МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Острозька академія»
Навчально-науковий центр заочно-дистанційного навчання
Кафедра міжнародних відносин

Кваліфікаційна робота

на здобуття освітнього ступеня магістра

на тему : «Гібридна війна як форма новітнього конфлікту»

Виконала
студентка групи зММВ - 2
спеціальності 291 Міжнародні відносини,
суспільні комунікації та регіональні студії,
освітньо-професійної програми
«Міжнародні відносини»
Ониськів Юлія Петрівна
Керівник:
Матвійчук Наталія Володимирівна
к.і.н., старший викладач

Рецензент–

Робота допущена до захисту
(протокол №___ засіданя кафедри міжнародних відносин від
_____20___року
Завідувач кафедри міжнарррдних відносин:_____

Острог – 2023

ЗМІСТ

ВСТУП

Обґрунтування актуальності дослідження теми. Розглядаючи класичні теорії воєн в XXI столітті, можна зробити висновок, що в сучасних реаліях глобалізації вони стають неефективними. Таким чином, вчені сучасності звертаються до виокремлення нового типу конфліктів, які називаються «гібридними війнами». Концепція таких воєн являє собою поєднання звичайних і нетрадиційних та нерегулярних військових операцій, які також включають економічне, дипломатичне, інформаційне (психологічне, кібер – і дезінформаційне політичне) протистояння. Поєднання військових і невійськових методів з використанням протестного потенціалу населення стає основним засобом ведення воєн нового покоління. Концепція «гібридної війни» спрямована на досягнення масштабних наслідків скромними засобами, такими як придушення ворожих військових дій або запобігання політичній підтримці з боку населення.

В цілому гібридні конфлікти – це координація тонких, продуманих дій з більш цілісною стратегією, інтенсивність якої змінюється на різних етапах конфлікту (початок, загострення, вирішення), спрямована на дестабілізацію внутрішніх і зовнішніх процесів держави. Перш за все, такий конфлікт спрямований на руйнування держави шляхом дестабілізації економіки, до зневіри населення, порушення прав національних меншин, створення умов, що сприяють контрольованій і неконтрольованій міграції, придушення громадянського опору і руйнування критично важливої інфраструктури.

Методи, що використовуються в гібридних конфліктах, часто є традиційними для воєн, які посилюються за рахунок використання нових технологій, що дозволяють краще проникати в критичні елементи і життєво важливі системи противника. Тиск на слабкі сторони може призвести до системних змін у критичних компонентах та пов'язаних з ними системах.

Методи ведення гібридної війни – це більше, ніж просто напади на життєво важливі системи, такі як зв'язок, інфраструктура чи транспорт. Держава, а також

неурядові організації все частіше виявляють слабкі місця в ідеологіях та інституціях або починають нові війни через соціальне невдоволення.

Таким чином, «гібридна війна» – це високотехнологічний конфлікт. Це продовження політики держави або коаліції політичних груп, транснаціональних корпорацій та неурядових організацій. Мета конфлікту – нав'язати своїм супротивникам перспективу, впливаючи на них в багатовимірному просторі і в різних сферах життя за допомогою комплексного адаптивного і асиметрично синхронізованого деструктивного впливу.

Гібридна війна раціонально поєднується з традиційними та нетрадиційними компонентами, з акцентом на численні джерела та методи нападу, загальний ефект результатів та високий рівень невизначеності для супротивників щодо того, якими можуть бути кінцеві стратегічні цілі. У гібридних конфліктах основними цілями є контроль над суспільством, вплив на загальний настрій людей і маніпулювання людьми, відповідальними за прийняття важливих рішень в державі. Мета противника – маніпулювати основними цінностями, мотиваційними факторами і культурними засадами країни, а також стратегічною інфраструктурою. Це досягається за рахунок комплексного, збалансованого застосування ефектів м'якої і жорсткої сили.

Актуальність даної проблеми для України обумовлена гібридною війною РФ проти нашої держави, свого роду феноменом асиметричного конфлікту. Боротьба з міжнародним тероризмом і нейтралізація збройного конфлікту в Україні вимагає розуміння логіки цих подій, розробки необхідних аналітичних інструментів і стратегічних знань для адекватного реагування.

Саме цим і зумовлена актуальність даного дослідження: сучасний світ стикається із «асиметричною», неоголошеною війною, регулювання та контроль якої ускладнюються частковою або повною нездатністю окреслити сторони, фронти, завдання та етапи розвитку конфлікту через його перехід через державні кордони та концепцію традиційної війни. Отже, необхідно проаналізувати причини типових «гібридних» конфліктів і розробити методи їх вирішення, які на сучасному етапі розвитку цієї проблеми чітко не визначені.

Аналіз стану наукової розробки проблеми. Все вищенаведене актуалізує тему дослідження і привертає увагу чисельних науковців і дослідників. Ф. Хоффман, відомий американський військовий теоретик, був одним із перших, хто стверджував, що з`явився дещо новий тип загроз – «гібридні загрози». Гібридну війну як феномен також досліджують такі закордонні вчені як Б. Гігеріх, Д. Кілкуллен, Т. Кузьо, Д. Ласіка, Дж. МакКуен, М. Міллер, Б. Неммет.

Серед українських вчених слід виділити О. Акульшина, В. Власюка, Р. Додонову, М. Кубявка, М. Лесіва, Є. Магду, К. Попович, Л. Чекаленко. Над дослідженням інформаційних війн та загалом над інформаційним компонентом гібридної війни працюють А. С. Дорошенко, Е. Вальц, Е. Ґіґґінз, Ю. Горбань, П. Доран, , М. Кіца, Т. Ніссен Г., Почепцов, І. Проноза, М. Сенченко, П. Ткачук, І. Феськов ,Дж. Штейн, та інші

К. Маклаклан, С. Маєрс, Є. Тюхтенко вивчали корупцію як один з елементів гібридного впливу на суперника. Особливості взаємодії ПВК з державами досліджували К. Каунерт, Н. Кастро, В. Короткий, Е. Фолі.

Економічний компонент гібридної війни став предметом дослідження С. Дейспрінг, М. Дудін, С. Кім, Т. Кустра, Р. Купер, Е. Каміллі, Г. Нордбі. Світовий досвід ведення та вирішення гібридних конфліктів вивчали Д. Джексон, Н. Зверко, Л. Коффі, Т. МакКулло, А. Мелдрам, М. Мерфі, А. Оленін, М. Сміт, Дж. Фланаган, Р. Шміц.

Фундаментальні праці перерахованих вчених цікаві, аргументовані, із залученням значної кількості документальних джерел і літератури. Однак окремих наукових розвідок щодо світового досвіду ведення та вирішеннягібридних конфліктів досить мало.

Метою дослідження є глибокий аналіз явища гібридної війни як сучасної форми конфлікту.

Відповідно до актуальності теми роботи та мети дослідження перед нами стоять такі **завдання**:

1. здійснити аналіз поняття «гібридної війни» як новітнього конфлікту;

2. розглянути вплив гібридних війн на світовий порядок;

3. проаналізувати інформаційний, політичний, воєнний та економічний компоненти гібридної війни;

4. дослідити світовий досвід ведення та вирішення гібридних конфліктів;

5. виокремити шляхи вирішення гібридної війни в Україні.

Об’єктом дослідження виступають гібридні війни.

Предметом дослідження є основні складові гібридних конфліктів та досвід їх вирішення.

Теоретико-методологічною основою роботи є сукупність вироблених і використовуваних сучасною наукою принципів і методів наукового дослідження. Роботу виконано на основі принципів історизму, об'єктивності та науковості. Також використані методи опису та теоретичного узагальнення.

Методологічна база дослідження заснована на методі історичної реконструкції та логіко–аналітичного моделювання. Нами був використаний системний та міждисциплінарний підходи, які передбачають комплексне застосування методів дослідження.

Хронологічні рамки роботи окреслені періодом існування феномену гібридної війни. Нижня межа зумовлена ранніми прикладами гібридних конфліктів, включаючи гібридну війну Радянського Союзу проти Тувинської Народної Республіки у 1944 році. Верхня хронологічна межа – це події сьогодення, а саме триваюча гібридна війна Росії проти України.

Географічні рамки роботи не обмежуються певною країної чи регіоном, адже ми розглядаємо досвід ведення та вирішення гібридних конфліктів глобально.

Аналіз джерельної бази. Під час написання роботи нами були використані такі види джерел:

1) міжнародно-правові документи, що стосуються питань вирішиння міжнародних конфліктів

2) матеріали міжнародних організацій (Декларація саміту НАТО в Уельсі від 5 вересня 2014 р. та інші)

3) офіційні сайти організацій (ООН, НАТО)

4) документи, що стосуються питань національної безпеки держави (Стратегічний огляд оборони Великобританії, Британська стратегія національної безпеки, Стратегія національної безпеки Литви 2017 р., Закон України «Про основні принципи забезпечення кібербезпеки України» тощо).

5) матеріали періодичної преси. Багатий фактичний матеріал про світові події та сучасні конфлікти містить періодика, а також ЗМІ країн світу. Періодичні видання є цінним джерелом інформації, оскільки дозволяють слідкувати за найважливішими подіями у сучасному житті країн і знайомитися з думкою експертів з питань розвитку гібидних загроз (svoboda.org, ukrinform.ua, The Independent, «The Times», «Forbes», «Reuters», «BBC News» тощо).

Практична значимість. Дослідження на тему «Гібридна війна як форма новітнього конфлікту» має практичну значимість для вирішення російсько-української війни. Ця війна є яскравим прикладом гібридного конфлікту, де використовуються різноманітні методи впливу, включаючи військові дії, інформаційну війну, кібератаки, психологічний тиск та інші інструменти. Вивчення цього конфлікту з гібридною складовою допомагає розкрити ключові аспекти та виклики, з якими стикаються держави в подібних ситуаціях.

Дослідження гібридної війни у російсько-українському контексті допомогло виділити ключові ознаки та індикатори, які можуть вказувати на наявність або розвиток подібних конфліктів в майбутньому.

Практична апробація. Ониськів Ю. П. Російсько-українська інформаційна війна в онлайн просторі. Науковий блоґ. Національний університет «Острозька академія». 2023. URL: https://naub.oa.edu.ua/2023/rosijsko-ukrayinska-informatsijna-vijna-v-onlajn-prostori/

Структура роботи: вступ, три основні розділи та висновки до них, загальні висновки, список використаних джерел та літератури. Загальний обсяг

роботи складає 94 сторіноки. Основний зміст дослідження розміщено на 79 сторінках. Список джерел та літератури складає 144 позиції.

РОЗДІЛ 1. ГІБРИДНА ВІЙНА ЯК ФЕНОМЕН

1.1. Поняття «гібридної війни», як новітнього конфлікту

З появою нових технологій та глибоких змін у геополітичній сфері, поняття війни також зазнало різноманітних трансформацій. Однією з найактуальніших концепцій в сучасному світі є гібридна війна. Гібридна війна є неоднозначним та складним поняттям, що визначається як комбінована стратегія ведення конфлікту, в якій використовуються не лише військові, а й інформаційні, економічні, політичні та інші інструменти для досягнення стратегічних цілей. Гібридна війна представляє собою новий рівень взаємодії між державами, де не менш важливою стає інформаційна та психологічна сфери.

Очевидно, що в основі таких конфліктів лежать цілком зрозумілі інтереси, концепції та цілі військово-політичних сил, які не можуть або не бажають розв’язувати існуючі конфлікти без застосування засобів збройної боротьби. І хоча термін «гібридна війна» не має загальноприйнятого поняття, неофіційно він використовується широко, без чіткого визначення.

Б. Гігеріх зазначає, що від «маленьких зелених чоловічків» у Криму до «маленьких блакитних чоловічків» у Південно-Китайському морі, ідея про те, що міжнароді конфлікти стають все більше гібридними, пожвавила дебати серед установ безпеки та оборони в НАТО та за її межами. Національні уряди, які розробляють документи з аналізу безпеки та оборони, часто згадують про необхідність боротьби з гібридними загрозами [78, p. 66]. У Декларації саміту НАТО в Уельсі від 5 вересня 2014 року говориться, що лідери Альянсу «забезпечуватимуть, щоб НАТО мало змогу ефективно протистояти конкретним викликам, пов’язаним із загрозами гібридної війни, де широко використовується широкий спектр відкритих і прихованих військових, воєнізованих і цивільних заходів. Важливо, щоб Альянс мав необхідні інструменти та процедури, необхідні для стримування та ефективного реагування на загрози гібридної війни, а також можливості для посилення національних сил» [9].

Хоча Уельська декларація поставила питання гібридної війни в особливий контекст російсько-української війни та спонукала до зусиль, спрямованих на підготовку НАТО до ефективної протидії таким загрозам, масштаб виклику набагато ширший, а основна динаміка часто знаходиться за межами військової сфери. Робота, проведена Командуванням НАТО з питань трансформації під назвою «Протидія гібридним загрозам», це підтверджує, але здається, що отримані в той час висновки не досліджувалися систематично, доки незаконна анексія Криму Росією не показала важливість проблеми [48].

Ще у 1998 році в Стратегічному огляді оборони Великобританії зазначалося, що кожна країна повинна продовжувати модернізувати свої сили таким чином, щоб мати змогу протидіяти як у звичайних, так і у нетрадиційних війнах, з відповідним поєднанням досвідченості, якості, численності та гнучкості сил [11].

Британська стратегія національної безпеки та її допоміжний Стратегічний огляд оборони та безпеки, опублікований наприкінці листопада 2015 року, стверджує, що «незаконна анексія Криму в 2014 році та підтримка сепаратистів на сході України шляхом використання гібридної тактики та маніпулювання засобами масової інформації показали готовність Росії підірвати ширші міжнародні стандарти співпраці. Ці стратегічні документи розглядають гібридні загрози як виклики першого рівня, які можуть безпосередньо вплинути на Великобританію, і як загрози другого рівня, які починаються як гібридна атака на союзника [8].

Визначенню поняття «гібридна війна» та дослідженню його змісту присвячено чимало наукових робіт та експертних заяв. Ф. Хоффман, відомий американський військовий теоретик, був одним із перших, хто стверджував, що з’явився дещо новий тип загроз – «гібридні загрози». За словами дослідника вони «…включають в себе низку різних способів ведення війни, а саме звичайні засоби, нерегулярні військові формування, терористичні акти (невибіркове насильство та примус), а також кримінальні заворушення». Щоб описати цю

нову військову реальність, Ф. Хоффман запропонував термін «гібридна війна» [82].

Існує ціла низка тлумачень терміну «гібридна війна». Наприклад, підполковник Корпусу морської піхоти США Б. Неммет розглядає «гібридну війну» як сучасний тип партизанської війни, який інтегрує інноваційні технології та сучасні методи мобілізації [4]. Дж. МакКуен, полковник армії США, стверджує, що гібридна війна є основним методом військових дій в асиметричній війні, яка ведеться на трьох бойових напрямках: серед населення зони конфлікту, місцевого населення та міжнародного суспільства [105, p. 110]. Цитований українськими ЗМІ представник ВМС США Р. Ворк пояснює, що у «гібридній війні» ворожі сили можуть використовувати навіть військових, замаскованих серед цивільного населення [47 , с. 41].

Щоб сформувати узгоджену точку зору щодо можливих майбутніх військових конфліктів, у 2009 році Командування ОЗС НАТО з питань трансформації представило дослідницький звіт під назвою «Проект багатогранного майбутнього – навігація до 2030 року» [76], у якому показано сприйняття та ставлення до потенційного сценарію розвитку безпекового середовища та характер можливих військових конфліктів. Одним із напрямків розвитку спроможностей Альянсу, які були розроблені в цьому звіті, була «адаптація до вимог гібридних загроз». Суть такого типу загрози полягає в тому, що потенційний противник уникатиме прямого контакту з силами НАТО в звичайних операціях, залучаючи замість цього нерегулярні сили та асиметричні форми протистояння. Очікується, що «гібридний ворог» включатиме регулярні та нерегулярні військові формування, терористів і злочинців, які співпрацюватимуть у «змішаних режимах». Варто підкреслити, що «гібридний ворог» не повинен дотримуватися міжнародних норм конфлікту.

Того ж року автор монографії «Strategic Implications of Hybrid War: A Theory of Victory» Д. Ласіка, офіцер ВПС США, розробив характеристики гібридних війн [76]. Він розглядав інформаційно-психологічний елемент як основу гібридної війни. Автор визначав суспільну свідомість, а не військові сили

чи інфраструктури, першочерговою мішенню ініціаторів війни. Крім того, зауважив, що гібридні загрози мають нечітку природу, їх важко визначити та ідентифікувати, оскільки неможливо організувати відповідне реагування.

Коментуючи ситуацію в Україні у квітні 2014 року колишній радник Ради безпеки ООН і НАТО, член верхньої палати парламенту Нідерландів генерал-майор у відставці Ф. ван Каппен дав таке визначення даного поняття: «Гібридна війна» є сумішшю класичної війни із застосуванням іррегулярних збройних формувань. Держава, яка веде гібридну війну, укладає угоди з недержавними виконавцями бойовиками, місцевими групами, організаціями, формально заперечує зв'язок. Ці виконавці можуть робити те, чого не може зробити сама держава, тому що будь-яка держава зобов'язана дотримуватися Женевської конвенції та Гаазької конвенції про закони сухопутної війни, договорів з іншими країнами. Усю брудну роботу можна перекласти на плечі недержавних формувань» [27].

Британський дослідник Т. Кузьо пише, що поєднання військових і невійськових методів з використанням протестного потенціалу населення стає основним засобом ведення воєн нового покоління [95, p. 164]. Л. Наполеоні зазначає, що концепція «гібридної війни» спрямована на досягнення масштабних наслідків скромними засобами, такими як придушення ворожих військових дій або запобігання політичній підтримці з боку населення [116, p. 18].

Концепція гібридної війни тісно пов'язана з концепцією військового теоретика В. Лінда про війну четвертого покоління. В. Лінд простежує еволюцію сучасної війни від Вестфальського миру 1648 р., до кінця XX століття та піднесення потужних недержавних акторів. Робота В. Лінда показує, як нові технології та тактика на полі бою впливали на стратегію, військову організацію та культуру. Він називає війну четвертого покоління «найрадикальнішою» зміною Вестфальської системи, оскільки в ній «держава втрачає монополію на війну». Характер цього типу конфлікту ставить під сумнів «легітимність держави» [96, p. 23].

М. Міллер зауважує, що гібридна війна – це використання звичайних і нетрадиційних способів і засобів будь-якою комбінацією державних та недержавних суб'єктів у межах одного бойового простору. Звичайні та нетрадиційні способи та засоби включають сили, зброю та тактику і характеризуються використанням сучасної технології та високим ступенем єдності зусиль між регулярними та нерегулярними силами [110, p. 38].

Також слід наголосити на тому, що гібридна війна – це високотехнологічний конфлікт. Це продовження політики держави або коаліції політичних груп, транснаціональних корпорацій та неурядових організацій. Мета конфлікту – нав'язати своїм супротивникам перспективу, впливаючи на них в багатовимірному просторі і в різних сферах життя за допомогою комплексного адаптивного і асиметрично синхронізованого деструктивного впливу [73, p. 233].

Аналізуючи погляди американських військових експертів, таких як Ф. Хоффман, Дж. Н. Меттіс, Г. Грант, та інші, ми приходимо до висновку, що під терміном «гібридна війна» вони мають на увазі:

1) негласні таємні воєнні дії, під час яких протилежна сила атакує державні органи та регулярні сили противника за допомогою місцевих повстанців та сепаратистів, які підтримуються зброєю та фінансами з-за кордону та деяких внутрішніх інституцій (олігархи, організована злочинність, націоналістичні та псевдорелігійні організації);

2) використання комбінації звичайних, нерегулярних та асиметричних дій разом з інформаційно-психологічними маніпуляціями, політичним та ідеологічним конфліктом.

У геополітичному контексті «гібридна війна» узагальнює нове поняття, яке в основному використовується у сфері операцій сил спеціального призначення; воно поєднує досвід насильницьких протистоянь, що становлять загрозу міжнародній безпеці, і боротьбу з тероризмом та екстремізмом державних і недержавних акторів. У свою чергу Корпус морської піхоти США використовує термін «гібрид», щоб відобразити потенційну загрозу регулярних і нерегулярних

збройних сил. Він не розглядає «гібридну війну» як нову форму війни, а радше як синонім «конфлікту повного спектру». Не дивно, що Міністерство оборони США запропонувало використовувати термін «операції повного спектру» замість терміна «гібридна війна» [124].

«Гібридна війна» ведеться внутрішніми силами, спрямованими на послаблення або повалення уряду, а також зовнішніми силами. Дії зовнішніх сил передбачають сприяння сепаратистам і терористам у вербуванні своїх прибічників та їх навчання, вплив на економіку та соціальну сферу, координацію дипломатичних зусиль, а також проведення окремих актів насильства. Для цих цілей залучаються сили спеціальних операцій, розвідувальні сили, попередньо сформовані сепаратистсько-терористичні угруповання, групи бойовиків та організовані злочинні угруповання. Їхня діяльність, поширювана за допомогою всього спектру інформаційно-комунікаційних технологій, також має масовий інформаційно-психологічний вплив на населення, військовослужбовців і правоохоронців, органи влади.

Аналіз досвіду ведення «гібридних воєн» в Югославії, Іраку, Афганістані, Сирії, Лівії, Грузії і Україні, показує, що така війна виходить за межі традиційних уявлень про неї, набуває комбінованого характеру, перетворюючись на клубок політичних інтриг, запеклу боротьбу за політичне та економічне панування над країною, за території, ресурси та фінансові потоки. Жертвами таких війн стають, як правило, мирні жителі і, в першу чергу, найбільш незахищені категорії населення: люди похилого віку, жінки та діти. У такому конфлікті важко відрізнити правду від зла, ворогів від союзників, простих мирних громадян від терористів, найманців і бойовиків [101, p. 14].

Аргумент того, що гібридна війна стане найбільш ймовірним типом конфлікту в майбутньому, ґрунтується на таких трьох складових як: трансформація традиційних управлінських структур, суперечки з приводу політичної влади, викликані давніми культурними відмінностями держав і фінансова підтримка заколотів та революцій з боку держав. В результаті війни

будуть вести звичайними та нетрадиційними способами та засобами, що у свою чергу спричинятиме поширення гібридних війн [143, p. 233].

М. Міллер зауважує те, що стратегічна основа, спрямована на запобігання гібридним війнам у світі базується на двох основних аспектах:

1. Підтримка слабшої сторони зі сторони міжнародного співтовариства;

2. Дії, спрямовані на послаблення сили гібридного противника (сильнішої сторони) за допомогою об’єднання держаних та недержавних акторів міжнародних відносин [122, p. 61].

М. Лесів говорить про те, що акторами гібридної війни виступають держави та різні недержавні актори міжнародних відносин. А причинами до ведення гібридної війни є: захист національних інтересів; релігійна та ідеологічна розбіжність держав; історичні «образи» та конфлікти; економічний фактор; трансформація традиційних управлінських структур; розповсюдження сучасної зброї та технологій [33, p. 21].

Методи, що використовуються в гібридних конфліктах, часто є традиційними для воєн, які посилюються за рахунок використання нових технологій, що дозволяють краще проникати в критичні елементи і життєво важливі системи противника. Тиск на слабкі сторони може призвести до системних змін у критичних компонентах та пов'язаних з ними системах. Методи ведення гібридної війни – це більше, ніж просто напади на життєво важливі системи, такі як зв'язок, інфраструктура чи транспорт. Держава, а також неурядові організації все частіше виявляють слабкі місця в ідеологіях та інституціях або починають нові війни через соціальне невдоволення [116, p. 18].

М. Міллер зауважує, що стримування та перемога над гібридними конфліктами в значній мірі залежать від збору та аналізу розвідувальної інформації для виявлення суб'єктів, які беруть участь у гібридному конфлікті, та сили, що спрямовують їх до насильства [110, p. 39]. Це надасть змогу здійснювати скоординоване та паралельне використання дипломатичних, інформаційних та економічних інструментів національної влади з метою запобігання виникненню гібридних конфліктів, стримування державного

спонсорства таких конфліктів та вирішення цих конфліктів до того як вони розпочнуться. Паралельно з цим має обов’язково бути присутня військова сторона протидії гібридній війні, спрямована на стримування агресії та відвернення повстанської діяльності. Тобто, кожна держава повинна чітко оцінювати потенційні загрози гібридної війни з боку інших держав та бути готовою їм протидіяти. Ворог, який володіє сумішшю високотехнологічної зброї та нетрадиційних способів і засобів ведення війни, представлятиме величезну загрозу. Тому, основним завдання для військових планувальників є розробка військової стратегії протидії таким загрозам.

Таким чином, нині сучасний світ стикається із «гібридною», неоголошеною війною, регулювання та контроль якої ускладнюються частковою або повною нездатністю окреслити сторони, фронти, завдання та етапи розвитку конфлікту з переходом через державні кордони та концепцію традиційної війни. Майже всі сучасні вчені переконані, що гібридна війна у близькому майбутньому стане найпоширенішим видом протистояння держав.

Гібридна війна раціонально поєднується з традиційними та нетрадиційними компонентами, з акцентом на численні джерела та методи нападу, загальний ефект результатів та високий рівень невизначеності для супротивників щодо того, якими можуть бути кінцеві стратегічні цілі. У гібридних конфліктах основними цілями є контроль над суспільством, вплив на загальний настрій людей і маніпулювання людьми, відповідальними за прийняття важливих рішень в державі. Мета противника – маніпулювати основними цінностями, мотиваційними факторами і культурними засадами країни, а також стратегічною інфраструктурою. Це досягається за рахунок комплексного, збалансованого застосування ефектів м'якої і військової сили.

1.2. Гібридні війни та світовий порядок

В сучасному світі поняття війни набуває нових відтінків, виходячи за межі традиційних військових сценаріїв. Гібридні війни стають все більш важливим явищем, яке підсилює суперництво та руйнує традиційні засади світового

порядку. Це поняття висуває на передній план необхідність переосмислення концепції безпеки, ролі держав та міжнародних організацій, а також змінює парадигму взаємодії міжнародних акторів [34, с. 208]. Відтак вважаємо за потрібне розглянути вплив гібридних воєн на становлення та збереження глобального порядку.

В сучасному світі, де технологічний розвиток та інформаційна доступність досягли небачених раніше рівнів, традиційне розуміння військового конфлікту та безпеки еволюціонувало. Гібридні війни стали суттєвим елементом зміни геополітичного пейзажу, впливаючи на дестабілізацію міжнародної безпеки та стабільності.

М. Кубявка виділяє одну з основних характеристик гібридних війн використання дезінформації та пропаганди з метою вплинути на громадську думку та дестабілізувати суспільство. Це може призвести до загострення конфліктів, спровокувати міжнаціональні напруження та зірвати можливість мирного врегулювання [31, с. 11].

Гібридні війни впливають на міжнародну безпеку та стабільність через зміни в стратегічних підходах держав. Традиційні військові дії можуть бути доповнені кібератаками або хакерськими атаками на важливу інфраструктуру. Такі атаки можуть спричинити руйнування та паралізувати економіку країни, порушити роботу урядових систем та вплинути на повсякденне життя громадян [52].

Гібридні війни також підривають міжнародні домовленості та договори, спрямовані на забезпечення миру та безпеки. Порушення правил міжнародного права може викликати реакцію інших держав, що призводить до ескалації конфлікту та подальшої дестабілізації регіону. Поширення дезінформації також підриває довіру між країнами та міжнародними організаціями, що ускладнює співпрацю та врегулювання конфліктів.

Для подолання впливу гібридних війн на дестабілізацію міжнародної безпеки та стабільності необхідно вжити комплексних заходів на різних рівнях. По-перше, важливо підвищити кібербезпеку та здатність країн захищати свою

інфраструктуру від кібератак. Розвиток міжнародних стандартів та співпраці в цій сфері може зменшити загрози хакерських атак.

По-друге, національні та міжнародні організації повинні працювати над покращенням відношення громадської думки до різної інформації. Зміцнення інформаційної грамотності та здатності аналізувати інформацію допоможе громадянам впізнавати дезінформацію та протидіяти їй.

Нарешті, держави повинні спільно працювати над зміцненням міжнародного правопорядку та врегулюванням конфліктів. Засудження порушень міжнародного права та спільна реакція на дестабілізуючі дії можуть послужити запобіганню ескалації конфліктів та збереженню стабільності [112].

Г. Меріно пише, що гібридні війни значно впливають на руйнування міжнародних правил та норм, що спричиняє глибокі зміни у сучасних міжнародних відносинах [109]. Перш за все, гібридні війни підіривають основні засади міжнародного права. Класичні норми та принципи, що регулюють поведінку держав на міжнародній арені, стають менш ефективними в умовах віртуальної агресії та дестабілізації. Ворожі держави можуть використовувати кібератаки, дезінформацію та інші методи для впливу на внутрішні справи інших країн без прямого відкритого військового конфлікту. Це призводить до підривання принципів суверенітету та незалежності держав, які є основоположними для міжнародних відносин [139 p. 16].

По-друге, гібридні війни знижують рівень довіри між державами. Засоби інформаційної війни дозволяють створити образ ворога, розповсюджуючи фейкові новини та дезінформацію. Це може призвести до зростання паранойї та недовіри між країнами, а також до руйнування дипломатичних зусиль із вирішення конфліктів мирним шляхом [139, p. 18].

Третє, гібридні війни породжують нові виклики для міжнародного співробітництва та колективної безпеки. Традиційні міжнародні організації та договори не завжди готові до ефективного протидії гібридним загрозам. Відсутність адекватних механізмів реагування може призвести до безладу та розпаду колективних структур безпеки [55].

З іншого боку, гібридні війни викликають необхідність переосмислення та адаптації міжнародного права до нової реальності. Міжнародне співтовариство повинно знайти способи реагування на ці виклики, зокрема шляхом розробки нових норм та принципів, які регулюватимуть поведінку держав у кіберпросторі, інформаційній сфері та інших аспектах гібридних конфліктів [139, p. 20].

К. Попович наголошує на тому, що завдяки гібридним війнам, традиційна роль суверенних держав як єдиних та визначальних акторів у міжнародних відносинах нині під питанням. Замість цього, ми спостерігаємо розширення поля дії незалежних суб'єктів, які раніше вважалися недостатньо впливовими або значущими. Терористичні організації, хакерські групи, приватні компанії та інші нетрадиційні актори тепер мають здатність впливати на глобальний порядок, навіть використовуючи обмежені ресурси та мінімальний обсяг військових дій [39, с. 76].

На думку Г. Кохан, однією з найважливіших змін, викликаних гібридними війнами, є перехід від прямого військового конфлікту до використання кібератак, дезінформації та інших нетрадиційних методів впливу. Це дозволяє незалежним суб'єктам здійснювати вплив без відкритого використання військової сили, порушуючи традиційні межі та обмеження. Такий підхід підриває традиційну ієрархію акторів у міжнародних відносинах та вимагає від суверенних держав адаптації до нових реалій [29, с. 147].

У підсумку, гібридні війни змінюють роль держав та незалежних суб'єктів у міжнародних відносинах. Динаміка міжнародних відносин постає більш складною, і вона вимагає від усіх акторів адаптації до швидкозмінюваної геополітичної реальності та пошуку нових способів досягнення стабільності та безпеки

Одним із ключових аспектів гібридних війн є їхня індивідуалізація та адаптивність. Традиційні блоки та альянси мають тенденцію до колективних стратегій та спільних підходів до вирішення конфліктів. Проте гібридні загрози вимагають більш гнучких, специфічних та інтелектуальних підходів. Актори гібридних війн можуть адаптувати свої дії до конкретних обставин,

використовуючи різноманітні методи та інструменти для досягнення своїх цілей. Це може призвести до того, що традиційні блоки і альянси будуть менше ефективними у протистоянні гнучким та інноваційним підходам гібридних агресорів.

Додатковою проблемою для традиційних блоків і альянсів є важкість координації в умовах гібридних загроз. Такі загрози можуть включати кібератаки, дезінформацію та інші методи, що не завжди можуть бути однозначно відстежені до конкретних держав чи суб'єктів. Це ускладнює процес прийняття рішень і може породжувати недовіру між членами альянсів, знижуючи їхню спроможність відповідати на загрози [18, с. 145].

Гібридні війни також можуть підірвати довіру до міжнародних структур та норм. Індивідуалізовані та мінливі методи гібридних конфліктів можуть заохочувати держави та інші суб'єкти діяти поза рамками міжнародних договорів та правил. Це може призвести до нестабільності та розпаду співпраці на міжнародній арені, виснажуючи потенціал для мирного врегулювання конфліктів та спільної дії [73].

Як було наголошено нами раніше, гібридні війни представляють собою нову реальність у сучасному світі. Їх характеризує використання різноманітних засобів та методів, які не завжди можуть бути чітко класифіковані як військові дії, політичні впливи або інформаційні атаки. Однією з ключових проблем у гібридних війнах є встановлення авторства та відповідальності за конкретні дії, що може мати серйозні наслідки для стабільності та безпеки міжнародного співтовариства [14, с. 34].

Сутність гібридних війн полягає в їх комплексності та мультиаспектності. Це може включати в себе воєнні дії, кібератаки, дезінформацію, економічний тиск, вплив на внутрішню політику та інші форми впливу. Часто такі дії здійснюються некерованими або псевдоанонімними суб'єктами, що ускладнює процес встановлення відповідальності. Наприклад, кібератаки можуть бути проведені через сервери різних країн, а інформаційні операції можуть бути

масковані так, що важко визначити їх джерело. Це викликає проблеми з ідентифікацією і розслідуванням винних сторін.

Додатковою проблемою є розмитість межі між державними та недержавними акторами у гібридних війнах. Поняття атрибуції в гібридних війнах також виникає як суттєва проблема. Для встановлення авторства необхідна наявність відповідних технічних, кібербезпекових та інтелектуальних ресурсів. Відсутність таких можливостей часто заважає знаходженню конкретних винних осіб або організацій. Крім того, вже існують випадки, коли навіть можна встановити авторство, відповідні санкції або дії відсутні, оскільки такі дії можуть залишитися за рамками традиційного міжнародного права [104, p. 117].

Складність встановлення авторства та відповідальності за вчинення дій у гібридних війнах є серйозною проблемою для міжнародного співтовариства. Це вимагає спільних зусиль держав, міжнародних організацій та експертів у галузі кібербезпеки та міжнародного права для розв'язання цієї проблеми й забезпечення стабільності та безпеки у сучасному світі.

Таким чином, гібридні війни трансформують світовий порядок, руйнуючи традиційні моделі та вимагаючи нових підходів. Вони ставлять під сумнів ефективність та стабільність міжнародних відносин. Тільки шляхом спільних зусиль та інновацій можна забезпечити адекватну відповідь на цей виклик та зберегти світовий порядок в епоху гібридних конфліктів.

Висновки до розділу 1

Гібридну війну можна визначити як форму конфлікту, де використовуються різні інструменти впливу, такі як військові дії, інформаційна пропаганда, кібератаки, фінансовий тиск та інші, з метою досягнення стратегічних цілей. Цей підхід дозволяє супернику приховувати свої наміри та створює враження невизначеності щодо реальних дій. Гібридні війни перетворюються на платформу, де різні компоненти взаємодіють та посилюють один одного, створюючи синергію ефектів.

Такий підхід до конфлікту має суттєвий вплив на світовий порядок. Відповідно до традиційних моделей міжнародних відносин, суверенні держави були основними акторами на арені міжнародної політики. Однак гібридні війни руйнують цю концепцію, відкриваючи двері для ролі нестандартних суб'єктів, таких як терористичні організації, приватні компанії та хакерські групи. Такі суб'єкти можуть легко впливати на конфлікт через невеликі зусилля та мінімальний обсяг військових дій.

Світовий порядок також стає дедалі більше децентралізованим. Традиційні блоки та альянси можуть бути менше ефективними в умовах гібридних війн, коли стратегії впливу та дії стають більш індивідуалізованими та адаптивними. Це може спричинити нестабільність та підірвати довіру до міжнародних структур.

Додатковою проблемою є велика складність визначення авторства та відповідальності за гібридні дії. Через використання різноманітних інструментів та можливість анонімних дій, важко встановити зв'язок між конкретними діями та їхніми ініціаторами. Це може призводити до відсутності належного реагування та покарання

РОЗДІЛ 2. СУЧАСНІ ГІБРИДНІ ВІЙНИ: ОСНОВНІ СКЛАДОВІ

2.1 Інформаційний компонент гібридної війни

Поруч з терміном «гібридна війна» з'являється ще один термін, що називається «інформаційною війною», це поняття трактується по-різному: деякі дослідники визначають його як частину гібридної війни, інші пишуть про нього як окремий повноцінний феномен нашого часу [40, с. 154]. В умовах технологічного прогресу використання у військових цілях різних технологій є повсякденністю, що разом з послабленням міжнародного співробітництва може призвести до підриву глобального потенціалу в галузі миротворчих ініціатив та попередження конфліктів і насильства у всіх формах [70, p. 256].

На нашу думку, інформаційна війна може бути одним із найважливіших способів ведення гібридних воєн. Для підтвердження цього факту необхідно навести теоретичні дослідження зарубіжних і вітчизняних учених для того, щоб, визначити інформаційну війну як дійсний спосіб ведення гібридних воєн.

У світі відбувається трансформація і модифікація воєн, розвиваються дедалі нові «нетрадиційні» способи ведення війни. Так, у XXI столітті особливу популярність набуває так звана «інформаційна війна» (ІВ), це явище стало одним із звичних факторів навколишньої дійсності [21, с. 26]. Сам термін «information warfare» не є новим, він був запроваджений Т. Роном у науковий обіг ще 1976 року [41, с. 79].

Зростаюча популярність цього явища пов'язана з глобалізацією інформаційних процесів, бурхливим розвитком інформаційних технологій та повсюдною цифровізацією. Для досягнення своєї мети різні міжнародні актори все частіше звертаються до прийомів та методів ведення інформаційної війни. В даний час багато країн розглядають інформаційну війну як ефективний інструмент ведення зовнішньої політики.

Неможливо уявити сучасні міжнародні відносини без інформаційних війн. Передбачається, що надалі ця тематика не тільки не втратить своєї актуальності, а й стане ще «гострішою» і всюдисущою. Процес глобалізації та цифровізації

виводить поняття «інформаційна війна» на новий рівень. Разом з розвитком цифрових комунікацій з'являються нові способи ведення інформаційної війни. У XXI столітті інформаційна війна стає одним із найвпливовіших світових політичних трендів. Засоби ведення нового виду війни можуть бути різними: поширення дезінформації, пропаганда, брехня, приховування суттєвої інформації, наклеп, відволікання уваги і т.д. [16, с. 138].

Таким чином, новим способом ведення війни без зброї сьогодні є інформаційна війна, головне завдання якої – знищення людей не як фізичної сили, а як суспільства. Феномен інформаційно-психологічного впливу ми можемо спостерігати в засобах масової інформації тих держав, які ведуть між собою цю «невидиму» боротьбу. Повідомлення, яке кожен може почути, побачити по телевізору, прочитати в газеті або в Інтернеті, може викликати сумніви і налаштувати людину вороже до влади, її приналежності до певної нації або до її становища в країні. Створення такої напруженої ситуації в державі, проти якої ведеться інформаційна війна, збільшує шанси противника послабити суспільство, щоб воно не могло чинити опір.

Вивчаючи численні дослідження на тему гібридних та інформаційних воєн, ми можемо виявити низку проблем. Перша проблема полягає у відсутності однозначного доктринального визначення гібридної війни. Кожен з авторів, концептуалізуючи феномен нового типу війни, використовують різні терміни, наприклад, як «нелінійна війна», «нетрадиційна війна», «війна нового покоління», «інформаційна війна» та ін [47 , с. 41].

Друга проблема полягає в тому, що зараз дослідники досі не дійшли єдиного поняття «інформаційної війни», а також не встановили конкретного спільного зв'язку між термінами гібридної та інформаційної війни. Дискусії про те є інформаційна війна самостійним елементом або вона лише складова частина гібридної війни, ведуться до сьогодні.

Третя проблема виявляється у розмиванні рамок простору ведення гібридної війни, оскільки вона може бути як на міждержавному рівні, так і на рівні суспільства за допомогою державних та недержавних акторів [53, p. 468].

Також це ускладнює вивчення мотивів і передумов початку ведення гібридних воєн, оскільки вони можуть змінюватись від політичних до економічних та інших цілей.

Таким чином, наявність вищезазначених проблем також передбачає вироблення єдиного підходу до боротьби з феноменами гібридної та інформаційної війни.

Інформаційна війна є явищем, що набуло великого значення в сучасному світі, впливаючи на політичні процеси, міжнародні відносини та суспільні структури. Визначення цього терміну, надане експертами, розкриває його складність та ключові аспекти.

Розглядаючи термін «інформаційна війна», наголошуємо, що на сьогоднішній день немає єдиного визначення такого типу війни. Це пов`язано з багатозначністю терміна «information warfare», що породило безліч різночитань під час його перекладу. Термін може трактуватися як «інформаційна війна», «інформаційне протиборство», «інформаційно-психологічна війна» та ін [19, с. 23].

Вітчизняний вчений, який вивчає інформаційні війни, М. Сенченко у своїй роботі дає таке визначення даного терміна: «інформаційна війна – спосіб створення системи управління інформаційними потоками з метою організації ноосфери та світового інформаційно-психологічного простору у своїх інтересах» [42, с. 6].

Ще один вітчизняний дослідник П. П. Ткачук характеризує це явище наступним чином: «інформаційна війна – це особливий вид збройного конфлікту, в якому зіткнення сторін відбувається у формі інформаційних операцій із застосуванням інформаційної зброї [43, с. 102]. Кінцева мета інформаційної війни, на думку П. П. Ткачука, зламати волю супротивника до опору та підпорядкувати його свідомість своїй волі. Також у своїй роботі автор вказує, що висока активність інформаційних операцій робить їх одним із основних елементів сучасних гібридних збройних конфліктів [43, с. 102].

У закордонній науковій літературі вивченням теорії інформаційних воєн займався К. Чіввіс, він пропонує таке визначення: «Інформаційна війна – це використання інформації задля досягнення цілей держави. Як і дипломатія, економічна конкуренція чи використання військової сили, інформація сама по собі, один із ключових аспектів влади і, що важливіше, національний ресурс, який якраз і підтримує дипломатію, економічну конкуренцію та ефективність збройних сил» [60, p. 4].

Інформаційна війна визначається як системний комплекс дій, спрямованих на зміну громадської думки, взаєморозуміння, поведінки або державної політики через використання різних засобів інформаційної комунікації. Зокрема, Дж. Штейн визначає інформаційну війну як «систему організованих дій для виробництва та розповсюдження невірної, спотвореної або неповної інформації з метою впливу на громадську думку та державну політику» [132, p. 36].

Інший визначальний аспект інформаційної війни – це використання сучасних технологій для досягнення своїх цілей. Е. Вальц наголошує, що інформаційні технології стали невід'ємною складовою інформаційної війни, а сама війна – це боротьба за надання певного змісту інформації в цифровому просторі [140, p. 132].

Інформаційна війна також має політичні та стратегічні аспекти. За твердженням Е. Ґіґінза, це «спрямований процес інформаційних операцій з метою створення національного та міжнародного образу держави або недержавної формації» [17, с. 55].

У контексті гібридної війни, інформаційна війна стає інструментом, що дозволяє досягти важливих політичних, економічних та військових цілей без відкритого використання військової сили. Серед ключових елементів інформаційної війни можна виділити дезінформацію, пропаганду, маніпуляцію соціальними мережами, кібератаки та інші форми впливу на інформаційне оточення [45, с. 69].

На нашу думку, інформаційна війна є найважливішим і ефективним способом ведення гібридних воєн, що набуває все більшої актуальності в

сучасному світі. Інформаційна війна може бути елементом гібридної війни і застосовуватися в комплексі з іншими її елементами, так і бути самостійною складовою.

Серед основних відмінностей інформаційної війни від традиційної війни виділяють:

- інформаційна війна має більш гнучкий арсенал, ніж традиційна, отже, може впливати на різні верстви населення по-різному;
- на відміну від класичної війни в інформаційній війні є можливість багаторазового захоплення уваги тих самих людей;
- інформаційна війна має більш непередбачуваний результат;
- небезпека інформаційної війни у тому, що вона не несе видимих руйнувань, отже не завжди може бути відразу розпізнана.

Основними характеристиками інформаційної війни, позначаючи її як один із способів гібридної війни, є:

- нестандартність: такі конфлікти відбуваються поза класичними полями бою;
- комплексність: використовуються різні методи для досягнення мети;
- масштабність: зачіпаються як відносини міждержавного рівня, так і життя простих громадян.
- висока непередбачуваність: результат інформаційної війни важко передбачити.

Зрозуміло, що інформаційна війна має потужний вплив на сучасну політику та міжнародні відносини. Країни, що мають розвинуті інформаційні технології, можуть з легкістю використовувати ці засоби для досягнення своїх цілей. Інформаційна війна також підкреслює значення кібербезпеки, адже кібератаки можуть спричинити значну шкоду економіці, інфраструктурі та національній безпеці.

Соціальні мережі, новинні портали, відеохостинги, месенджери – це лише деякі з каналів, через які може поширюватись дезінформація та пропаганда. Такі

дії можуть включати в себе розповсюдження фейкових новин, фото та відео, створення фальшивих облікових записів для поширення певних думок чи настроїв серед населення, а також здійснення кібератак на важливі інфраструктурні об'єкти [46, с. 152].

Додатковою складністю інформаційної війни є те, що інтернет дозволяє анонімність та прихованість джерел інформації. Це ускладнює завдання виявлення дезінформації та визначення, яка інформація є правдивою, а яка – ні. Водночас, така ситуація створює можливість для акторів, які зловживають цим, вплинути на думку громадськості та спотворити факти [25].

В сучасному цифровому столітті соціальні мережі стали не тільки засобом спілкування та обміну інформацією, а й потужним інструментом впливу на громадську думку та міжнародні події. Під час гібридних війн, коли комбінуються різноманітні методи ведення конфлікту, використання соціальних мереж набуває великого значення.

Соціальні мережі, такі як Facebook, Twitter, Instagram та інші, здатні швидко поширювати інформацію серед широкої аудиторії. Вони стали платформою для вираження поглядів, обговорення подій та формування громадської думки. Під час гібридних війн, сторони конфлікту використовують ці мережі для поширення пропаганди, маніпулювання інформацією та впливу на настрої громадськості.

Т. Ніссен зазначає, що соціальні мережі стали ідеальною платформою для поширення пропаганди та дезінформації. Вони дозволяють сторонам конфлікту швидко поширювати фейкові новини, спотворену інформацію та хибні наративи. Гібридні актори можуть використовувати вигадані історії для впливу на громадську думку, створення певних настроїв та навіть провокувати міжнародні конфлікти. Це може призвести до збурення громадськості, створення розколів у суспільстві та недовіри до державних інституцій [117].

Соціальні мережі дають можливість маніпулювати громадською думкою шляхом створення віральних та емоційних контентів. Зображення, відео та тексти можуть бути добре адаптовані для сприйняття цільовою аудиторією. Це

дозволяє сторонам конфлікту формувати певний наратив, змінювати ставлення громадськості до певних питань та подій, а також викликати емоційну реакцію, яка може вплинути на їхнє рішення.

Використання соціальних мереж під час гібридних війн впливає на всі аспекти конфлікту – від політичних рішень до суспільних настроїв. Інтернет став ареною, де відбувається боротьба за думки та підтримку громадськості. Для забезпечення стабільності та миру в цьому цифровому світі необхідно розробити ефективні методи протидії маніпуляціям та дезінформації, а також підвищити кібербезпеку для забезпечення безпеки та стабільності в міжнародних відносинах [117].

Також важливо наголосити на зростаючій ролі штучного інтелекту (ШІ) та автоматизованих систем у гібридних війнах сучасності. ШІ та автоматизовані системи набувають ключового значення, сприяючи не тільки зміні парадигми ведення війни, але й викликаючи нові етичні, правові та геополітичні питання.

Штучний інтелект та автоматизовані системи забезпечують гібридним конфліктам нові можливості та інструменти. Один із важливих аспектів – це здатність ШІ аналізувати величезні обсяги даних за короткий час. Це дозволяє отримувати важливу інформацію для прийняття рішень, прогнозування руху противника, а також для створення стратегій дезінформації та маніпулювання інформацією. Завдяки ШІ можливе швидке і точне розпізнавання паттернів та зв'язків, які були б недосяжні для людини [80, p. 10].

Поняття автоматизованих систем також включає в себе роботизовані військові системи та безпілотні апарати. Ці технології роблять можливим ведення військових дій з меншим ризиком для життя військових. Проте, це також породжує етичні питання стосовно використання смертельної сили без прямої участі людини в процесі прийняття рішень [83].

Важливим аспектом в ролі ШІ та автоматизованих систем є їхня здатність впливати на громадську думку та маніпулювати інформацією. ШІ може створювати великі обсяги контенту, який підтримує певний наратив, формуючи

сприйняття подій відповідно до бажаного результату [134]. Це відкриває можливість для створення фейкових новин, дезінформації та маніпуляцій.

Ця нова реальність військових конфліктів ставить перед суспільством, політичними лідерами, вченими та міжнародними організаціями низку складних завдань. Розвиток штучного інтелекту та автоматизованих систем вимагає відповідних правових, етичних та регуляторних рамок. Міжнародні договори та угоди, спрямовані на обмеження використання автономних систем у воєнних діях, стають надзвичайно важливими для підтримання стабільності та гуманітарних принципів.

Узагальнюючи, інформаційна війна – це комплекс дій, спрямованих на маніпуляцію інформацією з метою зміни громадської думки, політики чи поведінки. Вона включає в себе використання інформаційних технологій та соціальних мереж, розповсюдження дезінформації, пропаганди, а також інші методи впливу на суспільство. Інформаційна війна стає ключовою складовою гібридної війни, де засоби інформаційного впливу використовуються разом зі стратегіями політичних, економічних та військових дій для досягнення стратегічних цілей. Одним із головних аспектів інформаційної війни є використання пропаганди для формування певної картини світу та впливу на думку громадськості. Це може призвести до розпалювання емоційних реакцій, створення враження загрози та необхідності дій. Інформаційні кампанії можуть також спричинити поділ суспільства, підрив довіри до влади тощо.

2.2. Політичний компонент гібридної війни

Політичний вплив можна розглядати як здатність впливати на рішення, дії та настрої інших акторів за допомогою політичних, дипломатичних та інших засобів. У контексті гібридної війни, політичний вплив є компонентом, завдяки якому досягаються стратегічні цілі без відкритого військового конфлікту. Важливим аспектом є те, що політичний вплив може здійснюватися як на внутрішньому, так і на міжнародному рівнях.

Однією з ключових цілей є досягнення політичної дестабілізації в країні-жертві. За допомогою дезінформації, маніпуляцій та психологічного тиску, супротивник може підривати довіру громадян до своїх владних структур, створюючи атмосферу хаосу та невпевненості. Це може призвести до подальших соціальних розбіжностей та розколу в суспільстві [35, с. 113].

Один з ключових інструментів – це інформаційна війна. За допомогою розповсюдження фейкових новин, дезінформації та маніпуляцій, ворожа сторона може формувати певну картину подій, спотворюючи реальну ситуацію. Це не лише впливає на громадян, але й може кардинально змінити рішення міжнародних партнерів [32, с. 196].

На переконання Д. Дубової, політичний компонент гібридної війни також націлений на дискредитацію політичних інститутів та лідерів країни-жертви. Ворожа сторона може розповсюджувати компрометуючу інформацію, знижуючи довіру громадян до власних владних структур [20, с. 37].

Важливо підкреслити, що політичний вплив у гібридній війні може бути ефективнішим за військові дії. Він дозволяє досягти цілей з меншими витратами та меншим ризиком негативної міжнародної реакції [51 , p. 46].

Політичний вплив в контексті гібридної війни стає важливим інструментом здобуття стратегічної переваги без відкритого військового конфлікту. Він відіграє критичну роль у дестабілізації політичних процесів та створенні негативного впливу на суспільство і міжнародне співтовариство.

Політична дестабілізація та внутрішній конфлікт стають ключовими інструментами, які ворожі сторони можуть застосовувати для досягнення своїх стратегічних цілей. Політична дестабілізація передбачає цілеспрямовані дії, спрямовані на підрвання стабільності політичних інститутів та звичайного функціонування суспільства. Це може включати в себе підтримку опозиційних рухів, створення конфліктних ситуацій та зниження довіри до владних структур. Мета полягає в тому, щоб змусити країну-жертву витрачати свої ресурси на розв'язання внутрішніх проблем, замість спрямовувати їх на протидію зовнішнім загрозам.

Внутрішній конфлікт є одним із наслідків політичної дестабілізації, але також може бути свідомо заохочуваним та маніпульованим для досягнення гібридних цілей. Створення підгрунтя для конфлікту між різними групами суспільства може послужити ворогові як інструмент для відволікання уваги внутрішніх акторів від зовнішніх загроз. Поділ суспільства на протилежні табори створює ситуацію, коли державні ресурси спрямовуються на вирішення внутрішніх конфліктів, а не на відсічення гібридної агресії.

Політична дестабілізація та внутрішній конфлікт дозволяють ворожим сторонам забезпечити собі перевагу. Вони можуть маніпулювати інформацією та емоціями громадян, сприяючи поширенню недовіри. Це зазвичай веде до ослаблення політичних лідерів, збільшення напруженості в суспільстві та зниження здатності країни до опору [51 , p. 46].

Політичні інструменти, використовувані в рамках гібридної війни, включають різні методи впливу на ворожі держави. Однією з таких методик є підтримка опозиційних рухів, яку можна здійснювати через фінансування, надання технічної підтримки та поширення ідеологічних установок. Такий підхід може призвести до дестабілізації внутрішньої ситуації та послаблення влади в цільовій державі [37].

У той же час, корупція грає важливу роль у гібридних війнах. Ворожі сили можуть використовувати корупцію як інструмент для залучення впливових осіб і інституцій у цільовій державі до своїх інтересів. Це може включати в себе запропонування хабарів чи інших форм хабарництва посадовим особам для виконання дій, що сприяють інтересам ворожих сил. Корупція створює вразливості в системі влади та підриває довіру громадян до їхнього уряду.

Вона стає одним із інструментів політичного впливу в рамках гібридної війни, який може сприяти досягненню стратегічних цілей шляхом створення нестабільності та зниження здатності країни до опору. Також корупція стає ключовою складовою гібридних стратегій для досягнення політичних та стратегічних цілей без відкритої військової агресії.

Корупція, як інструмент гібридної війни, може включати в себе різні форми і вияви. Це може бути використання хабарів та впливу на ключових державних посадовців з метою отримання стратегічної інформації, порушення національної економіки чи підірвання довіри громадян до владних структур. Корупція може також використовуватися для створення негативного іміджу держави та дискредитації її політичного лідерства на міжнародній арені.

Внутрішня корупція може призвести до дестабілізації економічної, політичної та соціальної ситуації в країні. Забезпечення важливих державних послуг, здоров'я та освіти може бути під загрозою через відмову надавати їх у разі неправомірної вигоди.

У міжнародному контексті корупція може бути використана для втручання у внутрішні справи інших країн. Фінансування політичних партій, маніпулювання виборчими процесами та вплив на законодавчі рішення стають способами втручання у внутрішні справи інших країн [107].

К. Маклаклан запевняє, що держави та корумпована еліта звертаються до корупції для досягнення цілей зовнішньої політики та способу ведення гібридної війни. Цей вид корупції не спрямований на отримання економічної вигоди: скоріше, він спирається на готовність відмовитися від економічної вигоди на користь збільшення впливу, отримання бажаних політичних результатів і здатності поширювати політичні норми та практики [100].

У разі успіху використання корупції в рамках зовнішньополітичного арсеналу може дозволити елітам однієї країни утримувати цілі політичні класи в інших країнах з метою підривання урядових інститутів та здійснення незаконного впливу в цільовій державі.

У своїй найнебезпечнішій і довготривалій формі ці схеми «корупції як державного управління» побудовані на політичній та економічній залежності, як правило, у ключових секторах, таких як енергетика, оборонне та військове забезпечення або навіть інфраструктурні проеєкти.

Наприклад, у спробах Росії формувати внутрішньо- та зовнішньополітичні рішення України протягом останніх двох десятиліть використовувалися

корупційні схеми в енергетичному секторі. Ці схеми скористалися залежністю України від російського державного енергетичного гіганта «Газпром» щодо імпорту газу, щоб зміцнити та використати корумповані мережі в Україні для досягнення цілей зовнішньої політики. Коливання цін на газ, часто організоване політичними господарями Газпрому; загрози припинення поставок; використання непрозорих, анонімних посередників між «Газпромом» і українською державною енергетичною компанією «Нафтогаз» для перенаправлення прибутків олігархам і політичним партіям уможливило поєднання тиску та підкупу, що сприяло зовнішньополітичним інтересам Росії [100].

Корупція також може бути інструментом гібридної війни, поряд з дезінформацією та кібератаками. Внески на виборчу кампанію можна обміняти на політичний вплив або обіцянки прийняти рішення, вигідні окремим особам. Наприклад, колишнього президента Литви Р. Паксаса звинуватили в тому, що його кампанію фінансували особи, підозрювані у зв'язках з російською організованою злочинністю, в обмін на надання їм литовського громадянства та розголошення секретної інформації про розслідування їхніх ділових операцій [115]. Хоча з Р. Паксаса згодом зняли звинувачення в розголошенні державної таємниці, подібні схеми могли бути використані для підриву керівних установ сфери інфраструктури, оборони тощо.

«Азербайджанська пральня», схема відмивання грошей, перевела загалом 2,9 мільярда доларів США від азербайджанських компаній і урядових відомств через чотири британські підставні компанії [120]. Ці гроші фінансували як приватне збагачення, так і зовнішньополітичні схеми, спрямовані на покращення міжнародної репутації країни. Схоже, що азербайджанські офіційні особи використовували кошти, що проходили через «пральню», для підкупу членів Парламентської асамблеї Ради Європи, щоб послабити офіційну критику щодо дотримання прав людини в Азербайджані; у той же час високопосадовці використовували його як фонд для оплати товарів і послуг класу люкс [120].

Подібні схеми також створюють значні проблеми в розвинених демократіях. Зрештою, використання корупції для підриву національних і міжнародних інститутів становить загрозу системі, на якій базується багато суспільств [88].

У США вже визнали зв’язок між корупцією та безпекою, і Конгрес закликав вжити заходів для блокування фінансових потоків, які можуть не лише підірвати безпеку союзників, а й вплинути на політичну систему США. В ЄС було досягнуто ще більшого прогресу у вирішенні проблеми поширеності анонімних компаній і звітності про фінансові потоки, але перевірка даних, моніторинг фінансових потоків і розуміння їх мети постійно натикаються на певні перепони [100].

Є. Тюхтенко також зазначає, що небезпека корупції і пов'язаних з нею фінансових потоків полягає не тільки в зниженні здатності країни мобілізувати ресурси для фінансування сталого розвитку прав людини, але і в тому, що вони сприяють ослабленню державних інститутів, підривають принцип верховенства закону і функціонування системи кримінального правосуддя. В результаті корупція стає ефективною зброєю гібридної війни, оскільки корупційна ерозія суспільства відбувається за рахунок експорту корупційних впливів і завдає удару по найбільш важливим цілям цієї країни: інститутам демократії і верховенства закону [44].

Таким чином, політична сфера гібридної війни виявляється надзвичайно складною для цього нового виміру конфліктів. Вона включає в себе використання різноманітних інструментів, такі як дезінформацію, маніпуляції , корупцію та вплив на ключові політичні рішення. У світі, де міжнародні відносини стають все більше складними, а розмаїття технологічних можливостей надає нові інструменти для досягнення цілей, роль політичної сфери у гібридних конфліктах зростає.

2.3. Воєнний компонент гібридної війни

Одним із інструментів силової лінії у структурі гібридних воєн є приватні військові компанії (ПВК). Дані суб'єкти, отримавши санкцію застосування військової сили, можуть нести серйозну загрозу для міжнародної та національної безпеки і здійснювати на користь замовника різну діяльність, зокрема неправомірну і протизаконну [75, p. 178]. На практиці мають місце три форми участі ПВК у гібридних війнах:

1) ведення воєнних дій державою із залученням ПВК. У таких конфліктах держави беруть пряму участь, водночас використовуючи як регулярний озброєний контингент, так і приватні військові компанії у процесі здійснення військових операцій.

Ця модель взаємодії ПВК з державами активно використовується у XXI ст. Послуги військових фахівців дають змогу комплексно вирішувати завдання військового характеру, збільшувати ефективність військово-цивільного співробітництва, а також забезпечувати різнопланову підтримку регулярним військовим з'єднанням. Для держави в такій ситуації відсутня необхідність обґрунтовувати використання великого контингенту власних збройних сил при конфлікті;

2) найм державою ПВК для реалізації операцій. Держава, маючи певний політичний чи економічний інтерес у конкретному нестабільному регіоні, наймає приватні військові компанії для просування власної позицій. Така модель на легальному полі дозволяє владі впливати на стратегічний баланс сил, не вдаючись до прямої інтервенції та інших дій, які можна засудити з погляду міжнародного права.

Ця форма участі ПВК у гібридній війні забезпечує державі свободу дій: приватні військові компанії можуть бути залучені з метою усунення «незручних» політичних та громадських діячів, для забезпечення підтримки екстремістських чи націоналістичних угруповань або ведення підривної діяльності на території ворожої країни.

Також одним із різновидів даної моделі є використання стратегії «Proxy Warfare». Це війни, що проводяться між двома державами на території третьої країни під прикриттям вирішення внутрішньополітичного конфлікту з використанням частини робочої сили, ресурсів і території цієї країни як засіб для досягнення переважно іноземних цілей та іноземних стратегій.

У подібних конфліктах, де кілька сильніших держав можуть втрутитися у військове протиборство на території будь-якої держави та за допомогою ПВК активно просувати свою позицію, безпосередньо не беручи участі у конфлікті (Лівія, Сирія), озброєне протиборство збільшує свій масштаб і стає більш запеклим, військові дії продовжуються протягом тривалого часу і проводяться на шкоду мирному населенню та інфраструктурі держави (інтереси країни, на території якої відбувається конфлікт, як правило, не враховуються);

3) допомога ПВК у здійсненні військових дій, які ведуть інші держави. До цієї категорії відносяться конфлікти, де одній зі сторін надають підтримку приватні військові компанії держави, яка офіційно не входить у конфлікт. Така модель представляється допоміжною і здійснюється не лише у період гібридної війни, а й у процесі ведення традиційного військового протиборства.

Подібна форма військової допомоги союзникам або дружнім урядам здійснюється досить часто, тому що держава в даному випадку залучає лише фінансову складову. Подальше планування, контроль та координація дій військових фахівців та співробітників ПВК здійснюється країною, яка запросила відповідну підтримку.

Представлені вище основні моделі показують, що приватні військові компанії забезпечують інтереси держав та взаємодіють із різними акторами міжнародних відносин. Сама наявність військових конфліктів та збройних зіткнень стає причиною попиту «на військову експертизу та на військові послуги» [2].

Використання ПВК коштує дешевше, ніж розміщення регулярних військ за кордоном. ПВК мають певні операційні переваги, зокрема вони здатні:

- швидко та приховано розгортати війська та передислокуватися;

- менше обмежені бюрократичними процедурами контролю та швидше приймають рішення;
- швидко нарощувати бойові можливості без значних витрат;
- виконувати бойові та небойові завдання без залучення збройних сил [2].

Це дозволяє урядам використовувати ПВК для різноманітних завдань, у тому числі спеціальних місій. Крім виключно військових переваг, ПВК мають переваги і в політичному контексті.

Проблемою дислокації військовослужбовців ПВК на територіях інших держав є те, що це може здійснюватися без узгодження з міжнародними інституціями. Дислокація та участь ПВК у бойових діях у зоні конфлікту зазвичай не має сильного суспільного резонансу, на відміну від звичайних збройних сил [2].

Незважаючи на недавнє виникнення, ПВК стали складовою гібридних війн, що в той же час призвело до появи різноманітних проблем, починаючи від порушення прав людини і закінчуючи участю співробітників у військових операціях з метою повалення легітимного політичного режиму. Залучення ПВК може призвести до непередбачуваних наслідків та результатів для кожної із сторін, тому важливо, щоб при використанні приватних військових компаній державні структури не здійснювали безконтрольний аутсорсинг функцій збройних сил. Держава за такого співробітництва має бути домінантним членом [12].

У структурі гібридних воєн приватні військові компанії використовуються державами в комплексі з іншими стратегіями протистояння. Збільшення кількості приватних військових компаній як ефективного інструменту зовнішньої політики стимулює збільшення «числа малих та великих неоголошених воєн, у яких озброєне протиборство ведеться в умовах збереження між країнами формально мирних відносин» [58].

Використання приватних військових компаній у сучасному світі свідчить про необхідність врегулювати це питання на міжнародному рівні. Ми стали свідками активної участі приватних військових компаній у боротьбі з

міжнародним піратством і участі в зонах конфліктів – в Афганістані, Іраку, Лівії, Сирії та інших гарячих точках світу. На жаль, Україна має свій власний досвід щодо ПВК. Йдеться про використання Росією військових підрозділів під час окупації Кримського півострова та повномасштабну збройну агресію проти України [2].

У багатьох країнах законодавство, що регулює діяльність приватних військових компаній, є неповним. Водночас деякі країни створюють приватні військові компанії без законних підстав. В першу чергу це стосується нашого геополітичного противника – Російської Федерації. Деякі з цих формувань замасковані в РФ під громадські організації або військово-патріотичні клуби. Донедавна приватні військові компанії вважалися недержавними підрядниками, які надавали професійні консультації, допомогу та послуги з безпеки. Тим не менш, Москва використовує ПВК як інструмент для забезпечення правдоподібного заперечення, економічно і політично стійкого військового впливу за кордоном. В останні роки РФ вивела цю практику на новий рівень, продемонструвавши, що може виконувати наступальні завдання та фактично будувати кістяк окупаційної армії [2].

Початок російських приватних військових операцій було покладено розгортанням роти Слов'янського корпусу в Сирії. Приватна військова компанія «Slavonic Corps», зареєстрована в Гонконзі, була заснована в 2013 р. як дочірня компанія іншої російської «Moran Security Group». Мета її створення була визначена угодою з сирійським урядом, яка передбачала захист активів режиму Асада. Оскільки лідери групи безпеки Морана хотіли уникнути санкцій і втрати репутації за співпрацю з Асадом, «Слов'янський корпус» був створений в якості посередницької сили і одночасно «пілотного проекту» для наземних випробувань.

«Слов'янський корпус» був першим у Росії і багато в чому був досить експериментальним приватним військовим угрупуванням «нового типу», що займався завданнями, які зазвичай виконуються арміями, такими як фронтальні атаки та бойові дії, на відміну від західних ПВК, які в основному призначені для

допоміжних або навчальних цілей. Незважаючи на початковий невдалий досвід роботи з приватними військовими компаніями, Росія засвоїла уроки і використала досвід «Слов'янського корпусу» для подальшого розвитку більш ефективного недержавного військового формування «Вагнер».

Під час захоплення Криму в 2014 р. російські приватні військові компанії перебували в стадії формування і не могли служити прикриттям для так званої «самооборони Криму», «козаків» та інших проросійських радикальних груп і формувань. При цьому вони діяли спільно з підрозділами Сил спеціальних операцій і повітряно-десантних військ ЗС РФ відповідно до єдиної концепції і під єдиним командуванням.

Російська збройна агресія на сході України продемонструвала ефективність і важливість ПВК. На першому етапі їх основним завданням було розпалити і ще більше дестабілізувати ситуацію, спровокувавши її ескалацію від політичного протистояння до фази прямого насильства і бойових дій.

Російські ПВК зазвичай вербують бійців в Росії і з пострадянських держав. Багато найманців були завербовані з тимчасово окупованих територій України - окремих районів Донбасу і Криму. Бойовий досвід участі ПВК в Україні і Сирії дає Кремлю можливість використовувати цей інструмент для поширення впливу Росії на інші регіони.

Отже, в останні десятиліття сучасної світової політики спостерігається зростання значення приватних військових компаній у контексті гібридних війн. Гібридні війни, які поєднують в собі військові, інформаційні, економічні та політичні аспекти, створюють сприятливе середовище для діяльності цих компаній.

2.4. Економічний компонент гібридної війни

У глобально мережевому світі економіка нерозривно пов’язана з національною та міжнародною безпекою та впливає на ширші геополітичні сфери будь-якої країни [121].

Починаючи з афінської заборони на торгівлю з Мегарою напередодні Пелопоннеської війни держави використовували економічні важелі для

досягнення своїх стратегічних цілей [94]. Однак до кінця 1960-х років економічна безпека не була предметом спеціального дослідження. Наприкінці 1960-х років економічні питання стали більш важливими предметами національної безпеки [131]. Хоча раніше це розглядали як спосіб змусити цільовий уряд змінити свою політику, з кінця 1990-х критики зосередилися більше на дослідженні наслідків для громадян, ніж для уряду.

На тлі глобалізації за останні кілька десятиліть економіка та національна безпека стали нерозривно пов'язані. Як зазначив Е. Каміллі: «Однією з головних проблем, які пов'язують економіку з безпекою, є здатність першої перетворювати багатство на владу. Економіка, по суті, може визначити, який рівень безпеки держава здатна отримати; чим багатша держава, тим більше військових можливостей вона здатна мобілізувати. Таким чином, відносне економічне зростання відіграє важливу роль у визначенні могутності держав і, таким чином, її положення в системі безпеки» [57]. Ці зв'язки представляють як можливості, так і потенційні внутрішні та зовнішні загрози для національної безпеки будь-якої країни. Згідно з Р. Н. Купером, економічна влада здебільшого використовується як інструмент для покарання чи винагороди інших сторін, залежно від того, чи вони реагують так, як хоче сильніша сторона. Наявність сильної економіки є дуже важливим інструментом підтримки національної безпеки. Однак якщо ця влада використовується для просування національних інтересів однієї країни на шкоду іншій, тоді вона стає економічним примусом [62]. Тому питання про те, чи є вплив економічної влади доброякісним чи шкідливим, є дуже дискусійним і відкритим. Оскільки переважна більшість дослідників стверджує, що військова сила більше не має великого значення, майбутній характер суперництва між різними націями залежатиме від економічної сили [62]. На цьому тлі економічна безпека стала важливим стратегічним пріоритетом. «Загрози для життєво важливих економічних процесів» були названі однією з шести найактуальніших загроз національній безпеці в Інтегрованій стратегії міжнародної безпеки (IISS) 2018–2022 [121]. Ми

спробуємо розглянути наслідки, коли велика держава намагається економічно вплинути на малі держави.

Економічний примус є однією з найбільш застосовуваних форм гібридної війни як альтернативи застосуванню сили. У сучасному глобалізованому світі економічні відносини сприйнятливі до маніпуляцій заради політичних цілей [71, p. 5]. Основною загрозою економічній безпеці будь-якої країни є економічна залежність. Економічна безпека держави, у свою чергу, є основним гарантом незалежності, стійкості та успіху [72, p. 462].

Стратегія економічного примусу як елемент гібридної війни передбачає діяльність гібридного нападника, що спрямована на отримання вигоди від своєї економічної переваги та залежності жертви. Г. Нордбі визначив чотири типи економічного примусу: зовнішня допомога, грошова влада, фінансова влада та торгівля [118]. Кожен із цих «інструментів» походить від рівня залежності країни, яка є економічно підвладною.

Стосовно першого типу – зовнішньої допомоги – слід зазначити, що оскільки деякі країни економічно значно відстають від розвинутих країн, зовнішні санкції можуть завдати шкоди їхній економіці. Економічна дестабілізація, що включає санкції, погрози розірвати життєво важливі комерційні зв’язки, прихований або явний економічний примус, спрямований на послаблення держави-мішені, призводить до маніпулювання нею.

Що стосується третього типу, Г. Нордбі стверджує, що використання фінансової влади не є таким вільним у своїх діях, як грошова влада, оскільки уряд не має одноосібної влади над прямими іноземними інвестиціями. Проте фінансова та грошова влада певною мірою взаємопов’язані, оскільки обидві пов’язані з торгівлею валютними активами. Теоретично фінансова влада більшою мірою залежить від волі суспільства. Заходи фінансового примусу впливають на різні частини економіки [118].

Вплив економічного розвитку зовнішніх гравців на суверенітет і незалежність слабких країн неминучий. У разі маніпулювання цим важелем вплив закінчиться економічним примусом і сприятиме посиленню політичного

впливу. Примус – це політичний акт сильнішої країни, який змушує слабшу країну йти певним шляхом, якому сильніша держава віддає перевагу. К. Чейз-Данн підкреслює два види міжнародної економічної залежності:

1) залежність від інвестицій;

2) залежність від іноземного кредиту [59, p. 727].

Якщо певний аспект економіки країни повністю підтримується іноземною державою, такий тип економічної залежності може мати лише негативний вплив на цей сектор [118]. Звичайно, країна-донор може спрямувати уряд на бажані зміни без шкоди для інших сфер цільової країни, але це не завжди працює. Проте країнами, чия економіка значною мірою залежить від іноземних держав, легше маніпулювати. Наприклад, Республіка Вірменія, яка має дружні відносини лише з двома з чотирьох своїх сусідів (Грузією та Іраном), економічно залежить від Росії та Ірану.

Результати аналізу різних регіонів показують, що другий тип економічної залежності, представлений К. Чейз-Данном, є більш небезпечним. Насправді, якщо країни можуть створити баланс інвестицій і проводити політику диверсифікації, то перший тип взагалі не становить загрози. С. Кім виправдовує вразливість будь-якої маленької держави до примусу трьома факторами:

• концентрація торгівлі;

• непрозорість;

• залежність від зовнішньої допомоги [92, p. 16].

Через концентрацію експортних товарів будь-яке обмеження експорту завдасть серйозної шкоди малим економікам, але не завдасть великої шкоди регіональним чи глобальним державам. У двосторонніх відносинах ступінь прозорості внутрішньої політики малої держави впливає на її сприйнятливість до примусу. Умовно кажучи, непрозоре середовище в маленькій державі дає великій широкі можливості для втручання в процеси формування політики та впливу. Економічно залежні країни надзвичайно вразливі до зовнішнього тиску [92, p. 18].

В аналітичній роботі на тему «Виявлення та аналіз корозійних інвестицій в економіку України як елемент гібридної війни» підготовленій Центром аналітичних досліджень і протидії гібридним загрозам зазначається, що економічна війна – це особливий театр, на якому агресор намагається завдати фатальної шкоди економіці країни-жертви, використовуючи всі наявні засоби [45].

Існує два способи ведення економічної війни: «зіткнення» з економікою жертви і «проникнення» в неї. «Зіткнення» передбачає заходи, спрямовані на послаблення економіки країни-жертви без встановлення контролю над її підприємствами. Заходи спрямовані на припинення або ускладнення потоку товарів і технологій з країни-жертви в країну-агресора або у зворотному напрямку.

«Проникнення» в економіку передбачає встановлення власності або контролю над її підприємствами, а корозійний капітал є найпідступнішим способом. Він передбачає прямі чи непрямі інвестиції в підприємства з метою завдати шкоди економіці країни-жертви та національним інтересам, а іноді й на користь власної економіки агресора. Це зрештою має негативні наслідки для країни-жертви. Український експорт сирого титану, наприклад, контролюється Росією, забезпечуючи агресора матеріалом, необхідним для виробництва зброї та військової техніки, які використовуються у відкритій війні проти України. Іншими словами, корозійні інвестиції – це інвестиції в економіку, які переслідують не економічні, а політичні цілі, зокрема знищення або підкорення потерпілої держави.

На перший погляд, цілями корозійних інвестицій є конкретні підприємства. Але ширші цілі включають знищення певних секторів економіки та досягнення політичних цілей. Справжні цілі агресора прояснюються на завершальному етапі конкретної операції, коли запобігти руйнівним наслідкам важко, а в окремих випадках неможливо [5].

За 30 років незалежності України з понад 1500 стратегічних підприємств близько 42% були ліквідовані або перебувають у стані банкрутства. До найбільш

вразливих сфер належать виробництво (в якому ліквідовано близько 50% діючих компаній), гірничодобувна промисловість і розробка кар'єрів (близько 47%) та науково-технічна діяльність (близько 35%) [5].

На тлі наявності внутрішніх чинників, таких як збитковість і корупція серед вітчизняних еліт, дослідження виявляють корозійний вплив Російської Федерації як на окремі підприємства, так і на цілі галузі, які були або знищені, або взяті під контроль агресора.

З 2001 по 2014 р. видобуток і збагачення титану в Україні фактично перебували під монопольним контролем проросійського олігарха, а видобуток використовувався для задоволення потреб Російської Федерації. Навіть після першого етапу відкритого вторгнення Росії в Україну у 2014 р., коли держава повернула частину своїх виробничих потужностей, агресор удосконалив методи впливу, що дозволило зберегти прихований контроль над галуззю.

Гібридний вплив Російської Федерації в нафтопереробній промисловості призвів до того, що станом на 2014 р. лише одне з шести нафтопереробних підприємств могло функціонувати, і воно не могло отримувати сиру нафту з Російської Федерації. Руйнування галузі відбувалося в чотири етапи: гальмування українського виробництва сировини шляхом демпінгування експортних варіантів за низькими цінами; припинення переробки нафти на підприємствах, контроль над якими раніше встановила Російська Федерація; припинення перекачування сировини на інші українські НПЗ; та протидія диверсифікації поставок нафти в Україну з інших країн.

Ліквідація проросійським політиком єдиного на той час в Україні виробника офсетного паперу спричинила не лише посилення залежності України від російського імпорту цієї продукції, а й перешкоди в роботі українських видавництв. Водночас створювалися умови для збільшення потоку російської друкованої продукції, що сприяло негативному впливу на українське суспільство.

Проведене дослідження Центром аналітичних досліджень і протидії гібридним загрозам показало, що основний спосіб російського впливу на

економіку жертви – корозійні інвестиції – використовуються в поєднанні з іншими методами, такими як проникнення у топ-менеджмент підприємств без отримання корпоративних прав, припинення поставок стратегічної сировини, або пошкодження інфраструктури [5].

Оскільки сильна економіка кожної країни є головною привілегією у боротьбі з гібридною війною, першим завданням є подолання економічної неспроможності бідніших верств населення шляхом проведення конкретних реформ. Некінетичні гібридні стратегії паралізують здатність держави приймати рішення за несприятливих обставин. Якщо характер загрози змінюється швидко й агресивно, необхідно адаптувати нові правила, щоб уникнути ізоляції, деморалізації та глобальних втрат [127].

Економічна залежність є однією з найнеобхідніших умов успішної гібридної війни. Дебілізація економіки може призвести до прямого падіння будь-якої країни тому що економіка є одним із найважливіших елементів національної могутності [65]. Проте С. М. Дейспрінг стверджує, що економічні важелі слід використовувати до тих пір, поки вони не зруйнують спроможність або готовність цільової країни чинити опір, але не до тих пір, поки економічна система не буде непоправно зруйнована [64].

У гібридній війні агресор, перш за все, повинен мати можливість «ескалаційного домінування». Це концепція збалансованої потужності, коли зловмисник може атакувати ціль на різних рівнях ескалації [111]. Доказом цього є криза, яка сталася на початку січня 2022 р. в Казахстані. Ця криза зробила найбільш процвітаючу та стабільну країну Центральної Азії крихкою та слабкою. Це також довело, як економіку можна використовувати як інструмент для розхитання всієї країни та підриву її національної безпеки [85].

У все більш нестабільному глобальному торговельному середовищі використання економічного примусу великими державами для досягнення політичних цілей створює нові бізнес-ризики [136]. Потенціал економічного примусу в торгівлі є на користь імпортера, тому що він фактично може вибрати

будь-якого експортера для цієї продукції. Тому експортеру важче знайти альтернативні ринки для своєї продукції [118].

За словами С. Дейспрінга, здатність цільової держави захищати критично важливу економічну функцію може бути легко підірвана блокуванням імпорту будь-якого критично важливого ресурсу [64]. Це доводить гостроту економічної складової гібридної війни проти економічно незалежних країн.

Таким чином, економічна залежність є однією з головних причин, через які слабкі країни відмовляються від свого суверенітету перед обличчям гібридної війни, яка ведеться проти них. Найбільш поширеними інструментами примусу, які можуть бути застосовані проти країн є імпортні тарифи та заборони/обмеження на експорт, припинення іноземної фінансової допомоги, що, у свою чергу, послаблює економіку окремих країн регіону.

Висновки до розділу 2

Основою ведення гібридної війни є синхронне використання різноманітних засобів насильства, пристосованих до конкретних уразливих місць у всьому спектрі соціальних функцій для створення синергічного ефекту. Уразливість може бути в будь-якій критичній функції (секторі) держави і, таким чином, дати атакуючій країні можливість скористатися умовами та використати їх, залежно від засобів, які є в її розпорядженні. Будь-яка сфера мирних суспільств, політичний чи неполітичний, військовий чи невійськовий, може бути використаний як зброя для ведення війни.

Інформаційний компонент гібридної війни включає в себе маніпулювання інформацією, дезінформацію та психологічні операції. Посилення доступу до інформаційних ресурсів дозволяє створити образ ворога, змінити сприйняття ситуації та викликати паніку серед населення. Інформаційні атаки можуть викликати недовіру до власної влади, зробити некомфортними зовнішні відносини і порушити громадський порядок.

Вплив на політичний процес і рішення може бути досягнутий шляхом підкупу, шантажу або «підриву» політичних фігур. Відвертий або прихований

вплив на внутрішні суперечності держави може послабити її позицію на міжнародній арені.

В рамках воєнного компонента в гібридних війнах, приватні військові компанії (ПВК) відіграють значущу роль, впливаючи на сучасні воєнні конфлікти та їх наслідки. Економічний компонент в гібридній війні орієнтується на використання економічних засобів для підриву стійкості держави. Економічний тиск, санкції, вплив на зовнішньоекономічні зв'язки можуть призвести до економічного занепаду, що збільшує вразливість країни.

Загалом, інформаційний, політичний, воєнний та економічний компоненти гібридної війни взаємодіють і взаємопідсилюють один одного.

РОЗДІЛ 3. СВІТОВИЙ ДОСВІД ВЕДЕННЯ І ШЛЯХИ ВИРІШЕННЯ ГІБРИДНИХ КОНФЛІКТІВ

3.1. Світовий досвід ведення гібридних конфліктів

Переглядаючи припущення та дослідження різних питань пропаганди та управління державою за останні роки, можна виявити, що гібридна війна не є новою концепцією, як сьогодні вважають багато дослідників [52]. Поєднання звичайних і нерегулярних методів не є новими і використовувалися протягом всієї історії.

Деякі дослідники називають першою гібридною війною Пелопоннеську війну в п'ятому столітті до нашої ери. Проста загроза гібридної війни змусила спартанців шукати дипломатичні шляхи вирішення конфлікту.

Кілька прикладів такого типу бойових дій можна знайти у ході Війни за незалежність США (об’єднання Континентальної армії Джорджа Вашингтона з військами ополчення) та Наполеонівських війнах (британські регулярні війська співпрацювали з іспанськими партизанами) [81].

Можна знайти приклади гібридної війни в менших конфліктах протягом XIX століття. Наприклад, між 1837 і 1840 роками Р. Каррера, лідер консервативних селянських повстанців у Гватемалі, провів успішну військову кампанію проти лібералів і федерального уряду Центральної Америки, використовуючи стратегію, яка поєднувала класичну партизанську тактику зі звичайними операціями. Гібридний підхід Р. Каррери до війни дав йому перевагу над його чисельно переважаючими та краще озброєними ворогами [99].

Гібридна війна – це не лише явище західного світу, як показує Друга китайсько-японська війна 1937-1945 рр. Мао Цзедун та його генерали стали експертами у поєднанні регулярних і нерегулярних сил для нападу на ворога як симетричним, так і асиметричним способом. Зрештою, він явно сприймав партизанські та конвенційні сили як існуючі на одному континуумі. Після капітуляції Японії його комуністичні сили використовували техніки гібридної війни проти своїх націоналістичних ворогів. Регулярні дивізії комуністів були

дуже ефективними, як це показали бої не лише проти націоналістичних сил Чан Кайші в Китаї, але й проти американських сил в Кореї в 1950 р. Націоналістичні сили фактично переважали комуністів, але натиск сотень тисяч партизан призвів до розсіювання значної частини сил націоналістів. Гібридна війна дозволила силам здобути перевагу в критичних точках в Китаї під час кампаній 1948-1949 років, які завершилися вигнанням націоналістів з материка на Формозу (Тайвань). Комуністична перемога в китайській громадянській війні додатково підтвердила ефективність гібридної війни у відповідних географічних, історичних та культурних обставинах [54, p. 176].

У 1944 р. Радянський Союз розпочав гібридну війну. Коли тувинська армія перебувала в Європі, воюючи разом із Червоною армією проти Третього Рейху, Москва анексувала Тувинську Народну Республіку, змусивши тувинський уряд попросити приєднатися до Радянського Союзу [90].

У війні у В'єтнамі обидві сторони використовували тактику гібридної війни, при цьому США надали перевагу ЦРУ для підтримки партій громадянської війни в Лаосі та Камбоджійської громадянської війни, а також етнічних груп у В'єтнамі, а Радянський Союз підтримував міліцію В'єтконгу [98, p. 268].

Кінець холодної війни створив однополярну систему з переважаючою військовою силою США. Хоча це пом'якшило традиційні конфлікти, регіональні конфлікти та загрози, які використовують слабкі сторони звичайних військових структур, стають все більш частими [63].

Одним із найбільш часто цитованих прикладів гібридної війни є конфлікт 2006 р. між Ізраїлем і Хезболлою. Хезболла – це складна недержавна організація, яку спонсорує Іран. У цьому конфлікті Хезболла продемонструвала, як синергія різних методів ведення війни успішно примножила її перевагу над противником, заявленим як найпотужніші збройні сили Близького Сходу. Саме політика Хезболли, а не Ірану, призвела до викрадення ізраїльських військ, що стало поштовхом до війни [66]. У війні брали участь близько 3000 бійців Хезболли, які

були замасковані під місцеве населення, було атаковано приблизно 30 000 ізраїльських регулярних військ [79].

Група використовувала децентралізовані осередки, що складалися з партизанів і регулярних військ, озброєних зброєю, яку використовують національні держави, такою як протитанкові ракети, ракети, озброєні безпілотні літальні апарати та сучасні саморобні вибухові пристрої [81]. Осередки Хезболли збивали ізраїльські гелікоптери, пошкоджували танки Merkava IV, спілкувалися за допомогою зашифрованих мобільних телефонів і стежили за пересуванням ізраїльських військ за допомогою приладів нічного бачення та тепловізорів. Оперативники іранських сил Кудс виступали в якості наставників і постачальників передових систем [79].

Для розуміння гібридного контексту необхідно дослідити хронологію конфлікту та стратегічний контекст ситуації, тобто наявність факторів теорії та принципів гібридної війни. Друга ізраїльсько-ліванська війна 2006 р. загалом тривала 34 дні. З одного боку, була військова силу Ізраїлю, а з іншого – поєднання звичайних і нетрадиційних військових сил ліванського недержавного гравця, а саме Хезболли. Конфлікт розпочався 12 липня 2006 р. з нападу Хезболли на ізраїльські прикордонні служби безпеки, в результаті якого було вбито трьох і викрадено двох ізраїльських солдатів. Прем'єр-міністр Ізраїлю Е. Ольмерт дав дозвіл збройним силам розпочати наступальну операцію на об'єкти Хезболли на півдні Лівану, щоб впоратися з частими ракетними обстрілами Хезболли зазначених областей. Хоча ця атака була номінально зосереджена на Хезболлі, держава Ліван, уряд якої формально дистанціювалася від дій Хезболли, також була опосередковано атакована. Ізраїль спочатку відповів невдалою спробою врятувати своїх солдатів, а потім здійснив синхронні повітряні та наземні атаки на основні об'єкти інфраструктури разом із військово-морською блокадою портів Лівану на Середземному морі. Хезболла у відповідь випустила сотні ракет по півночі Ізраїлю та атакувала протикорабельними ракетами C-802 INS Hanit, корвет ВМС Ізраїлю, який здійснював морську блокаду портів Лівану. За цим послідували щоденні ракетні обстріли з обох

боків. Ізраїль вдарив по цілях ракетами із застосуванням забороненої хімічної зброї, а саме бомбами з білим фосфором, а Хезболла застосувала тактику партизанської та потужної інформаційної війни. За перші два тижні війни Хезболла випустила 2200 ракет по цілям в Ізраїлі, а ізраїльські ВПС відповіли жорстокими ракетними ударами по цивільних цілях у Бейруті [114, p. 184].

Атаки та бої тривали до 11 серпня 2006 року, коли збройні сили Ізраїлю (Ізраїльські сили оборони, IDF) чисельністю 30 000 солдатів спробували прорватися на південь Лівану, розпочавши операцію «Зміна оперативного напрямку 11», яка складалася з трьох місць атаки: перший був північний сектор, другий – центральний і західний сектори, а третій називався битвою за перетин стратегічної височини Ваді Салукі, яка мала забезпечити контроль над річкою Літані та проникнення в західні райони південного Лівану. Усі бої закінчувалися тим, що Ізраїльські сили оборони припиняли свою атаку, що підкреслило відсутність «чіткості політичних рішень і «системи командування та контролю» в Ізраїльських силах оборони, що спричинило великі втрати [91]. Великі втрати Ізраїльських сил оборони та сильний регіональний і міжнародний тиск разом із посередництвом ООН призвели до припинення вогню та ухвалення резолюції Ради Безпеки ООН № 1701.

Згідно з М. Метьюзом, війна врешті-решт закінчилася 1200 жертвами та понад мільйоном переміщених осіб у районі південного Лівану та північного Ізраїлю. З ізраїльської сторони було вбито 114 солдатів, а значну кількість ізраїльської військової техніки було пошкоджено або знищено, включаючи 10% звичайних танків, кілька вертольотів і кораблів. Понад 40 мирних жителів загинули, близько 4000 були поранені. За оцінками, Ізраїль зазнав збитків у розмірі близько 3,5 мільярдів доларів США через війну. З боку Лівану Хезболла втратила 600 бійців, і, за оцінками, їх військовий потенціал скоротився на 50%. Крім того, понад 1000 ліванських мирних жителів загинули і понад 4000 отримали поранення. Збитки від зруйнованої інфраструктури оцінили приблизно в 4 мільярди доларів США [102].

Ф. Хоффман стверджує, що під час 34-денного конфлікту Хезболла випустила майже 4100 ракет. Незважаючи на те, що більшість ракет були малої дальності та неточними, вони мали стратегічний ефект і змусили велику кількість жителів північного Ізраїлю евакуюватися. Ракетні атаки також мали психологічний вплив на Ізраїль, адже саме після конфлікту Ізраїль почав розвивати та будувати свою систему протиповітряної оборони під назвою «Залізний купол». Ізраїльські сили оборони здійснили майже 19 тис. польотів, скинувши майже 20 тис. бомб і 2 тис. ракет по майже 7 тис. цілей [81].

За словами Т. МакКулло та Р. Джонсона, при оцінці стратегічної концепції війни слід враховувати сильний історичний, політичний, релігійний та етнічний контекст і наступну напругу між Ізраїлем та Хезболлою [106, p. 19]. З одного боку, ми маємо Ізраїль як сильну єврейську державу, яка протягом всієї історії бореться за виживання на Близькому Сході та має сильну внутрішню економіку та розвинену оборонну промисловість; з іншого боку є Ліван, слабка мультикультурна країна з сумішшю східної та західної культури та релігії, поділом влади між низкою християнських і мусульманських релігій, поганою структурою уряду, слабкими Збройними Силами (LAF) і поганим управлінням оборонною сферою. Саме в цьому проміжковому просторі Хезболла знайшла можливість для своїх політичних та військових дій як шиїтська паремілітарна група, підтримувана антиізраїльськими союзниками. Хезболла доповнила свої асиметричні можливості партизанської війни та застосування злочинних і терористичних методів значними конвенційними здібностями використання ракет, артилерії, протиповітряної оборони, протикорабельних та протипротитанкових засобів.

Дії Хезболли у ізраїльсько-ліванській війні 2006 р. демонструють теорію, підтверджуючи важливість та синергію факторів гібридної війни відносно домінуючого опонента. Цей конфлікт показав здатність недержавного актора, який вивчив і проаналізував вразливості конвенційних сил з переважаючими військовими можливостями, успішно застосовувати гібридну війну.

Гібридні сили як недержавний актор завжди сприймають потенційних опонентів як загрозу та розуміють їх переваги. Цей підхід формує їх тактику і відводить від конвенційного підходу, змушуючи їх використовувати різні методи війни для забезпечення свого виживання. У даному випадку Хезболла сприймала Ізраїль як переважаючого опонента [114, p. 290], Ізраїльські Збройні Сили «рвонулися» в Ліван з надією швидко знищити свого опонента за допомогою своєї технології та конвенційної військової переваги. Але цього не сталося, тому що Хезболла вдалася до комбінування методів ведення війни, тобто до гібридного способу ведення війни. Ф. Хоффман стверджує, що війна на півдні Лівану вказала на слабкі сторони звичайних збройних сил [81].

Через очевидну асиметрію на полі бою гібридні сили, щоб забезпечити свою перевагу, змушені поєднувати звичайні військові технології з невійськовою партизанською тактикою дій. Порівняння можливостей і оснащення збройних сил показує, що ізраїльська армія мала у своєму складі танки Sabra Mark I і Merkava Mark IV, бойові броньовані машини Namer, бойові машини піхоти Golan Armored, самохідні артилерійські системи типу Lara і Sholef, а також ряд різних моделей безпілотних систем. На додаток до цього, його повітряний компонент мав винищувачі Kfir і F-16I, а також вертольоти, а також низку різних типів військових кораблів у військово-морському компоненті. З іншого боку, Хезболла залежала від наявних ресурсів під час конфлікту у вигляді різних типів протитанкової зброї, піхотної зброї, протитанкових і протипіхотних мін, саморобних вибухових пристроїв, артилерійської зброї малої дальності, а також кількох типів ракетних систем, які вона застосовувала в поєднанні звичайних і партизанських методів ведення війни.

Крім того, Хезболла воювала зі заздалегідь підготовлених і укріплених бункерів, які були розкидані глибоко по території південного Лівану. З цих точок опору, розподілених по глибині території, бойовики Хезболли здійснювали раптові атаки та дотримувались тактики «дій і залишай позицію», що ще більше дезорієнтувало противника. Цей тип війни називається тактикою ослаблення і проявляється у фізичній та психологічній сфері, що постійно знижує бойову міць

протиборчих сил. Особливо яскраво це проявилося у застосуванні мін, саморобних вибухових пристроїв, протитанкових реактивних снарядів, вогні з непрямої наводки в поєднанні з протитанковими та протипіхотними мінами та обстрілах піхоти із засідки, тоді як на самому початку конфлікту це відобразилося у викраденні людей.

Хезболла використовувала масову комунікацію, негайно розповсюджуючи фотографії та відео з поля бою. Ізраїль не програв війну на полі бою, але програв інформаційну битву [81].

Ще одним прикладом може слугувати досвід військових дій Ісламської держави Іраку та Леванту (ІДІЛ). ІДІЛ є недержавною організацією, яка використовує гібридну тактику проти звичайних іракських військових. ІДІЛ має перехідні прагнення та використовує нерегулярну та регулярну тактику та тероризм [87]. У відповідь Ірак сам звернувся до гібридної тактики, використовуючи недержавних і міжнародних акторів для протидії просуванню ІДІЛ. Сполучені Штати були гібридним учасником і використовували комбінацію традиційної військово-повітряної сили, радників урядових військ Іраку, курдських пешмерга; вони також тренували опозиційні сили в Сирії [126, p. 875].

У 2018 р. експерти звернули увагу на широке використання російським урядом у громадянській війні в Сирії та російсько-українській війні приватних військових підрядників, таких як група Вагнера, як ключової частини стратегії гібридної війни Росії для просування своїх інтересів і приховування своєїучасті та ролі [69]. Зокрема, Росія застосувала комбінацію традиційних бойових дій, економічного впливу, кіберстратегій і дезінформаційних атак проти України [141, p. 76].

У 2014 р. Росія почала військове втручання в Україну (розпочала так звану фазу Україна I), використовуючи низку гібридних заходів для вторгнення та захоплення контролю над Кримом. Згодом це втручання поширилося на Донбас. Прелюдією до цих подій можна спостерігати у впровадженні Росією гібридних заходів, зокрема втручання в Помаранчеву революцію в Україні 2004 р. (яку

Росія сприймала як керовану США) [137, p. 382] та протести на Євромайдані 2014 р. [129]. Росія також намагалася дискредитувати Захід в думці української громадськості, змінити європейський та євроатлантичний порядок денний і використовувати радикальні націоналістичні та прокремлівські групи для послаблення державної безпеки та створення суспільної поляризації [84, p. 186]. Частина останніх полягала в підтримці проросійських груп, які організовували протести та насильницькі інциденти. Російська дезінформація та пропаганда, спрямовані на створення суспільного розколу в Україні, надходили з багатьох джерел, у тому числі з неодноразових промов і коментарів президента Росії В. Путіна. Ці інформаційні кампанії допомогли прокласти шлях до «політики кордону», подібної до тієї, що спостерігалася в Грузії в 2008 р. Росія використовувала військові і воєнізовані формування (як «зелених чоловічків» Криму, так і відкритих російських військ, найманців, кримінальних групи та сепаратистів), що були зосереджені в російськомовних та російсько-орієнтованих районах Криму, Донецька та Луганська. Зокрема Росія використовувала кримінальні угруповання, найманців (не лише групу Вагнера), спецназ та інших як «зелених чоловічків» у Криму, як засіб «проксифікації» нападу на несуміжну територію. Нарешті, Росія також використовувала інші гібридні методи, включаючи DDOS-атаки та фінансовий тиск, щоб перервати український експорт зерна. Крім того, Кремль доклав значних зусиль, щоб залучити дипломатичну підтримку з боку інших країн і побудував Кримський міст, який з'єднує Крим з основними російськими військовими базами в Південному військовому окрузі Росії [13].

Слід зазначити, що так звана фаза «Україна 2», яка охоплює період повномасштабного вторгнення з 2022 р. до теперішнього часу, суттєво відрізнялася від фази «Україна 1». Під час «Україна 2» Росія зробила значно сильніший акцент на звичайних військових операціях, відійшовши від схеми акцентування на нетрадиційних заходах. Також срецслужби РФ намагалися вбити президента України В. Зеленського [128]. Вже на початку війни стало очевидним, що російські війська вчиняли військові злочини та звірства проти

мирного населення [135]. Несподіваним викликом для Росії стала її боротьба за збереження чисельності військ протягом усього конфлікту. Спочатку Росія спробувала провести багатопланову операцію, спрямовану проти великих міст України. Однак у міру розвитку конфлікту Росія зіткнулася з втратами та виснаженням, що призвело до мобілізації додаткових військ, змін у командуванні та збільшення залежності від найманців [50]. Наступним викликом для Кремля стала кількісна та якісна нестача військової техніки. Значна частина техніки, якою володіла російська армія, була технологічно застарілою та зношеною. Однак, незважаючи на ці обмеження, Росія все ще розгортає різноманітну передову зброю, таку як гіперзвукова зброя та термобаричні бомби, а також фосфорні бомби, безпілотники та низку неточної зброї, спрямованої по цивільних районах. Крім того, режим Путіна використовував різні літаки, використовуючи як глухі бомби, так і крилаті ракети [114]. Захід попередив світ, що Росія розглядає можливість використання біологічної та/або хімічної зброї, а Путін неодноразово погрожував застосуванням ядерної зброї, щоб змусити Україну здатися, а західні країни припинити свою допомогу [86]. Ці погрози силою явно стосуються військової сфери, навіть якщо вони часто оголошуються політичним або дипломатичним шляхом.

Під час війни в Україні Росія застосувала низку гібридних підходів, змішаних із звичайними військовими засобами. Це включає використання проксі-сил, таких як сили сепаратистів у Донецьку та Луганську, а також різноманітних формувань бойовиків. Ці заходи разом слугували мілітаризації східних територій, роблячи їх більш уразливими до кордонів, таким чином підриваючи державний суверенітет і територіальну цілісність шляхом встановлення «проксі-окупації» [123]. Отже, Кремль зміг «анексувати» Крим у 2014 р. та пізніше, у 2022 р. Херсон, Запоріжжя, Донецьк та Луганськ. Цю анексію можна розглядати як кульмінаційну точку та бажаний кінцевий стан політики кордону, навіть якщо це означає поглинання України по шматках, а не чіткий намір російської стратегії наприкінці лютого 2022 р. Крім того, Росія намагалася використати:

- економічний тиск, спочатку через свою газову зброю в Європі [142], а потім через зусилля з перекриття поставок зерна в Україну, що загрожує дестабілізувати світовий продовольчий ринок [108];
- дипломатію – намагаючись підкупити інші країни, щоб легітимізувати вторгнення РФ в Україну у 2022 р. та обійти дипломатичний тиск з боку Сполучених Штатів, НАТО та більшості країн світу, а також численні санкції, запроваджені багатьма з цих країн і кількома міжнародними організаціями [130];
- широкомасштабні інформаційні кампанії, як у Росії, так і проти України, особливо з використанням Російської православної церкви та Православної церкви України [119];
- знищення критичної інфраструктури, наприклад, для припинення постачання електроенергії взимку 2022-2023 рр., а також численні атаки на іншу критичну інфраструктуру, включаючи греблі (руйнування каховської дамби в червні 2023 р.) тощо [104].

Під час «Україна 1» багато російських експертів прогнозували, що Росія не буде і не зможе дотримуватися суто гібридного підходу, і справді, Росія переорієнтувалась на «Україну 2» і з самого початку посилила військовий компонент, при цьому обмежені гібридні підходи були успішно використані.

Таким чином, можна дійти висновку, що з розвитком людської цивілізації конфлікти завжди визначали хід історії. Однак із зміною часів, засобів комунікації та технологій еволюціонували і методи ведення війн. Останнє століття особливо відзначається популярність гібридних конфліктів, які характеризуються комплексністю та різноманітністю підходів до досягнення стратегічних цілей. Це можна ілюструвати через призму історії, від пелопонеської війни до сучасних конфліктів. Гібридні конфлікти є неодмінною частиною сучасного геополітичного пейзажу. Їхня складність та різноманітність вимагають інноваційних та диференційованих підходів до забезпечення стійкості та безпеки в умовах постійного розвитку технологій та засобів впливу.

3.2 Досвід вирішення гібридних конфліктів

Сучасний світ стикається з новими викликами, які передбачають ефективність та інноваційний підхід до розв'язання конфліктів. Одним з найскладніших завдань для міжнародної спільноти стає вирішення гібридних конфліктів, які поєднують в собі різні види загроз, включаючи військові, політичні, інформаційні та економічні.

Л. Коффі, старший науковий співробітник Інституту Гудзона, запевняє, що гібридній війні потрібно запобігати або стримувати її. Її не можна легко вирішити. Коли з’являться соціальні, політичні та економічні умови, що дозволяють гібридній тактиці бути ефективною, можливо, буде надто пізно її зупиняти.

Отже, гібридні війни потрібно вигравати ще до того, як їх розпочати. Для цього країни Центральної та Східної Європи з російською меншиною (або будь-якою групою меншини, яка ризикує бути маргіналізованою в суспільстві) мають створити умови, які не дозволятимуть Росії ефективно використовувати її гібридну тактику [61].

Дослідник зазначив, що є три основних способи зробити це. По-перше, встановити належне врядування на місцевому та національному рівнях. Якщо люди відчувають, що ними керують справедливо і добре, вони стають менш сприйнятливими до російської дезінформації та пропаганди. Там, де є корупція, відсутність сильного місцевого самоврядування та відсторонення центрального уряду від проблем на місцевому рівні, створено умови для російського втручання.

По-друге, має бути економічна свобода. Люди повинні відчувати, що вони мають економічну стабільність. Проведення політики, яка сприяє зростанню економічного процвітання, є важливою частиною протидії гібридній тактиці. Люди, які відчувають, що мають економічні можливості, менш сприйнятливі до російського втручання.

Нарешті, має існувати зв’язок довіри та поваги між звичайною людиною і правоохоронними та розвідувальними службами. Якщо люди вірять, що їх

охороняють чесно і що спецслужби не виходять за межі, тоді суспільство стане стійкішим проти російської гібридної тактики.

Крім того, правоохоронні органи часто є першою лінією захисту у сценарії гібридної війни. Зменшити ефективність агентів-провокаторів, які діють від імені Москви, можуть здібні та професійні правоохоронні органи та спецслужби.

Незважаючи на те, що ці три перераховані елементи не легко втілити в життя, якщо національні та місцеві уряди їх справді вживають, вони можуть стримати російську гібридну тактику або принаймні знизити ефективність такої тактики.

Прикладом країни, яка проробила чудову роботу щодо створення стійкості до гібридної війни Росії, є Естонія. Незважаючи на те, що російська меншина становить приблизно чверть населення, Москва не змогла створити ті ж проблеми, використовуючи свою гібридну тактику, як це було в інших державах [61].

Зрозуміло, чому російське населення Естонії не сприйнятливе до гібридної тактики Москви «зелених чоловічків» і пропаганди. Опитування показує, що переважна більшість дуже довіряє своїм урядовим інститутам. Наприклад, згідно з опитуванням громадської думки, проведеним Міністерством оборони Естонії на початку 2019 р., 66 відсотків естонців довіряли президенту країни і 56 відсотків – прем'єр-міністру. Згідно з тим же опитуванням, 87 відсотків естонців заявили, що довіряють поліції [93]. Можливо, не дивно, що Індекс економічної свободи The Heritage Foundation за 2023 р. поставив Естонію на шосте місце у світі за рівнем економічної свободи [6].

Довіра до уряду та поліції в поєднанні з економічними можливостями Естонії позбавляє Росію можливості використовувати гібридну тактику. Естонія змогла виграти гібридну війну ще до її початку.

Порівняємо ситуацію в Естонії сьогодні з ситуацією в Україні в 2013 і 2014 роках. Через жахливу економічну ситуацію та роки політичної та економічної корупції у верхівці уряду Росія змогла використати ситуацію в Україні. Як тільки в Криму з'явилися «зелені чоловічки», було вже пізно.

Л. Коффі впевнений в тому, що хоча політики повинні орієнтуватись на НАТО, щоб забезпечити надійне звичайне та ядерне стримування для членів Альянсу, лише національні столиці можуть створити політичні та економічні умови, які можуть перешкодити Росії використовувати ефективну гібридну тактику [61].

Також звернемо увагу на досвід ще однієї держави Балтійського регіону. Литва була в авангарді боротьби з гібридними загрозами з моменту здобуття незалежності в 1990 р. Намагання зменшити російський вплив і потенційні загрози почалися в 1990-х рр., коли Литва активно прагнула приєднатися до ЄС і НАТО, зрештою ставши повноправним членом у 2004 р.

Досягнення повної незалежності для Литви було нелегким, оскільки до 2014 р. експорт сильно залежав від російських ринків, але окупація Росією Криму стала тривожним дзвіночком. Короткостроковий вплив на литовську економіку був значним, але він спонукав бізнес повністю переорієнтуватися на ЄС та інші західні країни [67]. Литва рано усвідомила небезпеку покладатися на авторитарні режими, наприклад, коли її головний постачальник природного газу, Газпром, суттєво підняв ціни в 2008 р. [77].

Згодом, на початку 2010-х рр., Литва платила одну з найвищих цін на газ в ЄС [97]. Це спонукало Литву прагнути до енергетичної незалежності, чого вона нарешті досягла після вторгнення Росії в Україну в 2022 р. Вживши заходів на ранній стадії, вона стала першою країною ЄС, яка стала незалежною від транспортування російського природного газу, в основному завдяки використанню гнучких плавучих LNG-терміналів [77].

Цей досвід мав значний вплив на політику Литви, спрямовану на протидію зовнішньому зловмисному впливу [77]. Усі зусилля Литви протистояти російському впливу в країні та регіоні, а також її тверда політична позиція, заснована на цінностях, спонукали російську пропаганду називати її «маленькою русофобською нацією» [144].

У 2018 р. звіт Європейського центру цінностей (EVC) класифікував країни-члени ЄС на основі їх підходу до гібридних загроз з боку Росії. Литва, яка

стикається з постійними загрозами, починаючи від ціноутворення на газ і закінчуючи інформаційними атаками, зарекомендувала себе як європейський лідер із стійкості та отримала найвищий бал (15 із 15) у рейтингу EVC, за нею йшли Швеція та Великобританія з оцінками 13 [10]. У звіті Литва іменується як «повномасштабний захисник», який демонструє обґрунтовану стурбованість з приводу зловмисного впливу Росії та очолює європейську відповідь шляхом координації зусиль уряду, розвідувальних служб і громадянського суспільства. Литва надавала пріоритет питанням інформаційної та кібербезпеки, що спонукало деякі з її міністерств до активної боротьби з цими загрозами. Міністерство закордонних справ Литви створило Групу стратегічної комунікації, яка активно підтримує присутність у соціальних мережах і координує зусилля по боротьбі з дезінформацією з журналістами, неурядовими організаціями та академічними колами. Міністерство національної оборони також опублікувало кілька посібників щодо протистояння російському впливу та захисту від вторгнення в разі необхідності [10].

Загроза російської агресії проти Литви спонукала уряд прийняти підхід до національної безпеки як «тотальної або комплексної оборони». Цей підхід передбачає використання різноманітних військових і невійськових засобів, що здійснюються урядом у співпраці з місцевим населенням, для запобігання іноземній агресії та протистояння їй. Цей підхід було визначено в Стратегії національної безпеки Литви 2017 р. [7]. Стратегія окреслює план покращення психологічного захисту та стійкості населення [74]. Стратегія постійно переглядається, оновлюється та повторно приймається парламентом Литви, що свідчить про те, що влада серйозно ставиться до інформаційних операцій та їх наслідків.

У період з 2014 по 2016 рр. уряд Литви активно намагався стати «стратегічним економічним партнером» для Китаю та висловлював інтерес до китайського ринку [56]. Однак Литва накликала на себе гнів Китаю, дозволивши Тайваню відкрити представництво у Вільнюсі. Хоча Китай не становить прямої військової загрози, його спроби зловмисного впливу викликають занепокоєння,

особливо тому, що китайсько-литовські відносини погіршилися через створення представництва Тайваню у Вільнюсі. Китай також стає значним гравцем у розгортанні гібридних можливостей, особливо в морських діях у Південно-Китайському морі та у використанні своєї доктрини кібервійни в глобальній дипломатії.

Швидка та агресивна реакція Китаю на політику Литви, заснована на гібридній діяльності, привернула увагу світу наприкінці 2021 р. [68]. Хоча економічна відповідь Китаю обговорювалася найширше, супутня кампанія дезінформації була не менш важливою. Кампанія була проведена китайською владою та недержавними акторами, такими як тролі та боти [68]. Ці елементи є ключовими компонентами китайської машини дезінформації, яка використовується не лише в Литві, а й у всьому світі.

Разом з Москвою Пекін прагне поляризувати суспільство, використати розбіжності між політичними та бізнес-елітами та посіяти недовіру серед західних союзників і демократичних країн у всьому світі. Китаю не вистачає глибокого розуміння країн регіону, і, як наслідок, його операції з дезінформації є менш ефективними порівняно з Росією. Однак, Пекін почав переймати наративи Кремля, як-от представляти Литву як «fail state», залежну від Заходу, або фашистську країну.

Зазначимо, що Литва є чудовим прикладом впровадження найкращих практик у боротьбі з гібридними загрозами, особливо для держав Центральної та Південної Європи, які вагаються (наприклад, Угорщина, Греція). Досвід Литви як частини Радянського Союзу, а також схоже економічне та суспільне становище роблять її надійним промоутером такої практики в цих регіонах.

Таким чином, досвід Литви та Естонії у запобіганні гібридним загрозам свідчить про важливість інформаційної безпеки, кібербезпеки та дипломатичних зусиль для ефективної протидії новим викликам у сучасному світі. Ці країни продемонстрували, що активний підхід, співпраця та інновації можуть забезпечити ефективний захист національної безпеки та збереження стабільності у глобальному масштабі.

3.3 Шляхи вирішення гібридної війни в Україні

В сучасному світі, де технологічний прогрес створює можливості для нових форм конфліктів, гібридна війна стає предметом активної дискусії та дослідження. Сплетеність інформаційних, політичних, воєнних та економічних компонентів у рамках гібридної війни створює непередбачувані виклики для країн та їхніх геополітичних відносин. У цьому розділі ми розглянемо шляхи вирішення гібридної війни в Україні, зосереджуючись на розгляді окремих компонентів конфлікту – інформаційного, політичного, воєнного та економічного.

Кожен з цих компонентів має свої особливості та важливість у мозаїці гібридної війни. Інформаційний компонент визначає спосіб сприйняття подій, формує уявлення громадськості та впливає на настрої суспільства. Політичний компонент включає в себе стратегії дипломатії та міжнародного співробітництва, а також маніпуляції на політичній арені. Воєнний компонент передбачає не лише використання військової сили, але й гібридні форми конфлікту. Економічний компонент відображається в економічних санкціях, торговельних обмеженнях та фінансовому тиску.

Якщо розглянути інформаційний компонент гібридної війни РФ проти України, то можна проаналізувати низку інтернет-ЗМІ, які є учасниками інформаційної війни на боці Росії. Звідси можна побачити, що їхня діяльність заснована на поширювані неправдивої інформації, так званої «фейкової», яка спрямована на дезінформацію як українського, так і російського населення. Подібна політика російського уряду спрямована на розпалювання недовіри до української влади і суспільства шляхом пошуку найменших приводів для «обливання брудом» держави, проти якої ведеться агресивна діяльність. Інтернет-видання – як російських, так ДНР і ЛНР – поміщають під необґрунтованими заголовками матеріали, в яких згадуються вигадані «укрнаціоналісти», «націоналістичні батальйони». Під необґрунтованими заголовками публікуються образливі висловлювання на адресу українських

військових і влади, публікуються анонімні матеріали і описуються вигадані події без посилань на будь-яке джерело інформації.

Російська Федерація використовує фейкові новини як інструмент гібридної війни проти України, щоб впливати на громадську думку та створювати негативне уявлення про Україну [15, с. 53]. Ми можемо стверджувати, що дезінформація поширюється дуже швидко саме тому, що її автори намагаються використати наші емоції та упередження. І справа не тільки в негативних емоціях – іноді обнадійливі історії теж можуть стати вірусними. Вони піднімають моральний дух, але ускладнюють розуміння того, що насправді відбувається, і сприяють хаосу.

В мережі можна знайти багато сайтів, які поширюють неправдиву інформацію про російсько-українську війну. Інтернет-ЗМІ загарбників покликані, перш за все, дезінформувати населення окупованих територій про діяльність українського уряду і армії, а також українського суспільства, щоб посіяти страх, паніку і недовіру до дій тих, хто намагається захистити цілісність, незалежність, єдність і державність України. Поширення псевдоінформації та маніпулювання громадською думкою є найважливішими інструментами впливу на людей.

Можемо виділити характерні риси російсько-української інформаційної війни в онлайн просторі. Так, однією з особливостей є те, що інформаційні атаки здійснюються за допомогою соціальних мереж та інтернет-ресурсів. О. Іванова стверджує, що російські пропагандистські сайти та мережі часто маскуються під українські джерела, що ускладнює відрізнення правдивої інформації від фейкової [22, с. 48]. Також російські кібер-шпигуни використовують хакерські атаки та кібершпигунство. Ці методи дозволяють отримувати доступ до конфіденційної інформації та впливати на політичну ситуацію в обох країнах [38, с. 58]. О. Коваль виділяє й використання інформаційного шуму. Російська пропаганда часто створює багато різних інформаційних потоків, щоб «затуманити» правдиву інформацію та відрізнити її від фейкової стає важче [26,

с. 26]. Усі ці риси відрізняють російсько-українську інформаційну війну в онлайн просторі від традиційних конфліктів.

Оскільки онлайн-простір є глобальним, то російсько-українська інформаційна війна може впливати на інші країни та регіони. Наприклад, Росія може використовувати ті ж самі методи впливу на громадян Європи або США, щоб впливати на їхні політичні процеси. Т. Михайлова переконує, що боротьба з дезінформацією та інформаційними атаками стає актуальною задачею для всього світу [36, с. 78].

Нашій державі потрібен комплексний підхід до боротьби з цією проблемою. Україні потрібно використовувати різні інструменти для протидії інформаційним атакам. Деякі з можливих інструментів включають:

Розвиток кіберзахисту. Україні потрібно інвестувати у розвиток кіберзахисту для захисту від кібератак і кібершпигунства. Це може включати розробку паролів, двофакторну аутентифікацію, захист від фішингу та інших видів атак [24].

Розробка програм для виявлення дезінформації. Україна може розробити програми, що допоможуть виявляти дезінформацію та фейки. Це може допомогти у розповсюдженні правдивої інформації та зменшенні впливу дезінформації.

Підвищення кіберграмотності. Україна може проводити кампанії з підвищення кіберграмотності серед громадян. Це може допомогти зменшити ефективність фішингу, а також допомогти громадянам впізнавати дезінформацію та фейки [24].

Співпраця з міжнародними партнерами. Україна може співпрацювати з міжнародними партнерами, щоб обмінюватися даними та досвідом у боротьбі з інформаційними атаками. Це може допомогти зменшити вплив інформаційних атак та забезпечити безпеку даних. Проблема фейкових новин є глобальною, тому для її вирішення необхідна міжнародна співпраця. Україна може співпрацювати з міжнародними організаціями, такими як ООН, ОБСЄ, ЄС та інші, щоб отримати допомогу та підтримку в боротьбі з фейковими новинами.

Також важливо співпрацювати з медіа-організаціями, які дотримуються високих стандартів журналістики та етики, а також із соціальними мережами та пошуковими системами, які мають великий вплив на розповсюдження інформації в Інтернеті.

Використання соціальних мереж та інших каналів. Україні потрібно використовувати соціальні мережі та інші канали для виявлення та розповсюдження правдивої інформації. Це може допомогти зменшити вплив дезінформації та фейків, а також підвищити обізнаність громадськості щодо інформаційної безпеки та зменшити ризик піддачі дезінформації [23, с. 75].

Медіа-освіта. Україна може зробити ставку на медіа-освіту, яка буде спрямована на навчання громадян як правильно використовувати медіа-ресурси та інформацію, що надходить до них. Це може забезпечити більшу свідомість громадськості щодо того, які джерела інформації вважати довіреними та як перевіряти їх достовірність. На наше переконання, необхідно включати питання про фейкові новини в шкільну та вищу освіту, а також пропагувати медіа-грамотність серед населення, щоб люди могли розрізняти правдиві та фейкові новини.

Регулювання інформаційного простору. Україна може розглянути можливість введення регулювання діяльності медіа-компаній та інших джерел інформації в мережі. Це може допомогти зменшити поширення дезінформації та фейків та збільшити довіру до інформаційних джерел.

Розвиток внутрішнього кіберзахисту. Нашій державі слід також звернути увагу на внутрішній кіберзахист від дезінформації та фейків, забезпечивши захист від внутрішніх загроз та зловживань від працівників державних інституцій та захист своїх державних інформаційних систем від кібератак [24].

Найголовнішим інструментам, на нашу думку, має стати збільшення доступу до надійних джерел інформації. Держава та міжнародні організації можуть збільшити доступ до надійних джерел інформації про Україну та забезпечити її активне поширення через різноманітні канали комунікації.

Таким чином, російсько-українська інформаційна війна в онлайн просторі має серйозний вплив на громадян та політичні процеси в Україні та Росії, а також на міжнародну політику. Слід наголосити, що боротьба з цією проблемою потребує комплексного підходу, який включає не тільки технічні заходи з кібербезпеки, але і політичні та освітні ініціативи з метою підвищення медійної грамотності громадян

Важливо пам'ятати, що боротьба з фейковими новинами – це довгостроковий процес, який потребує спільних зусиль від держави, медіа-організацій, громадськості та міжнародної співпраці. Це вимагає уваги та активних дій, щоб захистити суспільство від впливу фейкових новин та зберегти свободу слова та право на інформацію.

Зазначимо, що Україна робить кроки для запобігання кібератакам та захисту від їх наслідків. У 2018 р. Україна ухвалила закон «Про основні принципи забезпечення кібербезпеки України» [1], який визначає правову базу для забезпечення кібербезпеки країни та встановлює механізми для виявлення, протидії та реагування на кібератаки. Також українські компанії та установи зміцнюють свої кіберзаходи, включаючи захист мереж та систем, використовуючи сучасні технології кіберзахисту та залучаючи кваліфікованих фахівців.

Проте, виконання цих заходів може бути складним через відсутність ресурсів та експертизи, а також через недостатню координацію між різними установами та компаніями. Тому Україна продовжує співпрацювати з міжнародними партнерами, такими як НАТО, ЄС та США, для отримання підтримки у забезпеченні кібербезпеки [89].

Розглядаючи питання про те, як прибрати російський вплив з сфери української політики, слід зазначити, що дестабілізація Росією України та боротьба українців за суверенітет тривала десятиліттями. Закінчення холодної війни та розпад Радянського Союзу в 1991 р. заклали основу для становлення України як незалежної держави. Проте російський підхід до цього переходу був

відзначений амбівалентністю. Переговори про кордони, розподіл активів і політичну реструктуризацію були затьмарені напругою.

Одним із найяскравіших випадків дестабілізуючих дій Росії була анексія Криму в 2014 р. Після протестів на Євромайдані в Україні та подальшого усунення президента В. Януковича Росія захопила Крим. Анексія не лише порушила територіальну цілісність України, але й викликала міжнародний осуд і посилила напруженість. Широко розкритикований референдум, проведений у Криму, став фасадом для наперед визначеного результату входження до складу Російської Федерації.

АТО є яскравою ілюстрацією дестабілізуючої ролі Росії. Незважаючи на те, що Росія досі заперечує пряму причетність, багато доказів свідчать про те, що сепаратисти отримували військову підтримку, зброю та підкріплення у живій силі (найманці та солдати збройних сил РФ) [30, с. 65].

Контроль Росії над енергетичними ресурсами, зокрема природним газом, використовувався як інструмент впливу на політику та економіку України. Маніпулюючи цінами та поставками енергоносіїв, Росія чинила значний економічний тиск на Україну. Ця енергетична залежність перешкоджала здатності України відстоювати свою незалежність і диверсифікувати джерела енергії, таким чином зберігаючи її вразливість до впливу Росії.

Усунення російського впливу з української політики – це складний і багатоаспектний процес, який вимагає широкого спектра заходів та стратегій. Ми пропонуємо кілька можливих кроків:

- Важливо боротися з дезінформацією та пропагандою з боку Росії. Інвестування в якісну журналістику, факт-чекінг та інформаційну освіту можуть допомогти українському суспільству бути критичним до оточуючої інформації.
- Здійснення глибоких реформ у сферах правосуддя, антикорупційної діяльності, економіки тощо може позитивно вплинути на стан політики та зменшити можливості для зовнішнього впливу.

- Підтримка незалежних громадських організацій, залучення громадян до політичного процесу може збільшити відповідальність політиків перед власним народом.
- Зменшення залежності від російського енергопостачання може зменшити політичний тиск та вплив з боку Росії.
- Підтримка української культури та мови, розвиток міжнаціональної толерантності, а також сприяння культурній та освітній інтеграції з Європою може знизити вплив російського культурного простору.
- Боротьба з корупцією дозволить зменшити можливості зовнішніх сил впливати на політичні рішення через хабарництво та інші корупційні практики.

Важливо розуміти, що це тривалий процес, і не існує одноразового рішення. Необхідно використовувати комплексний підхід та поєднувати різноманітні заходи для досягнення бажаного результату.

Зазначимо також, що досягнення стійкої безпеки та захисту суверенітету стали для України найважливішим завданням. Одним із можливих шляхів ефективної відповіді на цю загрозу є нарощування виробництва власної військової техніки та зброї.

Розвиток військово-промислового комплексу сприятиме не лише міцності наших Збройних сил, а й створенню нових робочих місць та підтримці національної економіки. Це також забезпечить розмаїття технологій, що може використовуватися не лише для військових цілей, а й для цивільних потреб, таких як медичні дослідження, наукові розробки та інфраструктурні проєкти.

Нарощування виробництва зброї дозволить Україні забезпечити себе військовою технікою та озброєнням без такої сильної залежності від поставок зброї з ЄС та США. Історія вже показала, як важливо мати власну військову потужність в умовах загострення конфлікту. Виробництво власної зброї сприятиме більш ефективній реакції на будь-які загрози.

Гібридна війна включає в себе різні аспекти, такі як інформаційна війна, дестабілізація суспільства та інші нестандартні методи. Ефективна боротьба з

такими загрозами вимагає відповідного технологічного та військового потенціалу. Виробництво власної військової техніки допоможе створити ефективнішу систему оборони та забезпечити відповідну реакцію на різні види агресії.

Необхідність нарощування виробництва зброї для протистояння російській гібридній війні стає більш нагальною зараз, в час повномасштабної війни. Забезпечення національної безпеки та захисту суверенітету – це завдання, до якого Україна повинна підходити з усією серйозністю та рішучістю.

Наголосимо, що економічну війну проти України слід розглядати як складову гібридної війни, яку веде Російська Федерація. Вона здійснюється у вигляді операцій на основі розробленої країною-агресором стратегії, а тому носить не спонтанний, а спланований характер і максимально довго приховується від жертви. На перший погляд, об’єктами агресивних дій є окремі підприємства. Але насправді сукупність уражених економічних цілей сприяє досягненню мети знищення певних секторів економіки, а іноді й досягненню певних політичних цілей. Справжня мета агресора стає зрозумілою на завершальному етапі операції, коли запобігти руйнівним наслідкам важко, а в окремих випадках і неможливо. Ці операції мають спільні риси через обмежену кількість доступних способів і методів реалізації сюжету.

Дослідження агресивного впливу на стратегічні підприємства України показало, що найбільших втрат зазнала «переробна промисловість», оскільки близько 50% підприємств припинили існування або розпочали процедури банкрутства, на другому місці – «гірничодобувна промисловість та розробка кар’єрів» (близько 47% втрат) та «науково-технічна діяльність» (близько 35%) [6].

Удар, завданий переробній промисловості, позбавив Україну доходу від доданої вартості від виробництва продукції кінцевого споживача, а також перетворив країну на аграрно-сировинний придаток світової економіки. Крім того, це призводило до зупинки або скорочення виробництва на відповідних підприємствах, створюючи втрату виробничих ланцюгів.

Руйнування третини підприємств науково-технічної сфери позбавило вітчизняну економіку прогресу в розвитку, призвело до залежності України від іноземних технологій (вартість яких подекуди перевищує вартість продукції, виготовленої за ними), а також відтік досвідчених кадрів.

Розуміння втрат і визнання помилок дає змогу визначити пріоритети при плануванні економічного відновлення після закінчення війни. Прикладом є видобуток і обробка титану.

Фактори, що сприяють успішному проведенню гібридних операцій РФ на економічний сектор України включають:

• некомпетентні органи влади;

• корумповані владні структури в усіх гілках влади;

• захоплення держави агресором шляхом прихованого проникнення в органи влади, включно зі встановленням прихованого контролю над регуляторними інституціями, зокрема економічними;

• проведення допоміжних операцій за іншими оперативними лініями;

• недостатня вивченість самого феномену гібридної війни, що сприяє нерозумінню процесів, що відбуваються [6].

На наше переконання слід провести низку заходів для захисту національних інтересів:

- терміново переглянути підхід до ведення Реєстру стратегічних підприємств;
- прискорити розробку та нормативне визначення поняття «стратегічне підприємство» з точки зору важливості суб'єктів господарювання для забезпечення потреб оборони держави та захисту національних інтересів, насамперед, в умовах повномасштабної війни;
- повністю оцінити весь наявний у державі економічний та промисловий потенціал, виходячи з нормативного визначення «стратегічного підприємства» та встановлених критеріїв;
- законодавче закріпити баланс інтересів держави та бізнесу щодо активів стратегічних підприємств приватного сектора економіки, які працюють

на оборону України. Це потрібно для забезпечення безперебійного виробництва необхідної продукції оборонно-промислового комплексу. Зокрема, ввести заборону на перепрофілювання або штучну зупинку виробництва під час війни; унормувати можливість запровадження тимчасової державної адміністрації на тих підприємствах, які вже припинили роботу або перебувають на різних стадіях банкрутства.

- законодавчо заборонити передавати права власності на активи стратегічних підприємств, незалежно від форми власності, громадянам і юридичним особам Російської Федерації, Білорусі та інших держав, які підтримали російську агресію в Україні.
- законодавчо закріпити примусове повернення у державну власність активів стратегічних підприємств, які прямо чи опосередковано належать громадянам України, до яких Указом Президента України на підставі рішень, оголошених РНБО, застосовано персональні економічні санкції.
- розробити цільову програму фінансової підтримки інноваційної діяльності стратегічних підприємств державного сектору економіки, включно з ресурсами реалізації проектів, що фінансуються фінансовими інституціями ЄС, США та інших країн-учасниць «Програми відновлення України».

Загалом, вирішення гібридної війни в Україні вимагає комплексного підходу та взаємодії різних сфер суспільства. Це включає зусилля на забезпечення стабільності та єдності нації, боротьбу з дезінформацією, активну дипломатичну діяльність та зміцнення кібербезпеки. Тільки за умови спільних зусиль усіх громадян та державних інституцій Україна зможе ефективно протистояти гібридній війні та забезпечити свою національну безпеку та суверенітет.

Висновки до розділу 3

Гбридні конфлікти є складним та мінливим явищем сучасності, яке об'єднує в собі різні аспекти конфліктів, починаючи від інформаційної війни до використання економічних та військових методів. Світовий досвід ведення

гібридних конфліктів показує, що їх важко передбачити та ефективно управляти ними через традиційні підходи. Наявність багатьох різних вимірів конфлікту вимагає комплексних та інноваційних стратегій відповіді.

Досвід вирішення та попередження гібридних загроз Балтійськими країнами, зокрема Естонії та Литви, є цінним прикладом для інших держав. Вони показали, що комплексний підхід, який об'єднує кібербезпеку, міжнародну співпрацю, інформаційну грамотність та політичну стабільність, може стати ефективною стратегією для протидії гібридним загрозам у сучасному світі.

Гібридна війна, яка ведеться проти України, представляє собою складне поєднання військових, інформаційних, економічних та політичних методів для досягнення стратегічних цілей. Цей конфлікт має нелінійний характер та потребує інноваційних та комплексних підходів до вирішення. Шляхи зупинення та врегулювання гібридної війни в Україні включають елементи внутрішніх реформ, міжнародної співпраці та активної інформаційної політики.

Лише шляхом зміцнення внутрішньої стійкості, співпраці з міжнародними партнерами та реалізації активної інформаційної стратегії Україна зможе досягти успішного вирішення гібридної війни та забезпечити стабільність та безпеку на своїй території.

ВИСНОВКИ

У процесі проведення дослідження ми вивчили феномен гібридної війни як форми новітнього конфлікту. Доведено, що гібридна війна представляє собою новітній конфлікт, який поєднує в собі різноманітні військові та неінформаційні стратегії. Цей феномен суттєво еволюціонував протягом останніх десятиліть, визначаючи нові реалії міжнародних відносин. Характер гібридної війни визначається загальним ефектом досягнених результатів та високим рівнем невизначеності для супротивників, щодо кінцевих стратегічних цілей. У гібридних конфліктах ключовими завданнями є контроль над суспільством, вплив на загальний настрій громадян та маніпулювання тими, хто приймає важливі рішення в державі.

Основною метою противника в цьому контексті є маніпулювання основними цінностями, мотиваційними факторами та культурними засадами, а також стратегічною інфраструктурою. Досягнення цієї мети відбувається завдяки комплексному та збалансованому використанню ефектів м'якої та військової сили. Гібридна війна покладається на взаємодію різноманітних впливових чинників, включаючи інформаційні кампанії, кібератаки, дипломатію та військові дії, для досягнення своїх стратегічних цілей. Такий підхід створює складний ландшафт, де непередбачуваність і складність є важливими характеристиками гібридної війни.

Доведено, що гібридні війни суттєво перетворюють роль суверенних держав у міжнародних відносинах, викликаючи необхідність переосмислення традиційних моделей та стратегій. Ці війни витісняють суверенні держави із центральної ролі, розширюючи вплив незалежних суб'єктів, які раніше не вважалися визначальними.

Перехід від прямих військових конфліктів до використання кібератак та дезінформації свідчить про значущі трансформації в природі конфліктів. Ці нові форми впливу дозволяють суб'єктам діяти ефективно, не вдаючись до відкритого використання військової сили, і вимагають від суверенних держав адаптації до нових реалій геополітичного ландшафту.

Індивідуалізація та адаптивність гібридних загроз ставлять під питання ефективність традиційних блоків та альянсів. Умови гібридної війни ускладнюють координацію та спільні дії, сприяючи розколам та недовірі між учасниками.

З`ясовано, що інформаційна складова гібридної війни відіграє вирішальну роль у формуванні громадської думки та сприйнятті подій. Засоби масової інформації, соціальні мережі та кіберпростір стають ареною битви за реальність. Дезінформація, фейкові новини та кібератаки використовуються для зміни перцепції, створення паніки та підриву внутрішньої стабільності.

Гібридні конфлікти найчастіше спрямовані на досягнення політичних цілей. Вони можуть включати в себе втручання в політичні процеси, підтримку агентів впливу та дестабілізацію урядів. Політичні санкції, агітація та лобіювання можуть стати ефективними інструментами для досягнення стратегічних цілей без прямого використання сили.

Хоча гібридна війна рідко виявляється відкритим військовим конфліктом, вона може включати елементи військової стратегії. Некеровані війська, терористичні акти та провокації на кордонах можуть стати частиною гібридного сценарію.

Економічний вимір гібридної війни виявляється через економічний тиск, санкції та контроль над ресурсами. Здатність впливати на глобальні фінансові ринки, блокування інвестицій та використання економічних інструментів стають важливою стратегією у сучасних конфліктах.

Усі ці компоненти взаємодіють та доповнюють один одного, створюючи комплексний характер гібридної війни. Здатність пристосовуватися та інтегрувати різноманітні стратегії дозволяє гібридним конфліктам бути ефективними в різних умовах та середовищах.

Визначено, що з історичної перспективи можна простежити еволюцію гібридних конфліктів від давньогрецької пелопонеської війни, де використовувалися як традиційні, так і нетрадиційні методи ведення бойових дій. Сучасні гібридні конфлікти, такі як російсько-українська війна, підсилені

сучасними технологіями та комунікаційними засобами, що робить їх надзвичайно складними та вимагає нових стратегій вирішення.

Сучасний геополітичний ландшафт визначається гібридними конфліктами, що підкреслюють їхню неодмінну роль у визначенні відносин між країнами та регіонами. Складність та різноманітність таких конфліктів вимагають інноваційних та диференційованих підходів для забезпечення стійкості та безпеки в умовах постійного розвитку технологій та засобів впливу.

Взявши до уваги досвід країн, таких як Литва та Естонія, важливо зазначити їхню активну роль у запобіганні гібридним загрозам. Ці країни підкреслили важливість інформаційної безпеки, кібербезпеки та дипломатичних зусиль для ефективної протидії новим викликам у сучасному світі.

Литва та Естонія визначили, що активний підхід до гібридних конфліктів, міжнародна співпраця, а також інновації в області кібербезпеки та інформаційної війни є вирішальними елементами для забезпечення ефективного захисту національної безпеки та збереження стабільності на глобальному рівні.

Усі ці аспекти свідчать про те, що гібридні конфлікти визначають не лише теперішнє, але й майбутнє міжнародних відносин. Світовий досвід демонструє, що лише шляхом активної співпраці, інновацій та визначення нових стратегій можна забезпечити ефективне вирішення гібридних конфліктів та зберегти стабільність у світі постійних змін.

Наголошено на необхідності використання соціальних мереж та інших каналів для розповсюдження правдивої інформації в Україні і про Україну. Відзначається, що це може зменшити вплив дезінформації та фейків, а також підвищити обізнаність громадськості щодо інформаційної безпеки. Також вказується на важливість медіа-освіти, що сприяє розвитку медійної грамотності серед населення. Пропонуються заходи, такі як регулювання інформаційного простору та розвиток внутрішнього кіберзахисту для запобігання поширенню дезінформації. Важливим є також збільшення доступу до надійних джерел інформації. Зазначається, що боротьба з російським впливом вимагає комплексного підходу, який включає технічні, політичні та освітні ініціативи.

Рекомендується проведення реформ у сферах правосуддя, антикорупції та економіки для покращення політичної ситуації та зменшення впливу зовнішніх сил.

Забезпечення національної безпеки та захисту суверенітету України вимагає комплексного підходу. Розвиток військово-промислового комплексу та нарощування виробництва власної військової техніки є ключовими елементами цього процесу. Виробництво зброї не лише забезпечить армію необхідними ресурсами, а й сприятиме економічному зростанню, створенню нових робочих місць і розвитку технологій, корисних як для військових, так і для цивільних потреб. Також важливо враховувати загрозу гібридної війни, яка включає економічні аспекти. Російська Федерація веде не тільки військові операції, але й економічні атаки, спрямовані на підрив галузей промисловості та суспільства в цілому. Реакція на ці загрози вимагає відповідного технологічного та економічного потенціалу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

Джерела

1. Закон України «Про основні принципи забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 16.05.2023).

2. Delivered by the Representative of the Ministry of Defence of Ukraine, Major General Vadym Skibitskyi to the 949th Meeting of the OSCE Forum for Security Co-operation, 17 June 2020. URL : https://vienna.mfa.gov.ua/en/news/vistup-na-temu-privatni-vijskovi-kompaniyi-ta-yih-rol-u-suchasnih-regionalnih-konfliktah (дата звернення: 15.03.2023).

3. Field Manual 3-0 «Operations». Department of the Army. 2017. URL: https://archive.org/details/FM3-0OperationsOctober2017 (дата звернення: 10.03.2023).

4. Hybrid warfare. *Wikipedia.org*. URL: https://en.wikipedia.org/wiki/Hybrid_warfare (дата звернення: 02.08.2023).

5. Identifying and analyzing corrosive investments into Ukraine`s economy as an element of hybrid warfare. Analytical Report. *Center for International Private Enterprise*. URL: https://www.cipe.org/wp-content/uploads/2023/02/Russian-Corrosive-Invements-CIPE-FINAL.pdf (дата звернення: 30.08.2023).

6. Index of Economic Freedom 2023. URL: https://www.heritage.org/index/country/estonia (дата звернення: 28.08.2023).

7. Lithuanian National Security Strategy. 2017. URL: https://e-seimas.lrs.lt/rs/legalact/TAD/TAIS.262943/format/OO3_ODT/ (дата звернення: 28.08.2023).

8. National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom, November 2015. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf (дата звернення: 02.08.2023).

9. NATO, «Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales,» 5 September 2014. URL: http://www.nato.int/cps/en/natohq/official_texts_112964.htm (дата звернення: 02.08.2023).

10. Ranking of countermeasures by the EU28 to the Kremlin's subversion operations. 2018. URL:https://www.europeanvalues.cz/ wp-content/uploads/2020/09/2018-ranking-of-countermeasures-by-the-eu28-to-the-kremlin-s-subversion-operations.pdf (дата звернення: 28.08.2023).

11. Strategic Defense Review. URL: https://www.gov.uk/government/publications/strategic-defence-review-1998 (дата звернення: 10.03.2023).

12. The Role of Irregular Forces in Russia'a Hybrid Warfare URL : https://www.coedat.nato.int/publication/researches/07-The_Role_Of_Irregular_Forces_In_Russia_Hybrid_Warfare.pdf (дата звернення: 15.03.2023).

13. Ukraine Conflict Updates. *Institute for the Study of War*. URL: https://www.understandingwar.org/backgrounder/ukraine-conflict-updates (дата звернення: 27.08.2023).

Література

14. Акульшин О. В. Гібридна війна: технології сугестії та контрсугестії. *Національна академія СБУ, Інститут філології Київського національного університету ім. Тараса Шевченка*. Київ : Національна академія СБУ, 2018. 235 с.

15. Андрусяк О. Інформаційна війна в Україні: сутність та особливості реалізації. *Наукові праці Кам'янець-Подільського національного університету. Серія: Політичні науки*. 2018. № 2. С. 50-55.

16. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. *Вісник НАДУ*. 2015. №1. С. 136-141.

17. Ґіґґінз Е. Ми - Bellingcat. Онлайн-розслідування міжнародних злочинів та інформаційна війна з Росією. Пер. з англ. Орина Ємельянова. Київ : Наш Формат, 2022. 235 с.

18. Додонова Р. О. Гібридна війна: in verbo et in praxi. Вінниця: Нілан, 2017. 411 с.

19. Дорошенко А.С. Гібридна війна в інформаційному суспільстві. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого»*. 2015. № 2(25). С. 21-28.

20. Дубова Д. В. Активні заходи» СРСР проти США: пролог до гібридної війни: аналітична доповідь. *Національний інститут стратегічних досліджень.* Київ : Фенікс, 2017. 88 с.

21. Дубровіна Л. Інформаційні механізми нейтралізації негативних зарубіжних впливів на регіони України в умовах гібридної війни. *НАН України, Національна бібліотека України ім. В. І. Вернадського*. Київ : НБУВ, 2018. 70 с.

22. Іванова О. Інформаційна війна як інструмент впливу на політичні процеси в Україні та Росії. *Політологічні дослідження*. 2019. № 2. С. 46-51.

23. Ільєнко О. Інформаційна війна та боротьба з нею в Україні. *Електронне наукове фахове видання «Публічне управління та національна безпека»*. 2019. № 3. С. 69-77.

24. Кіберзахист в Україні: стан і перспективи. URL: https://www.ukrinform.ua/rubric-society/2942221-kiberzahist-v-ukraini-stan-i-perspektivi.html (дата звернення: 16.03.2023).

25. Кіца М. Особливості та методи виявлення фейкової інформації в українських ЗМІ. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/16109/kitsa.pdf (дата звернення: 09.08.2023).

26. Коваль О. Вплив російсько-української інформаційної війни на громадян України та Росії. *Соціологічні дослідження.* 2021. № 4, С. 23-30.

27. Корнієнко С. Путін веде в Україні гібридну війну – генерал Каппен. URL: http://svoboda.org/content/article/ 25362031.html/ (дата звернення: 02.08.2023).

28. Короткий В. «Вагнер» і компанія. Найманці тоталітарного режиму. URL : https://www.ukrinform.ua/rubric-world/3048507-vagner-i-kompania-najmanci-totalitarnogo-rezimu.html (дата звернення: 15.03.2023).

29. Кохан Г. Приватні військові компанії в умовах ведення гібридної війни. *Знання європейського права.* 2021. С. 144-150.

30. Кравченко Н. Б.. Гібридна війна Росії проти України (1991-2021 рр.). Київ : НУБіП України, 2022. 157 с.

31. Кубявка М. Б. Моделі та методи управління інформаційним супроводженням в умовах гібридної війни: автореф. дис. ... канд. техн. наук : 05.13.06; Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2017. 21 с.

32. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі: навч. посіб. Київ: ВІКНУ, 2016. 286 с.

33. Лесів М. Гібридна війна як виклик національній безпеці. *Наукові записки Національного університету «Острозька академія». Серія «Політичні науки».* Вип. 24. 2016. С. 19-23.

34. Магда Є.М. Гібридна війна: сутність і структура феномену. *Міжнародні відносини: Серія. «Політичні науки».* 2014. № 4. С. 206-210.

35. Маркітантов В. Ю. Російська гібридна війна: від доктрини до тактики: навч. посіб. *Кам'янець-Подільський національний університет ім. Івана Огієнка.* Кам'янець-Подільський : Друкарня Рута, 2018. 232 с.

36. Михайлова Т. Роль онлайн-медіа в російсько-українській інформаційній війні та її вплив на міжнародну політику. *Міжнародні відносини.* 2020. № 3. С. 76-81

37. Парахонський Б. О., Яворська Г М. Дестабілізація Європи : гібридна війна РФ. *Strategic Panorama.* 2021. № 1–2. URL: https://doi.org/10.53679/2616-9460.1-2.2021.01 (дата звернення: 10.08.2023).

38. Петренко Ю. Сучасний стан російсько-української інформаційної війни та її вплив на політичні процеси в Україні та Росії. *Політика і право.* 2018. № 1. С. 56-60.

39. Попович К. В. Гібридна війна як сучасний спосіб ведення війни: історичний та сучасний виміри. *Науковий вісник Ужгородського університету. Серія : Історія.* 2016. Вип. 2. С. 75-79.

40. Почепцов Г. Від покемонів до гібридних війн: нові комунікативні техно логії XXI століття. Київ: ВД «Києво-Могилянська академія», 2017. 260с.

41. Проноза І. І. Інформаційна війна: сутність та особливості прояву. *Актуальні проблеми політики : збірник наукових праць. НУ «ОЮА», Південноукр. центр гендерних проблем.* Одеса : Фенікс, 2018. Вип. 61. С. 76-84.

42. Сенченко М І. Латентна світова інформаційна війна. Київ : Стебеляк, 2014. 382 с.

43. Ткачук П. П. Інформаційна війна і національна безпека. Львів: Академія сухопутних військ, 2015. 264 с.

44. Тюхтенко Є. Нові технології і методи гібридної війни –це виклик міжнародній безпеці. *Радіо Свобода.* 2018. URL: https://www.radiosvoboda.org/a/29591806.html (дата звернення: 13.08.2023).

45. Феськов І. В. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. *Актуальні проблеми політики.* 2016. Вип. 58. С. 66–76.

46. Худолій А. О. Інформаційна війна 2014 - 2022 рр. *Національний університет «Острозька академія».* Острог: Видавництво Національного університету «Острозька академія», 2022. 207 с.

47. Чекаленко Л. Про поняття «гібридна війна». *Віче.* 2015. № 5. С. 41-42.

48. Aaronson M., Dissen S., Long B., Miklaucic M. NATO Countering the Hybrid Threat. URL: http://www.act.nato.int/nato-countering-thehybrid-threat (дата звернення: 02.08.2023).

49. Atrews R. A. Cyberwarfare: Threats, Security, Attacks and Impact. *Journal of Information Warfare*, 2020. Vol. 19, No. 4. P. 17-28.

50. Axe D. It’s Possible 270,000 Russians Have Been Killed Or Wounded In Ukraine. *Forbes.* 2023. URL: https://www.forbes.com/sites/davidaxe/2023/02/07/its-

possible-270000-russians-have-been-killed-or-wounded-in-ukraine/ ?sh=19c6b1ce2eec (дата звернення: 27.08.2023).

51. Bachmann S. D., Gunneriusson H. Russia's hybridwar in the East: the integral nature of the informationsphere. *Georgetown Journal of International Affairs*. 2019. P. 45-49.

52. Ball J. The Changing Face Of Conflict: What Is Hybrid Warfare? *Global Security Review*. URL: https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/ (дата звернення: 02.08.2023).

53. Batyuk V. The US Concept and Practice of Hybrid Warfare. *Strategic Analysis*. Vol. 41. 2017. p. 464-477.

54. Bjorge G. Compound Warfare in the Military Thought and Practice of Mao Zedong and the Chinese People's Liberation Army's Huai Hai Campaign (November 1948 – January 1949). *Compound Warfare: That Fatal Knot*. 2002. p. 169–219.

55. Bratko A., Zaharchuk D., Zolka V. Hybrid warfare – a threat to the national security of the state. URL: https://seguridadinternacional.es/resi/html/ hybrid-warfare-a-threat-to-the-national-security-of-the-state/ (дата звернення: 02.08.2023).

56. Butkevičius A. Lietuva tampa strategine Kinijos partnere. *Irytas.lt.* 2015. URL: https://www.lrytas.lt/lietuvosdiena/aktualijos/2015/11/26/news/ abutkevicius-lietuva-tampa-strategine-kinijos-partnere--2802834 (дата звернення: 28.08.2023).

57. Camilli E. Understanding national security strategies. 2016. URL: https://www.academia.edu/21910174/Understanding_National_Security_Strategies (дата звернення: 17.08.2023).

58. Castro N. On Private Military Companies and Hybrid Warfare. *IJOIS.* 2021.Vol. 8 No. 1 URL: https://ugresearchjournals.illinois.edu/index.php/ IJOIS/article/view/765 (дата звернення: 13.08.2023).

59. Chase-Dunn C. The effects of international economic dependence on development and inequality: a cross-national study. *American Sociological Review*. 1975. Vol. 40. P. 720–738.

60. Chivvis C. Hybrid war: Russian contemporary political warfare. *Bulletin of the Atomic Scientists*. 2017. Vol. 73. P. 1-6.

61. Coffey L. How to Defeat Hybrid Warfare Before It Starts. URL: https://www.defenseone.com/ideas/2019/01/how-defeat-hybrid-warfare-it-starts/ 154296/ (дата звернення: 28.08.2023).

62. Cooper R.N. Is «economic power» a useful and operational concept? 2004. URL: https://dash.harvard.edu/handle/1/3677050 (дата звернення: 17.08.2023).

63. Cuomo S. J., Donlon B. «Training a «Hybrid» Warrior at the Infantry Officer Course». *Small Wars Journal. Small Wars Foundation*. 2008. URL: https://indianstrategicknowledgeonline.com/web/TRAINING%20A%20HYBRID%20WARRIOR%20AT%20THE%20INFANTRY%20OFFICER%20COURSE.pdf (дата звернення: 25.08.2023).

64. Dayspring S. M. Toward a theory of hybrid warfare: the Russian conduct of war during peace. Master's thesis, Naval Postgraduate School. 2021. URL:https://apps.dtic.mil/sti/pdfs/ADA632188.pdf(дата звернення: 17.08.2023).

65. De Waal T. In the south Caucasus, can new trade routes help overcome a geography of conflict? 2021. URL: https://carnegieendowment.org/files/ de_Waal_South_Caucasus_Connectivity.pdf (дата звернення: 17.08.2023).

66. Deep A. «Hybrid War: Old Concept, New Techniques». *Small Wars Journal. Small Wars Foundation*. 2015. URL: https://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques (дата звернення: 25.08.2023).

67. Dėl Rusijos efekto Lietuvos ekonomika neteks 0,5 mlrd. eurų, praneša „Danske Bank» *Bankai.lt.* 2015. URL: https://www.bankai.lt/infobankas/naujienos/ del-rusijos-efekto-lietuvos-ekonomika-neteks-0-5-mlrd-129.html (дата звернення: 28.08.2023).

68. Dempsey J. China’s Bullying of Lithuania Spurs European Unity. *Carnegie Europe*. 2022. URL: https://carnegieeurope.eu/strategiceurope/86208 (дата звернення: 28.08.2023).

69. Don't Be Fooled: Russia Attacked U.S. Troops in Syria: Mattis gave Putin «plausible deniability» for a military assault that went badly awry. *Bloomberg*. 2018. URL: https://www.bloomberg.com/view/articles/2018-02-16/russia-attacked-u-s-troops-in-syria (дата звернення: 26.08.2023).

70. Doran P.B. America’s new direction in foreign policy. *European View. 2015.* Vol. P. 253–261.

71. Ducaru S.D. Framing NATO’s approach to hybrid warfare. *Countering hybrid threats: lessons learned from Ukraine*. Amsterdam, Berlin, and Washington DC: IOS Press. 2015. P. 3–11.

72. Dudin M.N., Fedorova I.J., Ploticina L.A., Tokmurzin T.M. International practices to improve economic security. *European Research Studies Journal*. 2018. Vol. 21(1). P. 459–467.

73. Fabienne B. Hybrid warfare: Future challenges for NATO and the EU. *European View*. Vol. 15. Issue 2. 2016. P. 233–243.

74. Flanagan S. J. Deterring Russian Agression in the Baltic States Through Resilience and Resistance. *RAND.* URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2779/RAND_RR2779.pdf (дата звернення: 28.08.2023).

75. Foley E., Kaunert C. Russian Private Military and Ukraine: Hybrid Surrogate Warfare and Russian State Policy by Other Means. *Central European Journal of International and Security Studies.* 2022. Vol. 16, Iss. 3, P. 172-192.

76. Gates R., A Balanced Strategy. *Foreign Affairs.* Vol. 88, No. 1. URL: https://www.jstor.org/stable/20699432 (дата звернення: 02.08.2023).

77. Gazprom to hike Lithuania natural gas price – report. *Reuters*. 2008. URL: https://www.reuters.com/article/gazprom-lithuania-idUKL0212217920080102 (дата звернення: 28.08.2023).

78. Giegerich B. Hybrid Warfare and the Changing Character of Conflict. *Connections*. 2016. Vol. 15, No. 2. P. 65–72.

79. Grant G. Hybrid Wars. *Government Executive. National Journal Group.* 2008. URL: https://www.govexec.com/magazine/features/2008/05/hybrid-wars/26799/ (дата звернення: 25.08.2023).

80. Guilong Y. The impact of Artificial Intelligence on hybrid warfare. *Small Wars & Insurgencies*. 2020. Vol. 31. P. 1-20.

81. Hoffman F. Conflict in the 21st Century: The Rise of Hybrid War. Arlington: Potomac Institute for Policy Studies. 2007. URL: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf (дата звернення: 25.08.2023).

82. Hoffman F. Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict. *Strategic Forum. Institute for National Strategic Studies, National Defense University*. URL: https://www.files.ethz.ch/isn/98862/SF240.pdf (дата звернення: 02.08.2023).

83. Humais S. AL as a tool of hybrid warfare: challenges and responses. URL: https://www.jinfowar.com/journal/volume-21-issue-2/ai-tool-hybrid-warfare-challenges-responses (дата звернення: 09.08.2023).

84. Hutchings S., Szostek J. Dominant Narratives in Russian Political and Media Discourse during the Ukraine Crisis in Ukraine and Russia: People, Politics, Propaganda and Perspectives. *E-International Relations*. 2016. P. 184-188.

85. Iskandarov K, Gawliczek P. Economic coercion as a means of hybrid warfare: The South Caucasus as a focal point. URL: https://securityanddefence.pl/Economic-coercion-as-a-means-of-hybrid-warfare-The-South-Caucasus-as-a-focal-point,151038,0,2.html#citations(дата звернення: 17.08.2023).

86. Jackson J. Russia Starts Moving Nuclear Weapons to Ukrainian Neighbor. *Newsweek.* 2023. URL: https://www.newsweek.com/russia-starts-moving-nuclear-weapons-ukrainian-neighbor-1802721 (дата звернення: 27.08.2023).

87. Jasper S., Moreland S. The Islamic State is a Hybrid Threat: Why Does That Matter?. Small Wars Journal. *Small Wars Foundation*. 2014. URL: https://smallwarsjournal.com/jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter (дата звернення: 26.08.2023).

88. Judah B. The Kleptocracy Curse: Rethinking Containment. *Hudson Institute.* URL:https://s3.amazonaws.com/media.hudson.org/files/publications/20161020JudahTheKleptocracyCurseRethinkingContainment.pdf (дата звернення: 12.08.2023).

89. Juutilainen J. Cyber Warfare: A Part of the Russo-Ukrainian War in 2022. URL: https://www.theseus.fi/bitstream/handle/10024/780757/ Juutilainen_Jari.pdf (дата звернення: 16.05.2023).

90. Kamusella T. «Dreaming of Tannu-Tuva: Soviet precursors to Russia's hybrid warfare». *New Eastern Europe*. 2020. URL: https://neweasterneurope.eu/2020/03/20/dreaming-of-tannu-tuva%EF%BB%BF-soviet-precursors-to-russias-hybrid-warfare/ (дата звернення: 25.08.2023).

91. Katz Y. Wadi Saluki battle - microcosm of war's mistakes. *The Jerusalem Post.* 2006. URL: https://www.jpost.com/israel/wadi-saluki-battle-microcosm-of-wars-mistakes (дата звернення: 25.08.2023).

92. Kim S. C. China and its neighbors: asymmetrical economies and vulnerability to coercion. *Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs*, 2019. Vol. 55(4). P. 1–25.

93. Kivirähk J. Public opinion and national defence. Estonian Ministry of Defence. URL: https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/public_opinion_and_national_defence_2018_march.pdf (дата звернення: 28.08.2023).

94. Kustra T. Economic coercion and sanctions. 2021. URL:https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0289.xml (дата звернення: 17.08.2023).

95. Kuzio T. Hybrid Warfare: The Future Face of Conflict? *Journal of Slavic Military Studies.* Vol. 27. No. 2. 2014. P. 163-176.

96. Lind W. S. Fourth Generation Warfare: Another Look. *Marine Corps Gazette.* 1992. Vol. 76. No. 10. P. 22-26.

97. Lithuania looks for alternatives to counter Russia's high gas price. *Euractiv.* 2013. URL: https://www.euractiv.com/section/energy/news/lithuania-looksfor-alternatives-to-counter-russia-s-high-gas-price/ (дата звернення: 28.08.2023).

98. Lowe K., Murray W., Mansoor P. R. Hybrid War in Vietnam. *Hybrid Warfare,* Cambridge: Cambridge University Press. 2012. P 254–288.

99. Lasica D. Strategic Implications of Hybrid War: A Theory of Victory. School of Advanced Military Studies, United States Army Command and General Staff College. 2009. URL: https://apps.dtic.mil/sti/pdfs/ADA513663.pdf (дата звернення: 02.08.2023).

100. MacLachlan. Corruption as statecraft: Why urgent steps must be taken to guard against this form of hybrid warfare. *Transparency International Defence & Security.* URL: https://ti-defence.org/corruption-statecraft-urgent-steps-taken-guard-against-hybrid-warfare/(дата звернення: 12.08.2023).

101. Manko O., Mikhieiev Y. Defining the Concept of 'Hybrid Warfare' Based on the Analysis of Russia's Aggression against Ukraine. *Information & Security: An International Journal.* Vol. 41. 2018. P. 11-20.

102. Matthews M. We Were Caught Unprepared: The 2006 Hezbollah-Israeli War. Army Combined Arms Center, Combat Studies Institute Press. The Long War Series Occasional Paper 26. 2008. URL: https://www.armyupress.army.mil/ Portals/7/combat-studies-institute/csi-books/we-were-caught-unprepared.pdf (дата звернення: 26.08.2023).

103. Matuszak S. On the verge of blackout: Ukraine facing attacks on its electricity generation system. OSW Commentary. Centre for Eastern Studies, 2023. URL: https://www.osw.waw.pl/en/publikacje/osw-commentary/2023-01-18/verge-blackout-ukraine-facing-attacks-its-electricit (дата звернення: 27.08.2023).

104. Mazaraki N., Goncharova Y. Cyber dimension of hybrid wars: escaping a «grey zone» of international law to address economic damages. *Baltic Journal of Economic Studies*. Vol. 8. No. 2. 2022. P. 115-120.

105. McCuen J. Hybrid Wars. *Military Review*. Vol. 88, No 2. P. 107-113.

106. McCullah T., Johnson R. Hybrid Warfare. Florida: Joint Special Operations University. 2013. p. 19.

107. MCDC Countering Hybrid Warfare Project:'A Deadlier Peril': The Role of Corruption in Hybrid Warfare. URL : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795222/20190318-MCDC_CHW_Info_note_7.pdf (дата звернення: 12.03.2023).

108. Meldrum A. Russia suspends Ukraine grain export deal over claims of Crimea ship attack. *PBS News Hour*. 2022. URL: https://www.pbs.org/newshour/world/russia-suspends-ukraine-grain-export-deal-over-claims-of-crimea-ship-attack. (дата звернення: 27.08.2023).

109. Merino G. E. Hybrid World War and the United States–China rivalry. URL:https://www.frontiersin.org/articles/10.3389/fpos.2022.1111422/full?fbclid=PAAaacNAS8V4unDIekGcqTV5VsqkA8mqQtnXunN4hxernA_RtI3bG5tOq4kp0 (дата звернення: 02.08.2023).

110. Miller M. Hybrid Warfare: Preparing for Future Conflict. *Air & Space Power Journal.* 2010. Vol. 24. No. 3. P. 35-43.

111. Minniti F. Hybrid warfare and hybrid threats. 2018. URL: https://eeradicalization.com/hybrid-warfare-and-hybrid-threats/ (дата звернення: 17.08.2023).

112. Moldovanu V. The Kremlin's hybrid warfare techniques in a fading world order . URL: https://aspeniaonline.it/the-kremlins-hybrid-warfare-techniques-in-a-fading-world-order/ (дата звернення: 02.08.2023).

113. Murphy M. Ukraine war: Russia accused of using phosphorus bombs in Bakhmut. *BBC News*. 2023. URL: https://www.bbc.com/news/world-europe-65506993 (дата звернення: 27.08.2023).

114. Murray W., Mansoor P. R. Hybrid warfare: fighting complex opponents from the ancient world to the present. Cambridge University Press, 2012. 334 p.

115. Myers S. Lithuanian Parliament Removes Country's President After Casting Votes on Three Charges. *The New York Times*. URL: https://www.nytimes.com/2004/04/07/world/lithuanian-parliament-removes-country-s-president-after-casting-votes-three.html (дата звернення: 12.08.2023).

116. Napoleoni L. Hybrid Warfare and its Challenges for Security. *Journal of Strategic Security*. 2017. Vol. 10. No. 2. P. 13-26.

117. Nissen T. E. Social media`s role in hybrid strategies. URL: https://stratcomcoe.org/cuploads/pfiles/tomas_nissen_article_12-09-2016.pdf (дата звернення: 09.08.2023).

118. Nordby G. The four types of economic coercion. 2019. URL: https://medium.com/@gnorby01/the-four-types-of-economic-coercion-810f1fd7f11a (дата звернення: 17.08.2023).

119. Olenin A. Religious deception: what Russian propaganda portrays as ‘satanic rites’ by Orthodox Church of Ukraine. *Ukrinform.* 2023. URL: https://www.ukrinform.net/rubric-factcheck/3698750-religious-deception-what-russian-propaganda-portrays-as-satanic-rites-by-orthodox-church-of-ukraine.html. (дата звернення: 27.08.2023).

120. Raileanu C., Nitu C. The Azerbaijani Laundromat. URL: https://www.occrp.org/en/azerbaijanilaundromat/ (дата звернення: 12.08.2023).

121. Retter L., Frinking E., Hoorens S., Lynch A. Relationships between the economy and national security. Analysis and considerations for economic security policy in the Netherlands. Santa Monica, CA and Cambridge: RAND Corporation. 2020. URL: https://repository.wodc.nl/handle/20.500.12832/2425 (дата звернення: 13.08.2023).

122. Rosso M. Hybrid War and Its Countermeasures: A Conceptual Overview. *Journal of Strategic Security*. 2019. Vol.12. No. 4. P. 59-70.

123. Russia’s ‘Occupation by Proxy’ of Eastern Ukraine – Implications Under the Geneva Conventions. *Just Security.* 2022. URL:

https://www.justsecurity.org/80314/russias-occupation-by-proxy-of-eastern-ukraine-implications-under-the-geneva-conventions (дата звернення: 27.08.2023).

124. Scharre P. Spectrum of What?» *Military Review*. 2012. Vol. 92. No. 6. URL: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20121231_art012.pdf (дата звернення: 02.08.2023).

125. Schmitz R. Lithuania has become the 1st European country to stop using Russian gas. *NRP*. 2022. URL: https://www.npr.org/2022/05/26/ 1101568189/ lithuania-has-become-the-1st-european-country-to-stop-using-russian-gas (дата звернення: 28.08.2023).

126. Schroefl J., Kaufman S. J. Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid Wa». *Studies in Conflict & Terrorism*. 2014. Vol. 37. No.10. P. 862–880.

127. Sehgal I. Strategic coercion through hybrid warfare. 2019. URL: https://fp.brecorder.com/2019/02/20190215447229/ (дата звернення: 17.08.2023).

128. Singh N. Ukraine's Zelensky has survived more than a dozen assassination attempts, adviser claims. *Independent.* 2022. URL: https://www.independent.co.uk/news/world/europe/ukraine-zelensky-assassination-attempts-russia-b2032759.html (дата звернення: 27.08.2023).

129. Smith C. M. Russian Disinformation During Euromaidan. *International Policy Digest.* 2022. URL: https://intpolicydigest.org/russian-disinformation-during-euromaidan/. (дата звернення: 27.08.2023).

130. Smith E. It's not a pretty picture: Russia's support is growing in the developing world. *CNBC* News. 2023. URL: https://www.cnbc.com/2023/03/30/ ukraine-war-how-russias-support-is-growing-in-the-developing-world.html. (дата звернення: 27.08.2023).

131. Sperling J., Kirchner E. The changing definition of security. Paper delivered at the ECSA Conference Charleston, SC. 1995. URL: http://aei.pitt.edu/7020/1/sperling_james.pdf (дата звернення: 17.08.2023).

132. Stein G. J. Information warfare. *Airpower journal*. 1995. Vol. 9. No.1. P. 30-39.

133. Strassler R. The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War. 1998. 752 p.

134. Thiele R. Artificial Intelligence – A key enabler of hybrid warfare. Hybrid CoE Working Paper. URL: https://www.hybridcoe.fi/wp-content/uploads/2020/07/WP-6_2020_rgb-1.pdf (дата звернення: 10.08.2023).

135. Ukraine: Apparent War Crimes in Russia - Controlled Areas. *Human Rights Watch.* 2022. https://www.hrw.org/news/2022/04/03/ukraine-apparent-war-crimes-russia-controlled-areas (дата звернення: 27.08.2023).

136. Uren D. The growing threat of economic coercion. 2020. URL: https://aicd.companydirectors.com.au/membership/company-director-magazine/2020-back-editions/december/the-growing-threat-of-economic-coercion (дата звернення: 17.08.2023).

137. Van Zon N., Why the Orange Revolution succeeded. *Perspectives on European Policy and Society*. 2005. Vol. 6, No. 3. P. 382-383.

138. Visoni-Alonzo G., The Carrera Revolt and «Hybrid Warfare» in Nineteenth Century Central America. Springer International Publishing. 2017. URL: https://www.perlego.com/fr/book/3496819/the-carrera-revolt-and-hybrid-warfare-in-nineteenthcentury-central-america-pdf (дата звернення: 25.08.2023).

139. Vlasiuk V. Hybrid war? International law and Eastern Ukraine. *European political and law discourse*. Vol. 2. 2015. P. 14-28.

140. Waltz E. Information Warfare Principles and Operations. Artech House. 1998. 397 c.

141. Wither J. K. Making Sense of Hybrid Warfar». *Connections*. 2016. Vol. 15 (2). P. 73–87.

142. Yatsenyuk A. Europe must make this the last winter of weaponized Russian energy exports. *Atlantic Council.* 2022. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/putin-weaponizes-winter-europe-must-end-its-dependency-on-russian-energy/ (дата звернення: 27.08.2023).

143. Zarembo K., Solodkyy S. The Evolution of Russian Hybrid Warfare: Ukraine. *Center «New Europe».* URL: http://neweurope.org.ua/en/analytics/ evolyutsiya-rosijskoyi-gibrydnoyi-vijny-ukrayina/ (дата звернення: 02.08.2023).

144. Zverko N. Russians see Lithuania as small, Russophobic country – interview with ambassador Bajarunas. *LRT*. 2020. URL: https://www.lrt.lt/en/ news-in-english/19/1301536/russians-see-lithuania-as-small-russophobic-country-interview-with-ambassador-bajarunas (дата звернення: 28.08.2023).