

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ**

Кафедра міжнародних відносин та регіональних студій

ПЛИСЮК ЯНА ІВАНІВНА

ГІБРИДНІ ВІЙНИ ЯК ЗАГРОЗА МІЖНАРОДНІЙ БЕЗПЕЦІ

Спеціальність : 291 «Міжнародні відносини, суспільні комунікації та
регіональні студії»

Освітньо-професійна програма «Міжнародні відносини»

Робота на здобуття освітнього ступеня «Бакалавра»

Науковий керівник:

РОМАНЮК НАТАЛІЯ ІВАНІВНА

кандидат географічних наук, доцент

РЕКОМЕНДОВАНО ДО ЗАХИСТУ

Протокол № 9 засідання

кафедри міжнародних відносин

і регіональних студій

від 11 квітня 2025 р.

завідувач кафедри

_____ проф. Коцан Н.Н.

Луцьк 2025

АНОТАЦІЯ

Плисюк Я.І. Гібридні війни як загроза міжнародній безпеці.

Рукопис. Кваліфікаційна наукова робота бакалавра за спеціальністю Міжнародні відносини, суспільні комунікації та регіональні студії, ОПП Міжнародні відносини Волинський національний університет імені Лесі Українки, Луцьк, 2025. 60 с. укр.

У процесі написання бакалаврської роботи досліджено феномен гібридних війн як однієї з ключових загроз міжнародній безпеці у XXI ст. Розкрито суть поняття «гібридна війна», визначено її характерні риси та відмінності від традиційних форм збройних конфліктів. Автором зроблено висновок про те, що гібридна війна є складним конфліктом, який охоплює не лише військові аспекти, але й економічні, інформаційні та політичні чинники. В роботі проаналізовано основні елементи гібридної війни, зокрема інформаційні операції, пропаганду, кібератаки, а також політичні, економічні й військові елементи гібридних війн.

Виявлено, що інформаційні операції та пропаганда в умовах гібридних війн займають важливе місце, маючи суттєвий вплив на громадську думку, політичні процеси та мораль суспільства. Вони дозволяють здійснювати маніпуляції без застосування прямої військової сили, що робить їх потужними інструментами в конфліктах. Враховуючи швидкість, ефективність і відносну невидимість кіберзагроз, їх використання в гібридних війнах продовжить зростати, змінюючи природу конфліктів у майбутньому.

Політичні аспекти гібридної війни включають інформаційні та психологічні операції, маніпулювання масовою свідомістю, дезінформацію та пропаганду. Вони спрямовані на зміщення політичних лідерів, послаблення довіри до урядів та створення внутрішніх криз. Економічні аспекти гібридної війни спрямовані на послаблення економіки противника через знищення її фінансової стабільності, інфраструктури та вплив на соціальне становище населення. Військові аспекти гібридних війн не обмежуються традиційними збройними конфліктами, а включають також використання «сірих зон» війни, де агресор застосовує невизнані або неофіційні збройні формування. Зроблено висновок про те, що сучасні гібридні війни охоплюють широкий спектр впливу – від психологічного й інформаційного до воєнного й економічного.

У роботі досліджено наслідки гібридних конфліктів для глобальної стабільності та системи міжнародної безпеки, розглянуто стратегії протидії гібридним загрозам на міжнародному рівні, а також виклики, які постають перед міжнародним правом. Особливу увагу приділено впливу гібридної агресії росії проти України як прикладу комплексного застосування військових та невійськових методів з метою досягнення політичних і стратегічних цілей.

Зроблено висновок, що ефективна протидія гібридним війнам вимагає комплексної стратегії, яка передбачає консолідацію зусиль у сфері безпеки, міжнародної співпраці, кіберзахисту та інформаційної політики. Гібридні війни потребують нових підходів у воєнному плануванні, правовому регулюванні та дипломатії.

Рис. – 1, табл. – 3, бібліогр. – 52.

Ключові слова: гібридна війна, міжнародна безпека, кіберзагрози, інформаційні операції, пропаганда, росія, Україна.

ANNOTATION

Plisyuk Y. Hybrid wars as a threat to international security.

Manuscript. Qualification research work for a bachelor's degree in International Relations, Public Communications and Regional Studies, International Relations Department. Lesya Ukrainka Volyn National University, Lutsk, 2025. 60 p. in Ukrainian.

In the process of writing the bachelor's thesis, the phenomenon of hybrid wars as one of the key threats to international security in the XXI century is investigated. The essence of the concept of “hybrid warfare” is revealed, its characteristic features and differences from traditional forms of armed conflict are determined. The author concludes that hybrid warfare is a complex conflict that encompasses not only military aspects, but also economic, informational and political factors. The paper analyzes the main elements of hybrid warfare, including information operations, propaganda, cyber attacks, as well as political, economic and military elements of hybrid warfare.

It is found that information operations and propaganda in hybrid wars occupy an important place, having a significant impact on public opinion, political processes and public morality. They allow for manipulation without the use of direct military force, which makes them powerful tools in conflicts. Given the speed, effectiveness, and relative invisibility of cyber threats, their use in hybrid warfare will continue to grow, changing the nature of conflicts in the future.

The political aspects of hybrid warfare include information and psychological operations, manipulation of mass consciousness, disinformation and propaganda. They are aimed at removing political leaders, weakening trust in governments, and creating internal crises. The economic aspects of hybrid warfare are aimed at weakening the enemy's economy by destroying its financial stability, infrastructure, and impacting the social situation of the population. The military aspects of hybrid warfare are not limited to traditional armed conflicts, but also include the use of “gray zones” of war, where the aggressor uses unrecognized or unofficial armed groups. It is concluded that modern hybrid wars cover a wide range of impacts - from psychological and informational to military and economic.

The paper examines the consequences of hybrid conflicts for global stability and the international security system, considers strategies for countering hybrid threats at the international level, as well as the challenges faced by international law. Particular attention is paid to the impact of Russia's hybrid aggression against Ukraine as an example of the integrated use of military and non-military methods to achieve political and strategic goals.

It is concluded that effective counteraction to hybrid warfare requires a comprehensive strategy that involves consolidating efforts in the field of security, international cooperation, cyber defense and information policy. Hybrid wars require new approaches to military planning, legal regulation and diplomacy.

Fig. - 1, Tables - 3, Bibliography – 52.

Keywords: hybrid warfare, international security, cyber threats, information operations, propaganda, Russia, Ukraine.

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ГІБРИДНИХ ВІЙН.....	5
1.1. «Гібридна війна»: суть поняття та характерні риси.....	5
1.2. Стан досліджуваності проблеми в науковій літературі.....	9
1.3. Основні методи дослідження гібридних війн	14
РОЗДІЛ 2. ОСНОВНІ ЕЛЕМЕНТИ ГІБРИДНОЇ ВІЙНИ.....	18
2.1. Використання інформаційних операцій та пропаганди	18
2.2. Кібератаки як елемент гібридної війни	24
2.3. Політичні, економічні та військові аспекти гібридних війн.....	28
РОЗДІЛ 3. ОСОБЛИВОСТІ ГІБРИДНОЇ ВІЙНИ ЯК ЗАГРОЗИ МІЖНАРОДНІЙ БЕЗПЕЦІ.....	33
3.1. Вплив гібридних війн на глобальну стабільність та мир.....	33
3.2. Стратегії протидії гібридним загрозам на міжнародному рівні.....	38
3.3. Перспективи протидії гібридним війнам і виклики для міжнародного права.....	45
ВИСНОВКИ.....	51
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	53

ВСТУП

Актуальність теми. Тема гібридних війн є надзвичайно актуальною в сучасному міжнародному контексті через те, що ці конфлікти стають однією з основних загроз міжнародній безпеці. Гібридна війна поєднує в собі різноманітні форми боротьби, включаючи військові, інформаційні, економічні та психологічні методи, що дозволяє агресору досягати своїх стратегічних цілей без необхідності прямого збройного конфлікту. Це створює нові виклики для світової спільноти в боротьбі за підтримання стабільності та миру.

Гібридні війни призводять до значних змін на міжнародній арені, зокрема через економічні санкції, що застосовуються до країни-агресора, чи саботаж ключових елементів економіки супротивника. Це порушує глобальні торговельні потоки, створює економічні кризи, а також сприяє виникненню соціальної напруженості у постраждалих країнах. Така нестабільність може мати довгострокові наслідки для розвитку міжнародних економічних відносин. Гібридна війна спрямована на внутрішню дестабілізацію, зокрема через підтримку соціальних протестів, підбурювання до політичних криз та маніпуляції з суспільною свідомістю. Зокрема, розвиток кіберзброї, що дає змогу атакувати державні та економічні структури без фізичного вторгнення, а також маніпуляція інформацією через соціальні мережі, є одним з найважливіших аспектів гібридних війн.

Гібридні війни є важливою загрозою для міжнародної безпеки, оскільки вони змінюють традиційні уявлення про війну та збройні конфлікти, поєднуючи широкий спектр стратегій та засобів впливу. Урахування цих загроз є необхідним для зміцнення міжнародної стабільності та адаптації національних і міжнародних політик до нових реалій.

Об'єктом дослідження є гібридні війни як суспільно-політичне явище, а **предметом дослідження** – особливості гібридних війн як загрози міжнародній безпеці.

Метою бакалаврської роботи є дослідження гібридної війни як загрози

міжнародній безпеці.

Завдання дослідження:

- узагальнити теоретичні аспекти поняття «гібридна війна», виокремити її характерні риси;
- охарактеризувати основні методи дослідження гібридних війн;
- проаналізувати історію виникнення гібридних війн;
- розглянути особливості використання інформаційних операцій та пропаганди як елемента гібридної війни;
- проаналізувати кіберзагрози та атаки як складові гібридної війни;
- охарактеризувати політичні, економічні та військові аспекти гібридних війн;
- визначити вплив гібридних війн на глобальну стабільність та мир;
- проаналізувати стратегії протидії гібридним загрозам на міжнародному рівні;
- дослідити перспективи протидії гібридним війнам.

Практичне значення одержаних результатів. Одержані результати дослідження мають важливе практичне значення. Вони можуть використовуватися при дослідженні подібної тематики, в навчальному процесі ЗВО, для розробки та вдосконалення стратегій та політик у ряді сфер, що пов'язані з міжнародною безпекою, національною обороною та економічною стабільністю.

Апробація. Основні висновки роботи апробовані на IV Всеукраїнському науково-практичному форумі РЕПІТ (м. Луцьк, 15.05.2025 р.)

Структура бакалаврської роботи. Бакалаврська робота складається із вступу, трьох розділів, висновків та списку використаних джерел, що складається з 52 найменувань.

РОЗДІЛ 1.

ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ГІБРИДНИХ ВІЙН

1.1. «Гібридна війна»: суть поняття та характерні риси

Зважаючи на сучасний рівень суспільного розвитку, в умовах інформаційного суспільства розв'язання конфліктів між державами виключно військовим шляхом є неефективним, як і одночасне використання традиційних і нетрадиційних методів ведення війни. Поєднання цих методів і становить суть гібридної війни.

Концепція гібридної війни почала активно обговорюватися політичними та військовими експертами на початку 2000-х рр., але як явище вона існує з давніх часів. Концепція гібридної війни описує сучасну війну як поєднання різноманітних військових і невійськових методів для досягнення стратегічних цілей. Незважаючи на багатий досвід, накопичений у цій сфері за всю історію воєнних дій, поняття гібридної війни досі не має загальновизнаного змісту.

Основна ідея гібридної війни полягає в поєднанні різних тактик і стратегій для створення комплексного впливу на противника. Це можуть бути не тільки військові операції, а й елементи політичної, економічної та інформаційної стратегії.

Гібридні війни особливо важливі в контексті геополітичних конфліктів, коли держави використовують широкий спектр засобів для досягнення своїх цілей. Гібридна агресія росії проти України є прикладом такого використання різноманітних військових і невійськових впливів для досягнення політичних і стратегічних цілей [24]. Проте російсько-українська війна стала викликом не лише для України, а й для всього світу, для всієї міжнародної спільноти, а тепер створила серйозну загрозу світовому порядку.

Останніми роками гібридна війна стала для провідних країн світу ключовим і єдиним способом здійснення жорстоких дій, адже її сила,

поєднуючи традиційні та нетрадиційні форми, військові та абсолютно протилежні методи, перетворилася на жорстокого та безжального монстра в руках ворога.

Уздєнова Ю. М. вважає, що гібридна війна – це новий вид війни, війна четвертого покоління, потужний монстр, дії якого спрямовані на досягнення політичних цілей [40]. Але слід зазначити, що дослідження, проведені з проблеми гібридних війн, показують, що це явище не випадкове, а ретельно підготовлене, спрямоване на створення необхідної бази для створення конфлікту та нав'язування точки зору. Це маніпуляція суспільною свідомістю, розмивання довіри до влади, контроль усіх галузей з боку держави-агресора в країні-жертві. Інформаційний сектор відіграє значну роль у процесі гібридної війни, оскільки суттєво впливає на формування стабільності, формування довіри до влади, формування, підтримку та підтримку ідеології країни.

На думку Лисецького Ю.М., гібридна війна є всеохоплюючою та використовує всі засоби одночасно, причому як військовий, так і невійськовий вплив доповнюють один одного [27]. Застосовувані різноманітні методи створюють відчуття контролю над ситуацією в зоні ураження, що вимагає одночасного планування та координації дій у режимі реального часу за участю спецслужб, фінансових органів, дипломатів, міжнародних розвідувальних джерел, неурядових організацій, а також регулярних і найманських збройних формувань. Гібридна війна – спрямована на досягнення своєї мети шляхом витримування, виснаження та ослаблення зсередини, використання слабких місць противника.

Гібридна війна – це ідеологічна війна. В першу чергу вона бореться за народ, його погляди та переконання, а потім лише за державу. Дія вимагає об'єднання багатьох секторів – від флоту до хакерів, від банківських службовців до журналістів. Це неможливо без ідеологічної підготовки з боку народу. Обов'язкова умова – створення світогляду, розділеного на «добре» і «погано». На думку автора, пропагандистська складова – чи не найважливіша, адже будь-яка операція спрямована на вплив на людей. Зокрема, для

перетворення медіа на інформаційно-психологічну зброю необхідна участь медіа: їх лідерів і звичайних репортерів.

Гібридна війна – це тип військового конфлікту, який поєднує традиційні бойові дії з нетрадиційними методами, такими як кібератаки, інформаційні війни, економічний тиск, пропаганда, дезінформація та використання різноманітних неформальних або нелегальних збройних груп. Основні характеристики гібридної війни представлено на Рис. 1.1.

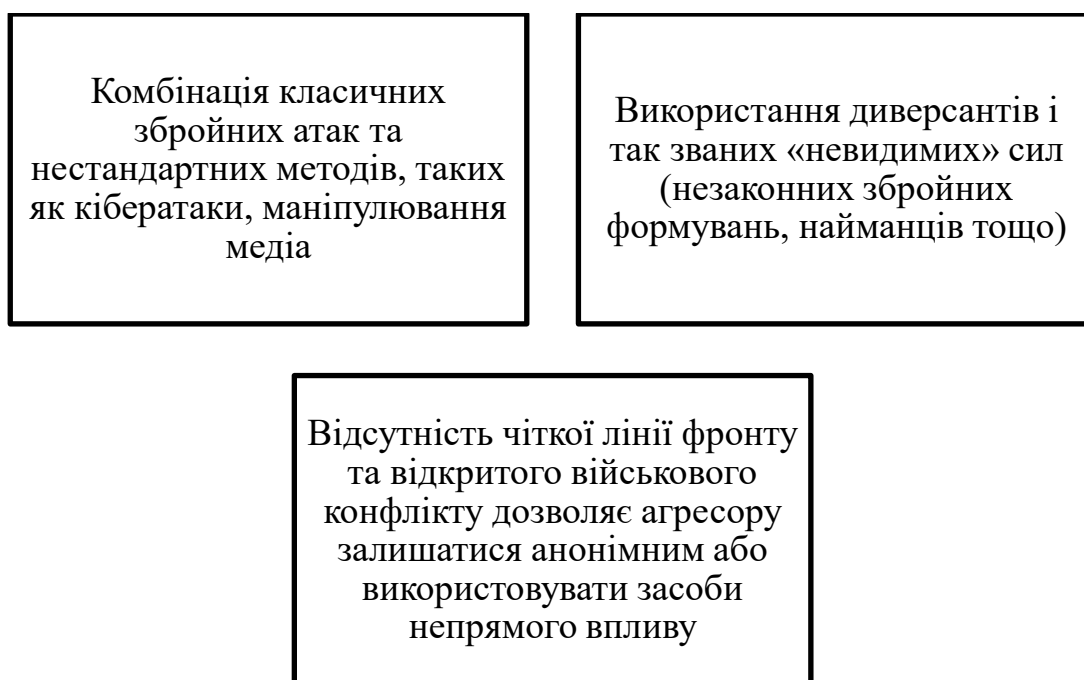


Рис. 1.1. Основні характеристики гібридної війни [6]

Цей тип війни характерний для сучасних геополітичних конфліктів. Однією з важливих складових гібридної війни є активне використання інформації як зброї. Це включає в себе як пропаганду, так і дезінформацію, створення фальшивих новин, маніпулювання громадською думкою як всередині країни-агресора, так і за її межами. Гібридні конфлікти можуть використовувати незаконні збройні формування, різноманітні партизанські групи або навіть добровольців, що створює додаткові труднощі у визначенні конкретного агресора. Агресор може використовувати економічні важелі, санкції, торговельні блокади, а також політичний тиск і маніпуляцію

міжнародними організаціями для досягнення своїх цілей

До основних ознак гібридної війни (згідно Великої української енциклопедії) належать наступні: може не мати формального оголошення війни, а конфлікти можуть відбуватись через тіньові структури, що робить їх складними для визначення і локалізації; використання пропаганди і створення фальшивих наративів для впливу на громадську думку, зокрема через соціальні мережі та медіа; кібератаки, зломи інформаційних систем, цифрові війни, які можуть паралізувати інфраструктуру або викликати паніку серед населення; участь сторонніх груп, зокрема незаконних збройних формувань, які не є офіційними військовими силами, але виконують завдання для іншої держави; паралельне застосування економічних санкцій, дипломатичних тисків та інших нетрадиційних заходів для досягнення політичних цілей [5].

Розуміння гібридної війни створює складний виклик сучасному міжнародному порядку та безпеці. Це новий тип конфлікту, насамперед завдяки його різноманітній тактиці, як традиційним військовим діям, так і нетрадиційним, таким як інформаційна війна, кібератаки, дезінформація, економічний тиск тощо. Гібридна війна відрізняється від традиційних конфліктів своєю складністю та ступенем впливу на суспільство, економіку та політичні процеси держави-мішені та її громадян. Наукова та практична діяльність, пов'язана з гібридною війною, включає розробку нових стратегій безпеки та оборони, які враховують не лише військові аспекти, а й інформаційні, економічні та політичні аспекти конфлікту. Розуміння природи і тактики гібридної війни є ключовим для ефективного захисту національних інтересів і підтримки стабільності в сучасному світі [3].

Гібридна війна використовує санкції, торговельні блокади та дипломатичні маніпуляції для досягнення своїх цілей, що дозволяє агресору тиснути на цільову країну без безпосереднього застосування військових сил. Використання диверсантів, найманців та інших нелегальних збройних груп у гібридній війні дозволяє уникати прямого військового зіткнення і залишатися анонімним. Гібридна війна часто є боротьбою за ідеологічні переконання,

зокрема через контроль за медіа та створення вигідних наративів, що вимагає маніпуляції свідомістю населення і створення розколу в суспільстві. Гібридна війна є складним і багатогранним конфліктом, який охоплює не лише військові аспекти, але й економічні, інформаційні та політичні чинники. Для успішної протидії такому типу конфлікту необхідна комплексна стратегія, що включає всі ці аспекти та враховує сучасні методи ведення війни.

Отже, гібридна війна як новий тип конфлікту поєднує традиційні методи ведення війни з нетрадиційними, такими як інформаційна війна, кібератаки, пропаганда, економічний тиск тощо. Це дозволяє агресору досягати своїх політичних і стратегічних цілей через комплексний вплив на країну-ціль, використовуючи широкий спектр засобів.

Гібридна війна не передбачає відкритих військових зіткнень і чітко визначених зон бойових дій. Це ускладнює ідентифікацію агресора та ведення традиційних бойових дій, що дозволяє застосовувати більш підступні й маніпулятивні методи впливу. Пропаганда та дезінформація грають ключову роль в гібридних війнах. Це дозволяє маніпулювати громадською думкою як всередині країни, так і за її межами, впливаючи на внутрішню стабільність і міжнародні відносини.

1.2. Стан досліджуваності проблеми в науковій літературі

Гібридні війни є однією з ключових загроз міжнародній безпеці у XXI ст., поєднуючи традиційні воєнні методи з інформаційною, кібернетичною, економічною та політичною агресією. Проблема гібридних війн активно досліджується у науковій літературі, особливо після подій у Грузії (2008 р.), анексії Криму та війни на Донбасі (2014 р.), а також повномасштабного вторгнення росії в Україну (2022 р.).

Історія гібридних війн має корені в різних формах конфліктів, де

поєднуються традиційні військові дії з іншими елементами, такими як інформаційні війни, кібер-атаки, економічні санкції та підтримка проросійських або сепаратистських рухів. Це поняття почало широко використовуватися у 21 столітті, але його корені можна відшукати в історії навіть століття тому.

В історії людства конфлікти між державами та різними недержавними акторами ніколи не зводилися лише до військових засобів. Гібридна війна є не лише історичним трендом, а й перспективним напрямом наукових досліджень. Але краще аналізувати їх сучасне використання та розуміння в контексті нагальних практичних потреб. Дослідники часто ігнорують політичні та правові чинники, що сприяли виникненню сучасних гібридних війн не як окремої події, а як окремих «незвичайних» (у міжнародному гуманітарному праві та зокрема Гаазької конвенції про право сухопутної війни 1907 р. та Гаазької конвенції 1907 р. про митні та акцизні збори Четвертої конвенції) методів конфлікту між державами, а натомість зосереджуються виключно на нових технологіях останніх [8].

В монографії Горбуліної В. П. «Світова гібридна війна: український фронт» визначено, що неодмінною передумовою виникнення гібридних війн стала заборона війни в міжнародному праві, що, безперечно, свідчить про суттєві зміни у світогляді значної частини людства. В монографії зазначено, що заборона війни в міжнародному праві викладена в сучасній і універсальній формі Статуту Організації Об'єднаних Націй, який починається з декларації про те, що Організація Об'єднаних Націй зобов'язана «рятувати наступні покоління від лиха війни», «жити разом у мирі як добрі сусіди, об'єднувати наші сили для підтримки міжнародного миру та безпеки, а також утримуватися лише від використання збройної сили та методів ведення війни». Цей документ передбачає заборону агресивної війни та колективні заходи «для запобігання та усунення загрози миру та для придушення актів агресії чи інших порушень миру». Ці принципи були послідовно виражені й уточнені в діях ООН.

Горбуліна В. П. у монографії досліджувала історію виникнення гібридної війни. Вона вважає, що концепція гібридного конфлікту виникла в Сполучених Штатах Америки із включенням тотальної та комбінованої (багатопартійної) війни як поєднання регулярних і нерегулярних військових дій. Термін «гібридна війна» був введений у США. Водночас зрозуміло, що це поняття ще не сформувалося. Наприклад, у Стратегії національної оборони США 2005 р. на додаток до традиційних збройних сил були перераховані нові загрози: «нерегулярні, терористичні та неорганізовані загрози, пов'язані з використанням нових технологій та їхнім потенціалом ненавмисного руйнівного впливу (кібербезпека, використання соціальних медіа тощо)» [9].

Хоча сучасна концепція гібридної війни стала популярною на початку 2000-х років, такі форми конфліктів існували ще в давнину. Грабовський С. в статті «Гібридна війна: історія і сутність» визначає, що у давнину, вже в період античності та середньовіччя, деякі елементи гібридної війни були присутні. Військові стратегії часто поєднували прямі збройні атаки з психологічними операціями, такими як облоги, пропаганда та маніпуляція населенням. Наприклад, у період Древнього Риму використовувалися методи психологічного тиску та «інформаційні війни» для підтримки влади та надання переваги на полі бою.

Як зазначає Грабовський С. одним із найбільш відомих прикладів гібридної війни є період Холодної війни між США та СРСР. Цей конфлікт не мав прямого військового зіткнення між двома наддержавами, проте в ньому широко використовувалися засоби психологічної війни, пропаганди, кібератак та економічного тиску. Інформаційна маніпуляція була важливою частиною боротьби за уми населення, а також здійснювалися «непрямі» військові втручання через проксі-війну, в тому числі в Африці, Латинській Америці та Азії [10].

Перша яскрава демонстрація сучасної гібридної війни відбулася під час війни Росії з Грузією в 2008 р. Росія застосувала традиційні військові сили, але одночасно використовувала інформаційну пропаганду, створення фальшивих

наративів і підтримку проросійських сепаратистських угруповань. Це поєднання військових і політичних методів створило ефективний інструмент для досягнення стратегічних цілей без прямого оголошення війни. Автор зазначає, що після 2014 р. росія активно використовує методи гібридної війни в Україні. Анексія Криму, підтримка сепаратистів на Донбасі, а також кібератаки, інформаційна пропаганда, економічні санкції і використання нелегальних збройних груп стали основними інструментами цієї гібридної агресії. Всі ці елементи поєднуються для дестабілізації ситуації в Україні та досягнення стратегічних цілей без формального оголошення війни [10].

Американський аналітик Дж. МакКен в статті Glenn R.W. Thoughts on «Hybrid» Conflict» досліджує гібридні війни. Він вважає, що «гібридні конфлікти є війнами як з фізичними, так і з ідеологічними аспектами: перший – це боротьба проти озброєного ворога, а другий – це боротьба за контроль і підтримку населення зони бойових дій, підтримку внутрішніх фронтів сторін конфлікту та підтримку з боку міжнародного співтовариства» [49].

У 2010 р. стратегічний документ Міністерства оборони Великої Британії «Природа майбутніх конфліктів» визначив гібридні або інтегровані загрози як «одночасне використання всіх форм війни, включаючи сучасну зброю, нетрадиційні методи, тероризм і деструктивні злочинні дії з метою зруйнувати існуючий порядок», з децентралізованим плануванням і виконанням [48].

Колектив авторів Пирожков С. І., Майборода О. М., Хамітов Н. В., Головаха Є. І., Дембіцький С. С., Смолій В. А., Скрипнюк О. В., Стоєцький С. В. в дослідженні «Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь», досліджують гібридні загрози як «різноманітне та динамічне використання звичайних збройних сил, нерегулярних формувань та/або злочинних елементів, об'єднане для досягнення взаємопідсилювальних результатів». Серед гібридних загроз згадується використання ЗМІ, цифрових мереж, технологій і корупції для створення нестабільності та відчуження населення від власних збройних сил [33].

Ситник Г. П. в статті «Філософія війни та миру» розглядає традиційні війни, коли держави зазвичай прямо вступають у конфлікт і відкрито визнають свою участь. Війна ведеться через сутички між арміями на визначених лініях фронту, що часто чітко визначено [37].

Дембіцький С., Злобіна О., Костенко Н. та ін. в колективній монографії «Українське суспільство в умовах війни» досліджують традиційні війни. На їх думку традиційна війна, зазвичай має конкретну мету – завоювання території, перемога в битві або звільнення певних територій. Це чітко визначена мета, яка досягається через військові дії [12]. Зазвичай традиційні війни мають чітко визначений початок і кінець, із встановленням конкретних умов миру або перемир'я.

Гібридні війни можуть бути спрямовані не на досягнення конкретної територіальної перемоги, а на створення нестабільності, послаблення супротивника, зміщення урядів, або вплив на суспільну думку. Часто кінцева мета – це дестабілізація, контроль над інформацією або підрив довіри до політичних інститутів.

Отже, дослідження гібридних війн є важливим напрямом у науковій літературі, з огляду на їхній вплив на міжнародну безпеку. Дослідження показують, що зростання популярності гібридних війн може бути частково пов'язане з обмеженнями, які накладаються міжнародним правом на ведення традиційних війн, зокрема через заборону агресії в рамках Статуту ООН. Незважаючи на широке дослідження гібридних війн, необхідно звернути більшу увагу на політичні та правові аспекти, які впливають на виникнення цих конфліктів, а також на практичне застосування сучасних методів ведення війни.

1.3. Основні методи дослідження гібридних війн

Дослідження гібридних війн вимагає використання міждисциплінарних методів, які дозволяють аналізувати як традиційні військові дії, так і інформаційні, економічні, кібернетичні та політичні аспекти. До основних методів дослідження належать: аналіз документів (при дослідженні інформаційних матеріалів, статей, зображень), історико-порівняльний метод (при дослідженні історичного розвитку та сучасних кібератак), SWOT аналіз (при порівнянні гібридної й традиційної війн).

Аналіз документів – це метод вивчення великих обсягів тексту (документів, відео, аудіо, зображень). Цей метод включає зміст медіа-повідомлень, пости в соціальних мережах, відповіді на відкриті запитання опитування тощо. Технології, які використовує метод, дозволяють обробляти та узагальнювати великі обсяги текстової інформації в найкоротші терміни. Ці технології включають: автоматичне визначення ключових слів у документах, аналіз веб-сторінок, автоматичний моніторинг повідомлень у соціальних мережах та веб-ЗМІ на певну тему, автоматичне транскрибування аудіо- та відеоматеріалів з високою точністю розпізнавання [36].

Аналіз документів – це метод дослідження, який передбачає аналіз контенту різних видів ЗМІ. За допомогою аналізу контенту дослідники сподіваються зрозуміти як людей, які створили контент, так і людей, які його використовували. Типовий проект аналізу документів не потребує складних експериментів. Натомість для аналізу потрібен доступ до відповідних засобів масової інформації, що робить цей тип дослідження простішою та дешевшою альтернативою іншим видам досліджень, які передбачають складні опитування [37].

Аналіз контенту використовують для дослідження інформаційної складової гібридних війн, зокрема: аналіз медійних матеріалів (статей, телевізійних сюжетів, постів у соціальних мережах) для виявлення маніпулятивних технологій та наративів; дослідження пропагандистських

меседжів і фейкових новин, які використовуються для впливу на суспільну думку; оцінка ефективності інформаційних кампаній та їхнього впливу на різні соціальні групи.

Аналіз документів є одним із ключових методів дослідження інформаційної складової гібридних війн, оскільки дозволяє систематично вивчати зміст повідомлень, що поширюються через ЗМІ, соціальні мережі, офіційні заяви та інші канали інформаційного впливу. Основним завданням цього методу є виявлення пропагандистських наративів, аналіз механізмів дезінформації, дослідження методів маніпуляції суспільною свідомістю та моніторинг інформаційних атак. Він застосовується для ідентифікації ключових меседжів, що використовуються для легітимації агресії або дискредитації опонентів, а також для виявлення цільових груп, на які спрямовані інформаційні кампанії.

Аналіз документів дозволяє досліджувати інформаційну складову гібридних війн, ідентифікуючи маніпулятивні технології, пропагандистські меседжі та механізми дезінформації. Він допомагає розкривати інформаційні атаки, оцінювати ефективність інформаційних кампаній та визначати їхній вплив на громадську думку.

Історико-порівняльний метод – це набір процедур, які використовують історики для вивчення подій минулого за допомогою першоджерел та іншої інформації. Історико-порівняльний метод допомагає виявити закономірності розвитку гібридних війн на основі аналізу історичних прецедентів, зокрема: порівняння сучасних гібридних конфліктів із війнами минулих століть, у яких використовувалися схожі методи; аналіз геополітичних та соціально-економічних умов, що сприяють використанню гібридних стратегій; дослідження змін у воєнній доктрині різних держав щодо застосування гібридних методів ведення війни.

Цей метод також дає змогу порівнювати геополітичні умови, в яких виникали гібридні конфлікти, та оцінювати їхній вплив на розвиток міжнародних відносин. Крім того, історико-порівняльний метод допомагає

визначити ефективність різних стратегій протидії гібридним загрозам, що застосовувалися в минулому, та оцінити їхню актуальність у сучасному контексті. Таким чином, він є важливим інструментом для прогнозування майбутніх сценаріїв розвитку гібридних конфліктів та вироблення ефективних механізмів їхньої нейтралізації.

Історико-порівняльний метод дає змогу простежити закономірності розвитку гібридних конфліктів, аналізуючи історичні прецеденти та зміни у воєнній доктрині різних держав. Він дозволяє порівнювати геополітичні умови виникнення гібридних воєн, оцінювати їхній вплив на міжнародні відносини та визначати ефективність стратегій протидії таким загрозам.

SWOT аналіз (аналіз сильних сторін, слабких сторін, можливостей і загроз) – цей метод є фундаментальним інструментом, який дозволяє не тільки чітко відобразити поточний стан певного явища, але й визначити подальші перспективи та напрямки подальшого розвитку [39].

SWOT-аналіз використовується для оцінки сильних та слабких сторін гібридних війн, а також можливостей та загроз, які вони створюють: сильні сторони гібридної війни: гнучкість, анонімність, поєднання різних форм тиску (інформаційного, економічного, військового); слабкі сторони: необхідність великої кількості ресурсів, ризик викриття та міжнародної реакції; можливості: використання новітніх технологій, можливість впливати на супротивника без відкритого військового вторгнення; загрози: міжнародні санкції, контрзаходи з боку інших держав, неможливість довготривалого утримання контролю над територією або суспільством.

SWOT-аналіз використовується для оцінки сильних та слабких сторін гібридних війн, а також для виявлення можливостей і загроз, які вони створюють. Цей метод дозволяє комплексно оцінити специфіку гібридних конфліктів, проаналізувавши їхні ключові характеристики та потенційні наслідки. SWOT-аналіз використовується для оцінки сильних і слабких сторін гібридних воєн, а також виявлення можливостей і загроз. Він допомагає систематизувати переваги, такі як гнучкість і анонімність гібридних методів,

а також недоліки, зокрема високі ресурсні витрати та ризик викриття. SWOT-аналіз також сприяє оцінці перспектив використання новітніх технологій у гібридних конфліктах та прогнозуванню можливих контрзаходів з боку міжнародної спільноти.

Отже, дослідження гібридних війн потребує комплексного підходу, що охоплює аналіз військових, інформаційних, економічних, кібернетичних та політичних аспектів. Основними методами вивчення цієї проблематики є аналіз документів, історико-порівняльний метод та SWOT-аналіз. Застосування цих методів дозволяє глибше зрозуміти природу гібридних війн, виявити ключові механізми їхнього ведення та розробити ефективні стратегії протидії, спрямовані на зміцнення інформаційної, кібернетичної та військово-політичної безпеки.

РОЗДІЛ 2.

ОСНОВНІ ЕЛЕМЕНТИ ГІБРИДНОЇ ВІЙНИ

2.1. Використання інформаційних операцій та пропаганди

Інформаційні операції та пропаганда є ключовими елементами гібридних війн, а також використовуються в традиційних конфліктах для впливу на населення, суспільну думку та політичні процеси. У сучасних війнах вони стали не менш важливими за військові дії, адже впливають на мораль, стабільність і навіть на політичні рішення держав.

Інформаційні операції є одними з найважливіших елементів гібридних війн, адже вони дозволяють досягати стратегічних цілей без використання відкритої військової сили, що робить їх ефективними та непомітними інструментами для досягнення політичних і військових переваг. Вони мають широкий спектр застосування та можуть включати різноманітні методи маніпуляції, дезінформації, психологічних впливів і медіа-операцій. У контексті гібридної війни інформаційні операції стають не лише доповненням до військових дій, а й основним способом впливу на супротивника і громадську думку [19].

Основна мета інформаційних операцій у гібридній війні – маніпулювання громадською думкою адже інформаційні операції спрямовані на формування позитивного образу агресора і негативного – супротивника. Це може включати поширення пропаганди через медіа, соціальні мережі, інтернет-ресурси, щоб створити у громадян враження, що одна зі сторін є «агресором», «диктатором» або «незаконним урядом» [22].

Методи інформаційних операцій у гібридній війні:

– дезінформація та фальшиві новини – створення та поширення неправдивої інформації з метою введення в оману супротивника або міжнародної громадськості. Дезінформація та фальшиві новини можуть включати підроблені документи, відео, аудіо або заяви, які є частинами

кампанії з дезінформації [41];

- псевдодокументи та маніпуляція фактами – оформлення фальшивих звітів або офіційних заяв, які виглядають як офіційні джерела інформації, з метою підриву довіри до опонента [11];

- використання медіа, зокрема телевізійних каналів, радіо, газет, соціальних мереж для просування ідеологічних наративів або для розповсюдження панічних чуток [35].

Інформація та інформаційні технології створили явища, які були прийняті різними акторами (державами, корпораціями, іншими організаціями тощо) як інструменти для впливу та досягнення коротко- та довгострокових цілей. Вплив інформації на відносно широку аудиторію пов'язаний насамперед з масовим суспільством і масовою свідомістю, психологічним і нейролінгвістичним програмуванням і багатьма іншими аспектами.

Інформаційні війни стали глобальним явищем у різних секторах як тип сучасного конфлікту в інформаційному суспільстві, головну роль у якому відіграє передача інформаційних конструкцій, повідомлень і наративів, які використовуються суспільствами. Одним із найефективніших і поширених засобів у контексті розгортання та ведення інформаційної війни є контрпропаганда, яка тісно пов'язана з пропагандистською діяльністю та використовується разом з нею.

Аналітики і теоретики вважають контрпропаганду продовженням пропаганди, але в протилежному сенсі. Тому вивчення поняття контрпропаганди необхідно починати з вивчення поняття пропаганди. Пропаганда, по суті, здійснюється через масову комунікаційну діяльність, яка за своєю формою має ефект переконання, але по суті вона здійснюється переважно через використання психологічного навіювання, яке є прямою передачею певних психічних станів від однієї особи іншій, без участі одержувача і часто без явного усвідомлення.

Масова інформація є засобом пропаганди та думки, але для пропаганди інформація є засобом передачі сенсу, а для думки – це вплив на розуміння цих

сенсів. Пропаганда, як правило, зосереджена на зміні та формуванні соціальних процесів, тоді як навіювання є індивідуальним психічним процесом. На нашу думку, пропаганда – це політично вмотивований інформаційно-психологічний вплив на емоційно-вольову сферу масової свідомості, за допомогою якого впроваджуються політичні ідеї, установки, уявлення та формується політична поведінка.

Основною психологічною метою пропаганди є вплив на ідеологічні, соціальні та політичні системи мислення людей, які можна змінити шляхом створення нових ідей або посилення (послаблення) існуючих. Основні елементи процесу пропаганди: суб'єкт (соціальна група, інтереси якої виражаються за допомогою пропаганди), зміст, форми і методи, засоби або канали пропаганди (радіо, телебачення, друк, система мовної пропаганди тощо), об'єкт (аудиторія або соціальна спільнота, на яку звернена пропаганда).

Вирішальне значення для розуміння процесу пропаганди мають соціальні інтереси суб'єкта, його зв'язок із загальними інтересами суспільства та окремими групами. Це визначає зміст і впливає на вибір форм, методів і засобів пропаганди [29]. Пропаганда функціонує як поширення знань про фундаментальні основи світогляду, прийнятних для активних політичних акторів. Аспект пропаганди полягає в тому, що результат її впливу має бути виявлений адміністрацією протягом певного часу, а пропагандистська інформація завжди подається в інтересах певних соціальних груп, тобто через ідеологічну призму [7; 13].

Терміни «пропаганда» і «обман» часто використовуються як синоніми, але це не зовсім правильно. Пропаганда завжди має на меті змусити когось виглядати певним чином: перевищувати виробничі плани, боротися за країну чи віру, підтримувати партію чи уряд. Але також можуть бути такі речі, як миття рук перед їжею або невживання наркотиків. Це означає, що пропаганда може повністю задовольнити певні потреби та бажання. Це не завжди щось нечесне або шкідливе. І це не обов'язково пов'язано з брехнею.

Пропаганда як рух виникла давно. Вже в давнину, в епоху запеклих

міжплемінних воєн, воїни всіляко намагалися залякати воїнів-супротивників, щоб зламати їх волю і переконати у своїй перевазі [43]. Пропаганда – це систематичне використання інформації для впливу на масову аудиторію з метою переконання або маніпуляції її поглядами, думками та поведінкою, часто в умовах війни або політичних конфліктів.

Пропаганда може бути як відкритою, так і прихованою, і зазвичай має на меті: сприяти зміцненню національної ідентичності та патріотизму серед громадян, підвищуючи їхню готовність до підтримки уряду чи ведення війни; через пропаганду можна створювати негативний образ ворога, наприклад, описуючи його як терористів, диктаторів або ворогів людства; пропагандистські кампанії часто використовуються для виправдання агресії або насильства, щоб переконати населення, що війна чи інші насильницькі дії є необхідними або правомірними. Пропаганда може бути різних типів (Табл. 2.1.).

Таблиця 2.1

Класифікація типів пропаганди*

Категорія	Тип пропаганди	Опис
1	2	3
За напрямом	Внутрішня пропаганда	Спрямована на внутрішнього користувача, з характерними ознаками: шкідливість, «прийняття зовнішнього ворога», контроль свідомості через психоемоційний вплив, залякування, нав'язування правильних поглядів, ізоляція від інших ЗМІ.
	Іноземна пропаганда	Розрахована на «відправку за кордон», часто прихована, її мета – створення лояльних до режиму груп за межами, приховання або спотворення справжніх намірів і дій режиму.
За сферою розподілу	Культурна пропаганда	Поширення політичних та ідеологічних поглядів через твори мистецтва, культових діячів культури або впливових осіб.
	Інформаційна пропаганда	Поширення агітації, використання неправдивої інформації та агітаційних матеріалів у ЗМІ.
	Політична пропаганда	Ідеологічні погляди, втілені у передвиборчих програмах, публічних виступах політиків чи партій, які переслідують політичну мету.

Продовження табл. 2.1

1	2	3
	Особиста пропаганда	Поширення пропаганди через особисте спілкування, зокрема через соціальні мережі та месенджери.
За рівнем достовірності інформації	Правдива інформація	Фактична інформація, яка може бути інструментом пропаганди, якщо вона представлена таким чином, щоб вплинути на споживача й сформувати конкретне бачення події.
	Часткова дезінформація	Часткове замовчування подій, вирвані з контексту фрази, неоднозначні кадри та відредаговані відеокліпи, що зручні для пропаганди.
	Відверта брехня	Повністю сфабриковані заяви та інформація, деякі з яких можуть виглядати правдоподібно, інші – межують з абсурдом.
Як платформа	Подієва пропаганда	Створення сприятливого середовища для поширення ідей, зондування громадськості, визначення рівня довіри до фейкових новин, аналіз суспільних настроїв, спотворення свідомості.
	Активна пропаганда	Мобілізація впливу на маси, підбурювання їх до реалізації планів режиму, підтримка активних дій через залякування чи примус до дії.
	Прикриття	Замовчування, заперечення або приховування злочинів, скоєних режимом, з метою приховати реальну ситуацію.

* Складено автором за: [17].

Інформаційних операцій та пропаганда мають спільну мету: поширення хибної інформації, яка має на меті заплутати або вплинути на суспільну думку. Дезінформація може включати неправдиві факти, підроблені документи або фальшиві заяви; пропагандистські повідомлення часто орієнтовані на виклик емоційного відгуку у слухачів – ненависть, страх, тривогу чи патріотичні почуття. Це може включати використання образливих або гіперболізованих зображень і звуків; інформаційні операції та пропаганда можуть бути спрямовані на різні групи: від загальної громадськості до конкретних соціальних, етнічних чи політичних груп, залежно від того, на кого хочуть впливати; багато інформаційних операцій ведеться через безліч анонімних джерел, що робить неможливим точне визначення авторства або спонукання до дій [17].

Важливо зазначити, що інформаційні операції та пропаганда в умовах

гібридних та традиційних війн займають важливе місце, маючи суттєвий вплив на громадську думку, політичні процеси та мораль суспільства. Вони дозволяють здійснювати маніпуляції без застосування прямої військової сили, що робить їх потужними інструментами в конфліктах. Зокрема, у гібридних війнах інформаційні операції стають основним засобом досягнення стратегічних цілей, націлених на розпалювання дезінформації, маніпулювання фактами та створення негативного іміджу супротивника.

Основні методи, які використовуються в інформаційних операціях і пропаганді:

- дезінформація – поширення неправдивих новин чи фальшивих документів для введення в оману;
- маніпуляція фактами – використання фальшивих звітів та офіційних заяв, що підривають довіру до опонента;
- медіа-платформи – активне використання телевізійних каналів, радіо, соціальних мереж для розповсюдження ідеологічних наративів та панічних чуток.

Пропаганда, в свою чергу, має чітко визначені цілі, такі як зміцнення національної ідентичності, формування патріотичних настроїв, виправдання агресії або насильства. Вона також може бути різної форми: внутрішня, іноземна, культурна, політична, особиста. Психологічний вплив пропаганди полягає в тому, що вона прагне змінити соціальні і політичні погляди громадськості, формуючи певне бачення подій, що відповідає інтересам того чи іншого режиму. Суттєвими аспектами є використання навіювання та масового психоемоційного впливу [17].

Отже, інформаційні операції та пропаганда в умовах сучасних конфліктів – це важливий інструмент впливу, здатний змінювати хід бойових дій через маніпуляцію інформацією та вплив на свідомість людей.

2.2. Кібератаки як елемент гібридної війни

Кіберпростір являє новітнє поле битви для використання відомих і, перш за все, невідомих вразливостей передбачуваного ворога або суперника. Кіберзброя – це шкідливі комп’ютерні програми, призначені для атаки на важливу кіберфізичну систему з метою порушення її нормальної роботи або знищення. На відміну від виробництва звичайної зброї, ці типи атак на критично важливу інфраструктуру не вимагають багатомільйонних інвестицій, і їх здатність до тиражування є високоефективною.

У традиційних умовах зброю можна побачити з літаків і супутників, а держави та великі коаліції, такі як НАТО, добре контролюють те, чим володіє інша сторона. Але кіберзброя майже нематеріальна, а мережі передачі даних усунули потребу навіть у чіпі пам’яті, щоб перетинати кордон. У разі кібервійни це ускладнює встановлення руйнівної здатності супротивника.

Ще менше десяти років тому будь-яка шкідлива комп’ютерна програма, здатна атакувати нашого ворога в будь-який час, вважалася кіберзброєю. Щоб уникнути виявлення та втрати користі перед розгортанням, атака зазвичай базується на одному або кількох методах використання вразливості в програмі, встановленій на комп’ютерних системах жертви, відомої як уразливість нульового дня [40].

Щоб ідентифікувати кіберзброю, слід виходити за межі кібервійни і шукати, наприклад, засоби спостереження та біометричну ідентифікацію, які можуть впливати на ланцюг поставок і потенційно збирати дані користувачів і громадян. Це «доступний» тип загрози, який не потребує багатомільйонних інвестицій, необхідних для виробництва військової техніки та зброї. Виявлення нових вразливостей і розробка інструментів для їх використання набагато дешевше. Перш за все, цю зброю можна копіювати сотні чи тисячі разів майже без додаткових витрат. Вони можуть бути розроблені сірими організаціями, які потім продають їх урядам, відкрито, і злочинним групам у більш прихований спосіб. Але каталог кіберзброї також може включати,

очевидно, менш войовничий інструмент: дезінформацію, яку також можна використовувати для атак на критичну інфраструктуру. Використовуючи звичайні інформаційні канали (соціальні мережі, медіа тощо), дезінформація вибірково націлена на людей із спроможністю керувати інфраструктурою та може доповнюватися кібер(контр)розвідкою.

Кіберзброю можна заховати де завгодно: в чіп, програму, карту пам'яті або зберігати в хмарі. Кіберзброя складається з «бітів», які можна приховати кількома способами, тому їх неможливо виявити. Вони можуть залишатися бездіяльними роками на заводі з виробництва енергії, на залізниці чи в центрі управління повітряним рухом, або в офісі урядовця чи керівника, ніхто цього не помічає.

Гібридний конфлікт – це війна з додатковим рівнем дистанційних операцій. На відміну від звичайної війни, де армію загарбників можна побачити на вулицях, підготовка до кібератаки непомітна, оскільки немає пересування військ через будь-які кордони. У кіберпросторі немає кордонів.

Кіберзброю можуть виробляти кібермафії, кіберпідрозділи звичайних армій чи урядів або компанії, що працюють від їх імені. Особливе занепокоєння держав викликає те, що розробка та створення кіберзброї доступна будь-якій невеликій країні чи організації, оскільки для виробництва не потрібна дорога сировина. Таким чином, гібридна війна є кращою перед традиційною війною, тому що вона більш прибуткова [41].

Гібридна війна поєднує традиційні військові засоби з невійськовою тактикою, включаючи кібератаки. Мета – завадити та послабити супротивника – самі атаки можуть бути не завжди помітні, але сутичка та результати, які виникають, безумовно, помітні. Використання кібератак у гібридній війні зростає, і на це є вагомі причини. Кіберзагрози швидкі, ефективні та часто майже непомітні. Візьмемо, наприклад, атаку на Хезболлу, де комунікаційні засоби дистанційно маніпулювали та знищували – поєднання проникнення та технічної диверсії, що завдало значної шкоди.

Відомо багато випадків сучасних конфліктів, які пов'язані з

використанням кібератак (Табл. 2.2).

Таблиця 2.2

Основні кібератаки сучасності *

Рік	Опис атаки
2015	Атака на енергетичну інфраструктуру України: в грудні 2015 року хакери з росії здійснили кібератаку на енергетичну мережу України, що призвело до відключення електроенергії для близько 300 тисяч споживачів на кілька годин.
2017	Використання програми-вимагача WannaCry: ця атака поширилася в травні 2017 року, використовуючи вразливість у системах Windows, що призвело до блокування доступу до даних на тисячах комп'ютерів по всьому світу .
2018	Витік даних готельної мережі Marriott: в 2018 році Marriott повідомив про витік персональних даних близько 500 мільйонів гостей, включаючи імена, адреси електронної пошти, номери телефонів та дані паспортів
2022	Кібератаки під час війни в Україні: починаючи з лютого 2022 року, росія здійснила серію кібератак на державні та приватні установи України, намагаючись дестабілізувати ситуацію та викрасти конфіденційну інформацію.
2024	В 2011 році мережа PlayStation зазнала масштабної кібератаки, в результаті якої були викрадені особисті дані 77 мільйонів користувачів, що призвело до тривалого припинення роботи мережі .

* Складено автором за: [40; 41].

Кібератаки на критичну інфраструктуру, таку як електромережі та водоочисні споруди, можуть викликати ланцюгову реакцію. Прикладом є російські атаки на українську енергомережу, через які мільйони людей залишилися без світла. Ці атаки, характерні для гібридної війни, викликають ефект доміно: лікарні виходять з ладу, системи виходять з ладу, транспорт зупиняється, паралізуючи суспільство в цілому. Злом конфіденційних даних з метою політичної дестабілізації – відомим прикладом є втручання Росії у вибори в США 2016 року. Кампанії з дезінформації, такі як просування маніпулятивного цифрового контенту, створюють розкол у суспільстві та заворушення [28].

Варто зазначити, що кіберзагрози та атаки стали невід'ємною частиною сучасних гібридних війн, відіграючи важливу роль у досягненні стратегічних цілей без застосування фізичної сили. Кіберпростір, на відміну від традиційних бойових полів, не має кордонів, що робить кібератаки

надзвичайно ефективними і важкими для виявлення. Кіберзброя, як правило, є доступною та відносно дешевою у виробництві, що дозволяє навіть малим країнам і неурядовим організаціям здійснювати кібератаки. Їхнє застосування стає особливо вигідним у контексті гібридної війни, оскільки кібератаки часто залишаються непомітними, але їхній вплив на критичну інфраструктуру може бути руйнівним і має широкомасштабні наслідки для суспільства.

Використання кіберзброї має низку переваг перед традиційними методами ведення війни: її низька вартість, здатність до тиражування та маневреність дозволяють здійснювати атаки на різноманітні об'єкти, від інфраструктури до політичних процесів. Приклади, такі як атаки на енергомережі України або втручання в політичні вибори, демонструють високий потенціал кіберзагроз для дестабілізації державних структур та маніпулювання громадською думкою.

Враховуючи швидкість, ефективність і відносну невидимість кіберзагроз, їх використання в гібридних війнах продовжить зростати, змінюючи природу конфліктів у майбутньому. Важливою складовою цих атак є не лише прямі технічні методи (злом, руйнування інфраструктури), а й психологічні операції, включаючи дезінформацію, що дозволяють посилити хаос і паніку серед цивільного населення [17].

Отже, кібератаки стали ключовим інструментом у сучасних гібридних війнах, де фізичні кордони та традиційна військова сила поступаються місцем цифровим загрозам. Кіберпростір перетворився на нове поле бою, на якому навіть невеликі держави чи недержавні актори можуть здійснювати високоефективні, масштабні й часто анонімні атаки на супротивника. Кіберзагрози дедалі частіше застосовуються у поєднанні з іншими елементами гібридної війни – економічними, політичними та інформаційними атаками. Це створює комплексний, багатовимірний тиск на противника, який важко ідентифікувати і ще складніше ефективно відбити.

2.3. Політичні, економічні та військові аспекти гібридних війн

Гібридна війна є складним та багатогранним конфліктом, що поєднує різні елементи: військові, політичні, економічні та інформаційні операції. Ці аспекти взаємопов'язані та використовуються комплексно, щоб досягти стратегічних цілей, при цьому мінімізуючи відкриту військову агресію і значні фізичні втрати. Головна мета гібридної війни полягає в тому, щоб підривати стабільність держави або її союзників, використовуючи різні види впливу [29]. Політика є центральним елементом гібридних війн, оскільки метою є не лише збройне протистояння, але й формування політичної волі, переконання урядів або суспільств змінити свої рішення чи поведінку [30].

Радикальні зміни у світі призводять до хворобливих процесів, які шукають або переглядають їхню внутрішню- та зовнішньополітичну ідентичність, доречність участі та місце в міжнародних інтеграційних організаціях. У деяких регіонах, особливо в Євразійському регіоні, є конкуренція інтеграційних проєктів. Ці процеси призводять до складних змін у міжнародних організаціях: послаблення або розпаду старих альянсів, спроб зміцнення існуючих або створення нових. На нашу думку, суть гібридного політичного конфлікту полягає в широкому застосуванні інформаційних, політичних, економічних та гуманітарних засобів поряд із прихованими військовими діями.

Зазначимо, що «гібридна війна» поєднує в собі методи інформаційної, психологічної, економічної війни та культурної експансії. Якщо в класичних війнах боротьба велася за багатство і території, то в нетрадиційних «гібридних війнах» ворог має на меті домінувати в суспільній свідомості громадян країни, змінити цінності та культурні основи народу, спотворити його історичну пам'ять. Конфлікти на міжнародній арені відбуваються у фізичному, інформаційному, кібернетичному, культурно-когнітивному вимірах, постійно зростає роль невійськових методів досягнення політичних і стратегічних цілей, які поступаються за ефективністю традиційним військовим методам

(що виключає активне використання останніх). Гібридна війна є сучасною формою конфлікту, що об'єднує військові, політичні, економічні та інформаційні компоненти для досягнення стратегічних цілей, при цьому мінімізуючи відкриту військову агресію та фізичні втрати. Її мета полягає не лише в збройному протистоянні, а й у використанні різних методів впливу на внутрішню і міжнародну політику, підриві стабільності держави або її союзників [1].

Політичні аспекти гібридної війни включають інформаційні та психологічні операції, маніпулювання масовою свідомістю, дезінформацію та пропаганду. Вони спрямовані на зміщення політичних лідерів, послаблення довіри до урядів та створення внутрішніх криз. Важливу роль відіграють економічні санкції, які використовуються для зміни поведінки агресора та досягнення мирного врегулювання конфлікту. Міжнародні санкції стали ключовим інструментом зовнішньополітичного впливу, зокрема у відповіді на російську агресію проти України.

Економічні аспекти гібридної війни спрямовані на послаблення економіки противника через знищення її фінансової стабільності, інфраструктури та вплив на соціальне становище населення. Санкції, економічні блокади та інші засоби економічного тиску використовуються для порушення стабільності ворожих держав, що сприяє їхній ослабленості та змушує до політичних змін.

Військові аспекти гібридних війн не обмежуються традиційними збройними конфліктами, а включають також використання «сірих зон» війни, де агресор застосовує невизнані або неофіційні збройні формування. Спеціальні операції, саботаж, тероризм та кібер-атаки також стають важливими компонентами військової стратегії, що дозволяють знищити важливу інфраструктуру або викрасти стратегічну інформацію без фізичних бойових дій. Більшість експертів мають спільне бачення: у цій концепції своє місце у світовій та регіональній політиці знайшло унікальне нове явище: концепція гібридних політичних конфліктів дає якісно новий погляд на

сучасну реальність і є унікальним феноменом [1].

Політичний вплив і маніпуляція виражається через:

- використання внутрішніх і міжнародних каналів для поширення дезінформації або пропаганди. Це може бути спрямоване на зміщення політичних лідерів, підриг довіри до урядів або створення сприятливих умов для політичних змін;
- створення внутрішніх політичних криз, заворушень чи революцій, що може включати підбурювання соціальних протестів, підтримку опозиційних сил або організацію антивладних рухів;
- вплив на міжнародну громадськість або інші держави через дипломатичні канали, зокрема через застосування економічних санкцій або формування альянсів, які підтримують або визнають агресивні дії в межах міжнародних організацій (ООН, ЄС, НАТО).

Санкції є важливим зовнішньополітичним інструментом, який уряди та міжнародні організації використовують для впливу на репресивні режими. Останнім часом велика увага в громадських, наукових та експертних колах приділяється питанню про те, наскільки ефективно діють міжнародні санкції, введені проти російської федерації багатьма провідними урядами та міжнародними організаціями. Ці санкції після незаконної анексії Кримського півострова та, зокрема, широкомасштабного вторгнення російських військ на територію України 24 лютого 2022 р., стосуються як окремих осіб, так і економіки, фінансової системи, торгівлі, логістики, імпорту та експорту товарів та інших сфер діяльності країни-агресора. Запроваджені санкції створили відчутний економічний стимул для розрядки конфлікту та забезпечення його подальшого врегулювання. Економічні санкції часто стають єдиним альтернативним методом для міжнародної спільноти та окремих урядів у відповідь на насильство.

Система санкцій стала одним із ключових інструментів впливу окремих урядів і міжнародних організацій на поведінку агресора на міжнародній арені. Санкції розглядаються як превентивні та обмежувальні заходи, які дозволяють

відповісти на політичні виклики, які суперечать цілям і цінностям держав, які їх впроваджують. Часто санкції запроваджуються поетапно: спочатку заборона на видачу віз і заморожування активів щодо певного списку осіб, а потім галузеві економічні санкції (щодо окремих галузей чи компаній). Посилення санкцій відбувається через значне зростання загрози національній безпеці та/або загострення ситуації [2].

Важливо відзначити, що гібридна війна стала частиною сьогоденної реальності, сприяючи значним змінам у всіх сферах: економічній, політичній, військовій, соціальній та інших. Слід також зазначити, що на початку російського наступу відбулися деструктивні процеси: руйнування інфраструктури, гуманітарна криза в процесі, значні соціальні втрати. Зазначимо, що РФ через збройний напад частково втратила можливість експортувати в Україну та на зовнішні ринки. Це надихнуло та практично змінило економічний ландшафт, що згодом дозволило країні адаптуватися та реорганізуватися до вимог війни [4].

Економічні стратегії гібридної війни спрямовані на те, щоб послабити економіку країни-супротивника, зламати її фінансову стабільність, а також вплинути на соціально-економічне становище населення. Гібридна війна, як різновид соціально-політичного конфлікту на міждержавному рівні, поступово розвивається як засіб маніпулювання масовою свідомістю, розпалювання суспільної ворожнечі, дезорганізації функціонування економіки, деформації демократичних процесів реалізації публічного права, дезорганізації публічної дипломатичної системи.

До невійськових форм боротьби відносяться застосування тактики «керованого хаосу», посилення різними способами антинаціональних, антисоціальних рухів, сепаратистських рухів, застосування терористичної тактики, громадські повстання, силове захоплення адміністративних будівель. Військова фаза гібридної війни починається на піку соціального та політичного конфлікту, і її метою є змусити країну-жертву укласти мир з державою-агресором.

Політичні стратегії та адміністративні рішення, які можуть зміцнити національну безпеку перед викликами гібридної війни, спрямовані на збільшення та інтеграцію людського капіталу всієї держави, створення передумов для розвитку комплексної законодавчої, освітньої, інформаційної та збройних сил [18].

Сучасні війни – це за своєю суттю «війни нового (четвертого) покоління», які не є пропорційними. У цих війнах держава втрачає свою монопольну владу, оскільки з'являються інші впливові недержавні гравці. В асинхронному конфлікті беруть участь держави та недержавні актори, включаючи нерегулярні організації – незаконні збройні формування, терористичні групи, партизанські або повстанські елементи. Вони не визнають правових норм і діють поза межами міжнародного та національного права. У сучасному політичному процесі дедалі більшого поширення набувають асиметричні конфлікти.

Військові елементи гібридної війни зазвичай не обмежуються тільки традиційними військовими діями, а також включають інші форми військового втручання. Військові сили можуть бути використані не у повномасштабних конфліктах, а в обмежених, точкових діях. Це може включати «сірі зони» війни, де агресор використовує свої війська в одязі місцевих сил або неофіційних збройних формувань. Спецпідрозділи можуть проводити операції без широкого розголосу і без офіційного визнання країною свого втручання. Такі операції можуть включати саботаж, тероризм, атаку на ключову інфраструктуру або здійснення прихованих військових операцій.

Отже, гібридна війна стає значним викликом для сучасного світу, оскільки поєднує різні форми боротьби, включаючи невійськові методи впливу, що дозволяють досягти політичних та стратегічних цілей без прямого військового протистояння. Тому гібридні конфлікти не тільки змінюють природу війни, але й змушують держави адаптувати свої стратегії національної безпеки та міжнародні відносини до нових реалій.

РОЗДІЛ 3.

ОСОБЛИВОСТІ ГІБРИДНОЇ ВІЙНИ ЯК ЗАГРОЗИ

МІЖНАРОДНІЙ БЕЗПЕЦІ

3.1. Вплив гібридних війн на глобальну стабільність та мир

Гібридні війни, які поєднують традиційні військові дії з нетрадиційними методами, такими як інформаційні кампанії, економічний тиск та кібероперації, мають значний вплив на глобальну стабільність та мир. Ці конфлікти ускладнюють визначення агресора та жертви, що ускладнює міжнародну реакцію та посилює невизначеність на світовій арені.

Гібридні війни сприяють внутрішній дестабілізації держав, що може призводити до політичних криз, економічного занепаду та соціальних заворушень. Це, у свою чергу, може створювати сприятливе середовище для терористичних організацій та інших нелегітимних акторів. Гібридні конфлікти часто не відповідають традиційним уявленням про війну та мир. Вони можуть включати елементи, які важко класифікувати, що ускладнює реагування міжнародної спільноти та підтримує постійну напругу [42].

Використання нетрадиційних методів ведення війни може призводити до порушень міжнародного гуманітарного права, що ускладнює механізми міжнародного реагування та підтримує атмосферу безкарності. Гібридні війни можуть виявляти обмеження таких організацій, як ООН, НАТО та ОБСЄ, у забезпеченні миру та стабільності, оскільки їхні традиційні механізми реагування не завжди ефективні проти нетрадиційних загроз.

Активне використання дезінформації та пропаганди в рамках гібридних війн може призводити до поляризації суспільств, втрати довіри до традиційних ЗМІ та ускладнення міжнародного діалогу. Гібридні методи, такі як кібернапади на енергетичну інфраструктуру, можуть мати серйозні економічні наслідки, підриваючи економічну стабільність та безпеку держав. Економічні санкції, блокади та інші економічні заходи, застосовувані в рамках

гібридних війн, можуть мати тривалий негативний вплив на глобальну економіку, впливаючи на торгівлю, інвестиції та економічне зростання [43].

Невизначеність, спричинена гібридними загрозами, може змушувати держави збільшувати військові витрати, що відволікає ресурси від соціальних та економічних потреб. Розглянемо приклади гібридних війн, які демонструють, як гібридні війни можуть поєднувати різні методи впливу, створюючи комплексні загрози для міжнародної безпеки.

Гібридні війни породжують складності у визначенні того, що саме є актом агресії, що значно ускладнює міжнародну реакцію. Наприклад, економічні санкції або кібератаки часто не відповідають традиційним уявленням про війну, що ставить під сумнів ефективність існуючих міжнародних правових та безпекових механізмів. Це веде до глобальної невизначеності і посилення безкарності для агресорів.

Гібридні війни можуть стати причиною внутрішніх політичних криз, економічного занепаду та соціальних заворушень. Це створює сприятливе середовище для терористичних груп й інших нелегітимних акторів, що можуть скористатися ситуацією для досягнення своїх цілей. Постійні стреси, спричинені гібридними конфліктами, підривають соціальний порядок у країнах-учасницях таких війн. Використання нетрадиційних методів ведення війни, таких як інформаційні маніпуляції та кібератаки, часто супроводжується порушеннями міжнародного гуманітарного права. Це створює ситуацію безкарності для агресорів і посилює відчуття несправедливості серед жертв. Дезінформаційні кампанії також здатні значно підривати довіру до традиційних ЗМІ, поглиблюючи соціальну поляризацію в суспільствах.

Російська агресія проти України включає застосування військових сил, інформаційних кампаній, кібератак та економічного тиску для дестабілізації ситуації в Україні [44]. Застосування кібератак росії в Україні можна умовно поділити на два етапи. 1 етап (2014-2021 рр): початковий період конфлікту, коли росія активно застосовувала пропаганду, інформаційні кампанії, а також

здійснювала перші кібератаки, щоб підірвати стабільність в Україні. У цей час росія використовувала різноманітні методи, такі як підтримка сепаратистських рухів, поширення фальшивих новин, та кібератаки на критичні інфраструктурні об'єкти.

Після анексії Криму в 2014 р. росія розпочала підтримку сепаратистських угруповань на сході України, що призвело до тривалого конфлікту в Донбасі. Російські державні ЗМІ активно поширювали пропаганду та дезінформацію, спрямовану на підірив довіри до української влади та створення образу ворога. Це включало фальшиві новини, маніпуляції фактами та негативне висвітлення подій в Україні [41].

Російські державні ЗМІ активно поширювали пропаганду та дезінформацію, спрямовану на підірив довіри до української влади та на створення образу ворога. Росія активно використовувала такі методи, як: фальшиві новини: маніпуляції фактами для того, щоб спотворити події, що відбуваються в Україні, і подати їх у негативному світлі; росія інтерпретувала події таким чином, щоб нав'язати думку про порушення прав людини в Україні, жорстоке поводження з цивільними, а також незаконну діяльність української армії; російські ЗМІ активно розповсюджували повідомлення про «фашистський режим» в Україні, що мало на меті підірвати довіру громадськості до української влади та її міжнародних партнерів. Пропаганда була спрямована на те, щоб представити український уряд як ворога, а проросійські сепаратистські угруповання – як «борців за права людини» і «захисників місцевого населення». У грудні 2015 року російські хакери здійснили атаку на енергетичну компанію «Прикарпаттяобленерго», внаслідок якої близько 230 тисяч осіб залишилися без електропостачання на кілька годин. Це була перша відома атака на енергетичну інфраструктуру держави [45].

Кібератака включала злам комп'ютерних систем енергетичної компанії, що дозволило хакерам відключити лінії електропередач. Такий напад став частиною стратегії росії для дестабілізації не лише української енергетики, але

й економіки країни загалом. Цей інцидент засвідчив, наскільки вразливими можуть бути критичні інфраструктурні об'єкти, і підкреслив важливість розробки ефективних засобів захисту від кіберзагроз.

У червні 2017 р. була здійснена масштабна кібератака з використанням вірусу NotPetya, яка призвела до значних економічних втрат як в Україні, так і за її межами. Ця атака вважається однією з найбільших хакерських атак в історії [46]. NotPetya спочатку маскувався під звичайний вірус-вимагач, проте швидко проявився як більш складний інструмент знищення даних. Вірус уразив тисячі комп'ютерів по всьому світу, зокрема в Україні, де атакував банки, урядові установи та енергетичні компанії. За оцінками, економічні втрати від цієї атаки склали мільярди доларів. Це була не просто кібератака, а операція з метою максимального дестабілізування економіки України. Ця атака стала підтвердженням того, що Росія використовує кібератаки як основний інструмент гібридної війни проти України, зокрема для впливу на економіку та інфраструктуру. В цих умовах важливо відзначити, що Росія постійно використовувала гібридні методи впливу, зокрема інформаційні кампанії та кібератаки, що доводить значення технологічних інструментів у сучасних міжнародних конфліктах.

2 етап (2022 рік - теперішній час): після початку повномасштабного вторгнення Росії в Україну в 2022 р., кібератаки стали більш інтенсивними і складними. Вони стали частиною загальної стратегії ведення війни, включаючи атаки на державні установи та інфраструктуру, що сприяли ще більшому посиленню хаосу та невизначеності.

Російські хакерські групи здійснювали численні кібератаки на українські державні установи та інфраструктуру. Наприклад, у лютому 2022 р. було атаковано системи зв'язку газети «Kyiv Post» та супутникову мережу «KA-SAT». У грудні 2024 р. кібератака призвела до тимчасової зупинки державних реєстрів в Україні, що вплинуло на тисячі громадян [41].

У першій половині 2023 р. було зафіксовано 762 кібератаки, що більш ніж удвічі перевищує показники другої половини 2022 року. Водночас

кількість критичних інцидентів зменшилася на 81 %, що свідчить про покращення заходів з кіберзахисту [47].

У 2024 р. спостерігалось використання нових тактик, включаючи застосування генеративного ШІ для дезінформаційних кампаній, що ускладнювало виявлення фальшивих повідомлень. 19 грудня 2024 р. російські хакери атакували сайти Національних інформаційних систем та Міністерства юстиції України, що призвело до порушення роботи державних реєстрів [48].

Кібератаки росії на Україну демонструють комплексний підхід до ведення гібридної війни, поєднуючи різні методи впливу для досягнення стратегічних цілей. Це вимагає від України постійного вдосконалення своїх кіберзахисних можливостей та активної міжнародної співпраці для протидії таким загрозам.

На першому етапі росія започаткувала інфраструктурні та інформаційні атаки, що стали фундаментом для більш масштабного і більш агресивного використання таких методів на другому етапі. Після початку повномасштабного вторгнення в 2022 р., методи ведення гібридної війни значно змінилися: росія почала використовувати новітні технології, зокрема в галузі кіберзагроз та дезінформації. Кібератаки стали регулярною частиною бойових дій і використовуються для підриву національної безпеки України, як і в 2014 році, але з більшими масштабами та новими технічними підходами. Обидва етапи є частинами одного процесу – ескалації гібридної війни, де методи та інструменти, використані на першому етапі, значно вдосконалюються і адаптуються до нових реалій на другому етапі.

Отже, гібридні війни, які поєднують традиційні військові методи з нетрадиційними, мають серйозний і комплексний вплив на глобальну стабільність і мир. Зокрема, ці конфлікти стають складними для розуміння та реагування з боку міжнародної спільноти через невизначеність агресора і жертви. Це підвищує рівень напруженості та вразливості на світовій арені, оскільки традиційні механізми реагування (наприклад, за допомогою ООН або НАТО) не завжди ефективні проти нових форм загроз.

3.2. Стратегії протидії гібридним загрозам на міжнародному рівні

Гібридні війни є набагато складнішими і багатограннішими, ніж традиційні конфлікти. Вони використовують різноманітні інструменти впливу на держави та суспільства, включаючи інформаційні, економічні, кібернетичні і військові стратегії. Традиційні війни зосереджуються на відкритих бойових діях з чіткими цілями і визначеними результатами. Гібридна війна дає більше свободи для маневру, але має більший ризик ескалації та непередбачуваних наслідків. Гібридні загрози, які поєднують традиційні військові методи з нетрадиційними, такими як інформаційні кампанії, економічний тиск та кібероперації, вимагають комплексного підходу до протидії на міжнародному рівні [49].

Міжнародні організації, зокрема Європейський Союз, розробляють стратегії та нормативно-правові акти для боротьби з гібридними загрозами. З 2016 р. ЄС поглиблює відповідну нормативно-правову базу, включаючи окремі розділи Стратегії безпеки ЄС- 2020, присвячені боротьбі з гібридними загрозами.

Стратегія ЄС у боротьбі з гібридними загрозами передбачає наступне: основна відповідальність за боротьбу з гібридними загрозами лежить на державах-членах ЄС. Однак, коли загрози виходять за межі національних кордонів, відповідальність переходить до інституцій ЄС, таких як Європейська Комісія; для ефективної протидії гібридним загрозам були створені спеціалізовані органи, включаючи Центр досконалості з боротьби з гібридними загрозами, які координують зусилля та обмінюються інформацією між державами-членами; ЄС застосовує комплексний підхід до боротьби з гібридними загрозами, поєднуючи військові, цивільні, дипломатичні та економічні інструменти для досягнення стійкості та захисту своїх громадян.

ЄС активно співпрацює з іншими міжнародними організаціями, такими як НАТО, для обміну досвідом та кращими практиками у боротьбі з гібридними загрозами. Ця співпраця включає спільні навчання, розробку

стратегій та обмін інформацією для підвищення колективної безпеки. ЄС постійно вдосконалює свої стратегії та механізми для боротьби з гібридними загрозами, визнаючи їхню складність та багатогранність. Цей комплексний підхід, що включає спільну відповідальність, створення спеціалізованих структур та тісну співпрацю з міжнародними партнерами, сприяє зміцненню безпеки та стабільності як у Європі, так і в усьому світі [49].

Ефективна протидія вимагає тісної співпраці між державами, міжнародними організаціями та приватним сектором. Наприклад, НАТО та ЄС активно обмінюються інформацією та кращими практиками для посилення колективної стійкості до гібридних загроз. Спільною ініціативою НАТО та ЄС є створення Європейського центру передового досвіду з питань гібридних загроз (Hybrid CoE). Він надає підтримку персоналу обох організацій через семінари, робочі групи та навчання, спрямовані на покращення розуміння гібридних загроз. У травні 2017 р. Центр сприяв проведенню практикуму для опрацювання сценарію щодо «Захисту портів за умови гібридних загроз», організованого ЄС за участю персоналу з ЄС і НАТО.

У грудні 2024 р. НАТО оголосило про намір посилити обмін розвідданими та покращити захист критичної інфраструктури у відповідь на акти саботажу, пов'язані з росією та Китаєм. Міністри закордонних справ НАТО планують розробити нову стратегію для боротьби з гібридними загрозами, яка охоплюватиме широкий спектр тактик, включаючи пропаганду, політичне втручання, дезінформацію, саботаж критичної інфраструктури та інші методи, що виходять за межі традиційних військових дій. Ці ініціативи підкреслюють важливість спільних зусиль НАТО та ЄС у боротьбі з гібридними загрозами, забезпечуючи обмін знаннями, ресурсами та стратегіями для підвищення колективної безпеки [50].

Оскільки гібридні атаки можуть націлюватися на об'єкти критичної інфраструктури, важливо впроваджувати заходи для їх захисту. Це включає захист секторів транспорту та телекомунікацій від потенційних атак. Міжнародні організації, зокрема Європейський Союз, відіграють ключову

роль у розробці стратегій та нормативно-правових актів для боротьби з гібридними загрозами. З

2016 р. ЄС поглиблює відповідну нормативно-правову базу, включаючи окремі розділи Стратегії безпеки ЄС-2020, присвячені боротьбі з гібридними загрозами. Ці розділи окреслюють заходи з підвищення стійкості держав-членів до таких загроз, зокрема через обмін інформацією, спільні навчання та розробку спільних стандартів безпеки.

Ефективна протидія гібридним загрозам вимагає тісної співпраці між державами, міжнародними організаціями та приватним сектором. Наприклад, НАТО та ЄС активно обмінюються інформацією та кращими практиками для посилення колективної стійкості до гібридних загроз. Спільні навчання, такі як командно-штабні навчання CORE20, проводяться для вдосконалення координації дій та обміну досвідом у сфері захисту критичної інфраструктури від гібридних атак.

Оскільки гібридні атаки можуть націлюватися на об'єкти критичної інфраструктури, важливо впроваджувати заходи для їх захисту. Це включає захист секторів транспорту та телекомунікацій від потенційних атак. Критична інфраструктура, до якої входять енергетика, водопостачання, транспорт, телекомунікації, охорона здоров'я та фінансові послуги, є основою функціонування держави та суспільства. Атаки на ці об'єкти можуть призводити до значних економічних та соціальних наслідків.

Основні складові стратегії захисту критичної інфраструктури: координація зусиль органів влади, силових відомств та служб: спільна робота державних структур забезпечує швидке реагування на загрози та ефективне управління кризовими ситуаціями; співпраця між державними органами та приватними компаніями, які управляють більшістю об'єктів критичної інфраструктури, є ключовою для забезпечення безпеки та стійкості систем; створення платформ для обміну інформацією про потенційні загрози та кращі практики дозволяє оперативно реагувати на нові виклики та адаптувати стратегії захисту [51].

Важливою складовою є формування узгоджених стратегічних комунікацій для протидії дезінформації та викриття гібридних загроз. Це включає спільні зусилля держав-членів щодо реалізації ефективних комунікаційних стратегій. ЄС та НАТО активно обмінюються інформацією та кращими практиками для посилення колективної стійкості до гібридних загроз. Ця співпраця включає: спільні навчання та тренінги; організація спільних заходів для підвищення готовності до реагування на гібридні загрози; обмін розвідданими; координація зусиль для виявлення та нейтралізації дезінформаційних кампаній; розвиток стратегічних комунікацій ЄС.

ЄС постійно вдосконалює свої підходи до стратегічних комунікацій, враховуючи новітні виклики: використання сучасних цифрових платформ для поширення правдивої інформації та боротьби з дезінформацією; залучення технологічних компаній до спільної боротьби з фейковими новинами та маніпуляціями. ЄС активно протидіє російським дезінформаційним кампаніям, які намагаються дестабілізувати ситуацію в Європі [51].

Розвиток національної стійкості (резильєнтності) є ключовим елементом у протидії гібридним загрозам. Це включає оцінку та зміцнення потенціалу держави для реагування на різні види загроз [52].

SWOT-аналіз дає змогу більш чітко визначити стратегічні напрямки для міжнародної протидії гібридним загрозам. SWOT-аналіз є потужним інструментом для порівняння гібридної війни з традиційними формами конфліктів. Він дає можливість чітко оцінити сильні та слабкі сторони, можливості та загрози кожного з типів війни, що є важливим для розробки стратегій протидії гібридним загрозам на міжнародному рівні. Гібридна війна має переваги в непередбачуваності, використанні різних форматів та мінімізації прямих бойових дій, тоді як традиційна війна характеризується чітко визначеними цілями та міжнародним правовим визнанням.

Європейський Союз активно вдосконалює стратегії безпеки та створює нормативно-правову базу для боротьби з гібридними загрозами. Це включає спеціалізовані органи, такі як Центр досконалості з боротьби з гібридними

загрозами, а також використання комплексного підходу, що поєднує військові, цивільні, дипломатичні та економічні інструменти [51].

Для ефективної протидії необхідна тісна співпраця між державами, міжнародними організаціями та приватним сектором. Наприклад, НАТО та ЄС обмінюються інформацією та кращими практиками для підвищення колективної стійкості.

Гібридні атаки можуть націлюватися на об'єкти критичної інфраструктури, тому важливо забезпечити їх захист. Це включає координацію зусиль державних органів та приватних компаній, що управляють критичними об'єктами. Стратегії стратегічних комунікацій, зокрема боротьба з дезінформацією та викриття гібридних загроз, є важливою складовою протидії. ЄС та НАТО активно працюють над вдосконаленням цих стратегій, включаючи використання цифрових платформ для боротьби з фейковими новинами. Ключовим елементом є розвиток національної стійкості, що включає оцінку та зміцнення потенціалу держави для реагування на різні види загроз.

Гібридні загрози є складними і багатограними, тому протидія їм вимагає комплексного підходу, що включає співпрацю між різними державами, міжнародними організаціями та приватним сектором. Використання новітніх технологій, спільні навчання, обмін інформацією і ресурсами є важливими аспектами ефективної боротьби з цими загрозами. Таким чином, успішна стратегія протидії гібридним загрозам повинна ґрунтуватися на тісній міжнародній співпраці, зміцненні стійкості та розвитку стратегічних комунікацій для виявлення та нейтралізації цих загроз.

SWOT-аналіз є ефективним інструментом для порівняння гібридної війни з традиційними формами конфліктів (Табл.3.1.). Він дозволяє оцінити сильні та слабкі сторони, можливості та загрози кожного типу війни, що є важливим для розробки стратегій протидії гібридним загрозам на міжнародному рівні [47].

Таблиця 3.1

**Порівняння гібридної й традиційної війн
за допомогою SWOT-аналізу***

Ключові фактори	Гібридна війна	Традиційна війна
Сильні сторони	Невизначеність, мультиформатність, мінімізація прямих бойових дій	Чітка мета, міжнародне правове визнання
Слабкі сторони	Розмита мета, важкість контролю, ризик ескалації	Високі витрати, великі людські втрати, масштабність
Можливості	Використання новітніх технологій, зменшення витрат	Завершення через перемогу або мир, можливість формування альянсів
Загрози	Противагресія з боку міжнародної спільноти, внутрішня напруженість, невизначеність результатів	Ескалація в глобальну війну, міжнародна ізоляція, зруйнування інфраструктури

* Складено автором

Гібридна війна і традиційна війна відрізняються значно за методами, цілями та впливом на держави і суспільства. Гібридна війна є більш «непрямою», використовуючи низку інструментів, таких як кібератаки, інформаційні війни та підривні дії, в той час як традиційні війни зосереджуються на відкритих бойових діях і чітких геополітичних цілях. Кожен тип конфлікту має свої переваги та ризики, що визначають можливу стратегію та способи реагування на агресію.

Традиційні війни передбачають великі відкриті бойові дії між державами, які використовують регулярні армії та традиційну зброю. Вони здійснюються в рамках міжнародних угод і стандартів, таких як Женевські конвенції, з чітким визначенням ліній фронту. У гібридних війнах крім традиційних військових дій активно використовуються економічні санкції, кібератаки, інформаційні війни, тероризм, маніпуляція громадською думкою та інші нестандартні методи впливу на супротивника. В традиційних війнах країни відкрито визнають свою участь у конфлікті, а бойові дії відбуваються

на визначених фронтах. Натомість у гібридних війнах одна зі сторін може уникати офіційного визнання своєї участі, використовуючи проксі-сили (сепаратистів чи терористичні групи) або маскуючи свої дії через кібератаки чи пропаганду, що значно ускладнює виявлення та ідентифікацію агресора [49].

Традиційні війни мають чітко визначену мету – територіальне завоювання або виграш битви. Вони завершуються миром або перемир'ям, що призводить до встановлення умов мирного врегулювання. Гібридні війни, у свою чергу, часто не мають конкретної мети, що пов'язана з територією, і можуть тривати багато років, орієнтуючись на створення нестабільності, підриг довіри до політичних інститутів, контроль за інформацією, зміщення урядів та інші непрямі цілі. Завершення таких конфліктів часто є неясним, з відсутністю чіткої перемоги. Традиційні війни зазвичай мають конкретний початок і кінець, часто після підписання мирних угод або перемир'я. Гібридні конфлікти, навпаки, можуть продовжуватися роками або навіть десятиліттями, переходячи в заморожену фазу або перетворюючись на тривалу боротьбу за вплив, де немає чіткої перемоги і відсутня офіційна завершена стадія [39].

SWOT-аналіз відмінностей між гібридною та традиційною війною показує ключові переваги і ризики обох типів конфліктів:

- 1) сильні сторони гібридної війни – мультиформатність, непередбачуваність та мінімізація прямих бойових дій, що дозволяє зберегти ресурси і уникнути великих втрат;
- 2) слабкі сторони гібридної війни – розмита мета та складність контролю, що може призвести до ескалації конфлікту чи внутрішньої напруженості;
- 3) можливості гібридної війни – використання новітніх технологій для дезінформації, зменшення витрат на великі військові кампанії;
- 4) загрози гібридної війни – потенційна протидія з боку міжнародної спільноти, внутрішні соціальні чи політичні конфлікти в агресора;

5) для традиційних війн характерні чітка мета і міжнародне правове визнання, але вони супроводжуються високими витратами, масштабними людськими втратами і можуть призвести до ескалації в глобальний конфлікт.

Отже, гібридні загрози, що поєднують військові, інформаційні, кібернетичні та економічні інструменти, формують багаторівневий виклик, який неможливо нейтралізувати суто силовими засобами. SWOT-аналіз підтверджує, що хоча гібридна війна володіє перевагами мультимедійності й непередбачуваності, її слабкість полягає у розмитості цілей і високому ризику ескалації, що може бути мінімізовано завдяки згуртованим міжнародним діям і прозорості. Відтак успішна стратегія протидії гібридним загрозам на міжнародному рівні повинна базуватися на постійній взаємодії держав і організацій, синхронізації ресурсів, посиленні інформаційної стійкості та безперервному вдосконаленні нормативної й технологічної основи колективної безпеки.

3.3. Перспективи протидії гібридним війнам і виклики для міжнародного права

Гібридні війни, як змішання традиційних і нетрадиційних методів ведення конфліктів, є значною загрозою для сучасної міжнародної безпеки. Вони використовують різноманітні інструменти, зокрема кібератаки, економічні санкції, пропаганду, тероризм, маніпуляцію інформацією та інші методи, що ускладнюють визначення агресора і правила ведення війни.

Зі зростанням технологій та цифрових платформ, зокрема соціальних мереж, кібератаки, а також використання штучного інтелекту для пропаганди, гібридні війни стають все складнішими. Атаки можуть бути здійснені з використанням новітніх технологій, таких як кібератаки, дронів, маніпуляція

даними через соціальні мережі, що дозволяє агресору уникати прямих зіткнень і зберігати більшу анонімність.

Крім класичних стратегій ведення війни, гібридні конфлікти дедалі частіше адаптуються до нових форм протистояння, зокрема між державами та недержавними акторами, такими як терористичні організації, радикальні політичні угруповання, приватні військові компанії або навіть окремі хакерські угруповання. Завдяки цьому конфлікти набувають асиметричного характеру, де традиційні армії стикаються з невидимими, розпорошеними і часто транснаціональними супротивниками. Такий підхід ускладнює ідентифікацію реального агресора, перешкоджає ефективному застосуванню міжнародного права та унеможливлює швидке реагування з боку міжнародних організацій, таких як ООН або НАТО [47].

Гібридна війна дозволяє державам діяти опосередковано: замість відкритої інтервенції вони можуть підтримувати лояльні сили або використовувати інструменти впливу для досягнення стратегічних цілей. До таких інструментів належить фінансування сепаратистських рухів, створення або підтримка озброєних формувань під прикриттям цивільного населення, вплив через інформаційні операції та економічний тиск. Такі дії можуть супроводжуватися кібератаками на критичну інфраструктуру, що підсилює ефект дестабілізації без застосування класичних військових засобів.

Особливу загрозу становлять інформаційні війни – кампанії дезінформації та пропаганди, спрямовані на деморалізацію населення, підриг довіри до уряду або створення політичного хаосу. Через маніпулювання масовою свідомістю агресор може досягти серйозних політичних результатів без жодного пострілу.

Гібридні війни часто спрямовані на створення «заморожених конфліктів» – ситуацій, у яких немає чіткої лінії фронту, але постійно зберігається напруження і нестабільність. Такі конфлікти складно вирішити дипломатичним шляхом, адже їхній характер розмитий, а сторони часто діють через посередників або під прикриттям. Яскравими прикладами таких

сценаріїв є ситуація на сході України, конфлікт у Сирії або протистояння в Лівії [36].

Таким чином, гібридні війни не лише змінюють форму сучасних конфліктів, а й розширюють можливості агресії без формального оголошення війни, що суттєво ускладнює роботу систем колективної безпеки й потребує нових механізмів реагування з боку міжнародної спільноти.

Гібридні війни часто проводяться з використанням проксі-акторів, таких як терористичні організації, або ж мають невизначеність щодо того, хто є агресором. Оскільки гібридна війна поєднує різноманітні засоби впливу, такі як кібератаки, інформаційні війни та економічний тиск, міжнародні правові норми, які традиційно регулюють лише відкриті бойові дії, можуть бути неефективними у таких умовах. Гібридні війни часто вимагають нових підходів до міжнародного гуманітарного права. Зокрема, питання щодо захисту цивільного населення, яке може стати жертвою економічних санкцій, кібератак або інформаційних маніпуляцій, не завжди чітко врегульовані міжнародним правом. Багато аспектів, наприклад, обмеження використання інформаційних технологій у війні чи захист від кібератак на критичну інфраструктуру, ще не отримали достатньої правової регуляції.

Сучасні угоди та протоколи, такі як Женевські конвенції, не враховують багато аспектів, характерних для гібридних війн, таких як кібератаки чи пропаганда. Міжнародне право потребує модернізації, щоб врахувати нові форми агресії, що використовуються у гібридних конфліктах, і забезпечити ефективний захист цивільного населення та інфраструктури.

Міжнародне право повинно бути невідкладно адаптоване до нових реалій сучасних конфліктів, у яких дедалі важливішу роль відіграють кібератаки, інформаційні війни, дезінформаційні кампанії та інші інструменти гібридної агресії. Традиційні норми міжнародного гуманітарного права, зосереджені переважно на фізичному збройному конфлікті, виявляються недостатніми для ефективного регулювання цифрового та інформаційного простору. Саме тому виникає нагальна потреба у створенні нових

міжнародних угод, нормативних актів і протоколів, які чітко визначатимуть відповідальність за кібератаки, маніпуляції громадською думкою, втручання у вибори та інші форми гібридної агресії.

Ці документи повинні охоплювати питання атрибуції кібератак (тобто встановлення, хто несе за них відповідальність), встановлення чітких критеріїв визнання таких дій актом агресії, а також регламентацію дій у відповідь у межах міжнародного права. Важливо також створити механізми моніторингу й оперативного обміну інформацією між державами, оскільки сучасні загрози можуть розвиватися блискавично і охоплювати кілька країн одночасно [36].

Розширення міжнародної співпраці є критично важливим для ефективної протидії гібридним загрозам. Організації, такі як ООН, НАТО, Європейський Союз, повинні активізувати зусилля у напрямку розробки єдиних стандартів кібербезпеки, створення спільних структур для реагування на надзвичайні ситуації у кіберпросторі, а також розвитку механізмів колективного захисту.

Одним із прикладів такого підходу є ініціатива НАТО щодо розширення концепції «п'ятого домену війни» – кіберпростору, який визнається таким самим важливим, як суша, повітря, вода та космос. Однак, ефективна боротьба з гібридними загрозами неможлива без залучення приватного сектору, зокрема великих технологічних компаній, які володіють критичною інфраструктурою і платформами поширення інформації. Компанії, що керують соціальними мережами, пошуковими системами та хмарними сервісами, повинні співпрацювати з урядами для виявлення і протидії фейкам, шкідливому ПЗ та кампаніям іноземного впливу. Водночас така співпраця має здійснюватися з дотриманням прав людини та свободи слова.

У майбутньому міжнародна спільнота повинна зосередитися на створенні ефективної архітектури цифрової безпеки, яка враховує як технічний, так і правовий виміри гібридної загрози. Лише через системний підхід і глобальну координацію можна забезпечити належний захист від нових форм конфліктів, що все більше визначають характер міжнародної безпеки у

XXI столітті [33].

Спільні зусилля міжнародної спільноти, урядів, міждержавних організацій і приватного сектору мають вирішальне значення для формування сучасної системи захисту від нових форм агресії, характерних для гібридних війн. Тільки об'єднавши зусилля, можна створити універсальні стандарти, здатні регулювати питання кібербезпеки, боротьби з дезінформацією та іншими інструментами впливу, що активно використовуються у гібридних конфліктах.

Необхідним кроком є розробка нових міжнародних механізмів моніторингу, попередження і реагування на гібридні загрози. Такі механізми повинні включати автоматизовані системи виявлення кібератак, платформи обміну інформацією між державами та компаніями, а також спеціалізовані аналітичні центри (наприклад, кіберкомандування при ООН або регіональні центри кібероборони при ЄС чи НАТО), які зможуть оперативно аналізувати загрози та координувати дії у відповідь.

Особливої уваги потребує створення єдиного протоколу реагування на кіберінциденти, який буде обов'язковим для підписантів міжнародних угод. У разі атаки він дозволить оперативно активувати відповідні структури, запровадити захисні заходи та, у разі потреби, притягти винних до відповідальності згідно з нормами міжнародного права. Це значно зменшить час реакції на загрози та дозволить запобігати їх ескалації. Крім того, важливим елементом ефективного реагування на гібридну агресію є розвиток спільних навчань, симуляцій та тренінгів, у яких братимуть участь представники держав, приватного сектору та громадських організацій. Такий міжсекторальний підхід дозволяє враховувати різні точки зору, покращує комунікацію та сприяє створенню більш гнучких і практичних стратегій реагування [31].

Ще одним перспективним напрямом є використання штучного інтелекту та машинного навчання для моніторингу інформаційного простору з метою виявлення дезінформаційних кампаній, фейків і спрямованого інформаційного

впливу на суспільство. Ці технології можуть стати ключовими інструментами в ранньому виявленні загроз і запобіганні дестабілізаційним процесам.

Отже, гібридні війни створюють нові виклики для міжнародного права, оскільки традиційні інструменти регулювання збройних конфліктів не завжди можуть бути застосовні до цих новітніх форм агресії. Тому для ефективної протидії гібридним загрозам необхідно адаптувати міжнародні норми, створити нові механізми моніторингу та посилити співпрацю між державами та міжнародними організаціями. Це дозволить зміцнити глобальну безпеку та забезпечити відповідну правову реакцію на сучасні загрози. Лише шляхом широкої, скоординованої та технологічно підкріпленої співпраці можливо сформувати ефективну систему колективної безпеки, здатну не тільки протистояти сучасним гібридним загрозам, а й попереджати їх ще на етапі планування. Формування таких систем повинно стати пріоритетом для світової спільноти у найближчі роки.

ВИСНОВКИ

В результаті проведеного дослідження можна зробити такі висновки.

Гібридна війна є новітньою формою збройного протистояння, що поєднує воєнні та невоєнні методи ведення конфлікту, зокрема збройну агресію, інформаційні атаки, кібератаки, економічний тиск, політичні диверсії, що дозволяє агресору досягати стратегічних цілей без формального оголошення війни.

Основні інструменти гібридної війни включають інформаційні операції, пропаганду, дезінформацію, кібератаки, використання нерегулярних збройних формувань, втручання у внутрішню політику країни-жертви. Вони спрямовані на підрив стабільності, довіри до влади та деморалізацію суспільства.

Кібератаки є ключовим елементом гібридної агресії. Їхніми цілями стають критична інфраструктура, системи управління, електромережі, банківська сфера та державні установи. Такі атаки дозволяють завдати значної шкоди без фізичної присутності противника.

Інформаційна складова гібридної війни має потужний деструктивний потенціал. Пропаганда, фейки, медіа-маніпуляції сприяють формуванню вигідних агресору наративів, розколу суспільства, дестабілізації політичної ситуації та створенню умов для внутрішнього конфлікту.

Політичні аспекти гібридної війни включають інформаційні та психологічні операції, маніпулювання масовою свідомістю, дезінформацію та пропаганду. Вони спрямовані на зміщення політичних лідерів, послаблення довіри до урядів та створення внутрішніх криз. Економічні аспекти гібридної війни спрямовані на послаблення економіки противника через знищення її фінансової стабільності, інфраструктури та вплив на соціальне становище населення. Військові аспекти гібридних війн не обмежуються традиційними збройними конфліктами, а включають також використання «сірих зон» війни, де агресор застосовує невизнані або неофіційні збройні формування.

Гібридні війни підривають засади міжнародної безпеки, створюючи нові

виклики для традиційних механізмів реагування. Вони змінюють уявлення про війну, стираючи межу між миром і збройним конфліктом, та ускладнюють правову кваліфікацію агресії.

Ефективна протидія гібридним загрозам вимагає комплексної стратегії, яка передбачає зміцнення інформаційної, кібернетичної, економічної, правової та військово-політичної безпеки. Необхідне удосконалення міжнародного права, розвиток механізмів колективної безпеки та міжнародної кооперації.

Російська агресія проти України є яскравим прикладом гібридної війни. Росія використовує як класичні збройні сили, так і кіберзагрози, пропаганду, економічний тиск, порушуючи основні принципи міжнародного права. Україна, попри складні умови, демонструє приклад стійкості, спротиву та міжнародної солідарності.

Гібридні війни створюють нові виклики для міжнародного права, оскільки традиційні інструменти регулювання збройних конфліктів не завжди застосовні до цих новітніх форм агресії. Тому для ефективної протидії гібридним загрозам необхідно адаптувати міжнародні норми, створити нові механізми моніторингу та посилити співпрацю між державами та міжнародними організаціями. Це дозволить зміцнити глобальну безпеку та забезпечити відповідну правову реакцію на сучасні загрози.

Гібридна війна потребує постійної адаптації механізмів безпеки. Успішна протидія можлива лише за умов активної взаємодії держав, міжнародних організацій, ЗМІ та громадянського суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Березовська-Чміль О., Кобець Ю. Політичний конфлікт гібридного типу: глобальний та регіональний виміри. *Sociology grani*. 23 (8) 2020. file:///C:/Users/1/Downloads/1545-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-2833-1-10-20201109%20(1).pdf (дата звернення: 14.03.2025).
2. Бобровицький А., Гавриленко Н., Гончарук А., Широкий І. Ус, Г., Юлдашев Р. Міжнародні санкції як інструмент стримування російської агресії проти України : аналіт. доп. Київ : НІСД, 2023. 76 с.
3. Буряченко О. Гібридна війна як нова форма глобального протистояння. *Наукові праці Міжрегіональної академії управління персоналом*. Політичні науки та публічне управління Випуск 2 (74), 2024. С. 24–32.
4. Возняк С. М., Демешок О. О., Андріянова Н. М., Шпура М. І. Економічні аспекти ведення гібридної війни. URL: <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/237/6407/13259-1?inline=1> (дата звернення: 14.03.2025).
5. Гібридна війна. *Велика Українська Енциклопедія*. URL: https://vue.gov.ua/%D0%93%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0 (дата звернення: 14.03.2025).
6. Гібридна війна – нові загрози, складність і «довіра» як антидот. URL: <https://www.nato.int/docu/review/uk/articles/2021/11/30/gbridna-vjna-nov-zagrozi-skladnst-dovra-yak-antidot/index.html> (дата звернення: 14.03.2025).
7. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України*. 2015. № 1. С. 136–141.
8. Горбуліна В. П. Світова гібридна війна: український фронт : монографія. К. : НІСД, 2017. 496 с.

9. Горбуліна В.П. Світова гібридна війна: український фронт: монографія. Київ: Національний інститут стратегічних досліджень, 2017. 494 с.
10. Грабовський С. Гібридна війна: історія і сутність. До постановки питання. *Вісник Київського національного університету імені Тараса Шевченка*. Українознавство. 2016. Вип. 1. С. 19–22.
11. Гребенюк А. Пропаганда: метод спеціальних інформаційних операцій чи акту зовнішньої інформаційної агресії? Наукові праці Національної бібліотеки України ім. В. І. Вернадського. 2022. Вип. 63. С. 65–74.
12. Дембіцький С., Злобіна О., Костенко Н. та ін. Українське суспільство в умовах війни. Колективна монографія. НАН України, д. філос. н. Є. Головахи, д. соц. н. С. Макеева. Київ: Інститут соціології НАН України, 2022. 410 с.
13. Денисюк Ж.З. Пропаганда та контрпропаганда в контексті стратегій державної інформаційної політики. *Механізми публічного управління*. Том 32 (71) № 2 2021. С. 46–52.
14. Дерев'янка І. П. Гібридна війна як різновид асиметричних дій. *Міжнародні відносини: теоретико-практичні аспекти*, (11), 2023. С. 6–16.
15. Десять найбільших кібератак в історії. URL: <https://itedu.center/ua/blog/top/10-najbilshix-kiberatak-v-istori%D1%97/?srsltid=AfmBOopglpdw8-AEcPI-Qvt3IkK6UQihSNQl04doj05WcQ3eeZkL6KmO> (дата звернення: 14.03.2025).
16. Довідник НАТО. URL: <https://www.nato.int/docu/other/ukr/handbook2001.pdf> (дата звернення: 14.03.2025).
17. Драбюк С.С. Пропаганда та її види. Шляхи протидії пропаганді. URL: <https://app-journal.in.ua/wp-content/uploads/2022/05/30.pdf> (дата звернення: 14.03.2025).
18. Єнін М. Н. Гібридна війна як різновид соціально-політичних конфліктів: сутність, технології, домінуючі дискурси. *Актуальні проблеми*

філософії та соціології : Науково-практичний журнал; Міністерство освіти і науки України ; Національний університет «Одеська юридична академія». Одеса, 2019. Вип. 25. С. 102–112.

19. Жадька В. О., Харитоненко О. І., Полтавець Ю. С. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник. Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. 356 с.

20. Кібератака на державні реєстри. URL: <https://texty.org.ua/fragments/114110/najmasshtabnisha-kiberataka-rosijskyh-hakeriv-na-derzhavni-reyestry-ukrayiny-yaki-dani-pid-zahrozoyu/> (дата звернення: 14.03.2025).

21. Кібератаки російської федерації. Хронологія. URL: <https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html> (дата звернення: 14.03.2025).

22. Кобець Т. Порівняльний аналіз технологій пропаганди та інформаційних операцій в умовах воєнного стану. URL: https://www.researchgate.net/publication/378789686_PORIVNALNIJ_ANALIZ_TEHNOLOGIJ_PROPAGANDI_TA_INFORMACIJNIH_OPERACIJ_V_UMOVAN_VOENNOGO_STANU (дата звернення: 14.03.2025).

23. Аналіз документів. URL: https://www.kiis.com.ua/?lang=ukr&cat=content_analysis (дата звернення: 14.03.2025).

24. Концепція «гібридної» війни та її складові. URL: <https://censs.org/concept-of-hybrid-warfare-and-its-components/> (дата звернення: 14.03.2025).

25. Копчак Ю., Лобунець Т., Луковський Р. SWOT-аналіз як важливий інструмент у розробці стратегії бізнесу. *Економіка та суспільство*, (61). 2024. URL: <https://doi.org/10.32782/2524-0072/2024-61-146> (дата звернення: 14.03.2025).

26. Кундеус О.М. Теоретичні аспекти гібридної війни РФ проти України. *Регіональні студії*. Ужгород, Видавничий дім «Гельветика». Вип. 20. 2020. С.120-124.

27. Лисецький Ю.М. Гібридні війни. Компоненти та особливості. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління. Том 32 (71) № 5. 2021. С. 63–72.*

28. Лук'янова Л. Аналіз документів як психолого-педагогічна процедура. URL: <https://lib.iitta.gov.ua/id/eprint/7538/1/%D0%9A%D0%BE%D0%BD%D1%82%D0%B5%D0%BD%D1%82-%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7.pdf> (дата звернення: 14.03.2025).

29. Лукашенко А.І. Ментальні структури агресора в інформаційній війні на прикладі російської федерації: погляд із минулого в сучасність, виклики західному суспільству. *Збірник наукових праць «Гілея»*. 2019. Вип. 144. С. 72–75.

30. Мідттун Г. П. Битва умів. Гібридна війна – це вплив на людей, з метою підвести їх до свідомого чи несвідомого вибору, корисного для агресора. 2020. URL: <https://surl.li/imtsxd/> (дата звернення: 14.03.2025).

31. Міжнародний досвід протидії гібридним загрозам: законодавче регулювання та організації з питань стратегічних комунікацій. URL: <https://infocenter.rada.gov.ua/uploads/documents/29377.pdf> (дата звернення: 14.03.2025).

32. Назаров М. Національна стійкість України: від концептуальних засад до практичної реалізації. *Політикус*, 2, 2023. С. 64–69.

33. Пирожков С. І., Майборода О. М., Хамітов Н. В., Головаха Є. І., Дембіцький С. С., Смолій В. А., Скрипнюк О. В., Стоєцький С. В. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь/ Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. Київ, 2022. 552 с.

34. Птешачник Я. Війна Росії проти України: хронологія кібератак. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI%282022%29733549_XL.pdf (дата звернення: 14.03.2025).

35. Рижук О. Поняття інформаційних та гібридних війн в умовах

глобалізації. Інформаційні війни. URL: <https://social-science.uu.edu.ua/article/1389> (дата звернення: 14.03.2025).

36. Свиридчук Ю. В Україні зафіксували майже 4 000 кібератак з боку РФ. 2023. URL: <https://suspilne.media/619941-v-ukraini-zafiksuvali-majze-4-000-kiberatak-z-boku-rf/> (дата звернення: 14.03.2025).

37. Ситник Г. П. Філософія війни та миру: курс лекцій. К: ТОВ САК ЛТД, 2023. 118 с.

38. Тарасюк В. Застосування інформаційних технологій в умовах гібридної війни: Монографія. Beau Bassin: Globe Edit, 2020. С. 59–60.

39. Тартачний О. Російсько-українська кібервійна: що та чому стає мішенню хакерів. URL: <https://thepage.ua/ua/it/yak-rosijsko-ukrayinska-vijna-prohodit-u-kiberprostorі> (дата звернення: 14.03.2025).

40. Уздєнова Ю. М. Гібридна війна: сутність, складові та ключові поняття. *Вчені записки ТНУ імені В.І. Вернадського*. Серія: Публічне управління та адміністрування. Том 35 (74) № 4 2024. С. 172–180.

41. Феськов І. В. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. *Актуальні проблеми політики*. 2016. Вип. 58. С. 66–72.

42. Хмель А. Боротьба із гібридними загрозами в ЄС (за нормативно-правовою базою Європейського Союзу). URL: https://www.researchgate.net/publication/361966359_Borotba_iz_gibridnimi_zagroзами_v_ES_za_normativno-pravovou_bazou_Evropejskogo_Souzu (дата звернення: 14.03.2025).

43. Шутов Р. Пропаганда та маніпуляції. URL: http://mediadriver.online/manipuliatsiyi_ta_propahanda/manipulyatsiyi-ta-propaganda/. (дата звернення: 14.03.2025).

44. Що таке історичний метод? URL: <https://metodologiasapiens.com/uk/metodos/mas-informacion-metodo-historico/> (дата звернення: 14.03.2025).

45. Arsalan Bilal Hybrid warfare – new threats, complexity and "trust" as an antidote. 2021. URL: <https://www.nato.int/docu/review/uk/articles/2021/11/30/gbridna-vjna-nov-zagrozi-skladnst-dovra-yak-antidot/index.html> (дата звернення:

14.03.2025).

46. Cyber Security: Hybrid Warfare. URL: <https://beyond.eu/en/blogs/cyber-security-hybrid-warfare> (дата звернення: 14.03.2025).

47. Dr Arnold C. Dupuy, Dr Dan Nussbaum, Vytautas Butrimas, Alkman Granitsas Energy security in the age of hybrid wars. 2021. Energy security in the age of hybrid wars. URL: <https://www.nato.int/docu/review/uk/articles/2021/01/13/energetichna-bezpeka-v-dobu-gbridnih-von/index.html> (дата звернення: 14.03.2025).

48. Future character of conflict. A study which seeks to describe what military forces are likely to experience in future conflicts out to 2029. Guidance. Ministry of Defense. 2 February 2010. URL: <https://www.gov.uk/government/publications/future-character-of-conflict> (дата звернення: 14.03.2025).

49. Glenn R.W. Thoughts on «Hybrid» Conflict. Small Wars Journal. 2009. URL: www.smallwarsjournal.com (дата звернення: 14.03.2025).

50. Hagelstam Axel Співпраця заради протидії гібридним загрозам. 2018. URL: <https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi-protid-gbridnim-zagrozm/index.html> (дата звернення: 14.03.2025).

51. Hybrid Threat. Headquarters, Department of the Army. TC 7-100. 26 November 2010. Washington, DC: Headquarters, 2010. P. V-VI.

52. Manel Medina Llinàs Hybrid Attacks on Critical Infrastructure. 2022. URL: <https://www.cidob.org/en/publications/hybrid-attacks-critical-infrastructure> (дата звернення: 14.03.2025).