завдяки стрімкому розвитку інформаційних технологій, кіберзброї та інших інструментів гібридної війни, навіть відносно

невеликі держави отримали можливість ефективно протистояти значно потужнішим супротивникам. Наприклад, невелика країна з розвиненим IT-сектором може успішно проводити кібероперації проти критичної інфраструктури великої держави або здійснювати масштабні інформаційні кампанії, що впливають на суспільну думку та політичні процеси в країні-супротивнику. Така зміна балансу можливостей змусила великі держави переглянути своє ставлення до менших країн - тепер вони змушені враховувати їхні інтереси та позиції не через формальну ввічливість, а через реальну здатність цих країн впливати на міжнародну ситуацію. Це призвело до формування більш складної та багаторівневої системи міжнародної взаємодії, де навіть невеликі держави можуть відігравати важливу стратегічну роль [3].

Важливу роль у взаємодії держав відіграє економічний фактор. Сучасні економічні взаємозв'язки між країнами характеризуються високим рівнем взаємозалежності, що створює парадоксальну ситуацію: держави, які перебувають у стані гібридного протистояння, часто змушені підтримувати економічні відносини через неможливість швидкого розриву усталених торговельних та фінансових зв'язків. Наприклад, країни можуть обмінюватися кібератаками та вести інформаційну війну, але при цьому продовжувати торгівлю стратегічними товарами або підтримувати спільні інвестиційні проекти. Така дуальність вимагає від урядів надзвичайно виваженого підходу до управління міжнародними відносинами, де необхідно постійно балансувати між забезпеченням національної безпеки та збереженням економічних вигод від міжнародної співпраці. Це призводить до формування складних механізмів взаємодії, які дозволяють поєднувати елементи конфронтації та кооперації.

Особливої уваги заслуговує питання формування коаліцій та союзів в умовах гібридних війн. Класичні військові союзи, що історично формувалися для протидії конвенційним загрозам, демонструють обмежену ефективність у протистоянні комплексним гібридним атакам, які можуть включати кібернетичні, інформаційні та економічні компоненти. Це спонукає держави до пошуку інноваційних форматів міжнародної співпраці, що виходять за межі

традиційних військових договорів. Нові коаліційні структури повинні характеризуватися високою адаптивністю та можливістю швидкого реагування на різноманітні гібридні загрози. Наприклад, сучасні альянси все частіше включають компоненти кібербезпеки, спільні центри протидії дезінформації та механізми економічної взаємодопомоги. Така багатовимірність союзницьких відносин вимагає створення більш гнучких організаційних структур, здатних ефективно координувати дії партнерів у різних сферах протистояння гібридним загрозам.

Взаємодія держав у контексті гібридних війн також сильно залежить від розвитку технологій. Стрімкий розвиток інноваційних технологій, таких як штучний інтелект, квантові обчислення чи системи автономної зброї, здатний кардинально змінювати співвідношення сил між державами у короткі терміни. Це створює ситуацію постійної технологічної гонки, де країни змушені не лише інвестувати значні ресурси в розвиток власного технологічного потенціалу, але й розробляти ефективні системи захисту від новітніх загроз. Особливої актуальності набуває питання міжнародного регулювання використання передових технологій у військових цілях, оскільки неконтрольоване застосування таких інновацій може призвести до непередбачуваних наслідків у глобальному масштабі. Це спонукає міжнародну спільноту до створення нових механізмів контролю та регулювання, які б забезпечували баланс між технологічним прогресом та підтриманням міжнародної безпеки в умовах гібридного протистояння [21].

Все це робить сучасні міжнародні відносини дуже складними та непередбачуваними. Держави опинилися в ситуації, де необхідно одночасно враховувати множинні аспекти взаємодії: від традиційної дипломатії та економічної співпраці до протидії кіберзагрозам та інформаційним атакам. Ця багатовимірність створює необхідність постійного балансування між різноманітними національними інтересами та міжнародними зобов'язаннями. Класичні дипломатичні інструменти та механізми врегулювання конфліктів, які ефективно працювали в минулому, часто виявляються неадекватними для

вирішення сучасних гібридних викликів. Це спонукає міжнародну спільноту до пошуку інноваційних підходів у вирішенні конфліктів та розбудови нової архітектури міжнародної безпеки, яка б враховувала комплексний характер сучасних загроз та забезпечувала ефективні механізми протидії гібридним викликам у глобальному масштабі.

3.2. Безпекові виклики та стратегічні наслідки для держав

Сучасні держави стикаються з новими серйозними викликами через гібридні війни, і старі методи захисту вже не справляються з ними так ефективно. Це як замок зі старими замками - раніше він надійно захищав від злодіїв, але тепер з'явилися хакери, які можуть проникнути всередину через комп'ютерну мережу. Традиційна армія та охорона кордонів вже не гарантують повної безпеки, бо загрози приходять з несподіваних напрямків: через інтернет, соціальні мережі, економічний тиск чи підривну діяльність усередині країни. Вороги можуть атакувати банківську систему, поширювати фейкові новини, щоб посварити людей між собою, або влаштовувати кібератаки на електростанції та водопостачання. Тому держави мають захищати не тільки свої кордони, але й інформаційний простір, економіку, критичну інфраструктуру та навіть свідомість своїх громадян від ворожого впливу (рис. 3.1).

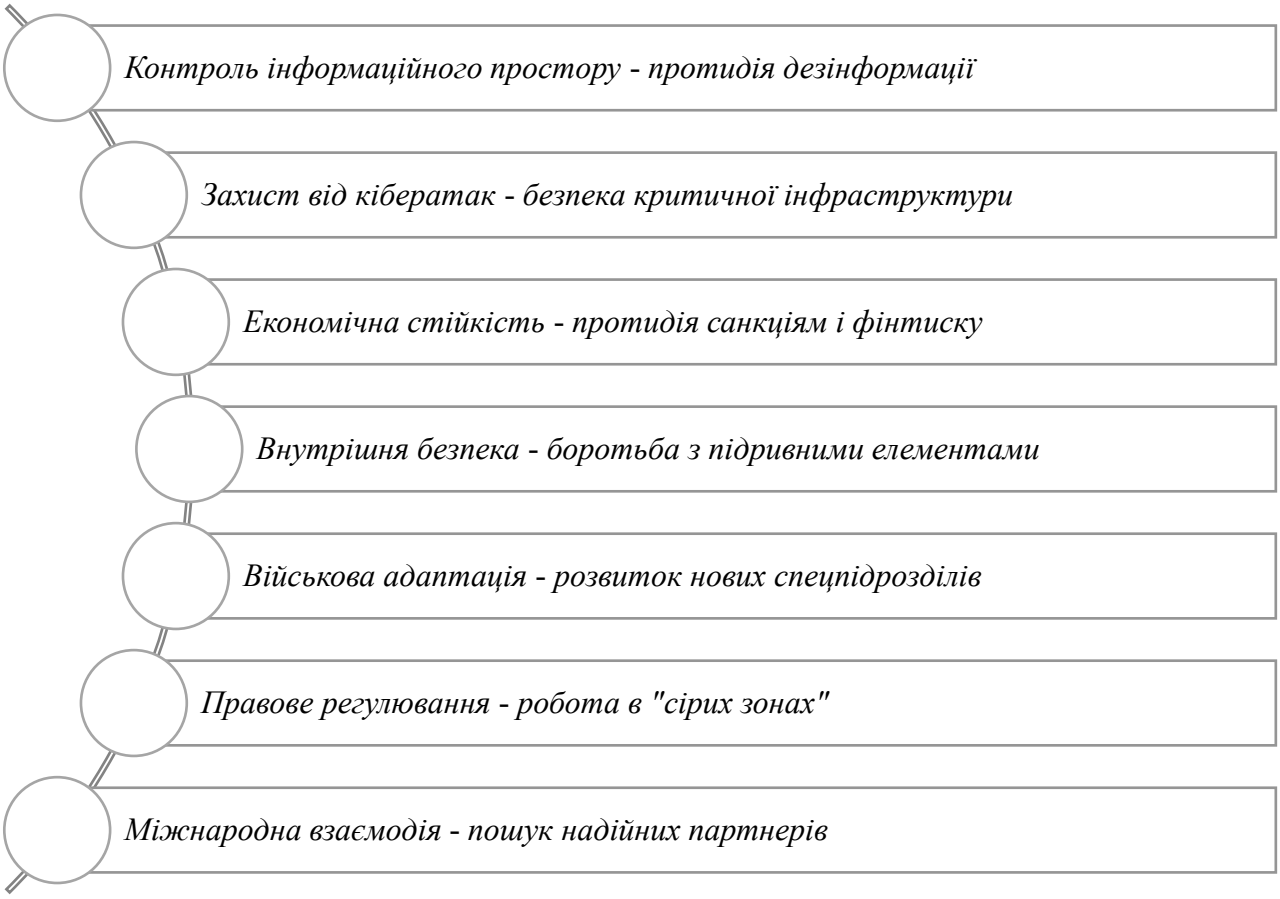

Рис. 3.1. Ключові безпекові виклики гібридні війни для сучасних держав

Один з головних безпекових викликів полягає в тому, що державам стає все складніше захищати свій інформаційний простір. Раніше достатньо було контролювати традиційні засоби масової інформації та основні канали комунікації. Зараз, з розвитком інтернету та соціальних мереж, інформація може поширюватися безліччю різних шляхів, і повністю контролювати цей процес практично неможливо. Це створює серйозні проблеми для безпеки держави, адже через інформаційний простір можуть поширюватися ідеї, які підривають довіру до влади, створюють розкол у суспільстві, викликають паніку або провокують конфлікти між різними групами населення. При цьому дуже складно визначити, хто стоїть за такими інформаційними атаками і як їм ефективно протидіяти [15].

Не менш серйозним викликом є захист критичної інфраструктури від кібератак. Сучасні держави сильно залежать від різних комп'ютерних систем, які

керують електростанціями, водопостачанням, транспортом, фінансовими установами. Якщо ці системи виходять з ладу через кібератаку, це може паралізувати життя цілого міста або навіть країни. Особливо небезпечним є те, що такі атаки можуть проводитися з будь-якої точки світу, і часто дуже складно визначити, хто за ними стоїть. Це змушує держави витрачати величезні ресурси на кібербезпеку та створювати спеціальні підрозділи для захисту від кібератак.

Економічна безпека також стає серйозним викликом в умовах гібридних війн. Противник може використовувати різні методи економічного тиску: від прямих санкцій до складних фінансових операцій, спрямованих на підрив економічної стабільності. Наприклад, може проводитися атака на національну валюту, створюватися перешкоди для міжнародної торгівлі, блокуватися доступ до важливих ресурсів. Особливо вразливими є країни з відкритою економікою, які сильно залежать від міжнародної торгівлі та інвестицій. Для них навіть відносно невеликий економічний тиск може мати серйозні наслідки [14].

В умовах гібридних війн виникають нові виклики для внутрішньої безпеки держави. Противник може підтримувати різні радикальні групи, створювати підставні організації, які діють в його інтересах, використовувати корупцію та кримінальні структури для досягнення своїх цілей. При цьому дуже складно довести зв'язок між такими діями та конкретною державою-агресором. Це змушує правоохоронні органи та спецслужби розробляти нові методи роботи, вчитися виявляти та протидіяти таким прихованим загрозам.

Стратегічні наслідки гібридних війн для держав можуть бути дуже серйозними (рис. 3.2).

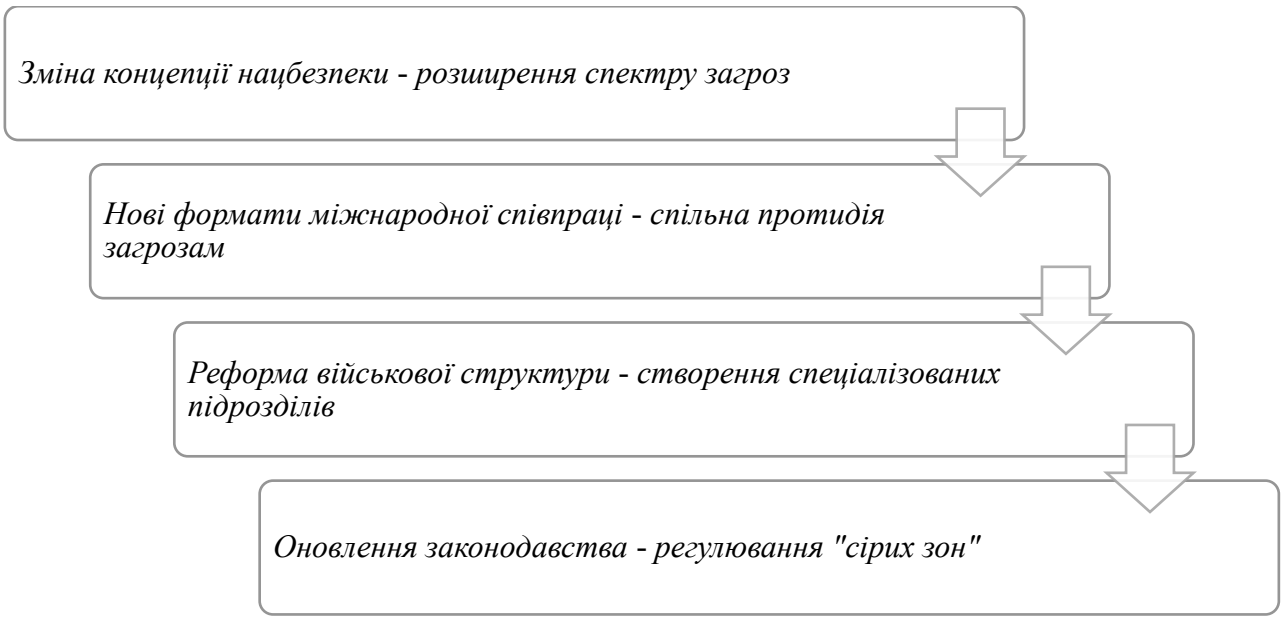

Рис. 3.2. Стратегічні наслідки гібридних війн

По-перше, змінюється сама концепція національної безпеки. Раніше держави в основному дбали про те, щоб захистити свої кордони від ворожих армій - будували укріплення, тримали армію напоготові та охороняли важливі об'єкти. Але зараз світ сильно змінився, і загрози стали набагато різноманітнішими. Тепер країнам потрібно захищатися не тільки від танків та літаків, але й від хакерських атак на важливі комп'ютерні системи, від фейкових новин та пропаганди в інтернеті, від економічного тиску та спроб посварити людей між собою. Це як замість одних міцних вхідних дверей тепер потрібно захищати цілий будинок - і вікна, і дах, і підвал, і навіть комп'ютерну мережу всередині. Для цього держави створюють нові служби безпеки, наймають спеціалістів з кібербезпеки, вчаться виявляти дезінформацію та захищають свою економіку. Все це коштує багато грошей і вимагає постійно вчитися новим методам захисту, бо загрози весь час змінюються та стають складнішими [21].

Важливим стратегічним наслідком є зміна підходів до міжнародної співпраці. Держави розуміють, що боротися з новими загрозами поодинці дуже важко, майже неможливо. Це як намагатися самому захистити величезний будинок - просто не вистачить очей і рук. Тому країни почали більше співпрацювати між собою: діляться важливою інформацією про нові небезпеки,

розповідають одна одній про свій досвід боротьби з хакерами чи фейками, створюють спільні системи, які можуть завчасно попередити про можливі атаки чи загрози. Але тут є один важливий момент - потрібно бути дуже обережними у виборі партнерів для такої співпраці. Адже не всі країни чесні у своїх намірах - деякі можуть прикидатися друзями, а потім використати отриману інформацію для власної вигоди або навіть нашкодити. Це як ділитися секретами з новим знайомим - ніколи не знаєш напевно, чи можна йому повністю довіряти [12].

Сучасні війни змінилися настільки, що вже недостатньо мати просто потужну армію з танками та літаками. Це як мати тільки міцні кулаки для бійки, коли противник використовує і отруту, і хитрощі, і навіть може атакувати через комп'ютер. Тому країни створюють нові спеціальні підрозділи: одні захищають від хакерів та кібератак, інші борються з ворожою пропагандою та фейками в інтернеті, треті слідкують за економічними загрозами та спробами підірвати фінансову систему країни. Але тут виникає нова складність - всі ці різні підрозділи повинні працювати разом, як злагоджений механізм. Це як оркестр, де кожен музикант грає свою партію, але всі мають грати в одному ритмі та слухати один одного. Якщо військові, кіберфахівці та інформаційники не будуть добре координувати свої дії, то захист країни не буде ефективним, навіть якщо кожен окремий підрозділ працює добре.

Ще одним важливим наслідком є необхідність постійного вдосконалення законодавства та адміністративних процедур. У світі гібридних війн постійно виникають ситуації, де незрозуміло, як діяти за законом. Наприклад: хтось у соціальних мережах активно поширює інформацію, яка сварить людей між собою - це просто чиясь думка чи вже напад на країну? Або інша ситуація: для захисту від кібератак спецслужбам потрібно перевіряти підозрілі повідомлення в інтернеті, але як це зробити, не порушуючи право людей на приватність? Це як балансувати на канаті - з одного боку треба захистити країну від нових загроз, а з іншого - не можна перетворити її на поліцейську державу, де за кожним стежать. Тому урядам доводиться постійно оновлювати закони, придумувати нові правила та процедури, які б дозволяли ефективно боротися із загрозами, але

при цьому не порушували основні права і свободи звичайних громадян. Це складна робота, яка вимагає участі і юристів, і експертів з безпеки, і захисників прав людини.

3.3. Роль міжнародних організацій у протистоянні гібридним загрозам

Міжнародні організації, такі як ООН, НАТО чи ЄС, відіграють ключову роль у боротьбі з сучасними гібридними загрозами - це як пожежна служба світового масштабу, яка координує дії всіх пожежних команд під час великої пожежі. Вони створюють майданчики, де країни можуть об'єднувати свої зусилля, ділитися досвідом та разом розробляти методи захисту від нових загроз. Наприклад, якщо одна країна зіткнулася з потужною кібератакою, вона може поділитися інформацією через міжнародні організації, щоб інші країни могли краще підготуватися до подібних атак. При цьому самі організації постійно адаптуються до нових викликів - якщо раніше вони більше займалися традиційними військовими загрозами, то тепер створюють спеціальні підрозділи для боротьби з кібератаками, дезінформацією та іншими сучасними загрозами. Це безперервний процес навчання та вдосконалення, адже нові загрози з'являються постійно (рис. 3.3).

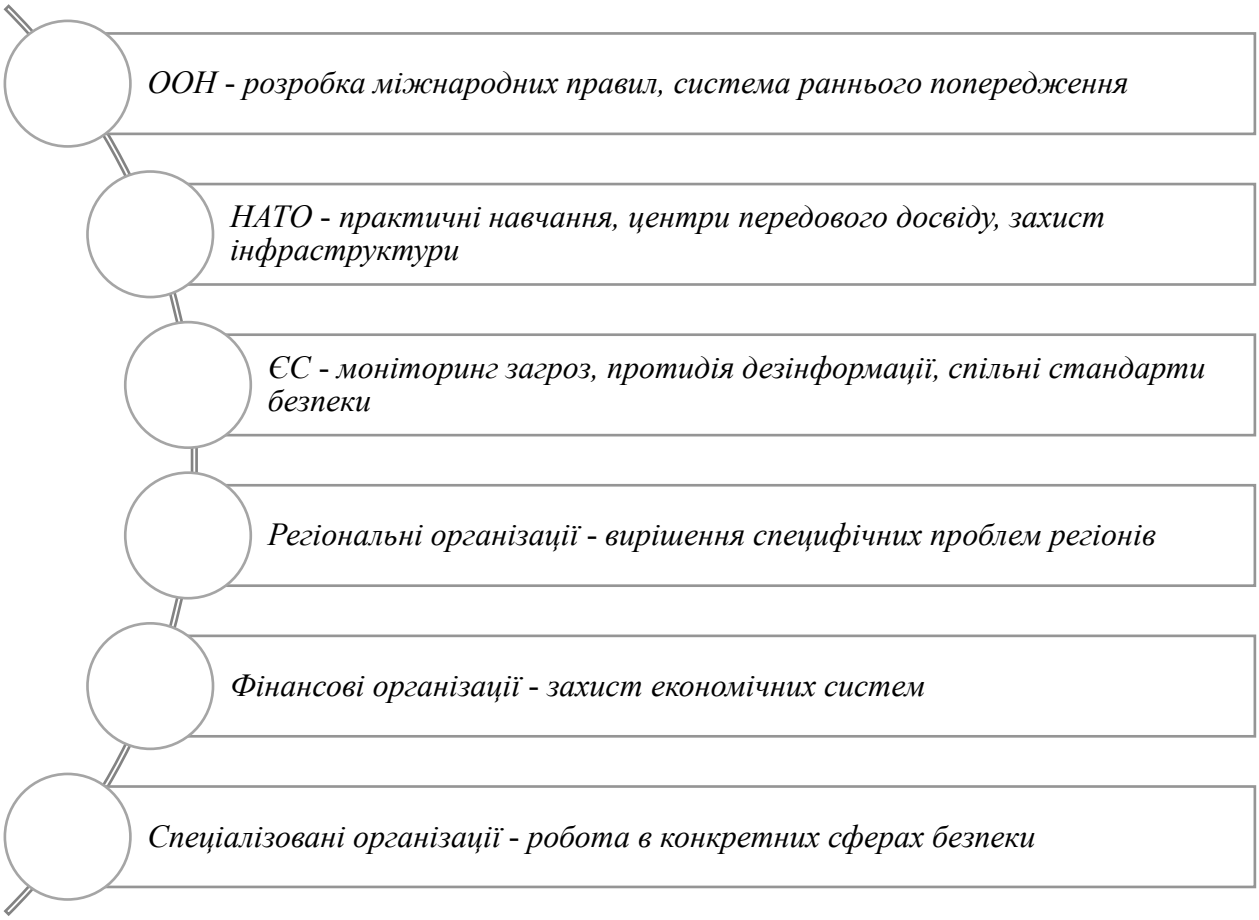

Рис. 3.3. Роль міжнародних організацій у протидії гібридним загрозам

Організація Об'єднаних Націй, як найбільша міжнародна організація, намагається адаптуватися до нових викликів, пов'язаних з гібридними війнами. ООН створює спеціальні комітети та робочі групи, які вивчають різні аспекти гібридних загроз та розробляють рекомендації для країн-членів. Особливу увагу приділяють питанням кібербезпеки та протидії інформаційним загрозам. Наприклад, експерти ООН працюють над створенням міжнародних правил поведінки в кіберпросторі, розробляють механізми співпраці між країнами у випадку масштабних кібератак. Також ООН намагається створити систему раннього попередження про можливі гібридні атаки, яка б допомагала країнам краще підготуватися до можливих загроз.

НАТО відіграє особливо важливу роль у протистоянні гібридним загрозам. Ця організація не тільки розробляє стратегії протидії таким загрозам, але й проводить практичні навчання, де відпрацьовуються різні сценарії гібридних

атак. НАТО створило спеціальні центри передового досвіду, де експерти з різних країн разом працюють над вивченням нових видів загроз та розробкою методів протидії їм. Особливу увагу приділяють питанням захисту критичної інфраструктури, протидії кібератакам та боротьбі з дезінформацією. НАТО також допомагає своїм членам покращувати їхні системи безпеки, проводить тренінги для фахівців та надає експертну підтримку.

Європейський Союз теж активно працює над створенням ефективних механізмів протидії гібридним загрозам. В ЄС створено спеціальні структури, які займаються моніторингом та аналізом таких загроз, розробляють рекомендації для країн-членів. Особливу увагу приділяють захисту спільного інформаційного простору від дезінформації та ворожої пропаганди. ЄС також працює над покращенням координації між різними країнами у випадку гібридних атак, створює спільні системи реагування на загрози. Важливим напрямком роботи є розробка спільних стандартів безпеки, особливо в сфері кібербезпеки та захисту критичної інфраструктури.

Регіональні організації також відіграють важливу роль у протистоянні гібридним загрозам. Вони часто краще розуміють специфічні проблеми свого регіону та можуть швидше реагувати на нові виклики. Наприклад, організації в Азійсько-Тихоокеанському регіоні приділяють особливу увагу питанням кібербезпеки та захисту від економічних загроз, оскільки ці проблеми особливо актуальні для їхнього регіону. Африканські організації більше зосереджені на протидії інформаційним впливам та запобіганні внутрішнім конфліктам, які можуть бути спровоковані зовнішніми силами.

Міжнародні фінансові організації, такі як Світовий банк і Міжнародний валютний фонд, зараз активно долучаються до боротьби з новими загрозами у фінансовому світі. Вони розуміють, що сучасні конфлікти часто ведуться не тільки зброєю, але й через економіку та фінанси. Тому ці організації розробляють спеціальні системи захисту, які допомагають країнам зберегти свої гроші та економіку в безпеці. Наприклад, вони створюють інструменти для виявлення підозрілих фінансових операцій, які можуть бути частиною ворожих дій інших

країн. Також вони допомагають державам зробити їхні економічні системи більш стійкими до різних атак, навчають, як захищатися від економічних маніпуляцій. Важливою частиною їхньої роботи є налагодження співпраці між різними країнами для спільної боротьби з фінансовими злочинами, які можуть використовуватися як інструмент тиску чи нападу в сучасних конфліктах. Все це допомагає країнам краще захищатися від спроб зашкодити їхній економіці через фінансові маніпуляції.

Важливу роль відіграють також спеціалізовані міжнародні організації, які займаються конкретними аспектами безпеки. Візьмемо, наприклад, Міжнародний союз електрозв'язку - це організація, яка дбає про безпеку телефонних мереж та інтернету, щоб наші розмови та повідомлення не могли перехопити зловмисники. А ось Інтерпол - це така міжнародна поліція, яка допомагає різним країнам разом боротися зі злочинцями, особливо коли ці злочинці діють у кількох країнах одночасно. Ці організації дуже добре знають свою роботу, мають багато досвіду та розуміють усі тонкощі у своїх сферах. Завдяки цьому вони можуть швидко помітити нові загрози та знайти способи захисту від них. Це особливо важливо сьогодні, коли злочинці та ворожі країни використовують все складніші способи атак, і звичайним організаціям важко з цим впоратися самостійно [20].

Міжнародні організації також відіграють важливу роль у розробці нових міжнародних норм та правил, які б регулювали поведінку держав у контексті гібридних війн. Це непроста справа, бо іноді важко зрозуміти - це просто звичайна конкуренція між країнами чи вже спланований напад. Наприклад, коли одна країна вводить торговельні обмеження проти іншої, це може бути як звичайний економічний крок, так і частина спланованої атаки. Тому міжнародні організації намагаються розробити чіткі правила та ознаки, за якими можна визначити, коли дії однієї країни проти іншої переходять межу нормальної конкуренції і стають атакою. Вони створюють спеціальні документи, де описують, як країни мають поводитися одна з одною, як вирішувати суперечки, і що робити, коли хтось порушує ці правила. Це допомагає країнам краще

захищатися та знати, коли і як вони можуть відповідати на недружні дії інших держав.

Проте роль міжнародних організацій у протистоянні гібридним загрозам має і свої обмеження. Часто вони не можуть діяти достатньо швидко через необхідність узгоджувати свої дії з усіма країнами-членами. Також буває складно досягти консенсусу щодо того, як саме потрібно реагувати на ті чи інші загрози. Крім того, самі міжнародні організації можуть ставати мішенями для гібридних атак, що ускладнює їхню роботу. Проте, незважаючи на всі ці виклики, міжнародні організації залишаються важливими майданчиками для координації зусиль різних країн у протистоянні гібридним загрозам.

ВИСНОВКИ

У результаті проведеного дослідження можна зробити ряд важливих висновків щодо природи гібридних війн та їх впливу на сучасні міжнародні відносини. Перш за все, дослідження показало, що гібридна війна є складним та багатовимірним явищем, яке суттєво відрізняється від традиційних форм військових конфліктів. Її головна особливість полягає в тому, що вона поєднує різні методи ведення протистояння – від класичних військових дій до інформаційних операцій, від економічного тиску до кібератак. При цьому всі ці елементи використовуються одночасно та узгоджено, створюючи синергетичний ефект та роблячи протидію таким загрозам особливо складною.

Дослідження історичного розвитку концепції гібридної війни показало, що хоча сам термін з'явився відносно нещодавно, методи, які ми зараз називаємо гібридними, використовувалися протягом всієї історії людства. Однак саме в сучасну епоху, завдяки розвитку технологій та глобалізації, ці методи набули нової якості та масштабу. Особливу роль у цьому відіграв розвиток інформаційних технологій, які створили нові можливості для впливу на суспільство та державні інституції. Інтернет та соціальні мережі перетворилися на потужний інструмент ведення гібридної війни, дозволяючи впливати на громадську думку та створювати розколи в суспільстві.

Аналіз основних компонентів гібридної війни дозволив виявити, що вона включає в себе військову, інформаційну, економічну, соціально-психологічну, дипломатичну та інші складові. Кожен з цих компонентів може використовуватися як самостійно, так і в поєднанні з іншими, створюючи складну систему впливу на противника. При цьому важливо розуміти, що різні компоненти гібридної війни не просто доповнюють один одного, а створюють принципово нову якість протистояння, де межі між війною і миром, між військовими та цивільними цілями стають все більш розмитими.

Дослідження типології гібридних конфліктів показало їх велику різноманітність та складність класифікації. Гібридні війни можуть відрізнятися

за складом учасників, за використовуваними інструментами, за географічним охопленням та іншими параметрами. При цьому важливо розуміти, що в реальності більшість гібридних конфліктів не можна чітко віднести до якогось одного типу – вони часто поєднують різні характеристики та можуть змінювати свою форму з часом.

Аналіз взаємодії традиційних і нетрадиційних методів ведення війни виявив, що в сучасних умовах вони все більше переплітаються та доповнюють один одного. Традиційні військові методи не втрачають свого значення, але їх ефективність значно зростає при правильному поєднанні з новими формами протистояння. Особливу роль у цьому відіграють сучасні технології, які створюють нові можливості для ведення бойових дій та координації різних елементів гібридної війни.

Дослідження впливу гібридних війн на міжнародні відносини показало, що вони створюють нові виклики для світової спільноти. Традиційні механізми міжнародної безпеки та співпраці часто виявляються неефективними проти гібридних загроз. Це змушує держави та міжнародні організації шукати нові форми взаємодії та створювати нові інструменти протидії таким загрозам. Особливо важливою стає роль міжнародних організацій, які можуть координувати зусилля різних країн у протистоянні гібридним загрозам.

В результаті дослідження стало очевидно, що протидія гібридним загрозам вимагає комплексного підходу, який би враховував усі аспекти цього явища. Держави повинні розвивати не тільки свої військові можливості, але й створювати ефективні системи кібербезпеки, протидії інформаційним впливам, захисту критичної інфраструктури. Важливу роль відіграє також підвищення стійкості суспільства до різних форм гібридного впливу, розвиток критичного мислення у громадян, створення ефективних систем виявлення та протидії дезінформації.

Таким чином, проведене дослідження підтвердило, що гібридна війна є одним з найсерйозніших викликів для сучасної системи міжнародної безпеки. Вона вимагає нових підходів до розуміння природи конфліктів та розробки

методів протидії їм. При цьому особливо важливим є розвиток міжнародного співробітництва, обмін досвідом та інформацією між різними країнами, створення спільних механізмів виявлення та протидії гібридним загрозам. Тільки об'єднавши зусилля, міжнародна спільнота може ефективно протистояти цим новим викликам та забезпечити стабільність і безпеку у світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 28 черв. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 30.01.2025).

2. Аналіз та систематизація підходів до розуміння поняття “гібридної війни” / A. Loishyn та ін. Journal of scientific papers "social development and security". 2021. Т. 11, № 1. С. 145–162. URL: https://doi.org/10.33445/sds.2021.11.1.15 (дата звернення: 30.01.2025).

3. Андрієвський Т. Г. Концептуалізація поняття гібридної війни: політологічний вимір. Сучасне суспільство. 2017. Вип. 1 (13). С. 4–15.

4. Валюшко І. О. Еволюція інформаційних війн: історія і сучасність. Історико-політичні студії. Серія "Політичні науки". 2015. № 2 (4). С. 127–134.

5. Гарькавий Є. М., Рубель К. В. Механізми ведення гібридної війни у гуманітарній сфері. Вісник Донецького національного університету імені Василя Стуса. Серія політичні науки. 2024. № 9. С. 30–35. URL: https://doi.org/10.31558/2617-0248.2024.9.4 (дата звернення: 30.01.2025).

6. Дирдін М. Є., Яцик Т. П. Протидія інформаційній складовій гібридної війни. Ірпінський юридичний часопис. 2023. № 1(10). С. 203–209. URL: https://doi.org/10.33244/2617-4154-1(10)-2023-203-209 (дата звернення: 30.01.2025).

7. Думанська В. Психолінгвістичні маркери дискурсу гібридної війни. Psycholinguistics in a modern world. 2020. Т. 15. С. 72–76. URL: https://doi.org/10.31470/10.31470/2706-7904-2020-15-72-76 (дата звернення: 30.01.2025).

8. Зонтова Є. Медіа як інструмент гібридної війни. Education and science of today: intersectoral issues and development of sciences / chair I. Петренко. 2024. URL: https://doi.org/10.36074/logos-29.03.2024.079 (дата звернення: 30.01.2025).

9. Качковська Л., Малеончук Г., Зінюк Д. Інформаційний вплив в умовах гібридної війни. Міжнародні відносини, суспільні комунікації та регіональні студії. 2022. № 3 (14). С. 87–102. URL: https://doi.org/10.29038/2524-2679-2022-03-87-102 (дата звернення: 30.01.2025).

10. Кіндратець О. М. Психологічна війна як елемент гібридної війни. Політичне життя. 2021. № 1. С. 84–88. URL: https://doi.org/10.31558/2519-2949.2021.1.10 (дата звернення: 30.01.2025).

11. Кобець Т. Когнітивна безпека в умовах гібридної війни. Вісник прикарпатського університету. серія: політологія. 2024. № 17. С. 67–73. URL: https://doi.org/10.32782/2312-1815/2024-17-9 (дата звернення: 30.01.2025).

12. Криськов А., Криськова С. Інформаційний простір як складова частина гібридної війни. Integración de las ciencias fundamentales y aplicadas en el paradigma de la sociedad post-industrial. 2020. URL: https://doi.org/10.36074/24.04.2020.v3.43 (дата звернення: 30.01.2025).

13. Крутій В. О. Витоки гібридних війн: досвід XX століття. Держава і право. Серія "Політичні науки". 2017. Вип. 77. С. 148–159.

14. Крутій В. О. Логіка гібридної війни: синергетичне пояснення. Держава і право. Серія "Політичні науки". 2018. Вип. 79. С. 15–25.

15. Новіков В. О. Аналіз сучасної концепції інформаційно-гібридної війни. Електронний журнал "Державне управління: удосконалення та розвиток". 2023. № 9. URL: https://doi.org/10.32702/2307-2156.2023.9.25 (дата звернення: 30.01.2025).

16. Петров В. В. Спеціальні служби: у "сірій зоні" гібридного миру й гібридних війн. Актуальні проблеми міжнародних відносин. 2018. Вип. 135. С. 35–48.

17. Почепцов Г. З історії поняття гібридної війни в США і Росії. ms.detector.media. URL: https://ms.detector.media/mediaanalitika/post/14619/2015-11-01-z-istorii-ponyattya-gibrydnoi-viyny-v-ssha-i-rosii/ (дата звернення: 30.01.2025).

18. Сохацький О. Ю., Шухманн В. А. Онлайн-ігри як інструменти гібридної війни. Journal of strategic economic research. 2023. № 1. С. 45–55. URL: https://doi.org/10.30857/2786-5398.2023.1.5 (дата звернення: 30.01.2025).

19. Швець А. В. Психофізіологічні аспекти розвитку «гібридної війни». Ukrainian journal of military medicine. 2021. Т. 2, № 4. С. 48–59. URL: https://doi.org/10.46847/ujmm.2021.4(2)-048 (дата звернення: 30.01.2025).

20. Шерр Д. Небезпека "гібридної" війни. Національна безпека і оборона. 2016. № 9/10 (167/168). С. 85–86.

21. Конов І. Ф. Епістемологія концепту «гібридна війна». Науково-теоретичний альманах "Грані". 2017. Т. 20, № 10. С. 61–80. URL: https://doi.org/10.15421/1717134 (дата звернення: 30.01.2025).

22. Про оборону України : Закон України від 06.12.1991 № 1932-XII : станом на 5 січ. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 30.01.2025).

23. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 15 листоп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 30.01.2025).

24. Про санкції : Закон України від 14.08.2014 № 1644-VII : станом на 21 листоп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1644-18#Text (дата звернення: 30.01.2025).

25. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII : станом на 9 серп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 30.01.2025).