Міністерство освіти і науки України
Національний університет “Острозька академія”
Навчально-науковий центр заочно-дистанційного навчання
Кафедра національної безпеки та політології

Кваліфікаційна робота
на здобуття освітнього ступеня магістра на тему:

“Мережеві війни як спосіб агресії в умовах сучасності”

Виконав студент ІІ курсу, групи ЗМНб-21
спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності)
Мокляк Микола Миколайович

Керівник – доктор філософських наук, професор
Шевчук Дмитро Михайлович
Рецензент – кандидат з державного управління, доцент
Шершньова Олена Володимирівна

Острог, 2025

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

DDoS-атаки (англ. Distributed Denial of Service) – напад на комп’ютерну мережу

NCW (англ. Network-Centric Warfare) – мережецентрична війна

OODA (англ. Observe, Orient, Decide, Act) – скорочення циклу прийняття рішень

PSYOP – психологічні операції

АСВП – автоматизовані системи військового планування

АСУ – автоматизовані системи управління

ЄС – Європейський союз

ІКТ – інформаційно-комунікаційні технології

ІПСО – інформаційно-психологічні операції

ІТ – Інформаці́йні техноло́гії (IT information and communication technologies)

НАТО – Організація Північноатлантичного договору (англ. North Atlantic Treaty Organization)

НЗФ – незаконні збройні формування

ОБЕ – операції базових ефектів

ОВТ – озброєння та військова техніка

ООН – Організація Об’єднаних Націй

ПВК – приватні військові компанії

ПЗ – програмне забезпечення

СБУ – Служба безпеки України

ЦРУ – центральне розвідувальне управління

ШІ – штучний інтелект

ШПЗ – шкідливе програмне забезпечення

ЗМІСТ

Війна — це велика справа держави, основа
життя і смерті, шлях до виживання або загибелі.
Це потрібно ретельно зважити й обміркувати.
СУНЬ-ЦЗИ

ВСТУП

Актуальність теми дослідження. Сучасне суспільство, динаміка і специфіка якого визначаються стрімким розвитком інформаційних технологій, інформаційно-комунікаційних систем і цифрових платформ, радикально змінило характер міждержавної конкуренції та збройного протиборства. В XXI столітті конфлікти постають у нових, ускладнених формах, серед яких мережеві війни набувають особливого змісту як ефективний інструмент прихованої агресії зі зламу базових характеристик національної ідентичності, зокрема державності, інформаційного суверенітету та інституцій громадянського суспільства у багатовимірному мережевому впливі на усі типи геополітичного простору — інформаційний, кіберпростір, соціокультурний, економічний, політичний та безпековий.

На зміну традиційним підходам до ведення воєн приходять нові форми, в яких пряма військова сила доповнюється — а подекуди й замінюється — методами інформаційного впливу, кібератак, маніпуляції громадською думкою та операцій у віртуальному, кібернетичному просторі. У цьому контексті й прослідковується стирання меж між воєнним і мирним станом, що унеможливлює чітко розмежувати початок та завершення конфлікту.

Формування нового типу протиборства вимагає перегляду стратегічних і тактичних уявлень про сучасні війни. У науковому та військово-політичному дискурсі з’являються нові категорії: інформаційна війна, мережева війна, мережецентрична війна, кібервійна, гібридна війна, інформаційні операції. Ці поняття відображають не лише зміну форм і засобів, але й трансформацію самого

середовища, в якому відбувається боротьба — з фізичного у цифрово-комунікаційний простір.

Умови глобалізації, активне поширення інформації, висхідна взаємозалежність держав, об`єднання зусиль у боротьбі з тероризмом, а також конкуренція за вплив у політичному, економічному та інформаційному середовищах — усе це формує “мережеву логіку” сучасного світу. Мережі, від соціальних до терористичних, від політичних до економічних, охоплюють практично всі сфери життя. Вони формуються як спеціально, так і стихійно, створюючи гнучкі структури впливу, здатні діяти поза межами державних кордонів і традиційної юрисдикції. Збройні сили та оборонні стратегії держав змушені адаптуватися до цих нових умов сьогодення.

Поняття “мережева війна” залишається відносно новим для української політичної, безпекової та інформаційної науки, воно є інноваційним і семантично незавершеним, перебуваючи на етапі становлення, що передбачає його системну концептуалізацію, зокрема з’ясування їх сутності, змісту, функціональних характеристик, механізмів та сфер застосування. Гострою є також необхідність осмислення практичного досвіду України, яка з 2014 року виступає мішенню для багатоаспектної мережевої агресії з боку Російської Федерації, а вторгнення 2022 року продемонструвало новий рівень координації між кінетичними й некінетичними (інформаційними, кібернетичними, психологічними) операціями. В цих умовах дослідження природи мережевої війни, її форм, каналів реалізації, стратегій та механізмів протидії набуває особливої ваги як з теоретичної, так і з прикладної точки погляду — для формування ефективної державної політики безпеки та розробки стратегії національної безпеки.

Метою дослідження є системний аналіз еволюції концепту мережевих війн, з’ясування їх ролі у трансформації сучасних форм агресії та збройного протиборства, а також виявлення ключових цілей і механізмів реалізації таких війн у глобальному безпековому просторі. Дослідження має на меті окреслити значення мережевих конфліктів у контексті сучасних геополітичних процесів,

особливо з урахуванням досвіду повномасштабного вторгнення Російської Федерації в Україну.

Визначена мета дослідження зумовлює постановку і вирішення наступних **дослідницьких завдань:**

• Провести історико-теоретичний аналіз виникнення, розвитку та типології мережевих війн у контексті трансформації воєнного мистецтва у XXI столітті;

• Визначити ключові ознаки, структуру, принципи ведення та стратегії мережевих війн як складника гібридної агресії;

• Розмежувати поняття “мережева війна”, “мережецентрична війна”, “кібервійна”, “інформаційна війна”, визначивши їх спільні риси та сутнісні відмінності;

• Проаналізувати міжнародний і національний досвід формування політик кібербезпеки, інформаційного захисту та протидії кіберзлочинності;

• Дослідити особливості функціонування безпекової політики України в умовах зростаючих мережевих загроз, із фокусом на політичні, військові та інформаційні аспекти;

• Оцінити ефективність стратегій міжнародного співробітництва в галузі інформаційної безпеки та формування механізмів реагування на мережеві загрози на міждержавному рівні.

Об’єктом дослідження є феномен мережевих війн як форма конфлікту нового покоління, що характеризується зміщенням акцентів з традиційного військового протиборства на асиметричні, децентралізовані форми агресії в межах інформаційного, кібернетичного, соціального та політичного просторів.

Предметом дослідження є специфіка проявів, механізми впливу та заходи протидії мережевим війнам як комплексному інструменту сучасного протиборства.

Джерельна база дослідження. Серед аналітиків, які здійснили вагомий внесок у становлення теорії мережевих війн, варто насамперед згадати Джон Аркілла та Девід Ронфельдт. Саме під їхнім авторством у 1997 році вийшло дослідження “В таборі Афіни: готуючись до конфліктів в інформаційне століття”,

після чого вийшла їхня узагальнююча праця “Мережі і мережі війни: майбутнє терору, злочину і збройної боротьби”.

Вивчення мережевих концепцій найширше представлене в західній політичній науці. Серед провідних дослідників цього напряму Артур Сібровскі та Джон Гарстка, Мануель Кастеллс, Едвард Сміт, Джеймс Моффат, Манабрата Губа, Девід Альбертс, Фредерік Стайн. Теоретичним аспектам мережевих війн присвячені також праці Джон Річардсон, Говард Джордан, Роджер Родес, Девід Марш. Над розвитком мережевого підходу в західній політичній науці активно працюють сучасні теоретики — Таня Бьорцель, Кіт Даудінг, Лоуренс О’Тул. На емпіричному рівні проблематика мережевих війн досліджує низка західних вчених, зокрема це Луїджі Пал, Ерік Кляйн, Джон Коппеньян. В Україні питання мережевих війн досліджують науковці: Дмитро Дроздовський, Вадим Гречанінов, Олег Данильян, Олександр Дзьобань, Олександр Курбан, Галина Куц, Оксана Сенченко, Віталій Цимбалюк, Наталія Хома.

Нормативною основою дослідження є положення вітчизняного та зарубіжного законодавства про розвідувальну діяльність, оборону та національну безпеку.

Методологію дослідження становить міждисциплінарний підхід, який поєднує елементи: військової науки, політології, кібербезпеки, теорії інформаційних комунікацій, соціології та міжнародних відносин. Даний підхід дозволяє комплексно осмислити явище мережевих війн як багатовимірного феномену сучасного конфліктного середовища.

У дослідженні мережевих війн як багатовимірного феномену застосовано комплексний методологічний апарат, що інтегрує провідні наукові підходи та методи.

Системний підхід став засадничим для аналізу мережевих війн, розглядаючи їх як складну, динамічну систему, що функціонує на багатьох взаємопов’язаних рівнях: технологічному, політичному, соціальному, інформаційному та безпековому. Це дозволило виявити взаємозалежності між компонентами системи та їхній вплив на загальну стратегічну архітектуру конфлікту.

Функціональний підхід використовувався для детермінації ролі та функцій мережевих структур у контексті конфліктів нового типу. Це дало змогу чітко ідентифікувати специфічні завдання, які виконують мережеві актори, та оцінити їхній внесок у досягнення стратегічних цілей агресора.

Кібернетичний підхід слугував основою для вивчення процесів інформаційного управління, комунікаційного впливу та обміну даними, що є ключовими в умовах сучасного інформаційного протиборства. Він дозволив проаналізувати механізми контролю та регулювання в мережевих структурах, а також виявити точки вразливості в їхній системі функціонування.

У межах дослідження було застосовано наступні наукові методи:

Аналіз і синтез були імплементовані для поглибленого вивчення широкого спектра наукових джерел, нормативно-правової бази, матеріалів міжнародних організацій та узагальнення практики ведення мережевих війн.

Порівняльно-правовий метод використовувався для зіставлення підходів різних держав до формування національних стратегій протидії кіберагресії та інформаційним загрозам. Це дало змогу виявити найкращі практики, а також визначити універсальні та специфічні елементи в міжнародному досвіді.

Метод аналогій застосовувався для виявлення подібностей і відмінностей між різними формами конфліктів, зокрема між традиційною війною, інформаційною та мережецентричною війною. Це дозволило краще зрозуміти еволюцію воєнних дій та особливості нових типів протистояння.

Системний аналіз був використаний для детального вивчення взаємозв’язків між кіберзагрозами, інформаційною війною та загальною архітектурою національної безпеки, що дозволило побудувати цілісну модель функціонування цих елементів у контексті конфлікту.

Метод прогнозування застосовувався для визначення можливих сценаріїв розвитку мережевих загроз та розробки відповідних стратегій їх нейтралізації, що є критично важливим для формування ефективної оборонної політики.

Емпіричний аналіз був залучений для вивчення конкретних кейсів, таких як вторгнення Російської Федерації в Україну як форми мережевої агресії, та оцінки

їхнього впливу на міжнародну і національну безпеку. Цей метод дозволив верифікувати теоретичні положення на основі реальних подій та фактів.

Таким чином, наукове дослідження ґрунтується на поєднанні теоретичних та практичних підходів, що забезпечує всебічне і глибоке вивчення феномену мережевих війн у сучасному безпековому контексті.

Структура й обсяг дослідження. Робота складається зі вступу, п’яти розділів, що сукупно охоплюють двадцять три підрозділи, висновків, переліку використаних джерел.

У розділі 1 “Мережеві війни як різновид сучасних воєнних дій” розглянуто трансформації способів і методів ведення воєн (підрозділ 1.1.), вивчено суть поняття “мережа” та формування мережевого суспільства воєнних (підрозділ 1.2.), досліджено основні аспекти мережевої війни, проведено аналіз мережевих війн як нового типу сучасних протистоянь (підрозділ 1.3.), проаналізовано концепцію “мережецентричної війни” (війни шостого покоління) розкрито її теоретичну основу для розуміння мережевих воєн (підрозділ 1.4.), розглянуто сфери протистояння та театри мережевих воєн (підрозділ 1.5.)

У розділі 2 “Операції базових ефектів” встановлено концептуальні засади ОБЕ у підходах до воєнного планування та застосування сили в умовах сучасної мережевої війни (підрозділ 2.1), розглянуто методи реалізації ОБЕ, які ґрунтуються на використанні широкого арсеналу інструментів (підрозділ 2.2.), вивчено механізми оцінки ефективності операцій що дозволяють прогнозувати ймовірні наслідки і швидко реагувати на зміни ситуації (підрозділ 2.3.), проаналізовано сучасні приклади застосування ОБЕ (підрозділ 2.4.).

У розділі 3 “Інформаційна війна: тенденції та перспективи розвитку” проведений аналіз різних аспектів інформаційної війни (підрозділ 3.1), досліджено стратегії інформаційної війни в окремих країнах (підрозділ 3.2), розглянуто інформаційну війну як чинник загрози національній безпеці (підрозділ 3.3), проведено дослідження інформаційного впливу як технології ведення бойових дій (підрозділ 3.4).

У розділі 4 “Кібервійна як вид та інструмент мережевих воєн” розглянуто кібервійна як інформаційне протиборство в кіберпросторі (підрозділ 4.1), досліджено кібершпигунство та несанкціонований збір даних (підрозділ 4.2) проаналізовано явище кіберсаботажу як навмисного порушення роботи інформаційних систем (підрозділ 4.3), проведено дослідження атак на критичну інфраструктуру та навмисних кіберзагроз комунікаційно-інформаційним системам (підрозділ 4.4), виявлено їхню особливу небезпеку для національної безпеки. Детально розглянуто поняття кібертероризм як злочинне використання кіберпростору (підрозділ 4.5)

У розділі 5 “Мережеві війни в умовах сучасності” розглянуто поняття “гібридна війна”, як інтегральна форма мережевої агресії (підрозділ 5.1), вивчено технологічний складник мережевих війн базується на використанні високоточних інформаційних систем (підрозділ 5.2), проведено аналіз різноманітності акторів мережевих війн. Поряд із державами, які мають високотехнологічні кіберпідрозділи, активну участь у війні беруть недержавні структури: хакерські угруповання, транснаціональні корпорації, окремі фахівці (підрозділ 5.3), досліджено міжнародно-правову базу щодо ведення мережевих війн, яка усе ще знаходиться на стадії формування (підрозділ 5.4), розглянуто Україну як одну з ключових цілей мережевої агресії Росії і яка опинилася в авангарді захисту в інформ-аційно-кіберпросторовому вимірі, намічено заходи протидії (підрозділ 5.5).

У загальних висновках сформульовано підсумкові результати дослідження.

Загальний обсяг роботи – 117 сторінок, з них основної частини – 97 сторінок. Перелік використаних джерел складає 163 найменувань.

РОЗДІЛ 1
МЕРЕЖЕВІ ВІЙНИ ЯК РІЗНОВИД СУЧАСНИХ ВОЄННИХ ДІЙ

1.1.Трансформація способів і методів ведення воєн

Уся історія людської цивілізації є невіддільною від історії воєн та збройних конфліктів. Сучасне розуміння війни визначає її як протистояння між політичними суб'єктами – державами, етнічними групами, політичними об'єднаннями – що відбувається у формі збройної боротьби із залученням військових сил та регулюється нормами міжнародного права, які встановлюють гуманітарні стандарти ведення бойових дій, зокрема, захист цивільного населення, ставлення до військовополонених та заборону на використання негуманних видів озброєння.

Однак, в умовах становлення інформаційного суспільства та епохи цифрових технологій, спостерігається фундаментальна зміна форм, методів та організаційних принципів ведення війни. Традиційні характеристики військових конфліктів, такі як наявність чіткої лінії фронту, мобілізація регулярних армій та територіальне протистояння, поступово поступаються місцем нетрадиційним моделям ведення бойових дій. Джон Аркілла, аналізуючи новітні форми військового протиборства, запропонував науковий термін "роювання", що проявляється як множинні асиметричні та децентралізовані дії – "мікросутички" та "мікродії", починаючи від публічних протестів та маніпулятивних медійних матеріалів і закінчуючи локальними бойовими зіткненнями, дипломатичними маневрами та навмисним поширенням дезінформації [13, С. 5].

У такому типі війни зникає класична фронтова лінія, натомість формується багатовимірний простір бойових дій, що охоплює політичну, культурну, економічну, наукову сфери, міський простір та цифровий вимір – інтернет. У цьому складному просторі одночасно можуть розгортатися терористичні акти, кампанії політичного впливу та навіть легітимні демократичні процеси. Уся ця сукупність формує структуру, яку Джон Аркілла та Девід Ронфельдт

характеризують як “мережа проти ієрархії”, тобто війну, що ведеться не централізованими арміями, а розгалуженими та динамічними структурами з мінімальним рівнем бюрократії [13, С. 15-22].

Згадані автори зазначають, що в умовах постмодерного світу владні повноваження все більше переходять від традиційних держав до нових впливових акторів, таких як транснаціональні корпорації, глобальні соціально-політичні рухи, терористичні та злочинні мережі, наркокартелі тощо. Ці недержавні актори здатні досягати військових цілей, використовуючи комунікаційні технології, соціальні медіа, недержавні організації, засоби масової інформації, інтернет-ресурси, спеціальні служби та приватні військові компанії. Така еволюція війни не тільки змінює тактику протиборства, а й значно ускладнює ідентифікацію джерела загрози.

Для розуміння сутності воєнних конфліктів фундаментальною основою залишаються теоретичні положення Карла фон Клаузевіца [75, С. 35-48]. Він визначав війну як політичний інструмент, що реалізується через насильство з метою примушення противника до виконання власної волі. При цьому війна розглядається як взаємодія двох протилежних воль, де перемога залежить не лише від наявних ресурсів, але й від рівня рішучості сторін. Водночас Клаузевіц визнавав, що війна є дією, яка не підпорядковується жорстким правовим обмеженням і в екстремальних формах може трансформуватися в “абсолютну війну” – тотальне насильство [75, С. 78-85].

Однак, у XXI столітті, в умовах глобалізації, ядерного стримування, розвитку міжнародного права та ускладнення геоекономічних взаємозв’язків, класична тотальна війна все частіше поступається місцем новим формам конфліктів. На на думку Збігнєва Бжезінського [15, С. 29-42], Самюела Гантінгтона [23, С. 55-72] та інших аналітиків, геоекономічне суперництво, глобальні економічні спади та боротьба за природні ресурси формують нову парадигму війни, в якій геополітичні переваги досягаються нетрадиційними, “гібридними” засобами. Це змушує держави та глобальних акторів шукати

інструменти для досягнення своїх цілей без прямого військового вторгнення [15, С. 58-71].

У цьому контексті ключову роль відіграють “операції базових ефектів”, спрямовані на вплив не стільки на матеріальні об’єкти, скільки на моделі поведінки, переконання та наміри противника. Метою таких операцій є встановлення м’якого, але системного контролю над суспільствами в умовах миру, конфлікту чи кризи.

Останнім часом в науковому колі широко використовуються терміни “гібридна війна”, “нестандартна війна”, “війна керованого хаосу”, “змішана війна”, “дифузна війна”. Усі ці поняття відображають фундаментальну зміну парадигми війни – від прямого збройного зіткнення на лінії фронту до комплексного багаторівневого впливу, що поєднує елементи жорсткої та м’якої сили, використовуючи інформаційні, економічні, психологічні, культурні, технологічні та кібернетичні інструменти впливу. Деякі дослідники визначають такі війни як “неконвенційні”, що передбачають одночасне використання всього наявного арсеналу засобів.

Сьогодні світ активно формує нову глобальну соціальну реальність, що діалектично поєднується з локальними мережевими соціальними утвореннями. На обох рівнях ми стикаємося зі значним ускладненням соціокультурної динаміки, безпрецедентними біфуркаціями та появою нових форм агресії й силового протиборства. В умовах глобалізації, культури, що зазнають змін, не лише активно опираються, а й рефлексують, прагнучи зберегти свою ідентичність. Для цього вони нерідко залучають різноманітні сучасні засоби та способи ведення війн.

Таким чином, сучасна війна поступово набуває ознак тотального соціального явища, що охоплює не лише збройні сили, але й інформаційний простір, суспільну свідомість, політичні системи та економічні процеси. Стає очевидним формування нової глобальної соціальної реальності, яка одночасно є і локальною – з мережею гнучких та адаптивних форм і механізмів протиборства. Тобто, мережева війна є якісно новим рівнем розуміння природи сучасних

конфліктів. Вона передбачає використання мережевих структур організації, інформаційно-комунікаційних технологій та відповідних стратегій, що дозволяють максимально ефективно досягати політичних та стратегічних цілей в постіндустріальному суспільстві.

Мережева війна є принципово новим рівнем осмислення цілей і завдань сучасних збройних конфліктів. По суті, це особлива форма ведення протистояння, де учасники використовують мережеві структури, доктрини, стратегії та технології, максимально адаптовані до реалій інформаційного суспільства.

1.2. Суть поняття “мережа” та формування мережевого суспільства

В епоху інформаційної революції та стрімкого розвитку комунікаційних технологій, поняття “мережа” набуває фундаментального значення для розуміння організації та функціонування сучасного суспільства. Традиційні ієрархічні структури поступово поступаються місцем більш гнучким та децентралізованим мережевим утворенням, що пронизують усі сфери людської діяльності – від міжособистісних відносин до глобальних економічних та політичних процесів.

У науковій літературі описані три основні типи мереж, які відрізняються характером зав’язків між елементами:

Рис. 1.1 Три базових типи мереж.

а) Ланцюгова або лінійна мережа. Вона функціонує як послідовний канал передачі інформації, ресурсів чи впливу. Такий тип характерний для тіньових

або кримінальних структур (наприклад, контрабандні мережі), де взаємозв'язки між кінцевими учасниками опосередковуються через численні вузли.

б) Зіркоподібна або центральна мережа. Усі актори мають зв'язок із фокальним центром, через який здійснюється координація. Така структура властива франшизам або картельним об'єднанням, у яких учасники взаємодіють із центром, але не обов'язково між собою.

в) Повноматрична (загальноканальна) мережа. Всі учасники безпосередньо пов'язані один з одним. Це найдемократичніший тип мережі, типовий для громадських рухів, коаліцій активістів, наприклад, мережі співпраці борців за мир. Така структура забезпечує високий рівень горизонтальної взаємодії та комунікації [40, С. 36].

Слід зауважити, що реальні мережі часто мають гібридний характер, тобто поєднують різні типи організації залежно від мети, середовища функціонування та конкретних завдань. Наприклад, суб'єкт мережної організації може мати директорат, сформований як повноматрична мережа, а водночас для оперативної діяльності використовувати ланцюгову модель комунікації. Така адаптивність робить мережі надзвичайно ефективними в умовах сучасного складного світу [15, С. 36].

У своїй фундаментальній праці "Мережеве суспільство", Мануель Кастельс визначає мережу як "сукупність взаємопов'язаних вузлів" [74, С. 69]. Ці вузли можуть бути різноманітними за своєю природою: індивідами, групами, організаціями, інституціями або навіть технологічними системами. Головною характеристикою мережі є їхня здатність до самоорганізації та масштабування, що забезпечується завдяки гнучким зв'язкам між вузлами. На відміну від ієрархічних структур, де комунікація та влада концентруються у верхніх рівнях, у мережах інформація та вплив циркулюють горизонтально між рівноправними вузлами, що забезпечує більшу адаптивність та стійкість до зовнішніх впливів.

Мережеві структури охоплюють широкий спектр суб'єктів: від фінансових установ, медіа та транснаціональних корпорацій до громадських, релігійних, неурядових організацій, політичних осередків і спецслужб. До них також

належать різноманітні медіаресурси — як великі видання, так і аматорські мережеві публікації чи блоги, які можуть бути заангажовані однією зі сторін конфлікту. Ці мережі можуть бути сформовані й на основі несподіваних зав'язків, як-от асоціації чи клуби за інтересами (мисливців, філателістів, колекціонерів), що підтримують контакти з подібними групами по всьому світу та проводять спільні зустрічі чи форуми. Зрештою, мережею є і невеликі терористичні групи, які координують свої дії через інтернет, мобільний чи супутниковий зв'язок, об'єднані спільними ідеологічними установками та цілями.

Ці різнорідні мережі поступово інтегруються у надзвичайно гнучку та різноманітну структуру, де елементи, які раніше ніколи не взаємодіяли, починають вступати у взаємозв'язок. По суті, мережа є провідником, через який можна передати певний сигнал, що буде сприйнятий, поширений далі та реалізований. Така мережа може бути як цілеспрямовано створена та налаштована, так і модифікована чи використана у своєму початковому вигляді з початковими параметрами для досягнення бажаних цілей [122, С. 37-41.].

Сутність мережі полягає не лише в наявності взаємопов'язаних елементів, але й у характері цих зав'язків. Мережеві зв'язки є динамічними, можуть встановлюватися, розриватися та змінюватися залежно від потреб та цілей учасників. Інтенсивність та спрямованість цих зав'язків визначають структуру та функціональні можливості мережі. Завдяки своїй гнучкості та здатності до швидкої реконфігурації, мережі виявляються більш ефективними у вирішенні складних завдань та адаптації до швидкозмінних умов порівняно з жорсткими ієрархічними системами.

Формування мережевого суспільства є результатом взаємодії низки ключових факторів, серед яких центральну роль відіграє розвиток інформаційно-комунікаційних технологій (ІКТ). Інтернет, мобільний зв'язок, соціальні мережі та інші цифрові платформи стали каталізаторами формування глобальних мереж, які об'єднують мільярди людей та організацій незалежно від їхнього географічного розташування. Ці технології забезпечують безпрецедентні

можливості для комунікації, обміну інформацією, співпраці та координації дій між різними учасниками та елементами мережі [115, С. 28-55].

Процес формування мережевого суспільства має глибокі соціальні, економічні та політичні наслідки. В економічній сфері спостерігається зростання значення мережевих форм організації бізнесу, таких як транснаціональні корпорації, стратегічні альянси та віртуальні підприємства. Ці мережеві структури дозволяють компаніям оптимізувати свої ресурси, розширювати ринки збуту та підвищувати свою конкурентоздатність в умовах глобалізації [74, С. 167-214].

У соціальній сфері формування мережевого суспільства призводить до змін у характері міжособистісних відносин та соціальної взаємодії. Зростає значення віртуальних спільнот та онлайн-платформ як просторів для спілкування, самовираження та колективної співпраці. Мережеві соціальні рухи набувають значної політичної сили, використовуючи можливості Інтернету та соціальних мереж для мобілізації своїх прихильників та координації демонстрацій та протестів.

У політичній сфері мережеве суспільство створює нові можливості для демократизації та громадянської участі, але водночас породжує нові виклики, пов’язані з поширенням дезінформації, кіберзлочинністю та загрозами національній безпеці. Мережеві структури можуть використовуватися як для позитивних цілей, таких як організація волонтерських рухів та громадський контроль за діяльністю влади, так і для деструктивних цілей, включаючи тероризм та екстремізм [104, С. 87-115].

Мережа — це, по суті, будь-яка сукупність елементів, що мають взаємозв’язок, але при цьому відсутня жорстка ієрархія. Ієрархічні структури можуть функціонувати як окремі вузли в рамках більшої мережі. Важливо розуміти, що кількість учасників чи розмір мережі не визначають її ефективності. Навіть найпростіший контакт між двома людьми, що обмінялися інформацією, є базовою моделлю мережі, яка зароджується. Наприклад, якщо чиновник у Києві з державної структури надсилає електронною поштою

інформацію незнайомому репортеру в Берлін — це вже початок формування мережі. Повторний же контакт перетворює її на діючу мережу, яку можна задіяти в поточній мережевій операції. Іншими словами, сучасне інформаційне суспільство стало ідеальним середовищем для створення, функціонування та використання мереж. Це вже не метафора, а об'єктивна реальність сьогодення [122, С. 37-41].

Отже, поняття "мережа" є ключовим для розуміння сутності сучасного суспільства. Мережа являє собою гнучку та децентралізовану структуру, що складається з взаємопов'язаних вузлів, здатних до самоорганізації та масштабування. Формування мережевого суспільства є результатом розвитку ІКТ та має глибокі соціальні, економічні та політичні наслідки, трансформуючи традиційні форми організації та взаємодії. Розуміння сутності мережі та закономірностей формування мережевого суспільства є необхідною умовою для аналізу сучасних соціальних процесів та розробки ефективних стратегій розвитку в умовах глобальної інформатизації для будь-якої сфери, зокрема військової.

1.3. Мережева війна: сутність, ознаки та особливості прояву

Мережева війна (Netwar) — це сучасна форма конфлікту, в якій сторони використовують мережеві структури, стратегії та технології, адаптовані до інформаційної епохи. Замість традиційних ієрархічних армій, у таких війнах діють децентралізовані, гнучкі соціальні мережі. Типовими учасниками мережевих війн можуть бути:

- терористичні та злочинні угруповання;
- громадські організації та соціальні рухи (наприклад, альтерглобалісти, радикальні екологи).

Вказані мережі покладаються на свою гнучкість і децентралізацію, щоб ефективно діяти в сучасному інформаційному просторі. Різні актори, від кримінальних структур до соціальних активістів, можуть використовувати

мережеві принципи для досягнення своїх цілей у конфліктних ситуаціях. У контексті глобальної інформатизації та зростаючої взаємозалежності держав, феномен мережевої війни набуває особливої актуальності як якісно новий рівень міждержавного протиборства.

Сутність мережевої війни полягає у використанні розподілених мережевих структур для досягнення стратегічних цілей агресора. Мережева війна, як спосіб агресії, спрямована на комплексний вплив на життєво важливі сфери функціонування держави, суспільства та особистості, використовуючи приховані та непрямі методи руйнування та дестабілізації. На відміну від традиційних військових конфліктів, де домінує ієрархічна організація та пряме зіткнення збройних сил, мережева війна характеризується децентралізованою структурою учасників, множинністю векторів впливу та опорою на інформаційні технології як основний інструмент ведення боротьби [40, С. 15-28]. Ключовим елементом є створення та використання складних мереж, що об'єднують різноманітні суб'єкти – державні та недержавні актори, політичні рухи, громадські організації, окремих індивідів – для здійснення скоординованих дій, спрямованих на підрив стійкості об'єкта агресії.

Аналізуючи сутність мережевої війни, необхідно виокремити її характерні ознаки. По-перше, це розмитість меж між агресором та жертвою. Мережеві атаки можуть здійснюватися анонімно або через підставних осіб, що ускладнює ідентифікацію та притягнення до відповідальності ініціаторів агресії. По-друге, багатовекторність впливу. Мережева війна не обмежується військовою сферою, а охоплює політичну, економічну, соціальну, культурну та інформаційну площини, створюючи комплексний тиск на об'єкт агресії [58, С. 45-52]. По-третє, використання інформаційних технологій як основної зброї. Кібератаки на критичну інфраструктуру, поширення дезінформації, маніпулювання громадською думкою через соціальні мережі та інші цифрові платформи стають ключовими інструментами мережевої війни [60, С. 78-85]. По-четверте, децентралізований характер управління. Мережеві операції можуть координуватися з єдиного центру, але значна частина дій здійснюється

автономно окремими учасниками мережі, що забезпечує гнучкість та стійкість до контрзаходів. По-п’яте, прихований характер дій. Мережева агресія часто здійснюється латентно, без відкритого застосування військової сили, що ускладнює її своєчасне виявлення та протидію.

Особливості прояву мережевої війни є різноманітними та постійно еволюціонують під впливом розвитку інформаційних технологій та геополітичної ситуації. Однією з ключових особливостей є активне використання соціальних мереж. Соціальні мережі вийшли за межі звичайних комунікаційних платформ, перетворившись на потужний інструмент для поширення пропаганди та організації різноманітної діяльності: протестів, координації деструктивних дій та психологічного впливу на населення [128, С. 112-125]. Кібератаки на об’єкти критичної інфраструктури (енергетичні системи, фінансові установи, транспортні мережі) є ще однією характерною особливістю мережевої війни, здатні завдати значної шкоди та паралізувати життєдіяльність держави. Інформаційно-психологічні операції (ІПСО), спрямовані на маніпулювання свідомістю населення, підрив довіри до державних інститутів, розпалювання соціальної напруги та формування вигідної агресору громадської думки, також є невід’ємною складовою мережевої війни [59, С. 92-105].

Важливою особливістю є саме стирання географічних меж конфлікту. Мережеві атаки можуть здійснюватися з будь-якої точки світу та мати глобальні наслідки. Це ускладнює визначення джерела загрози та розробку ефективних заходів протидії. Крім того, мережева війна характеризується високою динамічністю та адаптивністю. Агресор постійно вдосконалює свої методи та інструменти, використовуючи новітні технології та соціальні тренди, що вимагає від об’єкта агресії постійного моніторингу та оперативного реагування.

У сучасній українській науковій літературі виділяють низку характерних особливостей мережевих війн. Насамперед, інформаційна сфера розглядається як повноцінне поле бою, так само як повітряно-космічний, морський і наземний простір. Ці війни мають асиметричний характер, що дозволяє державі з невеликими збройними силами завдавати серйозної шкоди значно сильнішому

противнику. Мережеві війни безпосередньо або опосередковано впливають на події в реальному світі та суттєво впливають на когнітивні й емоційні процеси людей, на їхнє сприйняття подій та прийняття рішень. Характерними рисами є також неясність і невизначеність правил застосування, відсутність повних даних про можливості, швидкість та ефективність реакції радіоелектронних засобів і комп'ютерних систем, а також труднощі у розпізнаванні навмисних і ненавмисних дій у кіберпросторі.

Мережеві війни вимагають одночасного використання сил і засобів як для впливу на противника, так і для захисту власних військ і сил союзників. При цьому відстань до цілі впливу не має значення, а противник може наносити атаки анонімно і приховано. Основною метою мережевих війн є забезпечення ефективності бойових дій в умовах мережевого управління військами. Їх успіх ґрунтується на методології використання інтегрованих можливостей усіх сил інформаційних операцій, їх забезпечення або пов'язаних з їх застосуванням [95, С. 264-273].

Сучасні акти насильства, здійснювані через мережі, визначаються насамперед їхнім функціональним значенням, а не фізичним розташуванням суб'єктів. Території тепер стають вторинними по відношенню до функціональних вузлів інформаційної мережі. Це означає, що рішення приймаються в мережі, але реалізуються локально, на певній території. Саме ця особливість лежить в основі сутності сучасних агресивних практик, зокрема мережевих війн. Наприклад, агресор сьогодні здатен вести інформаційні війни на будь-якій території, перебуваючи при цьому у зручному для себе місці, в будь-який час, зберігаючи свою анонімність [17, С. 13.].

Теорія мережевих війн базується на уявленні, що мережі складаються з чотирьох тісно пов'язаних між собою рівнів: організаційного, доктринального, технологічного та соціального. Організаційний рівень визначає, яким має бути оптимальний масштаб окремого учасника або об'єднання, що формують мережу. Він є основою для того, щоб зрозуміти, хто може виступати учасником мережевої війни. Доктринальний рівень розкриває, що саме поєднує учасників

мережі — це можуть бути спільні переконання, ідеології, прагнення чи інші мотиви, які зумовлюють використання такої структури. Центральним у цьому аспекті є усвідомлення чинників, які утримують мережу цілісною та дозволяють її членам діяти скоординовано без централізованого керівництва.

Технологічний рівень фокусується на тих технологічних засобах, що забезпечують ефективне функціонування мережі, визначають її потенціал та інтенсивність інформаційних і комунікаційних потоків. Соціальний рівень охоплює особисті взаємини між учасниками мережі. Це сфера аналізу соціальних зав'язків, де міцна довіра формується на основі родинних, етнічних, релігійних зав'язків, дружби або спільного досвіду. Саме тому до мережевих воєн часто залучаються етнічні та націоналістичні рухи, сепаратисти, злочинні угруповання, терористи, радикальні активісти, хакери й інші групи, які здатні діяти без централізованої структури [47, С. 41].

Таким чином, мережева війна являє собою складний та багатогранний феномен, що якісно відрізняється від традиційних форм збройного протистояння. Її сутність полягає у використанні децентралізованих мережевих структур та інформаційних технологій для досягнення стратегічних цілей шляхом комплексного впливу на різні сфери життєдіяльності об'єкта агресії. Характерними ознаками мережевої війни є розмитість меж, багатовекторність впливу, домінування інформаційних технологій, децентралізоване управління та прихований характер дій. Особливості її прояву включають активне використання соціальних мереж, кібератаки на критичну інфраструктуру, інформаційно-психологічні операції, стирання географічних меж та високу динамічність. Розуміння сутності, ознак та особливостей прояву мережевої війни є критично важливим для розробки ефективних стратегій забезпечення національної безпеки в умовах сучасних геополітичних реалій.

1.4. Концепція "мережецентричної війни" (війни шостого покоління)

Концепція "мережецентричної війни" (Network-Centric Warfare – NCW), яка часто розглядається як теоретична основа для розуміння так званих війн шостого

покоління, являє собою революційний підхід до ведення бойових дій, що ґрунтується на інтеграції інформаційних технологій для створення високо інтегрованої та ситуаційно обізнаної бойової мережі. Ця концепція передбачає трансформацію збройних сил із традиційних ієрархічних структур на гнучкі та адаптивні мережеві утворення, здатні досягати інформаційної переваги, підвищувати швидкість прийняття рішень та значно збільшувати бойову ефективність [25, С. 35-48].

Витоки концепції “мережецентричної війни” сягають кінця ХХ століття та пов’язані з розвитком теорії інформаційної війни та усвідомленням зростаючої ролі інформації у військових конфліктах. “Мережецентрична війна” розглядається як нова концепція ведення війн, ця концепція була розроблена Управлінням Реформування Збройних Сил США під керівництвом віце-адмірала Артура Себровскі, який разом з Джоном Гарстка були одними з перших теоретиків, які заклали основи NCW [16, С. 103-116], вони у своїх працях наголошували на необхідності переходу від платформо-центричної до мережецентричної моделі ведення бойових дій для досягнення якісно нового рівня бойової спроможності [38, С. 98-111]. Мережецентричні трансформації зумовлені глибинними змінами в американському суспільстві. Ці зміни були наслідком взаємопов’язаної коеволюції економіки, інформаційних технологій та бізнес-процесів, які виділяють три ключові теми:

- перехід від фокусу на окремі платформи до мережевих структур;
- зміна сприйняття акторів: від незалежних одиниць до елементів єдиної, постійно адаптованої системи;
- вирішальне значення стратегічного вибору щодо адаптації або виживання в умовах динамічної зміни обстановки.

Розробники цієї концепції також вважають, що мережецентричний підхід до ведення бойових дій дозволяє відійти від виснажливих війн на користь швидшої та ефективнішої збройної боротьби. Для такої боротьби характерні висока швидкість управління та принцип самосинхронізації, що означає здатність

військової структури самоорганізовуватися “знизу”, без очікування вказівок “згори”. [16, С. 103-116].

Суть концепції “мережецентричної війни” полягає у створенні комплексної інформаційної мережі, яка об’єднує всі елементи бойової системи – від окремого солдата до вищого командного складу, сенсори, зброю та платформи. Завдяки безперервному обміну інформацією в режимі реального часу, учасники бойових дій отримують повніше та оперативніше розуміння бойової обстановки (ситуаційної обізнаності), що дозволяє їм приймати більш обґрунтовані та швидкі рішення, координувати свої дії та ефективніше вражати противника.

Основними принципами “мережецентричної війни” є:

Інтеграція інформаційних систем передбачає формування єдиної мережі, яка об’єднує всі компоненти бойової системи.

Ситуаційна обізнаність: забезпечення всіх учасників бойових дій повною та актуальною інформацією про бойову обстановку.

Самосинхронізація: здатність децентралізованих бойових одиниць координувати свої дії на основі спільного розуміння ситуації без прямого централізованого управління.

Швидкість прийняття рішень: скорочення циклу прийняття рішень (OODA – Observe, Orient, Decide, Act) завдяки швидкому обміну інформацією та підвищеній ситуаційній обізнаності. Підвищення бойової ефективності: досягнення якісно нового рівня бойової спроможності за рахунок інтеграції інформації, швидкості прийняття рішень та самосинхронізації [37, С. 98-111].

Концепція “мережецентричної війни” розглядається як основа для розуміння війн шостого покоління, які, на відміну від попередніх поколінь, характеризуються домінуванням інформаційного простору, високою швидкістю розгортання подій. У війнах шостого покоління інформаційна перевага стає ключовим фактором досягнення перемоги, а здатність швидко обробляти інформацію, приймати рішення та координувати дії в умовах невизначеності є вирішальною [85, С. 98-111].

Впровадження концепції “мережецентричної війни” вимагає значних змін в організаційній структурі збройних сил, системі управління, технологічному забезпеченні та підготовці особового складу. Необхідна інтеграція різнорідних інформаційних систем, забезпечення їхньої сумісності та захищеності від кіберзагроз. Крім того, вимагається розвиток нових навичок у військовослужбовців, пов’язаних з ефективним використанням інформаційних технологій та прийняттям рішень в умовах інформаційної перевантаженості [4].

Критики концепції “мережецентричної війни” вказують на її технологічний детермінізм та недооцінку людського фактора. Вони стверджують, що надмірна залежність від інформаційних мереж може зробити збройні сили вразливими до кібератак, а втрата зв’язку може призвести до паралічу управління. Крім того, швидкість прийняття рішень не завжди гарантує їхню якість, особливо в умовах неповної або недостовірної інформації. Незважаючи на інертність сприйняття, концепція “мережецентричної війни” мала значний вплив на розвиток військової думки та практику будівництва збройних сил у багатьох країнах світу. Ідеї інтеграції інформаційних технологій, підвищення ситуаційної обізнаності та децентралізації управління продовжують залишатися актуальними в умовах сучасних військових конфліктів, де інформаційна перевага відіграє дедалі важливішу роль [158].

Важливо ще раз підкреслити, що мережецентрична війна та мережева війна — це різні поняття. У широкому розумінні, мережева війна є конфліктом мережі проти ієрархії, де децентралізовані структури протиставляються традиційним ієрархічним системам, застосовуючи мережеві стратегії та методи. Вона може розгортатися на більш тонких рівнях, залучаючи інформаційні технології, дипломатичні мережі, неурядові організації, а також журналістів, ЗМІ, блогерів та весь арсенал інформаційного суспільства в парадигмі постмодерну. З огляду на це, мережеву війну можна визначити як соціально-політичну, соціально-економічну та культурну інновацію, що базується на інформаційно-комунікаційних технологіях. Вона використовується інститутами управління або певними групами для досягнення цілей управління та контролю Натомість, мережецентрична війна є військовою концепцією, являє собою важливий етап в еволюції військової справи і відображає

зростаючу роль інформаційних технологій у веденні бойових дій. Хоча її практична реалізація стикається з певними викликами та обмеженнями, ідеї, закладені в її основу, продовжують впливати на розвиток збройних сил та стратегічне мислення у контексті війн шостого покоління [16, С. 103-116].

1.5. Сфери протистояння та театри мережевих воєн

Мережева війна, як сучасна форма конфлікту, характеризується розмиванням традиційних просторових меж та охоплює широкий спектр сфер протистояння, що виходять далеко за межі фізичного поля бою. Її сутність полягає в інформаційно-комунікаційному протиборстві, яке розгортається як в реальному світі (офлайн), так і в кіберпросторі (онлайн), із залученням різноманітних мережевих структур. До типових офлайн мережевих утворень належать формальні та неформальні організації, а також тимчасові об’єднання індивідів, що формуються на основі спільної діяльності або об’єднуючих їх інтересів. Онлайн мережеві структури представлені інтернет-ресурсами епохи Web 2.0, зокрема, віртуальними соціальними мережами, такими як Facebook, Twitter (X) та інші подібні платформи, що стали потужними інструментами для комунікації та координації дій [46, С. 187-202].

Залежно від специфіки та цільового охоплення, інформаційні конфлікти, що є суттєвою складовою мережевих війн, розгортаються у п’яти основних просторових площинах: глобальній, міжнаціональній, міжгруповій, міжособистісній та внутрішньо-особистісній [137, С. 215-230]. Кожна з цих площин має свої особливості та механізми реалізації протистояння. Глобальний простір інформаційних конфліктів характеризується планетарним масштабом впливу та охоплює інформаційні процеси, що мають значення для світової спільноти. Цей простір значною мірою перетинається з філософсько-науковими концепціями ноосфери та інфосфери, відображаючи зростаючу роль інформації у планетарному масштабі. З точки зору технологічної реалізації, він також корелює з концепцією “глобального села” Маршалла Маклюена, підкреслюючи взаємопов’язаність світу через інформаційні потоки. Історичним прикладом глобального інформаційного

протистояння була “Холодна війна” між США та СРСР і їхніми союзниками. У сучасному світі подібні процеси спостерігаються у відносинах між великими державами, такими як США та Китай, Російська Федерація, де інформаційний вплив є важливим інструментом геополітичної боротьби [109, С. 95-110].

Міжнаціональний простір інформаційних конфліктів розгортається на рівні міждержавних відносин та взаємодії між різними націями. Ці конфлікти мають регіональний геополітичний вимір і можуть виникати навіть між країнами, що підтримують офіційно дружні відносини та мають спільні економічні інтереси. Прикладами можуть слугувати інформаційні кампанії, спрямовані на формування певного іміджу країни на міжнародній арені або на дискредитацію політичних опонентів на міждержавному рівні [102, С. 145-160].

Міжгруповий простір інформаційних конфліктів охоплює соціальні, етнічні, релігійні та професійні протистояння, що мають внутрішньополітичне забарвлення. Такі конфлікти зазвичай виникають у межах однієї держави внаслідок політичних, економічних або соціальних криз, коли інтереси різних соціальних груп вступають у протиріччя. Інформаційні кампанії в цьому просторі спрямовані на мобілізацію прихильників, дискредитацію опонентів та формування громадської думки на користь певної групи [69, С. 80-95].

Міжособистісний простір інформаційних конфліктів включає зіткнення, що відбуваються між окремими індивідами, які є представниками певних соціальних груп. Конфлікти в цій площині виникають через розбіжності у поглядах, цінностях або інтересах. У контексті мережевих війн, цей рівень є важливим, оскільки саме через міжособистісні комунікації поширюються інформаційні впливи та формуються громадські настрої [101, С. 25-40].

Внутрішньо-особистісний простір інформаційних конфліктів відображає внутрішні ідеологічні суперечності в психіці людини, відомі як когнітивний дисонанс. Це явище є результатом інтенсивних інформаційних атак, спрямованих на руйнування усталених світоглядних систем, морально-етичних норм, політичних та економічних переконань індивіда [21, С. 27-42].

Ключовими елементами для розуміння сучасних мережевих інформаційних протистоянь є поняття інформації та комунікації. Інформація визначається як

сукупність відомостей або даних про навколишній світ, а комунікація – як процес передачі або обміну цією інформацією. Будь-яке інформаційне протистояння ґрунтується на інформаційному процесі, що включає створення, накопичення, зберігання, пошук та розповсюдження інформації певної тематики. Історичний розвиток технологій безпосередньо впливав на особливості проведення інформаційних протистоянь у різні епохи.

Основні відмінності інформаційних процесів у різні історичні періоди залежали від технологій створення інформації, методів її накопичення та зберігання, носіїв (матеріальних чи нематеріальних) та суб'єктів, які її генерували. Кожен значний технологічний прорив у цій сфері призводив або до інформаційного вибуху – різкого збільшення обсягу та швидкості поширення інформації, або до інформаційної революції – якісної зміни методів роботи з інформацією. Прикладами інформаційних революцій є поява мовлення, писемності та комп'ютерної техніки. Інформаційні вибухи включають винайдення абеткового письма, друкарства та Інтернету [72, С. 15-30].

Важливим аспектом аналізу сфер протистояння в мережевих війнах є розуміння неоднорідності та ієрархічності інформаційного простору. Будь-які інформаційні процеси розгортаються в певних вимірах, які узагальнено називають інформаційним полем. Це поле можна визначити як соціальний або географічний простір, де між учасниками (суб'єктами) відбувається типовий обмін інформацією (об'єктом комунікації) [114, С. 35-50]. Основними елементами інформаційного поля є його суб'єкти — учасники комунікації, такі як окремі особи, соціальні групи та організації (наприклад, ЗМІ, громадські, державні чи комерційні структури). Іншою ключовою складовою є об'єкти інформаційних процесів — тобто сама інформація або ті, хто її сприймає під час комунікації. Взаємодія між цими суб'єктами та об'єктами відбувається за допомогою лінійних або діалогових моделей соціальних комунікацій. У комунікації, в свою чергу, можна виділити дві основні моделі: лінійна модель — це одностороння передача інформації (відправник надсилає повідомлення отримувачу без очікування зворотного зв'язку); діалогова модель, навпаки, передбачає взаємний обмін інформацією, де кожен учасник може бути як відправником, так і отримувачем.

Сучасна інформаційна війна розгортається переважно в політичній, дипломатичній, військовій та фінансово-економічній сферах. Головна мета таких інформаційних протистоянь — завдати шкоди противнику та забезпечити перевагу для сторони, що здійснює вплив [97, С. 84-99].

Теорія мережевих війн розглядає чотири основні сфери людської діяльності як театри воєнних дій: фізичну, інформаційну, когнітивну та соціальну. Ефективність мережевих війн досягається завдяки синергії дій у всіх цих сферах [38, С. 45-60]. Фізична сфера охоплює традиційні аспекти війни, такі як бойові дії на суші, в морі, повітрі та космосі, а також фізичну інфраструктуру комунікаційних мереж. Інформаційна сфера є середовищем створення, обробки та розповсюдження інформації, а також функціонування систем її передачі. Когнітивна сфера охоплює свідомість індивідів та колективні знання, включаючи доктрини, тактику та процедури. Соціальна сфера є полем взаємодії між людьми, де важливу роль відіграють культурні, релігійні цінності, психологічні установки та соціальні ієрархії.

Сучасні війни інформаційної епохи ґрунтуються на інтеграції дій у всіх цих сферах, формуючи складну мережу впливу. Мережеві війни ведуться одночасно проти всіх і у всіх вимірах – соціокультурному, когнітивному, інформаційному та фізичному. За своєю суттю, це війни психологічні, когнітивні та культурні, спрямовані на зміну світогляду та системи цінностей противника. Розробники теорії мережевих війн фактично ототожнюють трансляцію власного “культурного коду” та національної системи цінностей з сутністю війни. Це фундаментальна зміна світоглядної парадигми, де війна зі зброєю трансформується у війну ідей, понять.

Популяризація власного способу життя, нав’язування певних думок та системи цінностей, розробка та впровадження шкідливих для противника ідеологічних концепцій, управління протестними та релігійними рухами, створення “п’ятих колон”, маніпуляція опозицією, підтримка дисидентів та політичні вбивства поступово трансформуються в новітні форми ведення війни, що відповідають рівню розвитку інформаційного суспільства та потребують нових підходів до забезпечення національної безпеки [46, С. 210-225].

Висновки до розділу 1

Проведений у першому розділі аналіз мережевих війн як нового типу сучасних воєнних дій дозволив сформувати базове розуміння цього складного та багатогранного феномену. Розгляд трансформації способів і методів ведення воєн показав, як розвиток технологій, особливо інформаційно-комунікаційних, призвів до якісних змін у характері збройних конфліктів, зумовивши появу нових форм протистояння.

Аналіз суті поняття “мережа” та формування мережевого суспільства виявив ключові характеристики мережевих структур – децентралізацію, гнучкість, взаємозв’язок елементів – та їхній вплив на соціально-політичні процеси, зокрема на сферу безпеки та оборони. Стало очевидним, що принципи мережевої організації проникають у різні аспекти суспільного життя, включаючи військову справу.

Розгляд мережевої війни, її сутності, ознак та особливостей прояв дозволив визначити її як конфлікт, що розгортається у взаємодії кібернетичного, інформаційного та фізичного просторів, характеризується активною участю недержавних акторів, розмиттям меж між агресором та жертвою, а також використанням мережевих технологій для досягнення стратегічних цілей. Було виокремлено ключові ознаки, що відрізняють мережеві війни від традиційних збройних конфліктів.

Аналіз концепції “мережецентричної війни” (війни шостого покоління) розкрив її як теоретичну основу для розуміння воєн, де інформаційна перевага є ключовим фактором досягнення перемоги. Було розглянуто основні принципи такого формату ведення війни та її вплив на розвиток військової думки та практику будівництва збройних сил.

Розгляд сфер протистояння та театрів мережевих воєн показав, що вони охоплюють не лише традиційні географічні простори, але й кіберпростір та інформаційний простір, які стають ключовими аренами боротьби за вплив та контроль. Було визначено їхню сутність як нового типу воєнних дій, зумовленого розвитком мережевого суспільства та інформаційних технологій. Розглянуто ключові концепції, ознаки та сфери протистояння, що є необхідним підґрунтям для аналізу конкретних видів та інструментів мережевих війн у наступних розділах.

РОЗДІЛ 2
ОПЕРАЦІЇ БАЗОВИХ ЕФЕКТІВ

2.1 Концептуальні засади операцій базових ефектів

Концепція операцій базових ефектів (ОБЕ) являє собою відносно нову парадигму у військовій справі, яка набула значної актуальності наприкінці XX – початку XXI століття. Її сутність полягає у зміщенні акценту з фізичного знищення сил противника на досягнення бажаних стратегічних, оперативних та тактичних ефектів шляхом скоординованого застосування всіх доступних інструментів сили держави [127, С. 15]. ОБЕ передбачає глибоке розуміння складної системи противника, визначення ключових вузлів та зав'язків, вплив на які призведе до каскаду бажаних наслідків, мінімізуючи при цьому власні втрати та побічну шкоду [65, С. 28].

Історично, військова думка еволюціонувала від стратегій прямого зіткнення та виснаження до більш витончених підходів, орієнтованих на маневр та психологічний вплив. Поява високоточної зброї, розвиток інформаційних технологій та усвідомлення складності сучасних конфліктів стали каталізаторами формування концепції операцій базових ефектів. Військові теоретики та практики усвідомили, що просте знищення військової сили противника не завжди призводить до досягнення політичних цілей, а часто супроводжується значними гуманітарними та економічними наслідками [111, С. 45].

Одним із важливих етапів розвитку концепції ОБЕ стало застосування авіації під час операції "Буря в пустелі" у 1991 році, де стратегічні бомбардування були спрямовані не лише на військові об'єкти, але й на інфраструктуру, що підтримувала режим Саддама Хусейна, з метою підірвати його політичну волю до опору [14, С. 62]. Подальший розвиток інформаційних технологій та теорії системного аналізу сприяв формалізації концепції ОБЕ як комплексного підходу до планування та ведення бойових дій.

В Україні концепція операцій базових ефектів почала активно досліджуватися та впроваджуватися у військову практику в контексті реформування Збройних Сил України та адаптації до сучасних гібридних загроз [71, С. 10]. Розуміння необхідності асиметричної відповіді на дії противника, використання не лише військових, але й політичних, економічних, інформаційних та інших інструментів впливу зумовило зростання інтересу до принципів ОБЕ.

Операції базових ефектів базуються на низці ключових принципів, які визначають їхню сутність та особливості застосування. До основних з них належать:

- Системний підхід: Розгляд противника як складної системи взаємопов’язаних елементів, де вплив на один елемент може призвести до каскаду наслідків в інших частинах системи. Це вимагає глибокого аналізу вразливостей та сильних сторін противника, розуміння його функціонування та прийняття рішень.
- Орієнтація на ефекти: Фокус на досягненні конкретних бажаних ефектів, які безпосередньо сприяють досягненню поставлених цілей операції. Ці ефекти можуть бути як фізичними (наприклад, руйнування об’єкта), так і психологічними (наприклад, деморалізація особового складу противника) [48, С. 91].
- Комплексне застосування сил та засобів: Інтеграція зусиль усіх доступних компонентів військової та невійськової сили держави для досягнення синергетичного ефекту. Це передбачає тісну координацію дій між різними видами збройних сил, спеціальними службами, дипломатичними відомствами, органами державної влади та іншими суб’єктами.
- Адаптивність та гнучкість: Здатність оперативно реагувати на зміни обстановки, коригувати плани та перерозподіляти зусилля для досягнення бажаних ефектів. Це вимагає від командування високого рівня ситуаційної обізнаності та здатності до швидкого прийняття рішень.

- Мінімізація побічної шкоди: Прагнення до мінімізації негативних наслідків операцій для цивільного населення та інфраструктури, а також до зниження власних втрат. Це вимагає високої точності застосування зброї та ретельного планування операцій з урахуванням гуманітарних аспектів.

Характерними рисами операцій базових ефектів є їхня інтелектуальність, інформаційна насиченість, орієнтованість на запобігання ескалації конфлікту та досягнення політичних цілей з мінімальними втратами. В Україні застосування операцій базових ефектів регулюється низкою нормативних документів, включно із законами, підзаконними актами, а також військовими доктринами та настановами. Ключовим документом, що визначає основи національної безпеки та оборони, є Закон України "Про національну безпеку України". Цей закон закладає основи державної політики у сфері національної безпеки, зокрема військової, і встановлює правові засади для діяльності органів державної влади, військових формувань та правоохоронних органів у цій галузі. Цей закон визначає засади державної політики у сфері національної безпеки, включаючи військову безпеку, та встановлює правові основи діяльності органів державної влади, військових формувань та правоохоронних органів у цій сфері [2].

Військова доктрина України — це стратегічний документ, що керує оборонним плануванням країни. Вона окреслює ключові принципи та напрями військової політики, стратегію воєнної безпеки, а також форми й способи застосування Збройних Сил України та інших військових формувань. Хоча сама концепція "операцій базових ефектів" прямо не згадана в доктрині, її основні принципи — такі як комплексне використання сил і засобів, орієнтація на стратегічні цілі та мінімізація супутніх втрат — відображені в її положеннях.

Крім того, конкретні аспекти застосування операцій базових ефектів деталізовані у відомчих нормативно-правових актах Міністерства оборони України, Генерального штабу Збройних Сил України та інших військових формувань. Ці документи регламентують планування, підготовку та ведення бойових дій, використання різних видів озброєння та військової техніки, а також координацію між підрозділами та відомствами. Важливим аспектом є також

адаптація міжнародного досвіду застосування концепції ОБЕ та його імплементація у вітчизняну військову практику з урахуванням особливостей геополітичної ситуації та наявних ресурсів.

2.2. Інструменти реалізації операцій базових ефектів

Ефективна реалізація операцій базових ефектів (ОБЕ) вимагає комплексного та скоординованого застосування різноманітних інструментів впливу на противника та його оточення. Ці інструменти можуть варіюватися від традиційних військових засобів до некінетичних методів, спрямованих на інформаційну, економічну, політичну та соціальну сфери. Ключовим аспектом є їхнє комбіноване застосування для досягнення синергетичного ефекту, коли сукупний вплив перевищує просту суму окремих дій [52, С. 112].

Інформаційна кампанія є одним із ключових інструментів реалізації ОБЕ, спрямованим на формування бажаної громадської думки, вплив на прийняття рішень противником та його населенням, а також на забезпечення підтримки власних дій [105, С. 55]. Вона включає в себе поширення інформації через різноманітні канали комунікації, такі як засоби масової інформації, соціальні мережі, інтернет-платформи, а також проведення публічних заходів та спеціальних інформаційних операцій.

Ефективна інформаційна кампанія повинна бути стратегічно спланованою, цілеспрямованою та адаптованою до особливостей цільової аудиторії. Вона має бути узгоджена з іншими інструментами впливу та спрямована на досягнення конкретних інформаційних ефектів, таких як підрив морального духу противника, дискредитація його керівництва, формування позитивного іміджу власних сил та створення сприятливих умов для проведення інших операцій [93, С. 78]. В умовах сучасних гібридних конфліктів інформаційна кампанія набуває особливого значення, оскільки дозволяє впливати на противника без прямого військового зіткнення, використовуючи його інформаційну вразливість та маніпулюючи суспільною думкою [31, С. 93].

Економічні санкції являють собою потужний інструмент невійськового впливу, який може бути використаний в рамках ОБЕ для підриву економічної основи противника, обмеження його ресурсів та створення внутрішнього соціально-економічного напруження, що зрештою може призвести до зміни його поведінки або політичного курсу [125, С. 130]. Санкції можуть включати в себе торговельні обмеження, фінансові блокади, заморожування активів, ембарго на постачання певних видів товарів та технологій, а також інші заходи, спрямовані на обмеження економічної діяльності окремих осіб, компаній або цілих секторів економіки держави-противника.

Ефективність економічних санкцій залежить від їхньої цілеспрямованості, масштабності, тривалості та координованості з діями інших держав та міжнародних організацій. Важливим аспектом є також прогнозування та мінімізація потенційних негативних наслідків санкцій для власної економіки та населення [134, С. 145]. Закон України “Про санкції” встановлює правові засади для запровадження санкцій. Їхня мета — захист національних інтересів, безпеки, суверенітету й територіальної цілісності України, а також боротьба з тероризмом та іншою протиправною діяльністю [6].

Кібератаки стали важливим інструментом реалізації ОБЕ в умовах зростаючої залежності сучасних держав від інформаційних технологій та кіберпростору. Вони можуть бути спрямовані на порушення функціонування критичної інфраструктури противника (енергетичні системи, транспорт, зв’язок, фінансовий сектор), виведення з ладу систем управління та зв’язку, отримання конфіденційної інформації, а також на поширення дезінформації та пропаганди [119, С. 162]. Кібератаки мають ряд переваг, таких як можливість нанесення значної шкоди без фізичного проникнення на територію противника, складність ідентифікації джерела атаки та відносно низька вартість їх проведення. Водночас, вони також несуть певні ризики, пов’язані з можливістю ескалації конфлікту та непередбачуваними наслідками. Забезпечення кібербезпеки власних інформаційних систем та розвиток потенціалу для проведення

ефективних кібероперацій є важливими складовими реалізації ОБЕ в сучасних умовах.

Дипломатичні впливи є важливим інструментом реалізації ОБЕ, спрямованим на досягнення політичних цілей шляхом переговорів, укладення угод, використання міжнародних організацій та інших дипломатичних засобів. Дипломатія може використовуватися як для запобігання конфліктам, так і для їхнього врегулювання на різних етапах, а також для створення сприятливого міжнародного середовища для реалізації інших інструментів впливу. В рамках ОБЕ дипломатичні зусилля можуть бути спрямовані на ізоляцію противника на міжнародній арені, формування антикризових коаліцій, отримання підтримки міжнародних організацій, а також на створення умов для політичного врегулювання конфлікту на вигідних умовах. Ефективна дипломатія вимагає глибокого розуміння інтересів та позицій інших держав, вміння вести переговори та знаходити компроміси, а також координації зусиль з іншими інструментами впливу.

Спеціальні операції являють собою комплекс скоординованих дій, що проводяться спеціально підготовленими силами та засобами для досягнення конкретних стратегічних, оперативних або тактичних цілей. В рамках ОБЕ спеціальні операції можуть використовуватися для виконання широкого спектру завдань, таких як розвідка, диверсії, звільнення заручників, ліквідація ключових осіб противника, підтримка дружніх сил та проведення психологічних операцій [67, С. 195]. Характерними рисами спеціальних операцій є їхня точність, швидкість, скритність та високий рівень ризику. Успішне проведення спеціальних операцій може мати значний вплив на хід конфлікту, створюючи бажані ефекти та сприяючи досягненню поставлених цілей.

Найбільшої ефективності в рамках ОБЕ досягається шляхом комбінованого та скоординованого застосування всіх доступних інструментів впливу. Синергетичний ефект від одночасного або послідовного застосування інформаційних кампаній, економічних санкцій, кібератак, дипломатичних зусиль та спеціальних операцій може значно перевищувати суму ефектів від

їхнього окремого використання. Наприклад, інформаційна кампанія може підготувати громадську думку до введення економічних санкцій, кібератака може порушити систему управління противника перед проведенням спеціальної операції, а дипломатичні зусилля можуть забезпечити міжнародну підтримку для реалізації інших інструментів впливу. Успішне комбіноване застосування інструментів вимагає ретельного планування, чіткої координації між різними відомствами та структурами, а також глибокого розуміння складної системи противника та його слабких сторін.

2.3. Механізми оцінки ефективності операцій базових ефектів

Ефективне застосування концепції операцій базових ефектів (ОБЕ) неможливе без розробленої системи оцінки досягнутих результатів. Оцінка ефективності ОБЕ є складним та багатогранним процесом, що включає в себе визначення ступеня досягнення бажаних ефектів, аналіз впливу застосованих інструментів, виявлення сильних та слабких сторін стратегії, а також забезпечення зворотного зв’язку для її подальшої корекції [44, С. 215].

Оцінка досягнутого ефекту в ОБЕ вимагає застосування різноманітних методів, що дозволяють отримати об’єктивну картину змін у стані противника та його ключових вузлів та зав’язків. До основних методів належать:

- Кількісний аналіз: Використання статистичних даних та метрик для вимірювання змін у ключових показниках, таких як рівень бойової готовності противника, економічні індикатори, рівень підтримки населенням політичного режиму, інтенсивність інформаційних атак тощо [121, С. 88]. Цей метод дозволяє отримати чіткі та порівняльні дані, але може бути обмеженим у відображенні якісних змін.
- Якісний аналіз: Оцінка змін у поведінці, мотивації, прийнятті рішень противником, а також у громадській думці та політичному кліматі. Цей метод включає в себе аналіз змісту повідомлень у засобах масової інформації, соціальних мережах, експертних оцінок, результатів соціологічних опитувань та

інтерв’ю [98, С. 114]. Якісний аналіз дозволяє глибше зрозуміти причини та наслідки змін, але є більш суб’єктивним.

- Системний аналіз: Оцінка впливу застосованих інструментів на всю систему противника, виявлення каскадних ефектів та непрямих наслідків. Цей метод передбачає використання моделей та симуляцій для прогнозування та аналізу складних взаємозв’язків між різними елементами системи [12, С. 118].
- Експертні оцінки: Залучення кваліфікованих фахівців з різних галузей (військових, економістів, політологів, психологів, фахівців з інформаційної безпеки) для оцінки досягнутих ефектів на основі їхніх знань та досвіду. Експертні оцінки можуть бути особливо цінними у випадках, коли кількісні дані обмежені або недоступні. Комбіноване застосування цих методів дозволяє отримати більш повну та об’єктивну оцінку ефективності ОБЕ.

Однією з ключових особливостей ОБЕ є орієнтація на постійний зворотний зв’язок та адаптивність. Результати оцінки ефективності застосованих інструментів та досягнутих ефектів повинні використовуватися для оперативного коригування стратегії та планів. Зворотний зв’язок (фідбек) — це процес, під час якого збирають та аналізують дані про досягнуті результати, виявляють розбіжності з очікуваними показниками та на основі цього ухвалюють рішення щодо коригування подальших дій. [136, С. 135].

Ефективна система фідбеку повинна бути оперативною, всебічною та об’єктивною. Вона має забезпечувати надходження інформації про результати застосування всіх інструментів впливу, а також про реакцію противника та його оточення на ці дії. На основі отриманої інформації командування може приймати рішення щодо зміни цілей, перерозподілу зусиль, застосування інших інструментів або коригування методів їхнього використання. Принципи організації процесу зворотного зв’язку у Збройних Силах України визначені у відповідних настановах та керівних документах, що регламентують процес управління військами та планування операцій.

Для підвищення ефективності оцінки та прогнозування наслідків застосування ОБЕ важливе значення має використання сучасних аналітичних

інструментів та даних розвідки. Аналітика дозволяє обробляти великі обсяги інформації, виявляти закономірності та тенденції, а також будувати моделі для прогнозування потенційних наслідків застосування різних інструментів впливу [108, С. 152]. Дані розвідки, отримані з різних джерел, є критично важливими для розуміння стану противника, його вразливостей, сильних сторін та можливих реакцій на власні дії. Вони використовуються для формування інформаційної бази для аналізу та моделювання, а також для верифікації результатів оцінки ефективності.

Закон України “Про розвідку” [5] визначає правові основи організації та діяльності розвідувальних органів України, їхні завдання, функції та повноваження, а також порядок отримання, обробки та використання розвідувальної інформації. Сучасні інформаційні технології та програмне забезпечення дозволяють створювати комплексні моделі, що імітують поведінку складних систем, таких як держава-противник або регіон конфлікту. Ці моделі можуть використовуватися для оцінки потенційного впливу різних сценаріїв застосування ОБЕ та для прийняття обґрунтованих рішень. Один з перспективних напрямів — це використання штучного інтелекту та машинного навчання. Ці технології дозволяють аналізувати великі обсяги даних і виявляти неочевидні взаємозв’язки, що значно підвищує точність прогнозування наслідків від застосування Операцій Базових Ефектів (ОБЕ) [73, С. 168].

2.4. Приклади застосування операцій базових ефектів у сучасних конфліктах

Концепція операцій базових ефектів (ОБЕ) знайшла своє відображення у багатьох сучасних конфліктах, де сторони прагнули досягти стратегічних цілей не лише шляхом прямого військового зіткнення, а й через асиметричні впливи та нелінійні результати. Аналіз окремих операцій дозволяє краще зрозуміти практичне застосування принципів ОБЕ, його потенційні переваги та можливі обмеження.

Операція “Іракська свобода” (2003) є одним із прикладів застосування елементів концепції ОБЕ, хоча її кінцеві результати викликають багато дискусій. Основною метою операції було повалення режиму Саддама Хусейна та встановлення в Іраку демократичного уряду. Стратегія коаліційних сил включала не лише швидке військове вторгнення та захоплення ключових територій, але й інформаційні операції, спрямовані на деморалізацію іракської армії та населення, а також на формування позитивного сприйняття дій коаліції [34, С. 235].

Застосовувалися також економічні інструменти впливу, зокрема блокування фінансових активів іракського режиму. Однак, незважаючи на швидке повалення Хусейна, подальша окупація та спроби побудови нової політичної системи зіткнулися зі значними труднощами, включаючи зростання повстанського руху та міжконфесійну ворожнечу. Це свідчить про складність прогнозування та контролю довгострокових ефектів навіть при успішному досягненні початкових цілей [27, С. 250]. Аналіз операції в Іраку підкреслює важливість глибокого розуміння соціокультурного контексту та потенційних нелінійних наслідків військового втручання.

Конфлікт між Росією та Україною, що розпочався у 2014 році, є яскравим прикладом застосування Росією елементів ОБЕ, зокрема в рамках концепції “гібридної війни”. Російська стратегія включає комбіноване використання військових, політичних, економічних, інформаційних та кібернетичних інструментів впливу для досягнення своїх геополітичних цілей [149, С. 18].

Інформаційна кампанія відіграє ключову роль у російській стратегії, спрямованій на дезінформацію українського та міжнародного співтовариства, підрив довіри до української влади, розпалювання сепаратистських настроїв та виправдання власної агресії [56, С. 32]. Економічні санкції та енергетичний шантаж також використовуються як інструменти тиску на Україну. Кібератаки спрямовані на порушення функціонування критичної інфраструктури та державних установ.

Застосування нерегулярних військових формувань, підтримка сепаратистських рухів та проведення спеціальних операцій є військовою складовою гібридної стратегії. Анексія Криму та підтримка збройного конфлікту на сході України демонстрували прагнення Росії досягти своїх цілей шляхом асиметричних дій,

уникаючи відкритого широкомасштабного військового вторгнення на початковому етапі [81, С. 47]. Аналіз дій Росії проти України підкреслює важливість протидії інформаційній агресії та кіберзагрозам у контексті ОБЕ.

Протистояння між Ізраїлем та Іраном відбувається переважно в “сірій зоні”, включаючи кібератаки, диверсії, точкові ліквідації та підтримку опозиційних сил, спрямовані на стримування іранської ядерної програми та регіональної експансії [153]. Ізраїль використовує асиметричні методи, намагаючись завдати відчутної шкоди іранським інтересам, не провокуючи при цьому повномасштабний конфлікт. Прикладом можуть слугувати кібератаки на іранські ядерні об’єкти (наприклад, вірус Stuxnet), які мали на меті затримати розвиток ядерної програми без прямого військового удару. Також повідомлялося про диверсії на військових та промислових об’єктах в Ірані, приписувані Ізраїлю. Ці дії спрямовані на створення ефекту стримування та затримки, демонструючи рішучість Ізраїлю протидіяти іранським амбіціям [26, С. 81-94].

Періодично Ізраїль завдає також кінетичних ударів по цілях, пов’язаних з іранською військовою інфраструктурою або проксі-силами в регіоні. Ці дії є більш прямолінійними, але також спрямовані на досягнення конкретних ефектів, таких як зниження військового потенціалу противника або запобігання передачі зброї. Аналіз дій Ізраїлю проти Ірану демонструє застосування ОБЕ в умовах тривалого стратегічного протистояння без оголошеної війни.

Операції проти терористичних організацій також часто включають елементи ОБЕ. Замість традиційних військових кампаній, спрямованих на захоплення територій, зусилля зосереджуються на підриві здатності терористичних груп до діяльності шляхом ліквідації їхніх лідерів, руйнування фінансових мереж, протидії пропаганді та вербуванню нових членів [129, С. 98]. Інформаційні кампанії спрямовані на дискредитацію ідеології терористів та руйнування їхньої підтримки серед населення. Економічні санкції можуть бути спрямовані проти осіб та організацій, що фінансують терористичну діяльність. Спеціальні операції використовуються для точкових ударів по ключових фігурах та об’єктах інфраструктури терористів. Прикладом може слугувати міжнародна коаліція проти ІДІЛ, де поряд з військовими ударами здійснювалися масштабні інформаційні

операції в соціальних мережах для протидії пропаганді терористів та залучення нових членів [24, С. 114].

Застосування концепції ОБЕ в сучасних конфліктах порушує важливі питання щодо дотримання норм міжнародного гуманітарного права. Принципи розрізнення, пропорційності та запобігання зайвим стражданням цивільного населення мають бути враховані при плануванні та проведенні операцій, особливо при застосуванні некінетичних інструментів впливу, таких як кібератаки та інформаційні операції. Необхідно чітко визначати законні військові цілі та вживати всіх можливих запобіжних заходів для мінімізації супутньої шкоди.

Правові аспекти застосування Операцій Базових Ефектів (ОБЕ) потребують подальшого вивчення та розробки відповідних нормативних рамок, як на національному, так і на міжнародному рівнях. У цьому контексті, Закон України “Про боротьбу з тероризмом” є важливим, оскільки він визначає правові та організаційні основи протидії тероризму в Україні, що охоплює й аспекти застосування елементів ОБЕ [7]. Аналіз наведених прикладів демонструє, що концепція ОБЕ знаходить все ширше застосування в сучасних конфліктах. Сторони конфлікту прагнуть досягти своїх цілей не лише шляхом прямого військового зіткнення, а й через комбіноване використання різноманітних інструментів впливу, спрямованих на створення асиметричних ефектів та досягнення нелінійних результатів. Успішне застосування ОБЕ вимагає глибокого розуміння противника, ретельного планування, скоординованого застосування всіх доступних інструментів, ефективної системи оцінки та корекції стратегії, а також неухильного дотримання норм міжнародного гуманітарного права.

Висновки до розділу 2

Операції базових ефектів (ОБЕ) становлять собою фундаментальний зсув у підходах до воєнного планування та застосування сили в умовах сучасної війни. Замість традиційного зосередження на фізичному знищенні сил противника, ОБЕ спрямовують зусилля на досягнення системних ефектів, що спричиняють зміну поведінки, послаблення політичної волі, дестабілізацію ключових вузлів

управління та створення стратегічної переваги без масштабного збройного зіткнення. Цей підхід демонструє адаптацію до нових умов конфліктів, де міць вимірюється не лише кількістю техніки чи військ, а й здатністю змінювати хід подій через точкові, але глибоко вивірені впливи.

Концептуальні засади ОБЕ підкреслюють необхідність системного аналізу противника як цілісної структури, в якій кожен компонент — політичний, економічний, інформаційний чи соціальний — може виступати як критичний вузол, уразливість якого призведе до каскадного ефекту. Ціллю операцій базових ефектів є не стільки перемога в бойових діях, скільки досягнення політичних і стратегічних результатів через модифікацію контексту дій противника — його сприйняття, рішень і здатності діяти.

Реалізація ОБЕ ґрунтується на використанні широкого арсеналу інструментів: інформаційних кампаній, спрямованих на дезорієнтацію або зміну громадської думки; економічних санкцій як важеля тиску; кібератак, що виводять з ладу критичну інфраструктуру; дипломатичних механізмів, які ізолюють супротивника на міжнародній арені; а також спеціальних операцій, здатних завдати удару по об’єктах стратегічного значення. Ключовою особливістю операцій базових ефектів є динамічний підхід до оцінки їх ефективності. В умовах швидкоплинної інформаційної та бойової обстановки, командири та аналітичні центри повинні оперативно аналізувати результати, зворотний зв’язок, поведінкові зміни противника та інші індикатори для корекції дій. Це вимагає залучення сучасних аналітичних інструментів, даних розвідки, штучного інтелекту та комп’ютерного моделювання, що дозволяє прогнозувати ймовірні наслідки і швидко реагувати на зміни ситуації.

Аналіз сучасних прикладів застосування ОБЕ — зокрема, операцій США під час війни в Іраку (2003), дій Росії проти України (з 2014 року) та активності Ізраїлю щодо Ірану — наочно демонструє, що асиметричні дії, реалізовані в межах ОБЕ, можуть мати значно більший стратегічний ефект, ніж традиційні бойові дії. Наприклад, атаки на енергетичну інфраструктуру, кампанії з дезінформації чи цілеспрямовані санкції створюють нелінійні результати, які

послаблюють противника морально, економічно та політично, змушуючи його до зміни поведінки.

Отже, операції базових ефектів виступають ефективним, гнучким та ресурсозберігаючим інструментом реалізації національної безпекової стратегії. Їх використання дозволяє державам досягати стратегічних цілей, уникаючи затяжних і виснажливих збройних конфліктів. Для України, що перебуває в умовах гібридної війни, засвоєння принципів ОБЕ та розбудова відповідних спроможностей є не лише актуальним, але й життєво необхідним завданням у забезпеченні стійкості та перемоги в багаторівневому конфлікті.

РОЗДІЛ 3
ІНФОРМАЦІЙНА ВІЙНА:
ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

3.1. Інформаційна війна як феномен цифрового суспільства

Епоха цифрової трансформації, що характеризується повсюдним проникненням інформаційно-комунікаційних технологій у всі сфери суспільного життя, породила нові форми конфліктів та протистоянь. Одним з ключових феноменів цього нового середовища є інформаційна війна, яка стає визначальною складовою сучасних геополітичних процесів та міждержавних відносин. Інформаційна війна в умовах цифрового суспільства являє собою комплекс цілеспрямованих дій, що використовують інформацію та цифрові технології для впливу на свідомість, поведінку, ціннісні орієнтації та прийняття рішень окремих осіб, соціальних груп, організацій та держав з метою досягнення стратегічних переваг у політичній, економічній, соціальній або військовій сферах [117, С. 28-41].

У сучасній теорії, методології та методиці інформаційних війн центральне місце займає поняття гібридної війни. Вона визначається як протистояння, що інтегрує різноманітні інструменти політичного, економічного, військового та ідеологічного характеру. Іноді для опису цього явища використовують термін асиметрична війна, який підкреслює її нетрадиційний, специфічний та креативний характер. Такий конфлікт ведеться за допомогою нестандартних, комбінованих стратегій і тактик. Під час гібридної війни ресурси та характер дій сторін-противників суттєво відрізняються. Головна мета — за рахунок певної концентрації зусиль компенсувати недостатність ресурсів однієї зі сторін або отримати суттєву перевагу на конкретному напрямку в рамках конфлікту [96, С. 98].

Інформаційні війни – це контентні війни, спрямовані на зміну свідомості мас, груп та індивідів, нав’язування ворогу своєї волі та перепрограмування його

поведінки. Під час інформаційної війни відбувається боротьба за свідомість, цінності, переконання, моделі поведінки тощо. Вони виникли тисячі років тому, але Інтернет дав їм новий рівень інтенсивності, масштабу та ефективності. Об'єктами впливу інформаційних війн є різноманітні суб'єкти – від малих груп до конкретних народів і націй до населення держав. Засобами впливу є спеціально підготовлені смислові повідомлення у вигляді текстів, відео та аудіо матеріалів.

У цифровому суспільстві інформація набуває особливої цінності та стає ключовим інструментом впливу. Безпрецедентна швидкість поширення інформації через інтернет, соціальні мережі, цифрові медіа та мобільні комунікації створює нові можливості для проведення масштабних інформаційних кампаній. Ці кампанії можуть бути спрямовані на формування певного образу подій, дискредитацію політичних опонентів, маніпулювання громадською думкою, розпалювання соціальних конфліктів, підрив довіри до державних інститутів та поширення дезінформації [92, С. 63-76].

Інформаційна війна як феномен цифрового суспільства має ряд специфічних характеристик. По-перше, її транскордонний характер. Цифрові технології стирають географічні межі, дозволяючи здійснювати інформаційний вплив на аудиторії, що знаходяться на значній відстані від джерела впливу. По-друге, висока швидкість та великий обсяг поширення інформації. Цифрові канали комунікації забезпечують практично миттєве розповсюдження інформаційних повідомлень, що вимагає швидкої реакції та ефективних механізмів протидії. По-третє, складність верифікації інформації. У цифровому просторі циркулює величезна кількість інформації різного походження, що ускладнює відділення достовірних даних від фейків та маніпуляцій [106, С. 91-104]. По-четверте, активна роль недержавних акторів. Поряд з державами, суб'єктами інформаційної війни в цифровому суспільстві можуть виступати приватні компанії, політичні партії, громадські організації, хакерські групи та окремі особи, що володіють необхідними цифровими компетенціями та ресурсами. По-п'яте, гібридність. Інформаційна війна в цифровому суспільстві рідко існує

ізольовано, часто переплітаючись з кібератаками, економічним тиском, політичним втручанням та іншими формами впливу, утворюючи складні гібридні загрози [138, С. 47-60].

Володимир Алещенко визначає інформаційно-психологічний вплив як спрямований вплив на свідомість за допомогою інформаційних, психологічних чи інших засобів, що змінюють психіку людини, її погляди, думки, стосунки, цінності, мотиви та стереотипи з метою вплинути на її поведінку. Основними завданнями такого впливу є завдання шкоди інформаційно-технічним системам держави та її збройних сил (наприклад, ускладнення роботи або виведення з ладу озброєння і бойової техніки), а також дезінформація, дезорганізація та деморалізація керівництва і населення противника. Кінцева мета таких дій – досягнення реакції або зміни поведінки людини, що відповідає певним цілям психологічного впливу. [36, С. 6-10].

У сучасному мережевому суспільстві змінюється спосіб, у який ми сприймаємо світ і самих себе. За даними когнітивної психології, кожна людина сприймає зовнішній світ крізь призму власних переконань та досвіду. Фахівці, що займаються розробкою сучасних концепцій “нової теорії війни”, стверджують, що технологічні досягнення впливають на найглибші рівні людської свідомості, трансформуючи наш внутрішній світ. Сучасні мережеві конфлікти демонструють, що інформаційний образ стає важливішим за об’єктивні факти – реальність набуває значення лише тоді, коли вона потрапляє в інформаційний простір. Це підкреслює важливість контролю над інформаційним полем: той, хто володіє цією владою, має вплив на все. Сучасний інформаційний супровід війни більше схожий на саму сутність конфлікту, ніж на допоміжний елемент традиційної пропаганди. [122, С. 37-41.].

У цих умовах постає проблема формування захисної стратегії проти інформаційно-психологічних атак, організованих приватними військовими компаніями та неурядовими суб’єктами. Це створює труднощі не лише у виявленні впливу таких атак під час мережевих воєн, а й у розробці стійких стратегій для їх запобігання. ризикам і загрозам [36, С. 6-10]..

Основними інструментами ведення інформаційної війни в цифровому суспільстві є: Соціальні медіаплатформи: використовуються для поширення інформаційних наративів, організації онлайн-спільнот, проведення цільових рекламних кампаній та здійснення психологічного впливу на користувачів [25, С. 72-85]. Інтернет-медіа та блогосфера: слугують каналами для публікації матеріалів, формування громадської думки та просування певних ідеологічних поглядів. Месенджери та платформи обміну миттєвими повідомленнями: використовуються для координації дій, поширення чуток та організації закритих груп впливу. Пошукові системи: можуть бути об’єктом маніпуляцій з метою впливу на видачу результатів пошуку та формування певного сприйняття інформації. Технології штучного інтелекту та великих даних: використовуються для аналізу поведінки користувачів, створення персоналізованого контенту та автоматизованого поширення інформаційних повідомлень [159].

Протидія інформаційній війні в цифровому суспільстві є комплексним завданням, що вимагає системного підходу та об’єднання зусиль держави, громадянського суспільства та міжнародної спільноти. Ключовими напрямками протидії є:

- Підвищення рівня медіаграмотності та критичного мислення громадян: навчання навичкам аналізу інформації, розпізнавання маніпулятивних технік та перевірки достовірності джерел [154].
- Забезпечення прозорості та відповідальності цифрових платформ: встановлення правил щодо модерації контенту, боротьби з фейковими акаунтами та розкриття джерел політичної реклами.
- Підтримка незалежних та об’єктивних медіа: забезпечення плюралізму думок та доступу до якісної журналістики.
- Розвиток національних систем кібербезпеки: захист інформаційної інфраструктури від зовнішніх інформаційних атак та забезпечення стабільного функціонування цифрових комунікацій.

- Активізація міжнародного співробітництва: обмін інформацією, координація дій та розробка спільних стратегій боротьби з транскордонними інформаційними загрозами [156].

Отже, інформаційна війна є визначальним феноменом цифрового суспільства, що використовує його унікальні характеристики та інструменти для досягнення різноманітних стратегічних цілей. Ефективна протидія цьому явищу вимагає комплексного підходу, спрямованого на зміцнення інформаційної стійкості суспільства, підвищення рівня цифрової та медійної грамотності громадян, забезпечення відповідальності цифрових платформ та активну міжнародну співпрацю.

3.2. Стратегії інформаційної війни в окремих країнах

У сучасному геополітичному ландшафті, де інформаційний простір відіграє ключову роль у формуванні міжнародних відносин та національної безпеки, окремі країни розробляють та впроваджують власні стратегії ведення інформаційної війни. Ці стратегії відображають національні інтереси, геополітичні амбіції, рівень розвитку інформаційних технологій та специфіку політичних систем кожної держави. Аналіз стратегій інформаційної війни окремих країн дозволяє виявити загальні тенденції, унікальні підходи та потенційні загрози для міжнародної стабільності [50, С. 58-71].

Теорія мережевих війн передбачає, що дії відбуваються в чотирьох ключових сферах людського життя — фізичній, інформаційній, когнітивній та соціальній. Значні результати досягаються завдяки синергії всіх цих елементів. Фізична сфера. Це традиційна арена бойових дій, де стикаються фізичні сили. Вона охоплює середовища для ведення боїв (на суші, в морі, повітрі, космосі), бойові одиниці та фізичні носії комунікаційних мереж. У епоху інформаційних технологій фізичну площину варто сприймати як складову частину мережевого простору, де основну роль відіграють інші царини. Інформаційна сфера. У цій області формується, обробляється та розподіляється інформація, працюють

системи передачі даних і моделі їх опрацювання. Сфера інформації є пріоритетною, оскільки інтегрує всі рівні ведення боїв і координує їх взаємодію. Когнітивна сфера. Цей сегмент охоплює свідомість бійця, де формується сприйняття, командування, доктрини, тактика, техніка та встановлюються процедури. Саме тут ведуться основні “битви”, адже інформаційний вплив на когнітивну сферу є вирішальним у сучасних конфліктах. Соціальна сфера. Це простір взаємодії людей, де домінують історичні, культурні та релігійні цінності, психологічні установки та етнічні особливості. У соціальній зоні формуються стосунки між громадянами, виникають природні групові ієрархії (лідери, ведені) та встановлюються системи колективних взаємодій [122, С. 39.].

Стратегії інформаційної війни різних країн можуть суттєво відрізнятися залежно від їхніх політичних режимів. Авторитарні держави часто використовують інформаційну війну як інструмент внутрішнього контролю, придушення опозиції та формування лояльного громадської думки. Зовнішньополітично їхні стратегії можуть бути спрямовані на дискредитацію демократичних цінностей, втручання у виборчі процеси інших країн та поширення пропаганди для досягнення власних геополітичних цілей [131, С. 98].

Демократичні країни, у свою чергу, в своїх стратегіях інформаційної війни роблять акцент на захисті власних інформаційних систем, протидії дезінформації, підтримці свободи слова та просуванні демократичних цінностей на міжнародній арені. Вони також можуть використовувати інструменти інформаційного впливу для протидії агресивній пропаганді авторитарних режимів та підтримки демократичних рухів в інших країнах [139, С. 125].

Я приклад, приведемо стратегії інформаційної війни окремих країн:

Російська Федерація є одним з найбільш активних гравців на полі інформаційної війни. Її стратегія характеризується комплексним підходом, що поєднує використання державних медіа (таких як RT та Sputnik), соціальних мереж, бот-ферм, тролінгових армій та кібератак для досягнення політичних цілей як на внутрішній, так і на зовнішній арені. Основні напрямки російської інформаційної війни включають поширення дезінформації, підрив довіри до

західних інститутів, підтримку сепаратистських рухів, втручання у виборчі процеси інших країн та формування позитивного іміджу Росії [133, С. 116-129].

Китайська Народна Республіка також активно розвиває свої можливості у сфері інформаційної війни. Її стратегія зосереджена на внутрішньому контролі інформаційного простору, цензуруванні інтернету та формуванні позитивного іміджу Китаю на міжнародній арені. КНР використовує державні медіа, соціальні мережі та цифрові технології для просування своїх політичних та економічних інтересів, а також для протидії критиці з боку західних країн [29, С. 45-58].

Сполучені Штати Америки розглядають інформаційну війну як важливий елемент національної безпеки. Їхня стратегія включає захист власних інформаційних систем, протидію іноземній пропаганді, підтримку свободи слова та демократичних цінностей у світі. США використовують державні медіа (такі як Voice of America), соціальні мережі та інші цифрові платформи для просування своєї зовнішньої політики та протидії дезінформації з боку противників.

Україна з 2014 року перебуває на передовій боротьби з інформаційною агресією з боку Російської Федерації. Стратегія інформаційної безпеки України спрямована на захист національного інформаційного простору, протидію дезінформації та пропаганді, підвищення рівня медіаграмотності населення та зміцнення кібербезпеки [160].

Аналіз стратегій інформаційної війни окремих країн виявляє ряд спільних рис та тенденцій:

- Використання всього спектру інформаційних інструментів: від традиційних медіа до соціальних мереж та кіберпростору.
- Акцент на формуванні наративів: створення та просування вигідних для себе інтерпретацій подій.
- Застосування технологій штучного інтелекту та автоматизації: використання бот-ферм, автоматизованих систем поширення контенту та аналізу даних.

- Розмивання меж між внутрішньою та зовнішньою інформаційною політикою: інформаційний вплив спрямовується як на власне населення, так і на іноземні аудиторії.
- Постійна адаптація стратегій: швидка еволюція інформаційних технологій вимагає гнучкості та здатності до оперативного реагування на нові виклики.
- Протидія стратегіям інформаційної війни окремих країн вимагає комплексного підходу, що включає:
- Зміцнення національної інформаційної безпеки: захист інформаційної інфраструктури та протидія кібератакам.
- Розвиток критичного мислення та медіаграмотності громадян: навчання навичкам аналізу інформації та розпізнавання маніпуляцій.
- Підтримка незалежних та об’єктивних медіа: забезпечення доступу до достовірної інформації.
- Активна протидія дезінформації: виявлення та спростування фейкових новин та пропагандистських матеріалів.
- Міжнародне співробітництво: обмін інформацією та координація зусиль з іншими країнами для протидії спільним інформаційним загрозам.

Таким чином, стратегії інформаційної війни є важливим інструментом зовнішньої та внутрішньої політики багатьох країн. Їхній аналіз дозволяє краще розуміти сучасні геополітичні процеси та розробляти ефективні механізми протидії інформаційним загрозам. Подальші дослідження у цій сфері є важливими для забезпечення національної та міжнародної безпеки в умовах зростаючої ролі інформаційного простору.

3.3. Інформаційна війна як чинник загрози національній безпеці

У сучасному геополітичному середовищі, що характеризується зростанням міждержавної конкуренції та гібридних конфліктів, інформаційна війна набуває статусу одного з ключових чинників загрози національній безпеці. Цілеспрямований вплив на інформаційний простір держави з боку зовнішніх та внутрішніх акторів може мати далекосяжні негативні наслідки для її суверенітету,

територіальної цілісності, економічної стабільності, соціальної злагоди та обороноздатності. Розуміння сутності, механізмів та наслідків інформаційної війни є критично важливим для розробки ефективних стратегій протидії цим загрозам [99, С. 38-51].

Інформаційна війна, спрямована проти національної безпеки, являє собою комплекс скоординованих дій, що використовують інформацію та комунікаційні технології для підриву основних сфер життєдіяльності держави та суспільства. Її метою може бути дестабілізація політичної ситуації, розпалювання внутрішніх конфліктів, формування негативного іміджу країни на міжнародній арені, підрив довіри громадян до державних інститутів, маніпулювання суспільною свідомістю та створення умов для зовнішнього втручання [83, С. 96].

Загрози національній безпеці, що виникають внаслідок інформаційної війни, є різноманітними та охоплюють різні сфери. У політичній сфері інформаційні кампанії можуть бути використані для дискредитації політичних лідерів, маніпуляцій виборчими процесами, підтримки радикальних рухів, спричинення політичної нестабільності та підриву демократичних інститутів. [151, С. 77-90]. Соціальна сфера: інформаційна війна може призводити до поляризації суспільства, поширення ворожнечі та ненависті між різними соціальними групами, руйнування національної ідентичності та цінностей, а також до масових заворушень та соціальних конфліктів [113, С. 112-125]. Економічна сфера: інформаційні атаки можуть бути спрямовані на підрив довіри до національної валюти та фінансової системи, поширення неправдивої інформації про економічний стан країни, провокування паніки на ринках та завдання значних економічних збитків. Сфера оборони та безпеки: інформаційна війна може включати дезінформацію про діяльність збройних сил, підрив морального духу військовослужбовців, розповсюдження фейкових новин про бойові дії, кібератаки на військові інформаційні системи та пропаганду, спрямовану на деморалізацію населення в умовах конфлікту.

У сучасному цифровому суспільстві інформаційна сфера становить безпосередню загрозу національній безпеці. Це проявляється через систематичне розповсюдження дезінформації, фейкових новин, пропагандистського контенту та

шкідливих матеріалів, а також через кібератаки на державні інформаційні ресурси та ЗМІ. Ефективність інформаційної війни як загрози національній безпеці сучасного цифрового суспільства обумовлена кількома ключовими чинниками [9].

По-перше, це швидке та широке поширення інформації через інтернет та соціальні мережі, що дозволяє миттєво охоплювати величезну аудиторію. По-друге, значну складність становить верифікація інформації та розпізнавання фейків через надмірний обсяг даних та витонченість маніпулятивних технік. По-третє, анонімність та транскордонність кіберпростору ускладнюють ідентифікацію джерел загроз та притягнення винних до відповідальності. Крім того, висока швидкість та низька вартість проведення інформаційних кампаній роблять їх надзвичайно привабливим інструментом для агресорів. Нарешті, можливість цілеспрямованого впливу на окремі групи населення з використанням big data та штучного інтелекту дозволяє персоналізувати інформаційні атаки, роблячи їх максимально ефективними [25, С. 88-101].

Протидія інформаційній війні як загрозі національній безпеці вимагає комплексного підходу, що включає низку взаємопов’язаних заходів. Необхідним є удосконалення законодавчої бази у сфері інформаційної безпеки, що передбачає розробку та впровадження норм, які регулюють діяльність в інформаційному просторі та передбачають відповідальність за поширення дезінформації та пропаганди [8]. Також важливим є зміцнення національної системи кібербезпеки, що охоплює захист критичної інформаційної інфраструктури та протидію кібератакам, спрямованим на порушення функціонування державних інформаційних систем та поширення дезінформації. Ключовим елементом є підвищення рівня медіаграмотності населення через навчання громадян навичкам критичного аналізу інформації, розпізнавання фейків та маніпулятивних технік [154]. Крім того, ефективна протидія передбачає підтримку незалежних та об’єктивних засобів масової інформації, що забезпечує плюралізм думок та доступ до достовірної інформації.

Важливе значення має створення ефективних механізмів виявлення та спростування дезінформації (фактчекінгу), що вимагає оперативного реагування на поширення недостовірних повідомлень. Активізація міжнародного співробітництва

є невід'ємною частиною, що полягає в обміні інформацією та координації зусиль з іншими країнами у сфері протидії інформаційним загрозам. Нарешті, необхідно продовжувати розвиток національних інформаційних ресурсів та контенту, що передбачає створення якісного та достовірного інформаційного продукту, здатного конкурувати з ворожою пропагандою та формувати стійкий національний інформаційний простір.

Інформаційна війна є потужним та багатогранним чинником загрози національній безпеці в сучасному цифровому суспільстві. Ефективна протидія цим загрозам вимагає скоординованих зусиль держави, громадянського суспільства, медіа та міжнародної спільноти, спрямованих на зміцнення інформаційної стійкості країни, підвищення рівня медіаграмотності громадян та розвиток національних інформаційних спроможностей для забезпечення довгострокової безпеки та стабільності.

3.4. Інформаційний вплив як технологія ведення бойових дій

У сучасній військовій доктрині інформаційний вплив розглядається не лише як допоміжний інструмент, але й як самостійна технологія ведення бойових дій, здатна суттєво впливати на хід та результати збройних конфліктів. Інформаційний вплив у військовому контексті являє собою скоординоване застосування інформаційних операцій для досягнення військових цілей шляхом впливу на свідомість, волю, можливості та дії противника, власного населення та міжнародної спільноти.

Еволюція військової справи в інформаційну епоху призвела до інтеграції інформаційного впливу у всі фази та рівні військових операцій. Від стратегічного планування до тактичного виконання, інформаційні операції використовуються для створення сприятливого інформаційного середовища, введення противника в оману, підриву його бойового духу, забезпечення інформаційної переваги та легітимізації власних дій в очах громадськості [53, С. 78-91].

Інформаційний вплив як технологія ведення бойових дій включає широкий спектр методів та засобів:

- Психологічні операції (PSYOP): плановані дії, спрямовані на передачу інформації та образів іноземним аудиторіям з метою впливу на їхні емоції, ставлення, поведінку та, зрештою, на досягнення військових цілей.
- Операції введення в оману (Deception Operations): дії, спрямовані на навмисне введення противника в оману щодо власних намірів, можливостей та дій з метою отримання тактичної або стратегічної переваги [68, С. 95-108].
- Інформаційна боротьба (Information Warfare): дії, спрямовані на досягнення інформаційної переваги шляхом атаки на інформаційні системи противника та захисту власних. Включає кібероперації, радіоелектронну боротьбу та операції впливу на інформаційні мережі [28, С. 112-125].
- Операції впливу на громадську думку (Public Opinion Influence Operations): дії, спрямовані на формування сприятливого ставлення власного населення та міжнародної спільноти до військових дій, легітимізацію їхніх цілей та протидію ворожій пропаганді [114, С. 145-158].

Стратегічні комунікації (Strategic Communications): скоординоване використання комунікаційних засобів для просування державної політики та досягнення стратегічних цілей у сфері безпеки, включаючи інформаційний вплив у воєнний час [162].

Ефективність інформаційного впливу у військових конфліктах залежить від низки ключових факторів:

- Цільова аудиторія: точне визначення її психологічних, культурних та інформаційних характеристик.
- Створення наративів: розробка переконливих інформаційних повідомлень.
- Канали поширення: використання традиційних медіа, соціальних мереж та прямих комунікацій.
- Синхронізація: узгодження інформаційних операцій з військовими діями.
- Гнучкість: оперативне реагування на зміни в інформаційному середовищі.
- Достовірність: забезпечення правдоподібності інформації, навіть у випадках введення противника в оману [11].

Інформаційний вплив застосовується на різних рівнях:

• Стратегічний: вплив на політичне керівництво противника, його населення та міжнародну спільноту.

• Оперативний: підтримка військових операцій через дезінформацію та підрив морального духу противника.

• Тактичний: безпосередній вплив на особовий склад противника для зниження його боєздатності та деморалізації.

Протидія інформаційному впливу противника включає:

• Захист власних інформаційних систем від кібератак.

• Моніторинг інформаційного простору для виявлення ворожих операцій.

• Спростування дезінформації шляхом надання достовірних даних.

• Проведення власних інформаційних операцій для нейтралізації ворожого впливу.

• Підвищення рівня медіаграмотності населення та військових.

• Забезпечення безпеки військових комунікацій.

Таким чином, інформаційний вплив є важливим елементом сучасних бойових дій, а його ефективне застосування та протидія ворожим інформаційним атакам відіграють ключову роль у досягненні військових цілей. Інформаційний вплив є потужною та багатогранною технологією ведення бойових дій у сучасному світі. Його ефективне застосування може суттєво впливати на хід та результати збройних конфліктів, а протидія ворожому інформаційній агресії є критично важливим елементом забезпечення національної безпеки та досягнення військової перемоги.

Висновки до розділу 3

Проведений аналіз різних аспектів інформаційної війни у дозволяє сформувати комплексне розуміння цього складного та багатогранного феномену цифрового суспільства. Розглядаючи інформаційну війну як невід’ємну складову сучасних соціально-політичних процесів, ми визначили її ключові характеристики в контексті глобального інформаційного простору, швидкого поширення інформації. Очевидним є те, що цифрові технології не лише полегшують ведення інформаційної війни, але й суттєво розширюють її масштаби та потенційні наслідки.

Дослідження стратегій інформаційної війни в окремих країнах виявляє значні відмінності в підходах, зумовлені політичними режимами, національними інтересами та геополітичними амбіціями. Авторитарні держави часто використовують інформаційну війну для внутрішнього контролю та зовнішньої агресії, тоді як демократичні країни зосереджуються на захисті власних інформаційних систем та просуванні демократичних цінностей. Аналіз конкретних прикладів, таких як стратегії Росії, Китаю, США та України, підкреслює різноманітність інструментів та цілей інформаційного впливу на міжнародній арені.

Розгляд інформаційної війни як чинника загрози національній безпеці висвітлює її деструктивний потенціал у політичній, соціальній, економічній та оборонній сферах. Інформаційні атаки можуть підривати довіру до державних інститутів, розпалювати внутрішні конфлікти, завдавати економічних збитків та навіть створювати передумови для військової агресії. У цьому контексті особливої ваги набуває розробка ефективних стратегій протидії інформаційним загрозам на національному рівні.

Дослідження інформаційного впливу як технології ведення бойових дій підкреслило його інтеграцію у сучасну військову доктрину. Інформаційні операції, включаючи психологічні операції, введення в оману, інформаційну боротьбу та стратегічні комунікації, розглядаються як важливий елемент досягнення військової переваги на всіх рівнях збройного конфлікту. Протидія інформаційному впливу противника стає ключовим завданням для забезпечення власної обороноздатності та досягнення перемоги.

Отже, інформаційна війна є складним, динамічним та багатовимірним феноменом цифрового суспільства, який становить значну загрозу національній та міжнародній безпеці. Тенденції розвитку інформаційних технологій, зокрема штучного інтелекту та великих даних, лише посилюватимуть можливості для проведення масштабних та високотехнологічних інформаційних атак. Перспективи розвитку інформаційної війни пов’язані з подальшою інтеграцією інформаційного впливу у всі сфери суспільного життя, розмиттям меж між війною та миром, а також з появою нових форм інформаційної агресії.

РОЗДІЛ 4
КІБЕРВІЙНА ЯК ВИД ТА ІНСТРУМЕНТ МЕРЕЖЕВИХ ВОЄН

4.1. Кібервійна як інформаційне протиборство в кіберпросторі

У сучасних умовах геополітичної нестабільності та зростання міждержавної конкуренції, феномен гібридної війни набуває все більшого поширення. Однією з ключових складових гібридної війни є використання кіберпростору як платформи для здійснення деструктивних дій, спрямованих на підрив національної безпеки, економічної стабільності та соціальної злагоди противника. У цьому контексті кіберзлочинність, традиційно розглядувана як сфера кримінальної діяльності, все частіше інтегрується в стратегії мережевої війни, стаючи важливим інструментом досягнення політичних та військових цілей [50, С. 35-48].

У XX столітті з’явився новий формат інформаційно-комунікаційних протистоянь – кібервійна. Це боротьба сторін на рівні програмного забезпечення, що включає здобуття конфіденційної інформації та недопущення нормальної роботи програмно-апаратних засобів супротивника. Такий підхід дає змогу отримувати значні переваги у економічних, політичних та військових протистояннях. [96, С. 95-100].

Піраміда кіберзагроз має кілька рівнів. На базі розташовані загрози, які здійснюють традиційні кіберзлочинці, орієнтовані виключно на фінансову вигоду та націлені на рядових користувачів. Середній рівень охоплює атаки корпоративного кібершпіонажу і використання шпигунського програмного забезпечення, яке застосовують держави для моніторингу діяльності своїх громадян і підприємств. На верхівці піраміди знаходяться кіберзагрози, створені державами для проведення кібератак на інші країни, що є складовою частиною мережевої війни.

Переосмислення ролі кіберзлочинності в контексті мережевої війни зумовлене низкою факторів. По-перше, кіберпростір став критично важливою

інфраструктурою для функціонування сучасної держави та суспільства. Від його стабільної роботи залежить діяльність урядових інституцій, фінансової системи, енергетичного сектору, транспорту, зв'язку та багатьох інших життєво важливих сфер. Вразливість цих систем до кібератак створює широкі можливості для завдання значної шкоди противнику без застосування традиційних військових засобів [61, С. 112-125].

По-друге, кіберзлочинні угруповання часто володіють високим рівнем технічної експертизи та розвиненою організаційною структурою. Їхні можливості у сфері проникнення в захищені інформаційні системи, розробки та використання шкідливого програмного забезпечення можуть бути використані державами-агресорами для проведення складних та скоординованих кібератак. При цьому, залучення недержавних акторів дозволяє зберігати певну дистанцію та ускладнює офіційну атрибуцію агресії [76, С. 67-81].

По-третє, кіберзлочинність може використовуватися як інструмент для фінансування інших деструктивних дій у рамках гібридної війни. Кошти, отримані від кібершахрайства, вимагання, крадіжки інтелектуальної власності або незаконної торгівлі в даркнеті, можуть спрямовуватися на підтримку терористичних організацій, сепаратистських рухів, інформаційних кампаній з дезінформації та інших підривних елементів [83, С. 92-105].

Основні риси кібервійн, що відрізняють їх від традиційних військових дій, включають:

- невизначеність початку операцій;
- дуже високий рівень анонімності учасників;
- мінімальну залишковість слідів;
- відсутність чітких понять "фронт" і "тил";
- брак правового міжнародного регулювання.

Сьогодні глобальною мережею Інтернет управляє ICANN (Internet Corporation for Assigned Names and Numbers) за принципом "один світ – один Інтернет". Такий підхід унеможливлює застосування традиційних міжнародних угод у сфері військового права, оскільки ICANN не визнає права окремих держав

регулювати або нести відповідальність за окремі сегменти мережі. Водночас, Інтернет та інші цифрові мережі мають наднаціональний характер, тоді як кібератаки націлені на конкретні держави та їхні структури.

Наразі відсутні ефективні юридичні та узгоджувальні механізми для профілактики та запобігання кібервійнам, що робить їх особливо небезпечними. Їхня легкість розгортання та практично відсутній контроль спричиняють значні виклики для сучасної безпеки. [96, С. 95-100].

Зв’язок між кіберзлочинністю та мережевою війною проявляється у різних формах. Однією з них є спонсорована державою кіберзлочинність. У цьому випадку державні структури можуть безпосередньо координувати або таємно підтримувати діяльність кіберзлочинних угруповань для досягнення своїх стратегічних цілей. Це може включати завдання кібератак на критичну інфраструктуру противника, проведення шпигунських операцій, викрадення важливих даних або розповсюдження шкідливого програмного забезпечення. Залучення кіберзлочинців дозволяє державі заперечувати свою причетність до атак, використовуючи принцип “правдоподібного заперечення” [124, С. 45-58].

Іншою формою взаємодії є використання кіберзлочинних інструментів та методів у державних кібероперацій. Державні хакерські групи можуть застосовувати ті ж самі техніки проникнення, експлуатації вразливостей та приховування слідів, що й звичайні кіберзлочинці. Це ускладнює розмежування між кримінальною діяльністю та державними атаками, що створює додаткові труднощі для правоохоронних органів та служб безпеки.

Крім того, кіберзлочинність може використовуватися для створення хаосу та дестабілізації суспільства противника. Масові кібератаки на фінансові установи, системи комунального господарства або державні сервіси можуть викликати паніку серед населення, підірвати довіру до влади та створити умови для соціальних заворушень. Ці дії, хоча формально і є кримінальними, можуть бути частиною ширшої стратегії гібридної війни, спрямованої на послаблення держави зсередини [132, С. 102-115].

Важливим аспектом є також використання кіберзлочинності для проведення інформаційно-психологічних операцій (ІПСО). Кіберзлочинні угруповання можуть бути залучені до розповсюдження фейкових новин, пропагандистських матеріалів та дезінформації через соціальні мережі та інші онлайн-платформи. Їхні технічні можливості можуть використовуватися для створення бот-ферм, організації скоординованих кампаній з тролінгу та маніпулювання громадською думкою на користь агресора [147, С. 128-141].

Аналіз сучасних збройних конфліктів, зокрема агресії Російської Федерації проти України, свідчить про активне використання кіберзлочинності як складової гібридної війни. Кібератаки на критичну інфраструктуру, державні установи та приватний сектор, часто замасковані під дії невідомих хакерських угруповань, супроводжуються масштабними інформаційними кампаніями. Їхня мета — дестабілізація суспільства та підрив довіри до української влади, що створює додаткові виклики для національної безпеки.

Протидія кіберзлочинності як елементу мережевої війни вимагає комплексного підходу, що поєднує зусилля правоохоронних органів, служб безпеки, державних інституцій та приватного сектору. Важливим є зміцнення національних кібернетичних можливостей, підвищення рівня кібербезпеки критичної інфраструктури, розробка ефективних механізмів виявлення та атрибуції кібератак, а також посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю [150, С. 152-165]. Крім того, важливе значення має підвищення рівня обізнаності суспільства щодо загроз у кіберпросторі та формування культури кібергігієни. Громадяни повинні бути навчені розпізнавати кібершахрайство, протидіяти дезінформаційним кампаніям та дотримуватися правил безпечної поведінки в Інтернеті. Це сприятиме підвищенню стійкості суспільства до гібридних загроз, що використовують кіберпростір як один зі своїх ключових інструментів [152, С. 98-111].

Кіберзагрози займають дедалі вагоміше місце у спектрі загроз національній безпеці, і ця тенденція буде посилюватися в найближче десятиліття з розвитком інформаційних технологій та їх інтеграцією зі штучним інтелектом. Зростаючий

вплив кіберзагроз на управлінські структури як національного, так і транснаціонального рівня формує нову безпекову реальність, що супроводжується викликами технологічного характеру. Світові центри сили активно розподіляють сфери впливу у кіберпросторі, використовуючи цей процес для реалізації власних геополітичних інтересів та зміцнення позицій у глобальній конкуренції.

4.2. Кібершпигунство та несанкціонований збір даних

У контексті зростаючої взаємозалежності держав та їхньої критичної залежності від інформаційних технологій, кібершпигунство набуває особливої актуальності як важливий інструмент розвідки та стратегічного впливу. Кібершпигунство являє собою вид діяльності в кіберпросторі, спрямований на несанкціоноване проникнення в інформаційні системи з метою отримання конфіденційної інформації політичного, економічного, військового, науково-технічного або іншого важливого характеру. Цей вид кібернетичної діяльності є невід'ємною складовою сучасних мережевих війн, забезпечуючи агресору стратегічні переваги шляхом отримання доступу до чутливих даних без прямого військового зіткнення [83, С. 112-125].

Сутність кібершпигунства полягає у прихованому отриманні інформації, що становить цінність для держави, організації або окремої особи, без відома та згоди власника цієї інформації. На відміну від інших видів кібератак, метою кібершпигунства, як правило, не є руйнування або порушення функціонування інформаційних систем, а саме непомітне викрадення даних. Отримана в результаті кібершпигунства інформація може бути використана для прийняття політичних рішень, розробки військових стратегій, отримання економічних переваг у конкурентній боротьбі, здійснення технологічної розвідки або проведення інших деструктивних дій [61, С. 145-158].

Кібершпигунство стає дедалі серйознішою загрозою для бізнесу в умовах цифрової епохи. Цей вид кіберзлочинності передбачає незаконне отримання

конфіденційної або розвідувальної інформації через комп'ютерні технології. Зловмисники, що займаються кібершпигунством, можуть переслідувати різні цілі, зокрема економічну вигоду, політичні інтереси або шантаж. Кібершпигунство охоплює збір та передачу інформації з обмеженим доступом іноземним державам, організаціям або їхнім представникам, здійснювані у кіберпросторі.

Останнім часом кібершпигунство включає також аналіз поведінки користувачів у соціальних мережах, таких як Facebook і Twitter. Це робиться за допомогою спеціальних служб для виявлення екстремістської, терористичної чи антиурядової діяльності. Наприклад, програма Athena, розроблена ЦРУ спільно з американською кібербезпековою компанією Siege Technologies, дозволяє агентам дистанційно змінювати налаштування операційної системи Windows, вводити віруси та завантажувати файли із заражених пристроїв [103, С.95-130.].

Кібершпигунство здійснюється різними методами із застосуванням широкого спектру інструментів. Одним із найпоширеніших способів є використання шкідливого програмного забезпечення (ШПЗ), зокрема троянських програм, шпигунських програм (spyware), кейлоггерів (keyloggers) та програм віддаленого доступу (RATs). Таке ПЗ може непомітно проникати на комп'ютери та сервери жертви, фіксувати дії користувачів, перехоплювати мережевий трафік, копіювати файли та надавати зловмисникам віддалений контроль над системою. [45, С. 88-101].

Іншим поширеним методом є фішинг, який полягає у розсиланні електронних листів або повідомлень, що маскуються під офіційні повідомлення від довірених організацій або осіб, з метою спонукати жертву розкрити свої облікові дані (логіни, паролі) або перейти за шкідливим посиланням, що призводить до зараження системи ШПЗ [143, С. 92-105].

Соціальна інженерія є ключовим інструментом кібершпигунства. Зловмисники застосовують психологічні прийоми та маніпуляції, щоб змусити співробітників компанії-жертви добровільно розкрити конфіденційні дані або виконати дії, які допоможуть їм несанкціоновано проникнути в інформаційні

системи [89, С. 67-80]. Експлуатація вразливостей програмного забезпечення та мережевого обладнання є ще одним ефективним методом кібершпигунства. Зловмисники виявляють невідомі помилки та недоліки в програмному коді або конфігурації систем і використовують їх для отримання несанкціонованого доступу до інформації [66, С. 115-128].

Протидія кібершпигунству є складним завданням, що вимагає комплексного підходу та постійного вдосконалення систем захисту інформації. Основними напрямками протидії є:

- Посилення систем кібербезпеки: впровадження сучасних засобів захисту від несанкціонованого доступу, виявлення вторгнень та запобігання витоку інформації [55, С. 132-145].
- Регулярне оновлення програмного забезпечення: своєчасне встановлення оновлень безпеки для усунення виявлених вразливостей.
- Підвищення рівня обізнаності користувачів: проведення навчань та тренінгів з кібергігієни для запобігання фішинговим атакам та соціальній інженерії.
- Використання засобів шифрування: захист конфіденційної інформації шляхом її криптографічного перетворення [90, С. 105-118].
- Моніторинг та аналіз мережевого трафіку: виявлення підозрілої активності та аномалій у роботі інформаційних систем [42, С. 62-75].
- Міжнародне співробітництво: обмін інформацією та координація зусиль між державами для боротьби з кібершпигунством на глобальному рівні [140, С. 78-92].

Кібершпигунство може здійснюватися різними акторами, включаючи державні розвідувальні служби, приватні хакерські групи, промислових шпигунів та окремих зловмисників. Державне кібершпигунство є особливо небезпечним, оскільки воно може бути спрямоване на стратегічно важливі об’єкти та здійснюватися з використанням значних ресурсів та високого рівня організації [123, С. 55-68]. Наслідки успішних кібершпигунських операцій можуть бути різноманітними та мати далекосяжні наслідки. Викрадення

політичної інформації може вплинути на міжнародні відносини та національну безпеку. Отримання економічних секретів може завдати значних збитків підприємствам та підірвати їхню конкурентоздатність. Викрадення військових технологій може порушити баланс сил та створити загрозу для обороноздатності держави. Науково-технічне шпигунство може призвести до втрати інтелектуальної власності та уповільнення інноваційного розвитку [135, С. 78-91].

4.3. Кіберсаботаж як навмисне порушення роботи інформаційних систем

У сучасному світі, де суспільство дедалі більше залежить від інформаційних технологій, кіберсаботаж є руйнівною діяльністю в кіберпросторі. Його мета — навмисно порушити нормальну роботу інформаційних систем, вивести з ладу обладнання або знищити критично важливі дані.

На відміну від кібершпигунства, що прагне несанкціоновано отримати інформацію, кіберсаботаж зосереджений на завданні прямої шкоди працездатності систем. Це може мати серйозні наслідки для національної безпеки, економіки та повсякденного життя громадян. [89, С. 112-125].

Сутність кіберсаботажу полягає у навмисному впливі на інформаційні системи з метою їхньої дестабілізації, руйнування або виведення з ладу. Ці дії можуть бути спрямовані проти різноманітних об’єктів, включаючи урядові установи, військові структури, об’єкти критичної інфраструктури (енергетичні мережі, транспортні системи, фінансові установи, телекомунікації), промислові підприємства та інші організації, стабільна робота яких є важливою для функціонування держави та суспільства [61, С. 130-143].

Кіберсаботаж може здійснюватися різними способами та з використанням різноманітних інструментів. Одним з поширених методів є використання шкідливого програмного забезпечення (ШПЗ), такого як віруси-руйнівники (wiper malware), логічні бомби, програми-вимагачі (ransomware), які можуть блокувати доступ до даних або шифрувати їх з метою отримання викупу, а також ШПЗ, спеціально розроблене для виведення з ладу промислового обладнання [45, С. 95-108].

Іншим поширеним видом кіберсаботажу є розподілені атаки типу “відмова в обслуговуванні” (DDoS), які полягають у надсиланні великої кількості запитів на сервери жертви з метою перевантаження їхніх ресурсів та унеможливлення доступу легітимних користувачів до сервісів [144, С. 108-121].

Атаки на цілісність даних також є формою кіберсаботажу, що полягає у навмисному спотворенні, видаленні або модифікації важливої інформації, що може призвести до помилкових рішень, фінансових втрат або порушення технологічних процесів [83, С. 128-141].

Кіберсаботаж може здійснюватися як окремими хакерами або кіберзлочинними угрупованнями, так і під егідою державних структур в рамках військових або політичних конфліктів. Державне спонсорування кіберсаботажу є особливо небезпечним, оскільки такі атаки можуть бути добре спланованими, скоординованими та мати значні ресурси для їхньої реалізації.

Наслідки кіберсаботажу можуть бути надзвичайно серйозними та мати далекосяжні наслідки для різних сфер життєдіяльності. Порушення роботи енергетичних систем може призвести до відключення електроенергії для великих регіонів. Блокування транспортних систем може спричинити колапс у логістиці та переміщенні людей. Атаки на фінансові установи можуть призвести до нестабільності на ринках та втрати коштів. Виведення з ладу систем управління промисловими процесами може призвести до техногенних катастроф та екологічних забруднень. Протидія кіберсаботажу вимагає комплексного підходу, що поєднує технічні та організаційні заходи.

Основні напрямки такої протидії включають:

- Впровадження надійних систем кібербезпеки: Сюди входить використання міжмережевих екранів, систем виявлення та запобігання вторгненням, сучасного антивірусного програмного забезпечення та інших засобів захисту.
- Резервне копіювання та відновлення даних: регулярне створення резервних копій критично важливої інформації та розробка планів відновлення у випадку кібератаки [41, С. 76-89].

- Резервне копіювання та відновлення даних — це регулярне створення копій всієї критично важливої інформації та розробка детальних планів для її відновлення у разі кібератаки.
- Сегментація мереж: поділ інформаційних систем на окремі сегменти для обмеження поширення наслідків кібератаки.
- Посилення контролю доступу: впровадження строгих правил автентифікації та авторизації для запобігання несанкціонованому доступу до критичних систем [89, С. 119-132].
- Моніторинг та аналіз подій безпеки — це безперервний контроль за функціонуванням інформаційних систем. Його мета — виявляти підозрілу активність та оперативно реагувати на інциденти.
- Співробітництво з правоохоронними органами та іншими організаціями: обмін інформацією про кіберзагрози та координація зусиль для їхнього запобігання та розслідування [32, С. 92-105].

Кіберсаботаж є серйозною загрозою для сучасного суспільства, здатною завдати значної шкоди критичній інфраструктурі та національній безпеці. Ефективна протидія цьому виду кібернетичної агресії вимагає комплексних зусиль з боку держави, бізнесу та суспільства, спрямованих на зміцнення кібербезпеки, підвищення рівня готовності до реагування на кіберінциденти та посилення співпраці між усіма зацікавленими сторонами.

4.4. Атаки на критичну інфраструктуру та навмисні кіберзагрози іформаційно-комунікаційним системам

В умовах зростаючої цифровізації всіх сфер життєдіяльності, об’єкти критичної інфраструктури (КІ) стають дедалі привабливішою мішенню для кібератак. Критична інфраструктура включає в себе життєво важливі системи та об’єкти, такі як енергетичні мережі, транспортні системи, фінансові установи, телекомунікації, системи водопостачання та охорони здоров’я, порушення або виведення з ладу яких може мати катастрофічні наслідки для держави, економіки та безпеки її громадян [77, С. 95-108]. Навмисні кіберзагрози, спрямовані на ці

системи, становлять серйозний виклик для національної безпеки та вимагають комплексних заходів для їхнього запобігання та нейтралізації [32, С. 258].

Кібератаки на критичну інфраструктуру спрямовані на використання кібернетичних засобів для пошкодження або порушення роботи автоматизованих систем управління технологічними процесами (АСУ ТП) та інших інформаційних систем, що забезпечують функціонування цих об’єктів. Метою таких атак може бути спричинення техногенних аварій, економічних збитків, порушення життєво важливих послуг населенню, дестабілізація суспільства або досягнення політичного впливу [112, С. 112-125].

Кіберзагрози для критичної інфраструктури є різноманітними та постійно еволюціонують, охоплюючи широкий спектр атак, спрямованих на порушення її функціонування. До основних видів цих загроз належить шкідливе програмне забезпечення (ШПЗ), таке як віруси, черв’яки, троянські програми, програми-вимагачі, а також спеціально розроблене ШПЗ для атак на промислові системи, як-от Stuxnet, що може використовуватися для порушення роботи обладнання, знищення даних або блокування доступу до критичних систем. Поширеними є також атаки типу “відмова в обслуговуванні” (DoS/DDoS), метою яких є перевантаження мережевих ресурсів об’єктів КІ, що унеможливлює їхню нормальну роботу та надання послуг [145, С. 132-145].

Особливу небезпеку становлять цілеспрямовані атаки (APT) – складні, довготривалі кібероперації, що здійснюються висококваліфікованими зловмисниками, часто за підтримки держав, з метою проникнення в захищені системи КІ та завдання значної шкоди. Окрім цього, зростає кількість атак на ланцюги постачання, коли компрометуються постачальники обладнання, програмного забезпечення або послуг для отримання доступу до систем КІ. Не варто забувати й про інсайдерські загрози, що походять від навмисних або ненавмисних дій співробітників об’єктів КІ, які можуть призвести до порушення безпеки систем.

Наслідки успішних кібератак на критичну інфраструктуру можуть бути руйнівними, викликаючи масштабні відключення електроенергії, параліч транспортних систем, крах банківських систем або неможливість надання медичної

допомоги. Такі інциденти здатні призвести до техногенних катастроф, значних економічних збитків та навіть людських жертв [32, С. 118-132].

Забезпечення кібербезпеки критичної інфраструктури (КІ) є першочерговим державним завданням, що вимагає комплексного та скоординованого підходу. Серед основних напрямків діяльності у цій сфері можна виділити кілька ключових.

По-перше, це розробка та впровадження нормативно-правової бази, яка регулює питання кібербезпеки об’єктів КІ та встановлює відповідальність за порушення [10]. Паралельно з цим відбувається визначення об’єктів критичної інфраструктури та їхня категоризація, що дозволяє ідентифікувати життєво важливі системи та застосовувати відповідні заходи захисту.

По-друге, важливим є впровадження комплексних систем захисту інформації. Це передбачає використання як технічних, так і організаційних заходів для запобігання несанкціонованому доступу, оперативного виявлення кібератак та ефективного реагування на них [54, С. 159-172]. Регулярні аудити та тестування на проникнення — невід’ємна частина цього процесу. Вони дозволяють оцінити рівень захищеності систем критичної інфраструктури (КІ) та виявити потенційні вразливості.

По-третє, критично важливим є підвищення рівня обізнаності та підготовка персоналу. Навчання співробітників об’єктів КІ правилам кібергігієни та діям у разі кіберінцидентів сприяє формуванню культури кібербезпеки [87, С. 132-145]. Нарешті, міжнародне співробітництво та обмін інформацією з іншими державами та міжнародними організаціями є життєво необхідним для обміну досвідом та даними про актуальні кіберзагрози.

4.5 Кібертероризм як злочинне використання кіберпростору терористами

Кібертероризм являє собою використання кібернетичних засобів та методів терористичними групами для здійснення атак на інформаційні системи, поширення пропаганди, вербування нових членів, координації терористичної діяльності та фінансування своїх операцій. Це явище становить серйозну загрозу

для національної та міжнародної безпеки, поєднуючи руйнівний потенціал тероризму з можливостями кіберпростору [100, С. 118-131].

Сутність кібертероризму полягає у використанні кіберпростору як інструменту для здійснення терористичних актів або підтримки терористичної діяльності. На відміну від традиційних кібератак, мотивом кібертероризму є політична, ідеологічна або релігійна мета, спрямована на залякування населення, примушення урядів до певних дій або дестабілізацію суспільства. Об'єктами кібертерористичних атак можуть бути урядові вебсайти, засоби масової інформації, транспортні системи, енергетичні мережі, фінансові установи та інші елементи критичної інфраструктури [39, С. 95-108].

Кібертероризм спрямованою на підрив стабільності держави через цифрові загрози. Загрози національній безпеці України в інформаційній сфері охоплюють сукупність умов і факторів, що ставлять під загрозу ключові інтереси держави, суспільства та громадян. Вони включають негативний інформаційний вплив на свідомість і поведінку населення, а також атаки на інформаційні ресурси та інфраструктуру, що можуть призвести до дестабілізації [120. С. 178–185.].

Кібертерористичні організації використовують різноманітні методи та інструменти для досягнення своїх цілей у кіберпросторі. Одним з основних є поширення пропаганди та екстремістської ідеології через соціальні мережі, вебсайти, форуми та інші онлайн-платформи. Кіберпростір надає терористам можливість охоплювати широку аудиторію, залучати нових прихильників та радикалізувати потенційних членів [146, С. 145-158]. Вербування нових членів та налагодження комунікації між ними також активно здійснюється через зашифровані канали зв'язку, месенджери та даркнет. Кіберпростір забезпечує терористичним групам анонімність та ускладнює їхнє виявлення правоохоронними органами [79, С. 102-115]. Фінансування терористичної діяльності є ще одним важливим аспектом використання кіберпростору терористами. Збір коштів може здійснюватися через онлайн-пожертви, криптовалюти, шахрайські схеми та інші незаконні фінансові операції в кіберпросторі [83, С. 145-158]. Безпосередньо здійснення кібератак на

інформаційні системи з метою завдання шкоди, викликання паніки або порушення роботи критичної інфраструктури є найбільш небезпечним проявом кібертероризму. Хоча на сьогоднішній день масштабних кібертерористичних атак, що призвели б до значних фізичних руйнувань або людських жертв, зафіксовано не було, потенціал таких атак є надзвичайно високим [19, С. 177-194].

Протидія кібертероризму вимагає багатовекторних зусиль як на національному, так і на міжнародному рівнях. Серед основних напрямків боротьби з цим явищем можна виділити посилення законодавчої бази, що передбачає розробку та впровадження ефективного законодавства, яке криміналізує кібертерористичну діяльність і передбачає належну відповідальність за її вчинення [1]. Зміцнення кібербезпеки об’єктів критичної інфраструктури є ключовим завданням, що передбачає надійний захист інформаційних систем, які забезпечують функціонування життєво важливих сфер держави. Важливим аспектом також є постійний моніторинг та аналіз кіберпростору для своєчасного виявлення і блокування терористичного контенту, пропагандистських матеріалів та каналів комунікації терористичних угруповань.

Крім того, міжнародне співробітництво відіграє ключову роль, обмін інформацією, координація дій та проведення спільних операцій між правоохоронними органами та спецслужбами різних країн є критично важливими для ефективної боротьби з кібертероризмом (140, С. 107-120). Необхідно також підвищувати рівень обізнаності суспільства, інформуючи громадян про загрози кібертероризму та навчаючи правилам безпечної поведінки в Інтернеті. Нарешті, розробка та впровадження передових технологій виявлення та протидії кібертерористичним атакам, зокрема використання штучного інтелекту та машинного навчання для аналізу даних і прогнозування кіберзагроз, є суттєвим для оперативної та ефективної відповіді на загрози, що постійно еволюціонують [42, С. 90-103].

Злочинне використання кіберпростору терористичними організаціями для поширення своєї ідеології, вербування нових членів, фінансування діяльності та підготовки атак вимагає консолідованих зусиль з боку держав, міжнародних організацій та громадянського суспільства для ефективної протидії цій небезпеці. Україна визначила поглиблення євроінтеграції як ключовий зовнішньополітичний пріоритет у сфері кібербезпеки. Це передбачає уніфікацію підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО. Країна також активно співпрацює з іноземними партнерами для посилення своєї кіберстійкості, розвитку спроможностей національної системи кібербезпеки та захисту національних інтересів у кіберпросторі. Особливу увагу держава приділяє спільній протидії міжнародному тероризму та іншим протиправним діям, що загрожують миру, безпеці та міжнародному правопорядку. Вона розвиває взаємовигідний обмін інформацією та досвідом у сфері кібербезпеки з партнерськими спецслужбами країн ЄС і НАТО. Для зміцнення наукової, матеріально-технічної бази та кадрового потенціалу, Україна активно використовуватиме кращі світові практики та здійснюватиме інші спільні заходи. [161].

Висновки до розділу 4

Проведений у дрозділі аналіз кібервійни як важливого виду та інструменту мережевих воєн дозволяє розкрити її сутність, форми прояву та роль у сучасному інформаційному протиборстві. Розглянувши кібервійну як інформаційне протиборство в кіберпросторі, ми визначили її ключові характеристики та відмінності від традиційних форм збройної боротьби, підкресливши її специфіку, пов’язану з віртуальним середовищем та швидкістю поширення інформації.

Дослідження кібершпигунства та несанкціонованого збору даних виявило їхню важливість як інструменту отримання стратегічно цінної інформації, що може бути використана для досягнення військових, політичних та економічних

цілей. Було підкреслено різноманітність методів кібершпигунства та зростаючу складність виявлення та протидії цим загрозам. Аналіз кіберсаботажу як навмисного порушення роботи інформаційних систем показав його деструктивний потенціал, здатність завдавати значної шкоди критичній інфраструктурі та порушувати функціонування важливих державних і приватних структур. Було розглянуто різні види кіберсаботажу та їхні можливі наслідки. Дослідження атак на критичну інфраструктуру та навмисних кіберзагроз комунікаційно-інформаційним системам виявило їхню особливу небезпеку для національної безпеки. Порушення роботи цих систем може мати катастрофічні наслідки для життєдіяльності суспільства та обороноздатності держави.

Кібервійна є важливим та багатогранним видом мережевих війн, що охоплює широкий спектр дій в кіберпросторі, спрямованих на досягнення інформаційної переваги, завдання шкоди противнику та підрив його можливостей. Кібершпигунство, кіберсаботаж, дезінформаційні кампанії та атаки на критичну інфраструктуру є ключовими інструментами кібервійни, кожен з яких має свої особливості та потенційні наслідки. Розуміння сутності та форм прояву кібервійни є необхідною умовою розвитінтересів у кіберпросторі та протидії загрозам у мережевих війнах. Подальші дослідження у цій сфері є важливими для виявлення нових тенденцій розвитку кібервійни та розробки адекватних заходів реагування на них.

РОЗДІЛ 5
МЕРЕЖЕВІ ВІЙНИ В УМОВАХ СУЧАСНОСТІ

5.1. Гібридна війна, як інтегральна форма мережевої агресії

Феномен гібридних війн є однією з визначальних рис сучасних збройних конфліктів, що характеризується розмиванням чітких меж між станом миру та війни. Сутність гібридної війни полягає у комплексному та скоординованому застосуванні як військових, так і невійськових інструментів впливу для досягнення стратегічних цілей. Це включає поєднання кінетичних військових дій з інформаційними операціями, економічним тиском, кібератаками, дипломатичними зусиллями, використанням недержавних акторів та іншими засобами, спрямованими на дестабілізацію противника зсередини та ззовні.

На відміну від класичних міждержавних війн, де домінує пряме військове протистояння, гібридна війна характеризується прихованістю агресора, використанням проксі-сил, активним маніпулюванням інформаційним простором та розмиванням відповідальності. Це створює значні труднощі у визначенні початку конфлікту, ідентифікації агресора та формуванні ефективної відповіді [64, С. 25].

Хоча термін “гібридна війна” набув широкого вжитку відносно недавно, елементи гібридних підходів можна простежити в історії збройних конфліктів задовго до його появи. Застосування нерегулярних формувань, підтримка повстанських рухів, економічна блокада, пропаганда та диверсії використовувалися як допоміжні засоби ведення війни поряд з традиційними військовими діями [111, С. 40].

Прикладами можуть слугувати дії “флібустьєрів” у колоніальних війнах, використання партизанських загонів у війнах XIX століття, підтримка “п’ятої колони” перед Другою світовою війною. Однак, сучасні гібридні війни відрізняються якісно новим рівнем інтеграції та координації різних інструментів

впливу, а також використанням новітніх технологій, зокрема в інформаційній та кібернетичній сферах [22, С. 55].

Розвиток засобів масової комунікації, глобалізація та зростання взаємозалежності держав створили нові можливості для застосування гібридних стратегій, дозволяючи впливати на противника на значній відстані та в різних сферах його життєдіяльності.

Сучасні гібридні війни мають ряд ключових характеристик, які визначають їхню специфіку та відрізняють від традиційних конфліктів:

- Асиметричність: Застосування противником нетрадиційних методів та засобів боротьби, які компенсують його слабкість у традиційній військовій сфері. Це може включати використання недержавних збройних формувань, терористичних актів, інформаційних атак, економічного тиску тощо [70, С. 70].
- Багатовимірність: Одночасне ведення боротьби у різних сферах. Кожна з цих сфер використовується для досягнення синергетичного ефекту та підриву стійкості противника [78, С. 85].
- Використання недержавних акторів: Активна залученість до конфлікту недержавних збройних формувань, приватних військових компаній, волонтерів, кримінальних елементів та інших недержавних суб’єктів, що дозволяє агресору зберігати формальну непричетність до конфлікту [49, С. 100].
- Інформаційна складова: Інформаційна війна є невід’ємною частиною гібридних конфліктів, спрямована на маніпулювання громадською думкою, поширення дезінформації, підрив довіри до інститутів влади, розпалювання ворожнечі та виправдання власних дій [118, С. 115].

Важливо розрізняти гібридні війни від традиційних міждержавних конфліктів, де основною формою боротьби є пряме військове зіткнення регулярних армій. Гібридні війни характеризуються розмиванням лінії фронту, відсутністю чіткого оголошення війни та переважним використанням невійськових засобів на початковому етапі. Термін “нелінійні конфлікти” часто використовується як синонім гібридних війн або як один з їхніх аспектів, що підкреслює нестандартність застосовуваних методів та непередбачуваність

розвитку подій. Однак, гібридна війна є більш широким поняттям, що включає в себе не лише нелінійні тактики, але й комплексне застосування всього спектру інструментів впливу.

Закон України “Про національну безпеку України” [3] визначає гібридні загрози як один з ключових викликів національній безпеці, підкреслюючи необхідність розробки комплексних заходів для їхнього відбиття. Розуміння сутності, ознак та особливостей гібридних війн є критично важливим для ефективної

Гібридні війни характеризуються широким спектром інструментів та методів впливу, які агресор використовує для досягнення своїх цілей, уникаючи відкритого широкомасштабного військового конфлікту. Ці інструменти охоплюють військову, економічну, інформаційну та політико-дипломатичну сфери, застосовуються комплексно та скоординовано для створення синергетичного ефекту [116, С. 130].

Військові інструменти в гібридних війнах істотно відрізняються від традиційного застосування регулярних армій, зосереджуючись на асиметричних діях та використанні сил, які важко ідентифікувати як представників держави-агресора. Тут ключову роль відіграють Сили спеціальних операцій (ССО), які залучаються для розвідувально-диверсійних дій, точкових ударів по ключових об’єктах, підготовки та підтримки нерегулярних збройних формувань, часто під прикриттям або без прямого розголошення їхньої державної належності [107, С. 45]. Також широко застосовуються нерегулярні збройні формування (НЗФ), включаючи добровольчі батальйони, незаконні збройні групи та сепаратистські угруповання, які можуть підтримуватися, фінансуватися та озброюватися агресором, дозволяючи йому заперечувати пряму участь у конфлікті та створювати ілюзію внутрішнього протистояння. Крім того, держави-агресори можуть використовувати проксі-сили – інші держави або недержавні актори, надаючи їм військову, фінансову, політичну або інформаційну підтримку для опосередкованого впливу на ситуацію в регіоні, уникаючи прямого зіткнення та відповідальності [110, С. 72].

Економічні інструменти є важливим елементом гібридних стратегій, спрямованих на підрив економічної стабільності противника, створення соціальної напруги та обмеження його ресурсів. До них належать санкції, тобто застосування економічних обмежень проти держави-противника, її окремих осіб або компаній з метою змусити змінити політику або поведінку [20, С. 88]. Це також включає торговельні обмеження, такі як введення тарифів, квот або заборон на імпорт/експорт певних товарів для завдання шкоди економіці противника або використання торговельних відносин як інструменту політичного тиску. Окремим аспектом є фінансова підтримка дестабілізуючих сил, що надається опозиційним рухам, сепаратистським угрупованням або іншим силам, зацікавленим у розхитуванні ситуації в країні-противнику, що може включати прямі виплати, кредити, інвестиції або інші форми фінансової допомоги. Закон України “Про санкції”від 14 серпня 2014 року № 1644-VII є прикладом законодавчої бази для застосування таких інструментів.

Інформаційна сфера відіграє ключову роль у гібридних війнах, будучи ареною боротьби за свідомість та підтримку населення. Це виявляється через пропаганду – систематичне поширення інформації, часто упередженої або неправдивої, з метою формування певних поглядів або поведінки цільової аудиторії, спрямованої на власне населення, населення противника та міжнародну спільноту. Важливим інструментом є дезінформація, яка полягає у поширенні завідомо неправдивої інформації для введення в оману противника, підриву його довіри до власних інститутів, створення хаосу та паніки. Кібератаки є невід’ємною частиною інформаційної війни, спрямованої на дестабілізацію роботи інформаційних систем і критичної інфраструктури, викрадення конфіденційних даних, розповсюдження шкідливого програмного забезпечення або пропагандистського контенту. Крім того, соціальні мережі та інтернет-платформи активно використовуються для поширення пропаганди та дезінформації, проведення інформаційних кампаній, маніпулювання громадською думкою та координації дій сил, що прагнуть дестабілізації [84, С. 135].

Політичні та дипломатичні інструменти використовуються для легітимізації власних дій, дестабілізації політичної системи противника та створення сприятливих міжнародних умов. Це включає підтримку опозиційних рухів, що надається внутрішнім опозиційним силам у країні-противнику для розхитування політичної стабільності та створення внутрішнього конфлікту. Також має місце втручання у внутрішні справи, що полягає у прямому або опосередкованому впливі на внутрішню політику країни-противника, включаючи втручання у виборчі процеси, підтримку певних політичних сил, організацію протестів та заворушень. Нарешті, держави-агресори можуть використовувати міжнародні організації та майданчики для просування власних інтересів, дискредитації противника, блокування небажаних рішень або отримання підтримки своїх дій.

Ключовою особливістю гібридних воєн є комбіноване та скоординоване застосування всіх перелічених інструментів. Синергетичний ефект від одночасного або послідовного використання військових, економічних, інформаційних та політико-дипломатичних засобів значно підвищує ефективність агресії та ускладнює протидію [126, С. 150]. Наприклад, інформаційна кампанія може підготувати підґрунтя для військового втручання під приводом “захисту” певних груп населення, економічні санкції можуть послабити державу-противника та зробити її більш вразливою до політичного тиску, а підтримка опозиційних рухів може створити внутрішній фронт дестабілізації.

Успішна протидія гібридним загрозам вимагає комплексного підходу, що включає зміцнення національної стійкості у всіх сферах, розвиток спроможностей для ефективної відповіді на кожен з інструментів гібридної агресії, а також тісну міжнародну співпрацю. Сучасний світ є свідком численних конфліктів, які несуть у собі ознаки гібридної війни, поєднуючи військові та невійськові інструменти для досягнення політичних цілей. Аналіз конкретних прикладів дозволяє глибше зрозуміти особливості застосування гібридних стратегій та їхні наслідки.

Російсько-українська війна є одним із найбільш показових прикладів гібридного конфлікту. Агресія Росії проти України розпочалася з використанням військових інструментів, таких як залучення сил спеціальних операцій без розпізнавальних знаків для захоплення стратегічних об'єктів у Криму, підтримка сепаратистських рухів на сході України та постачання їм зброї та військової техніки [35, С. 165]. Паралельно Росія розгортає масштабну інформаційну війну, спрямовану на дезінформацію українського та міжнародного співтовариства, виправдання агресії, розпалювання ворожнечі та підрив довіри до української влади. Використовувалися економічні інструменти тиску, включаючи торговельні обмеження та енергетичний шантаж. Кібератаки на державні установи та критичну інфраструктуру України також стали елементом гібридної стратегії Росії [82, С. 192]. Цей конфлікт демонструє комплексне застосування військових, інформаційних, економічних та політичних інструментів для досягнення геополітичних цілей, що є характерною рисою гібридної війни.

Втручання іноземних держав, які підтримують протилежні сторони конфлікту може включати військову підтримку, постачання зброї, фінансування, політичний вплив та інформаційні операції. Використання проксі-сил є поширеною практикою в цих конфліктах, що ускладнює визначення прямих учасників та відповідальність за ескалацію насильства [62, С. 218].

Релігійний екстремізм є потужним фактором, що підживлює конфлікти в регіоні та використовується різними акторами для мобілізації прихильників та виправдання насильства. Інформаційна війна також відіграє значну роль у цих конфліктах, використовуючись для пропаганди, вербування бойовиків та розпалювання міжконфесійної ворожнечі.

Діяльність терористичних організацій може розглядатися як специфічна форма гібридної війни, оскільки вони використовують асиметричні методи боротьби проти держав та суспільств. Терористичні акти, інформаційні кампанії (включаючи використання соціальних мереж для поширення пропаганди та вербування), фінансування через незаконні канали та створення паралельних структур влади є елементами гібридної стратегії терористичних організацій.

Терористичні організації прагнуть досягти політичних цілей шляхом залякування населення, дестабілізації державних інститутів та провокування радикальних дій у відповідь. Їхня діяльність часто поєднує насильство з інформаційним впливом, спрямованим на формування певного сприйняття їхніх дій та ідеології [43, С. 245].

Ефективна боротьба з тероризмом потребує комплексного підходу, що охоплює не лише військові та правоохоронні заходи, а й протидію пропаганді, ліквідацію фінансових мереж терористів та запобігання їхньому впливу на суспільство. Важливу роль у цьому відіграє Закон України “Про боротьбу з тероризмом” [7] визначає правові основи протидії терористичній діяльності в Україні, що є важливим аспектом реагування на цю форму гібридної війни.

Аналіз наведених прикладів підтверджує, що гібридні війни є складним та багатогранним явищем сучасності. Вони характеризуються поєднанням військових та невійськових інструментів, використанням недержавних акторів, активною інформаційною боротьбою та розмиванням меж між війною та миром.

5.2 Технологічні основи та інструментарій мережевих війн

Як вже говорилось, мережеві війни, як форма сучасного протистояння, значною мірою залежать від стрімкого розвитку інформаційно-комунікаційних технологій. Технологічні основи та інструментарій, що використовуються в мережевих війнах, є різноманітними та постійно еволюціонують, охоплюючи як наступальні, так і оборонні кібернетичні та інформаційні засоби. Розуміння цих технологічних аспектів є критично важливим для аналізу сутності мережевих війн та розробки ефективних стратегій протидії [41, С. 35-48].

Однією з ключових технологічних основ мережевих війн є інтернет та пов’язані з ним мережеві протоколи (TCP/IP). Глобальна мережа забезпечує платформу для швидкого поширення інформації, здійснення кібератак, координації дій різних акторів та проведення інформаційних кампаній без географічних обмежень. Анонімність та складність атрибуції в інтернеті

створюють додаткові виклики для виявлення та протидії агресивним діям у кіберпросторі [157].

Кібернетичні технології є важливим інструментарієм мережевих війн. До них належать різноманітні види шкідливого програмного забезпечення (ШПЗ), такі як віруси, черв'яки, троянські програми, програми-вимагачі, а також спеціально розроблене ШПЗ для атак на промислові системи управління (АСУ ТП) та критичну інфраструктуру. Кібератаки можуть бути спрямовані на порушення працездатності інформаційних систем, знищення або викрадення даних, отримання несанкціонованого доступу до конфіденційної інформації та шпигунство [45, С. 95-108].

Технології розподілених атак типу "відмова в обслуговуванні" (DDoS) використовуються для перевантаження мережевих ресурсів противника, унеможливлення доступу легітимних користувачів до сервісів та порушення нормального функціонування онлайн-платформ та інформаційних систем [145, С. 112-125].

Соціальні мережі та онлайн-платформи стали потужним інструментом ведення інформаційних війн. Вони використовуються для поширення пропаганди, дезінформації, фейкових новин, маніпулювання громадською думкою, організації онлайн-протестів, вербування нових членів та координації дій різних угруповань. Алгоритми соціальних мереж можуть сприяти швидкому та широкому поширенню як правдивої, так і недостовірної інформації, створюючи ефект "інформаційної бульбашки" та посилюючи поляризацію суспільства [33, С. 67-80].

Технології штучного інтелекту (ШІ) та машинного навчання (МН) набувають все більшого значення в мережевих війнах. ШІ може використовуватися для автоматизованого створення та поширення пропагандистського контенту, аналізу великих обсягів даних для виявлення цільових аудиторій та розробки персоналізованих інформаційних впливів, а також для проведення складних кібератак та розробки засобів кіберзахисту [63, С. 76-89].

Технології аналізу великих даних (Big Data Analytics) дозволяють збирати, аналізувати та обробляти великі масиви інформації з різноманітних джерел (соціальні мережі, онлайн-медіа, державні бази даних) для виявлення тенденцій, прогнозування поведінки цільових аудиторій та розробки ефективних стратегій інформаційного впливу [57, С. 92-105].

Таким чином, технологічні основи та інструментарій мережевих війн є надзвичайно різноманітними та продовжують стрімко розвиватися. Від базових інтернет-технологій до складних систем штучного інтелекту, ці інструменти надають акторам мережевих війн потужні важелі для здійснення кібератак, проведення інформаційних кампаній та впливу на свідомість і поведінку цільових аудиторій.

5.3. Особливості ведення мережевих війн різними акторами

Мережеві війни, як і багато інших явищ, що кардинально змінюють сучасний світ, постійно еволюціонують у своїх формах, методах ведення та масштабах поширення. Вони мають регіональні особливості та впливають на суспільне життя, соціальну структуру, внутрішні відносини та функціонування ключових інститутів. На відміну від традиційних конфліктів, мережеві війни ведуть не держави чи військові блоки, а глобальні інституціоналізовані структури. Мас-медіа, транснаціональні корпорації, релігійні організації, політичні еліти та спецслужби інтегруються у складну, гнучку та багаторівневу мережу впливу.

Мережевий принцип дозволяє позбавляти держави суверенітету та політичної незалежності, перетворюючи їх на контрольовані механізми, що стають частиною глобальної системи управління. Це не просто вплив на окремі суб’єкти, а маніпуляція їхнім змістом, мотиваціями, діями та намірами. Такий підхід формує нову модель світового панування, засновану на прямому планетарному контролі, що перетворює інформаційний простір на інструмент глобальної маніпуляції та тотального контролю [47. 558 С.].

Мережеві війни, як складна форма сучасного протистояння, ведуться різноманітними акторами, кожен з яких має власні цілі, можливості, стратегії та тактики. Основними учасниками мережевих війн є держави, недержавні угруповання (терористичні організації, кіберзлочинні спільноти, політичні екстремісти) та окремі особи (хактивісти, “самотні вовки”). Розуміння особливостей ведення мережевих війн кожним з цих акторів є ключовим для розробки ефективних механізмів запобігання та протидії їхнім деструктивним діям [51, С. 42-55].

Держави є найбільш потужними акторами в мережевих війнах, володіючи значними ресурсами, технологічною перевагою та розгалуженими структурами для проведення складних кібероперацій та інформаційних кампаній. Їхні цілі можуть варіюватися від кібершпигунства та саботажу критичної інфраструктури до втручання у політичні процеси інших країн та ведення масштабних інформаційних воєн для досягнення стратегічних переваг. Держави часто використовують висококваліфікованих фахівців, підтримувані державою хакерські групи (Advanced Persistent Threats – APT), а також координують зусилля різних відомств (розвідки, збройних сил, дипломатичних служб) для досягнення своїх цілей у кіберпросторі та інформаційному просторі [123, С. 69-82].

Стратегії держав у мережевих війнах часто характеризуються довгостроковістю, ретельним плануванням та використанням комбінованих методів впливу. Вони можуть включати розробку та застосування складного шкідливого програмного забезпечення, проведення скоординованих дезінформаційних кампаній через різні медіаканали, використання соціальних мереж для маніпулювання громадською думкою та кібератаки на об’єкти критичної інфраструктури [28, С. 148-161].

Недержавні угруповання відрізняються від держав меншими ресурсами, але можуть мати високу мотивацію та здатність до асиметричних дій. У 2006 році у світі існувало понад 3000 приватних військових компаній (ПВК), які налічували близько 2 мільйонів співробітників. Ці компанії функціонують у понад ста

країнах світу. Більшість із них зареєстровані в США (55%), значна частина — 27% — в країнах ЄС (переважно у Великій Британії), а 9% — на Близькому Сході та в Африці. Основними замовниками послуг ПВК є уряди (62% контрактів), тоді як комерційні структури становлять 29%. Решта замовлень припадає на неурядові організації та приватних осіб. За даними Брукінгського інституту (США), річний прибуток ПВК сягає $180 мільярдів [163].

Згадані формування істотно відрізняються від звичних загонів найманців. Сучасні приватні військові компанії (ПВК) у своїй основі мають висококваліфікованих і досвідчених фахівців: від армійських генералів та офіцерів до колишніх співробітників спецслужб і військ спеціального призначення, а також інших профільних спеціалістів.

Терористичні організації використовують кіберпростір для поширення своєї ідеології, вербування нових членів, фінансування терористичної діяльності, координації атак та проведення обмежених кібератак з метою залякування та пропаганди [100, С. 132-145]. Кіберзлочинні спільноти зацікавлені у фінансовій вигоді та можуть здійснювати атаки на фінансові установи, викрадати персональні дані, використовувати програми-вимагачі та продавати незаконно отриману інформацію. Хоча їхні дії не завжди мають політичне підґрунтя, вони можуть бути використані іншими акторами для досягнення власних цілей [94, С. 95-108]. Політичні екстремісти та хактивісти використовують кіберпростір для вираження своїх політичних поглядів, організації протестів, проведення кібератак на вебсайти урядових установ або компаній, що не відповідають їхнім переконанням, та поширення пропагандистських матеріалів [88, С. 119-132].

Стратегії недержавних угруповань у мережевих війнах часто є більш гнучкими та адаптивними, оскільки вони менш обтяжені бюрократичними процедурами. Вони можуть використовувати доступні інструменти та технології, швидко змінювати тактику та координувати свої дії через зашифровані канали зв’язку та соціальні мережі.

Окремі особи також можуть відігравати значну роль у мережевих війнах. Хактивісти-одинаки можуть здійснювати кібератаки з політичних або

ідеологічних мотивів, часто діючи самостійно або приєднуючись до тимчасових онлайн-кампаній. “Самотні вовки”, радикалізовані через інтернет, можуть здійснювати як фізичні, так і кібератаки, керуючись екстремістськими ідеями. Інсайдери, маючи доступ до внутрішніх інформаційних систем організацій або державних установ, можуть завдати значної шкоди, передаючи конфіденційну інформацію або здійснюючи саботаж.

Стратегії окремих осіб у мережевих війнах часто є непередбачуваними та залежать від їхньої мотивації, рівня технічної підготовки та доступних інструментів. Їхні дії можуть варіюватися від нескладних кібератак до участі у масштабних інформаційних кампаніях. В умовах широкого застосування засобів, стратегій і тактик мережевих війн приватними військовими компаніями (ПВК) та неурядовими організаціями (НУО) виявляється низка характерних особливостей, що якісно відрізняють їхні дії від традиційних військових конфліктів.

Ці особливості зумовлюють нові виклики для національної безпеки держав та потребують переосмислення підходів до їхнього забезпечення. Однією з ключових особливостей мережевих війн є можливість завдання шкоди без фізичного вторгнення на територію держави-супротивника. ПВК та НУО можуть здійснювати деструктивний вплив дистанційно, використовуючи інформаційний простір як головне поле бою. Це значно знижує ризик прямих військових зіткнень та пов’язаних із ними втрат, водночас зберігаючи потенціал для серйозного підриву стабільності [1].

Ще однією важливою характеристикою є раптовість та прихованість інформаційних атак. На відміну від традиційної військової підготовки, що потребує значного часу, інформаційні операції можуть розгортатися миттєво, без попередження. Прихована підготовка таких атак у цифровому просторі ускладнює їхнє своєчасне виявлення та нейтралізацію, що дає агресору значну перевагу. Крім того, жертва мережевої війни часто демонструє військову бездіяльність, оскільки традиційні механізми реагування, такі як мобілізація та розгортання сил, виявляються неефективними проти інформаційно-психологічного впливу. Держава може опинитися в стані паралічу, не маючи чіткого розуміння джерела загрози та

дієвих інструментів для протидії, що створює серйозні виклики для національної безпеки.

Мережеві війни відкривають широкі можливості для приватних військових компаній (ПВК) та недержавних організацій завдавати значної інформаційно-психологічної шкоди жертві без застосування військових дій чи зміни дипломатичних відносин між державами. Маніпулювання громадською думкою, поширення дезінформації, кібератаки на критичну інфраструктуру та психологічний тиск на населення можуть спричинити серйозні соціальні, економічні та політичні наслідки, не потребуючи формального оголошення війни або розриву дипломатичних зав’язків.

Однією з найбільших проблем є складність або навіть неможливість встановлення джерела інформаційно-психологічної агресії та точного визначення рівня загроз національній безпеці, реальних масштабів і цілей військової операції. Анонімність у цифровому просторі, використання складних мережевих структур та транскордонний характер інформаційних потоків значно ускладнюють атрибуцію атак. Це, у свою чергу, перешкоджає точній оцінці ризиків та розробці ефективних контрзаходів, створюючи серйозні виклики для національної безпеки держави-жертви.

Загалом, ведення мережевих війн різними акторами має свої особливості, зумовлені їхніми цілями, ресурсами та стратегіями. Держави володіють значними можливостями та здійснюють складні, скоординовані операції. Недержавні угруповання, хоча й мають обмежені ресурси, можуть бути високо мотивованими та здатними до асиметричних дій. Окремі особи можуть діяти самостійно або приєднуватися до інших суб’єктів, керуючись різними мотивами. Розуміння цих особливостей є критично важливим для розробки ефективних стратегій запобігання, виявлення та протидії загрозам у кіберпросторі.

5.4. Міжнародні правові та етичні аспекти ведення мережевих війн

Ведення мережевих війн, що охоплюють кібернетичні атаки та інформаційний вплив, породжує складний комплекс правових та етичних

питань, які потребують ретельного осмислення та регулювання. Існуючі міжнародні правові норми, розроблені переважно для регулювання збройних конфліктів у фізичному просторі, часто виявляються недостатніми або неоднозначними у застосуванні до дій у кіберпросторі та інформаційному середовищі. Окрім правових викликів, мережеві війни піднімають важливі етичні дилеми, пов’язані з відповідальністю за кібератаки, допустимістю інформаційного впливу на цивільне населення, захистом свободи слова та приватного життя в умовах конфлікту [80, С. 88-101].

Одним із ключових правових аспектів є застосування міжнародного гуманітарного права до кібернетичних атак, зокрема дотримання принципів розрізнення, пропорційності та запобігання надмірним стражданням цивільного населення. Визначення того, які кібератаки можуть вважатися збройним нападом, які об’єкти є військовими цілями в кіберпросторі, та як оцінювати пропорційність кібернетичних заходів у відповідь, залишаються предметом дискусій серед юристів-міжнародників [30, С. 152-165].

Іншою важливою правовою проблемою є питання суверенітету держав у кіберпросторі. Транскордонний характер кібератак ускладнює визначення юрисдикції та відповідальності держав за дії, що здійснюються з їхньої території або їхніми громадянами. Питання про те, чи є кібератака порушенням суверенітету іншої держави та за яких умов держава може вживати заходів у відповідь на кіберагресію, залишаються невирішеними на рівні міжнародного права [142, С. 129-142].

Правові аспекти інформаційної війни також є складними та суперечливими. Міжнародне право не містить чітких норм, що регулюють ведення інформаційних кампаній. Питання про допустимість пропаганди, дезінформації та психологічних операцій у контексті збройного конфлікту залишаються відкритими. Свобода вираження поглядів є одним із ключових прав людини, що забезпечує можливість відкрито висловлювати думки, обговорювати суспільно важливі питання та сприяти демократичному розвитку. Водночас, неконтрольоване поширення неправдивої або маніпулятивної інформації може

мати серйозні наслідки, зокрема дестабілізувати суспільство, підірвати довіру до державних інституцій, спричинити соціальну напругу та навіть загрожувати національній безпеці.

У сучасному інформаційному просторі, де технології дозволяють миттєво розповсюджувати контент на глобальному рівні, особливо важливо знайти баланс між захистом свободи слова та протидією дезінформації. Надмірне обмеження висловлювань може призвести до цензури та порушення демократичних принципів, тоді як відсутність контролю над фейковими новинами та пропагандою може сприяти маніпуляціям громадською думкою та загостренню конфліктів.

Ефективна стратегія має включати розвиток механізмів перевірки інформації, підвищення рівня медіаграмотності населення, відповідальність платформ за поширення контенту та створення правових норм, які запобігають зловживанням, не порушуючи при цьому основоположні права людини. Тільки комплексний підхід дозволить забезпечити відкритий інформаційний простір, що сприяє суспільному розвитку, водночас мінімізуючи ризики, пов’язані з дезінформацією [9].

Етичні аспекти ведення мережевих війн є не менш важливими. Однією з ключових етичних дилем є питання відповідальності за кібератаки. Анонімність та складність атрибуції в кіберпросторі ускладнюють визначення винних у проведенні деструктивних кібероперацій. Це породжує питання про відповідальність держав за дії недержавних акторів, що діють з їхньої території, а також про етичність використання “хакерів за наймом” [18, С. 98-111]. Іншою важливою етичною проблемою є допустимість інформаційного впливу на цивільне населення. Цілеспрямоване поширення дезінформації та пропаганди може мати серйозні психологічні наслідки для окремих осіб та суспільства в цілому, підриваючи довіру, викликаючи страх та ненависть. Етичні принципи вимагають захисту цивільного населення від навмисного інформаційного впливу, що може призвести до насильства та порушення прав людини [91, С. 115-128].

Захист свободи слова та приватного життя в умовах мережевих війн також є важливою етичною проблемою. Заходи, спрямовані на протидію інформаційним загрозам, не повинні призводити до необґрунтованого обмеження прав громадян на отримання та поширення інформації, а також на приватність їхнього спілкування в цифровому просторі [155]. Розробка правових та етичних норм, що регулюють ведення мережевих війн, є складним завданням, що вимагає міжнародного співробітництва та широкої дискусії з залученням юристів, політиків та представників громадянського суспільства. Важливо забезпечити гармонійний баланс між національною безпекою та захистом фундаментальних прав і свобод людини, враховуючи сучасні виклики, спричинені розвитком інформаційних технологій та їх використанням у конфліктах. Правові та етичні аспекти ведення мережевих війн є складними та багатогранними. Існуючі міжнародні правові норми потребують адаптації та уточнення для адекватного регулювання дій у кіберпросторі та інформаційному середовищі. Етичні принципи вимагають врахування наслідків мережевих війн для цивільного населення, захисту свободи слова та приватного життя.

5.5. Український аспект мережевих війн. Прогнозування та заходи протидії

Україна стала унікальним полем для вивчення та протидії мережевим війнам, оскільки з 2014 року, а особливо після повномасштабного вторгнення Росії у 2022 році, вона перебуває в епіцентрі безпрецедентної за масштабами та інтенсивністю гібридної агресії. Цей досвід дає цінний матеріал для глибокого розуміння природи сучасних мережевих загроз, їхньої динаміки, а також для розробки та вдосконалення ефективних механізмів протидії, що є критично важливим для національної безпеки.

Україна демонструє непересічну здатність до стратегічної адаптації у протистоянні мережевим загрозам. Російська Федерація активно застосовує весь спектр гібридних інструментів, системно поєднуючи кібератаки, масштабні

дезінформаційні кампанії, економічний тиск та використання нерегулярних військових формувань. У відповідь на ці комплексні виклики Україна не лише розвиває власні механізми захисту, а й проактивно діє в інформаційному та кіберпросторі.

У площині мережецентричної війни та технологічної переваги Збройні Сили України активно інтегрують елементи, що спрямовані на досягнення інформаційної переваги через об'єднання військових об'єктів у єдину мережу. Яскравими прикладами є широке використання цифрової системи управління військами "Delta", безпілотних літальних апаратів (БПЛА), супутникового зв'язку "Starlink" та інших тактичних систем, як-от "Кропива". Така інтеграція дозволяє значно скорочувати цикл "виявлення – прийняття рішення – дія", що надає вирішальну перевагу на полі бою завдяки підвищенню швидкості реагування та ефективності ведення бойових дій. Україна також активно застосовує принципи операцій базових ефектів (ОБЕ), комбінуючи різні інструменти впливу для досягнення бажаних політичних, економічних та психологічних наслідків. Це проявляється у поєднанні міжнародних санкцій проти агресора, активних публічних звернень до світової спільноти, дипломатичного тиску та обмежених, але ефективних військових дій для досягнення стратегічних цілей. Наприклад, міжнародна ізоляція Російської Федерації та значна військово-технічна допомога Україні є прямими наслідками скоординованих інформаційних та дипломатичних операцій, спрямованих на зміну сприйняття та поведінки ключових акторів на міжнародній арені.

У сфері інформаційної війни та стратегічних комунікацій Російська Федерація системно використовує дезінформацію, пропаганду та психологічний тиск для дестабілізації українського суспільства, деморалізації військ та підриву довіри до державних інститутів. У відповідь Україна розгорнула масштабні контрпропагандистські кампанії, активно використовуючи власні медіа-ресурси, соціальні мережі та міжнародні платформи. Ключову роль у цьому відіграє Центр протидії дезінформації при РНБО України, який оперативно забезпечує виявлення, аналіз та ефективну протидію дезінформації, системно бореться з

ворожою пропагандою та деструктивними інформаційними впливами. Розвиток стратегічних комунікацій є пріоритетом, адже вони визначені у Воєнній доктрині України як скоординоване використання повного спектру комунікативних можливостей держави для формування позитивного іміджу, підтримки єдності суспільства та забезпечення національної безпеки.

Щодо кібервійни та кіберстійкості, Україна перебуває під постійними та інтенсивними кібератаками, більшість з яких пов'язані з російськими хакерськими групами, що підтримуються державою. Проте, незважаючи на безпрецедентний тиск, Україна демонструє високий рівень кіберстійкості та ефективності у захисті своїх систем. Активно діє ІТ-армія України, яка є унікальним прикладом самоорганізації громадянського суспільства у кібервійні, завдаючи значних збитків ворожим інформаційним ресурсам та підриваючи їхню інфраструктур. Заходи щодо захисту критичної інфраструктури, зокрема енергетичного сектору, фінансових установ та виборчих систем, від зовнішнього втручання постійно вдосконалюються, адаптуючись до нових загроз та тактик противника [45, С. 128-141].

Досвід України переконливо підтверджує, що мережева війна є поєднанням відкритої військової агресії з економічним тиском, кібератаками, інформаційними операціями та спробами внутрішньополітичної дестабілізації. Це вимагає від держави не лише традиційного військового захисту, а й формування комплексної та багатошарової системи національної безпеки, що інтегрує військові, кібернетичні, інформаційні, економічні та соціальні компоненти, спрямовані на забезпечення стійкості суспільства та функціонування держави в умовах постійного тиску. Мережеві війни продовжуватимуть еволюціонувати, а їхня інтенсивність та складність зростатимуть, стаючи ще більш інтегрованими та технологічно залежними. Можна виділити кілька ключових тенденцій, які визначатимуть їхній подальший розвиток.

По-перше, очікується посилення інтеграції інструментів, що призведе до ще більшого стирання меж між традиційними військовими діями, кібератаками,

інформаційними та психологічними операціями. Операції ставатимуть все більш синхронізованими, а синергетичний ефект від їх комбінації значно зростатиме, створюючи багатовимірний тиск на противника. По-друге, ключову роль у мережевих війнах майбутнього відіграватимуть штучний інтелект (ШІ) та “великі дані” (Big Data). ШІ стане незамінним інструментом для автоматизації дезінформаційних кампаній, створення глибоких фейків (deepfakes), які будуть майже невідрізними від реальності, а також для аналізу величезних обсягів даних з метою виявлення вразливостей та прогнозування поведінки цільової аудиторії. Big Data слугуватиме основою для цільового впливу, дозволяючи створювати високоперсоналізовані інформаційні кампанії, що враховують психологічні профілі та вразливості окремих груп населення.

По-третє, відбудеться розширення сфери впливу мережевих війн на нові домени. Це включатиме використання інтернету речей як потенційної поверхні для кібератак, а також більш активний вплив на глобальні фінансові системи та логістичні ланцюги, що може спричинити значні економічні збитки та соціальну напругу. По-четверте, прогнозується зростання ролі недержавних акторів. Окрім державних хакерських груп та спецслужб, значну роль відіграватимуть недержавні угруповання, такі як хакерські групи, волонтерські кіберрухи та проксі-сили, що діють більш гнучко та децентралізовано, спираючись на ідеологічну мотивацію та власні технологічні можливості, що ускладнить ідентифікацію джерела атак. Нарешті, концепція “посткібербезпеки” стане домінуючою. Акцент зміщуватиметься з простого відбиття атак на проактивні заходи, постійне прогнозування загроз, швидку адаптацію та здатність до відновлення систем після інцидентів, визнаючи, що абсолютної кібербезпеки досягти неможливо [148, С. 288].

Для ефективної протидії мережевим загрозам та забезпечення національної стійкості Україна повинна продовжувати розвивати комплексний підхід, що охоплює кілька ключових напрямків, які потребують постійного вдосконалення та синхронізації. Наріжним каменем є посилення національної кібербезпеки. Це включає безперервний захист критичної інфраструктури через впровадження

багаторівневих систем безпеки, використання передових технологій захисту, таких як хмарні рішення для підвищення гнучкості та стійкості, а також постійний моніторинг загроз. Важливим є підвищення кіберстійкості шляхом регулярного проведення аудитів, тестів на проникнення та комплексних кібернавчань для державних органів та приватного сектору. Окрім того, необхідним є розвиток кібервійськ та спеціалізованих підрозділів, що потребує значних інвестицій у підготовку висококваліфікованих фахівців з національної безпеки, здатних протистояти складним та еволюціонуючим загрозам.

Паралельно з цим, необхідно постійно удосконалювати систему стратегічних комунікацій та інформаційної безпеки. Це вимагає проактивної протидії дезінформації шляхом розвитку спроможностей Центру протидії дезінформації, розширення його міжнародного співробітництва та використання інноваційних технологій для виявлення та оперативного спростування фейків. Ключовим є формування проукраїнського наративу, що передбачає активне просування об’єктивної інформації про Україну у світі, зміцнення міжнародної підтримки та ефективну нейтралізацію ворожих інформаційних впливів. Не менш важливим є підвищення медіаграмотності населення через впровадження освітніх програм, просвітницьких кампаній та проектів, спрямованих на розвиток критичного мислення та здатності громадян розрізняти достовірну інформацію від маніпуляцій [86, С. 180].

Також суттєвою є адаптація військових доктрин та підходів до реалій мережевих війн. Це передбачає інтеграцію мережевих аспектів у стратегічне планування, перегляд військових доктрин з урахуванням домінуючої ролі інформаційного та кіберпростору, а також принципів ОБЕ. Необхідним є розвиток сил оборони та безпеки, що означає цілеспрямовану підготовку особового складу до ведення бойових дій у мережевому середовищі, оволодіння новітніми технологіями та методами гібридного протиборства.

Особлива увага має приділятися міжнародному співробітництву та правовим рамкам. Україна повинна активно брати участь у розробці міжнародних норм та правил поведінки у кіберпросторі, що є життєво

необхідним для притягнення до відповідальності за кіберзлочини та кіберагресію на державному рівні[141, С. 200]. Також ключовим є обмін досвідом та посилення співпраці з міжнародними партнерами у сфері кібербезпеки, включаючи обмін інформацією про загрози та передовими практиками протидії.

Нарешті, законодавче забезпечення та інституційний розвиток є фундаментом для всіх вищезазначених заходів. Це вимагає удосконалення законодавства, приведення національного законодавства у відповідність до сучасних викликів мережевих війн, зокрема у сфері національного спротиву [3]. Також необхідно забезпечити ефективну координацію зусиль між усіма суб'єктами національної безпеки, включаючи державні органи, приватний сектор, академічну спільноту та громадянське суспільство, для створення єдиного та стійкого фронту проти гібридних загроз.

Таким чином, у контексті мережевих війн, майбутнє належить тим, хто володіє не лише традиційною зброєю, а й знаннями та технологіями для ефективної діяльності в інформаційному просторі. Для України, яка продовжує протистояти повномасштабній агресії, здатність до швидкої адаптації, постійного прогнозування та ефективної протидії мережевим загрозам є запорукою національної безпеки та, зрештою, перемоги.

Висновки до розділу 5

У сучасному безпековому середовищі мережеві війни постають як мультивимірне та гібридне явище, що суттєво впливає на національну безпеку, суверенітет держав і глобальну стабільність. Аналіз цього явища свідчить про інтеграцію інформаційно-психологічних, кібернетичних, економічних та технологічних компонентів у рамках єдиної стратегічної матриці впливу, яку умовно визначаємо як мережеву агресію.

Гібридна війна, як інтегральна форма мережевої агресії, вирізняється складною структурою, де класичні форми збройного протистояння поєднуються із кібернападами, дезінформаційними кампаніями та економічним тиском. Саме

така багатовекторність унеможливлює застосування традиційних моделей захисту та вимагає нових підходів до виявлення, прогнозування і нейтралізації загроз.

Технологічна складова мережевих війн базується на використанні організованих мережевих структур, високоточних інформаційних систем, програмно-апаратних засобів атак та штучного інтелекту, що робить атаки надзвичайно точними та динамічними. Мережеві платформи — від соціальних мереж до автономних бот-мереж — трансформуються у інструменти інформаційного впливу, маніпуляції свідомістю, збору даних і глушіння альтернативних джерел інформації.

Особливу увагу слід приділити різноманітності акторів мережевих війн. Поряд із державами, які мають високотехнологічні кіберпідрозділи, активну участь у війні беруть недержавні структури: хакерські угруповання, транснаціональні корпорації, навіть окремі фахівці, здатні ініціювати атаки на критичну інфраструктуру. Це посилює невизначеність і ускладнює атрибуцію атак.

Міжнародно-правова база щодо ведення мережевих війн усе ще знаходиться на стадії формування. Існуючі норми не враховують багатьох аспектів кіберзагроз, а етичні стандарти ведення війни в онлайн-просторі часто ігноруються або навмисно обходяться. Це потребує створення нових універсальних підходів до міжнародного регулювання та відповідальності сторін.

Україна як одна з ключових цілей мережевої агресії Росії опинилася у авангарді захисту в інформаційно-кіберпросторовому вимірі. Досвід останніх років засвідчує, що ефективна протидія можлива лише за умови поєднання стратегічного прогнозування, державного та громадського партнерства, технологічного вдосконалення засобів безпеки та постійного оновлення нормативної бази. Мережеві війни сьогодення є не лише формою конфлікту, а й дзеркалом глибоких трансформацій у сфері глобальної безпеки, де інформація, швидкість та мобільність стали ключовими ресурсами як оборони, так і нападу.

ВИСНОВКИ

Проведене наукове дослідження присвячене всебічному та поглибленому аналізу феномену мережевих війн як якісно нового, багатогранного та визначального виду сучасних воєнних дій. У роботі здійснено комплексне теоретичне узагальнення, що охоплює розкриття сутності, ключових ознак, специфічних особливостей прояву та різноманітного інструментарію мережевих війн. Окрім того, детально розглянуто їхній зростаючий вплив на фундаментальну трансформацію збройних конфліктів у сучасному, динамічному світі, що характеризується стрімким розвитком технологій та зміною геополітичних ландшафтів. В ході дослідження був проведений комплексномий та системномий аналіз мережевої війни як особливої форми конфлікту в умовах сучасної глобалізованої взаємодії. Автором застосовано сучасні методи наукового пізнання, що ґрунтуються на міждисциплінарному підході.

У межах дослідження здійснено комплексний аналіз взаємозв’язків і меж між суміжними категоріями: “мережева війна”, “мережецентрична війна”, “операції базових ефектів”, “інформаційна війна”, “кібервійна”, “гібридна війна”. Проведене розмежування дозволяє уникати термінологічної плутанини та поглиблює розуміння природи кожного з феноменів. Дослідження формує теоретичну базу для подальших наукових досліджень у сфері безпеки, стратегічних комунікацій та воєнної науки. Також було здійснено всебічне узагальнення результатів дослідження мережевих війн в умовах сучасності, простежено еволюцію концепції мережевих війн від перших теоретичних розробок до їхнього активного практичного застосування у збройних конфліктах.

У розділі 1 було ґрунтовно обґрунтовано, що мережеві війни є закономірним результатом глибокої та всеосяжної трансформації традиційних способів і методів ведення воєн, яка безпосередньо зумовлена безпрецедентним розвитком інформаційних технологій та формуванням глобального мережевого суспільства. Детально визначено сутність фундаментального поняття “мережа”

та розкрито специфічні особливості його застосування у військовій сфері, що якісно відрізняються від його використання в інших галузях. Ретельно проаналізовано сутність, ключові ознаки та характерні особливості прояву мережевих війн, включаючи їхню притаманну асиметричність, складну багатовимірність, можливість дистанційного впливу та вирішальну роль активного використання інформаційного простору як основного поля бою. Розглянуто концепцію “мережецентричної війни” як якісно новий та революційний етап розвитку військової стратегії, що передбачає глибоку інтеграцію всіх елементів військової та невійськової могутності держави в єдину, гнучку та ефективну інформаційну мережу для досягнення вирішальної стратегічної переваги над противником. Нарешті, було чітко визначено основні сфери протистояння та потенційні театри мережевих воєн, що охоплюють кіберпростір, інформаційний простір у всій його повноті, соціальні мережі як інструмент впливу на інфраструктуру держав.

У розділі 2 було проведено детальне дослідження операційна базових ефектів (ОБЕ) як надзвичайно важливого та дієвого інструменту впливу в контексті мережевих війн, з особливим акцентом на їхнє застосування в інформаційному просторі. Ретельно розкрито концептуальні засади ОБЕ, їхню фундаментальну орієнтацію на досягнення конкретних стратегічних ефектів шляхом скоординованого та комплексного застосування всього спектру доступних інструментів впливу. Детально проаналізовано ключові інструменти реалізації ОБЕ, включаючи масштабні інформаційні кампанії, різноманітні економічні санкції, складні кібератаки, багатовекторні дипломатичні впливи та високоточні спеціальні операції, при цьому було підкреслено критичну важливість їхнього синергетичного та комбінованого застосування для максимізації ефективності. Окрім того, було розглянуто основні механізми оцінки ефективності ОБЕ, що включають кількісний та якісний аналіз, системний аналіз та залучення експертних оцінок, а також наведено конкретні приклади їхнього успішного застосування в сучасних збройних конфліктах, особливо в контексті досягнення асиметричних впливів та нелінійних результатів.

У розділі 3 було проведено глибокий аналіз інформаційної війни як ключового та всеосяжного феномену цифрового суспільства, що є невід'ємною та критично важливою складовою сучасних мережевих воєн. Ретельно розкрито її сутність, основні стратегії, що активно застосовуються окремими провідними країнами світу, та її значний вплив як вагомого чинника загрози національній безпеці держав. Детально досліджено інформаційний вплив як складну технологію ведення бойових дій, що має на меті маніпулювання свідомістю як військово-політичного керівництва противника, так і широких верств його населення.

У розділі 4 кібервійна була всебічно розглянута як окремий, але надзвичайно важливий вид та потужний інструмент мережевих воєн. Детально проаналізовано різні критично важливі аспекти кіберпротиборства, включаючи кібершпигунство з метою отримання стратегічно важливої інформації, кіберсаботаж, спрямований на руйнування інфраструктури, масштабні дезінформаційні кампанії, націлені на цілеспрямоване маніпулювання інформацією, руйнівні атаки на критично важливу інфраструктуру держав та кібертероризм як злочинне використання кіберпростору терористичними організаціями. Чітко визначено їхню ключову роль та місце у загальній стратегії ведення мережевих воєн.

У розділі 5 було проведено комплексне дослідження впливу гібридних війн на глибоку трансформацію сучасних збройних конфліктів. Детально розкрито сутність, характерні ознаки та специфічні особливості гібридних війн як складного поєднання військових і невійськових інструментів впливу, спрямованих на досягнення стратегічних цілей. Ретельно проаналізовано різноманітні інструменти та методи ведення гібридних воєн, включаючи військові, економічні, інформаційні та політико-дипломатичні засоби. Розглянуто основні напрями ефективної протидії гібридним загрозам, включаючи всебічну розбудову стійкості держави та суспільства до інформаційних впливів, постійне удосконалення системи кібербезпеки, розвиток спеціальних військових спроможностей для протидії асиметричним загрозам та активну міжнародну співпрацю на всіх рівнях.

Таким чином, в науковій роботі здійснено: систематизацію існуючих наукових підходів до розуміння мережевої війни; уточнення структури, механізмів і логіки ведення мережевих війн; виокремлення ключових чинників і суб'єктів впливу;

поглиблено наукове розуміння феномену мережевих війн, оцінено його вплив на національну безпеку та визначено шляхи ефективної протидії в умовах сучасності; детально розглянуто технологічні основи та різноманітний інструментарій мережевих війн, а також специфічні особливості їхнього ведення різними типами акторів, включаючи держави, недержавні збройні угруповання та окремі особи; проаналізовано складні міжнародні правові та етичні аспекти ведення мережевих війн; проведено аналіз особливостей сучасних викликів для національної безпеки в умовах повномасштабного вторгнення Російської Федерації в Україну; визначено загальний сучасний перебіг мережевих війн та ключові тенденції їхнього подальшого розвитку, а також розглянуто перспективні підходи до розробки ефективних методів протидії цим новітнім загрозам.

Результати проведеного комплексного дослідження дозволили дійти таких загальних висновків:

1. Мережеві війни являють собою якісно новий та фундаментально відмінний вид збройних конфліктів, що характеризується розмиванням чітких меж між станом миру та війни, інтегрованим поєднанням військових і невійськових інструментів впливу, притаманною асиметричністю, складною багатовимірністю та домінуючою роллю інформаційної складової у досягненні стратегічних цілей.

2. Концепція “мережецентричної війни” відображає прогресивну еволюцію військової стратегії в умовах інформаційного суспільства, передбачаючи глибоку інтеграцію всіх елементів військової організації в єдину, гнучку, стійку та високоефективну інформаційну мережу для забезпечення вирішальної стратегічної переваги над противником.

3. Операції базових ефектів (ОБЕ) є надзвичайно важливим та дієвим інструментом реалізації загальної стратегії мережевих війн, особливо в інформаційному просторі, надаючи можливість досягати бажаних стратегічних ефектів шляхом скоординованого та синергетичного застосування широкого спектру різноманітних засобів впливу на ключові вузли та зв’язки противника.

4. Інформаційна війна та кібервійна є критично важливими та невід’ємними складовими сучасних мережевих воєн, що активно розгортаються у віртуальному та інформаційному просторах і мають значний та деструктивний вплив на

свідомість окремих людей та цілих суспільств, стабільне функціонування критично важливої інфраструктури держав та їхню національну безпеку в цілому.

5. Гібридні війни є практичною та найбільш інтегральною реалізацією концепції мережевих війн у сучасному світі, ефективно поєднуючи військові, економічні, інформаційні та політико-дипломатичні інструменти для досягнення стратегічних цілей без формального оголошення війни та відкритого широкомасштабного військового вторгнення.

6. Ефективна протидія складним та багатогранним мережевим і гібридним загрозам вимагає розробки та реалізації комплексного, системного та скоординованого підходу, що включає всебічну розбудову стійкості держави та суспільства до ворожих інформаційних впливів, постійне удосконалення системи кібербезпеки на всіх рівнях, активний розвиток спеціальних військових спроможностей для ефективної протидії асиметричним загрозам та налагодження тісної міжнародної співпраці на двосторонній та багатосторонній основі.

Проведене наукове дослідження має значне теоретичне та практичне значення для широкого кола фахівців у галузі національної безпеки, військової справи, міжнародних відносин, інформаційних технологій та державного управління. Отримані в ході дослідження результати можуть бути ефективно використані для розробки прогресивних стратегій та доктрин протидії сучасним воєнним загрозам, постійного удосконалення комплексних систем інформаційної та кібербезпеки, а також для якісної підготовки висококваліфікованих фахівців у відповідних критично важливих галузях. Подальший глибокий розвиток теоретичних засад та практичних методів протидії мережевим війнам є нагальним та вкрай важливим завданням у контексті забезпечення національної безпеки України, зміцнення регіональної та глобальної стабільності в умовах постійно зростаючої інформаційної залежності сучасного світу та складної геополітичної напруженості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Нормативно-правові акти:

1. Закон України “Про боротьбу з тероризмом” від 19 березня 2003 року № 638-IV. Режим доступу: https://zakon.rada.gov.ua/laws/main/638-iv (дата звернення: 11.05.2025).

2. Закон України “Про національну безпеку України” від 21 червня 2018 року № 2469-VIII. Режим доступу: https://zakon.rada.gov.ua/laws/main/2469-viii (дата звернення: 10.05.2025).

3. Закон України “Про національну безпеку України” від 21 червня 2018 року № 2469-VIII. Режим доступу: https://zakon.rada.gov.ua/laws/main/2469-viii (дата звернення: 11.05.2025).

4. Закон України “Про основні засади забезпечення кібербезпеки України” від 5 липня 2017 року № 2163-VIII. Режим доступу: https://zakon.rada.gov.ua/laws/main/2163-viii (дата звернення: 11.05.2025).

5. Закон України “Про розвідку” від 22 березня 2001 року № 2331-III. Режим доступу: https://zakon.rada.gov.ua/laws/main/2331-iii (дата звернення: 10.05.2025).

6. Закон України “Про санкції” від 14 серпня 2014 року № 1644-VII. Режим доступу: https://zakon.rada.gov.ua/laws/main/1644-vii (дата звернення: 11.05.2025).

7. Закон України “Про боротьбу з тероризмом” від 20.03.2003 № 638-IV // Відомості Верховної Ради України. – 2003. – № 25. – ст. 180.

8. Закон України “Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері” від 05.07.2018 № 2504-VIII // Відомості Верховної Ради. – 2018. – № 31. – ст. 241.

9. Закон України “Про інформацію” від 02.10.1992 № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – ст. 650.

10. Закон України “Про критичну інфраструктуру” від 17.08.2021 № 1681-IX // Відомості Верховної Ради. – 2021. – № 41. – ст. 344.

11. Закон України “Про оборону України” від 06.12.1991 № 1932-XII // Відомості Верховної Ради України. – 1992. – № 9. – ст. 106.

Література:

12. Alberts D. S., Hayes R. E. Understanding Command and Control. — Washington, DC : CCRP Publication, 2006. — 222 p.

13. Arquilla, J., Ronfeldt D. Cyberwar is Coming! — Santa Monica : RAND Corporation, 1993. — 38 p.

14. Atkinson R. Crusade: The Untold Story of the Persian Gulf War. — Boston : Houghton Mifflin, 1993. — 575 p.

15. Brzezinski, Z. The Grand Chessboard: American Primacy and Its Geostrategic Imperatives. — New York : Basic Books, 1997.

16. Cebrowski A. K., Garstka J. J. Network-centric warfare: Its origin and future // Proceedings of the U.S. Naval Institute. – 1998. – Vol. 124, No. 1. – P. 103-116.

17. Danilyan O., Dzoban A. Existence-network dimension of information security in modern society // Схід. Аналітично-інформаційний журнал. — 2021. — Т. 1, № 1. — С. 13.

18. Deibert R. J. Black Code: Surveillance, Privacy, and the Dark Side of the Internet. — Toronto : McClelland & Stewart, 2013. — 336 p.

19. Denning D. E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Political Action. — Thousand Oaks : Sage Publications, 2000. — 32 p.

20. Drezner D. W. Sanctions Tell Tales: The Impact of Economic Coercion on International Relations // International Security. — 2010. — Vol. 35, No. 1 (Summer). — P. 96–137.

21. Florini E., Goodman S. E., Best L. Cyber Norms: Charting a Course Toward Responsible State Behavior in Cyberspace. — Oxford : Oxford University Press, 2020. — 320 p.

22. Hoffman F. G. Hybrid Warfare and Challenges // Potomac Institute for Policy Studies. — 2007.

23. Huntington, S. P. The Clash of Civilizations and the Remaking of World Order. — New York : Simon & Schuster, 1996. — 367 p.

24. Jones S. G. The ISIS Insurgency: The Rise of the Islamic State and Its Dangerous Legacy. — Washington, DC : Center for Strategic and International Studies, 2016. — P. 114–128.

25. O'Neil C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. — New York : Crown, 2016. — 259 p.

26. Raz Z. The Logic of Israel's "Gray Zone" Warfare Against Iran. The Institute for National Security Studies. INSS Insight No. 1475, 2021. P. 81-94.

27. Record J. Dark Victory: America's Second War Against Iraq. — Annapolis : Naval Institute Press, 2004. — 203 p.

28. Rid T. Cyber War Will Not Take Place. — Oxford : Oxford University Press, 2013. — 218 p.

29. Roberts M. Censored: Distraction and Diversion Inside China's Great Firewall. — Princeton : Princeton University Press, 2018. — 288 p.

30. Schmitt M. N. (Ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. — Cambridge : Cambridge University Press, 2017. — 596 p.

31. Singer P. W., Brooking E. T. LikeWar: The Weaponization of Social Media. — Boston : Houghton Mifflin Harcourt, 2018. — 416 p.

32. Valeriano B., Maness R. C. Cyber War Versus Cyber Realism: Theory and Practice // Strategic Studies Quarterly. — 2014. — Vol. 8, No. 1 (Spring). — P. 43–70.

33. Van Dijck J., Poell T., De Waal M. The Platform Society: Public and Private Interests in Contested Online Spaces. — Oxford: Oxford University Press, 2018. — 240 p.

34. Woodward B. Plan of Attack. — New York : Simon & Schuster, 2004. — 467 p.

35. Абальмаз О. Є. Російська гібридна агресія проти України: військовий аспект // Вісник Національної академії сухопутних військ імені гетьмана Петра Сагайдачного. 2016. № 1(1). С. 165-173.

36. Алещенко В. Інформаційно-психологічний вплив у ході збройної боротьби // Вісник Київськогонаціонального університету імені Тараса Шевченка. Військово-спеціальні науки. 2018. Вип. 1. С. 6-10.

37. Алєксєєв О. О. Мережево-центрична війна як концепція ведення бойових дій у XXI столітті // Вісник Національного університету оборони України імені Івана Черняховського. – 2019. – № 2(49). – С. 35-48.

38. Альбертс Д. С., Гарстка Дж. П. Розуміння інформаційної епохи: війна, злочинність та суспільство. – Вашингтон: DOD Command and Control Research Program, 2002. – 312 с.

39. Антоненко О. М. Кібертероризм як сучасна загроза національній та міжнародній безпеці // Право і суспільство. – 2020. – № 6. – С. 95-108.

40. Аркілла Дж., Ронфельдт Д. Мережі та мережеві війни: майбутнє терору, злочину і збройної боротьби. – Київ: Видавничий дім “Києво-Могилянська академія”, 2007. – 368 с.

41. Банах В. В. Методи резервного копіювання та відновлення інформації в умовах кіберзагроз // Захист інформації. – 2019. – № 3. – С. 76-89.

42. Банах В. В. Моніторинг та аналіз комп’ютерних мереж для виявлення кібератак // Вісник Національного університету “Львівська політехніка”. Серія “Інформаційна безпека”. – 2019. – № 914. – С. 62-75.

43. Бедрицький Є. В. Тероризм як форма гібридної війни: сутність та особливості // Науковий вісник Національної академії внутрішніх справ. 2018. № 4(109). С. 245-257.

44. Богданов А. В. Оцінка ефективності військових операцій: теоретичні та практичні аспекти. — Київ : Академія, 2022. — 208 с.

45. Бурячок В. Л., Дзюбановська Н. В., Ревунов Я. О. Кібербезпека критичної інфраструктури: навчальний посібник. — Київ : КПІ ім. Ігоря Сікорського, 2017. — 212 с.

46. ван Кревельд М. Трансформація війни / пер. з англ. — Львів : Літопис, 2003. — 272 с.

47. Війни інформаційної епохи: міждисциплінарний дискурс : монографія / за ред. В. А. Кротюка. — Харків : ФОП Федорко М. Ю., 2021. — 558 с.

48. Воронцов В. А. Психологічні операції в контексті операцій базових ефектів. Військово-науковий вісник. 2021. № 2(35). С. 91-105.

49. Воронцов В. А. Роль недержавних акторів у гібридних війнах // Військово-науковий вісник. 2021. № 2(35). С. 100-114.

50. Голубєв В. О. Інформаційна війна як інструмент геополітичного впливу // Держава і право. Юридичні і політичні науки. – 2017. – Вип. 77. – С. 58-71.

51. Голубєв В. О. Суб'єкти інформаційної війни: класифікація та особливості діяльності // Держава і право. Юридичні і політичні науки. – 2016. – Вип. 74. – С. 42-55.

52. Голубєв С. О. Синергія інструментів впливу в операціях базових ефектів. — Київ : Сфера, 2021. — 192 с.

53. Гончаров В. М. Інформаційні операції в контексті гібридної війни // Інформаційна безпека людини, суспільства, держави. – 2020. – № 1(29). – С. 78-91.

54. Гончаров В. М. Комплексний підхід до захисту критичної інформаційної інфраструктури // Інформаційна безпека людини, суспільства, держави. – 2021. – № 2(32). – С. 159-172.

55. Гончаров В. М. Сучасні засоби захисту інформації від кіберзагроз // Інформаційна безпека людини, суспільства, держави. – 2021. – № 1(31). – С. 132-145.

56. Горбулін В. П. Гібридна війна як інструмент російської геополітики // Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. — Київ : НІСД, 2017. — С. 32–45.

57. Гречаний М. М. Аналіз великих даних у контексті інформаційної війни // Безпека інформації. – 2020. – № 3. – С. 92-105.

58. Гречанінов В. В. Мережеві війни як феномен сучасної геополітики // Вісник Національного університету "Львівська політехніка". Серія: Політологія. – 2016. – № 846. – С. 43-53.

59. Данильян О. Г. Інформаційна війна: теоретико-методологічні засади дослідження // Вісник Харківського національного університету імені В. Н. Каразіна. Серія “Соціологічні дослідження сучасного суспільства: методологія, теорія, методи”. 1 – 2017. – № 39. – С. 89-109.

60. Дзьобань О. П., Куц М. М. Інформаційна безпека держави в умовах гібридної війни: монографія. – Харків: Право, 2018. – 336 с.

61. Дзьобань О. П., Куц М. М. Кібернетичне стримування як елемент стратегії національної безпеки // Стратегічні пріоритети. – 2020. – № 3(57). – С. 136-149.

62. Жирохов М. С. Війна на Донбасі. — Харків : Фоліо, 2017. — 320 с.

63. Журавель В. П. Штучний інтелект як інструмент ведення та протидії мережевим війнам // Інформаційні технології та кібербезпека. – 2023. – № 2. – С. 109-122.

64. Загородній В. К., Мельник С. В. Гібридна війна як феномен XXI століття. — Львів : Видавництво Львівського національного університету, 2020. — 248 с.

65. Загородній В. К., Мельник С. В. Операції, орієнтовані на ефект: теоретичні аспекти. — Львів : Видавництво Львівського національного університету, 2020. — 148 с.

66. Зайцев Є. В. Аналіз вразливостей програмного забезпечення як елемент кіберрозвідки // Системи обробки інформації. – 2019. – № 7(162). – С. 115-128.

67. Зайцев С. В. Спеціальні операції в контексті гібридної війни. — Львів : Видавництво Національної академії сухопутних військ, 2023. — 168 с.

68. Закутній О. В. Операції введення в оману у військовій справі: історичний досвід та сучасні тенденції // Воєнна історія. – 2019. – № 1-2(97-98). – С. 95-108.

69. Зіссерман О. М. Інформаційна війна: теоретичні засади та практичні аспекти. — Київ : ДУТ, 2017. — 204 с.

70. Іванов І. С. Асиметричні методи ведення війни в гібридних конфліктах // Вісник Національної академії оборони України. 2023. № 1(27). С. 70-84.

71. Іванов І. С. Впровадження концепції операцій базових ефектів у Збройних Силах України: сучасний стан та перспективи. Вісник Національної академії оборони України. 2023. № 1(27). С. 8-17.

72. Інформаційні війни: з історії конфліктів XX століття. — Київ : Видавничий дім "Києво-Могилянська академія", 2000. — 312 с.

73. Карпенко С. І. Застосування штучного інтелекту в аналізі військової інформації. Інформаційні технології та безпека. 2023. № 4(12). С. 168-181.

74. Кастельс М. Мережеве суспільство. – Київ: Видавничий дім "Києво-Могилянська академія", 2000. – 604 с.

75. Клаузевіц К. фон. Принципи ведення війни / пер. з нім. — Київ : Професіонал, 2023. — 274 с.

76. Князев В. В. Кібертероризм як складова гібридної війни // Вісник Національної академії правових наук України. – 2016. – № 3. – С. 67-81.

77. Коваленко О. О. Кіберзагрози критичній інфраструктурі України та шляхи їх нейтралізації // Інформаційні технології та безпека. – 2019. – № 3(6). – С. 95-108.

78. Коваленко О. П. Багатовимірність сучасних збройних конфліктів. — Київ : Основа, 2019. — 248 с.

79. Ковальчук В. В. Міжнародно-правові аспекти боротьби з кібертероризмом // Вісник Національної академії правових наук України. – 2021. – № 1(120). – С. 102-115.

80. Ковальчук В. В. Міжнародно-правові проблеми регулювання кіберпростору в умовах збройних конфліктів // Вісник Національної академії правових наук України. – 2020. – № 2(121). – С. 88-101.

81. Ковальчук О. О. Асиметричні дії в гібридній війні: український досвід // Військова думка України. — 2020. — № 2. — С. 47–60.

82. Козак О. П. Кібернетична безпека України в умовах гібридної війни // Безпека інформації. 2019. № 2(25). С. 192-201.

83. Кормич Б. А. Кіберзлочинність: кримінологічна характеристика, детермінація та запобігання. — Одеса : Одеський юридичний інститут Національного університету внутрішніх справ, 2015. — 304 с.

84. Корнієнко М. В. Вплив соціальних мереж на сучасні збройні конфлікти // Вісник Національної академії Державної прикордонної служби України. 2023. № 4(49). С. 135-148.

85. Король О. Г. Війни шостого покоління: теоретичні засади та особливості прояву // Стратегічні пріоритети. – 2020. – № 4(58). – С. 98-111.

86. Король О. Г. Контроль доступу як елемент системи кібербезпеки // Безпека інформації. – 2018. – № 4. – С. 119-132.

87. Король О. Г. Управління ризиками кібербезпеки критичної інфраструктури. — Львів : Магнолія 2006, 2018. — 288 с.

88. Король О. Г. Хактивізм як форма політичної активності в кіберпросторі // Безпека інформації. – 2017. – № 2. – С. 119-132.

89. Корченко О. Г. Кібербезпека критичної інфраструктури: навчальний посібник. — Київ : Національний авіаційний університет, 2016. — 352 с.

90. Корченко О. Г. оціальна інженерія в кіберпросторі: загрози та протидія. — Київ : Академперіодика НАН України, 2016. — 288 с.

91. Костенко Є. Г. Етичні аспекти інформаційного впливу в умовах гібридної війни // Філософські проблеми сучасності. – 2018. – Вип. 25. – С. 115-128.

92. Костенко Є. Г. Маніпулювання суспільною свідомістю в цифровому просторі: соціально-психологічний аспект. Харків: Видавництво “Друкарня Мадрид”, 2017. – 184 с.

93. Кравець А. П. Психологічні операції як елемент операцій базових ефектів // Вісник Національної академії державної прикордонної служби України. 2022. № 3(45). С. 78-90.

94. Кривов’яз О. В. Кіберзлочинність як загроза національній безпеці України // Право та державне управління. – 2020. – № 1. – С. 95-108.

95. Курбан О. В. Інтернет-технології та онлайнові соціальні мережі у сучасній гібридній війні // Наукові записки Української академії друкарства. 2017. № 1. С. 264-273.

96. Курбан О. В. Теорія інформаційної війни: базові основи, методологія та понятійний апарат // Наук. журнал “Science Rise”.– 2015.– № 11 (1). – С. 95-100.

97. Лассуелл, Г. Структура і функція комунікації в суспільстві / пер. з англ. — Нью-Йорк : Harper & Brothers, 1948. — 32 с.

98. Лисенко О. М. Якісний аналіз у процесі оцінки ефективності військових дій // Гуманітарні студії. — 2021. — Вип. 32. — С. 112–118.

99. Литвиненко О. В. Інформаційна війна як загроза національній безпеці України: сутність, напрями та механізми протидії // Стратегічні пріоритети. – 2016. – № 4(41). – С. 38-51.

100. Ліпкан В. А., Максимець Ю. О. Кібертероризм: навчальний посібник. — Київ : КНТ, 2015. — 344 с.

101. Ліппман, В. Громадська думка / пер. з англ. — Київ : Центр учбової літератури, 2004. — 320 с.

102. Мангейм, Дж. Б. Психологія політики: лідери, послідовники, громадяни / пер. з англ. — Київ : Основи, 2011. — 432 с.

103. Манжай О.В Правові заходи захисту інформації. — Харків : Панов, 2020. — 162 с.

104. Мануель Х. Від масової комунікації до мережевої комунікації: нові медіа та трансформація влади. – Кембридж: Політі Прес, 2004. – 216 с.

105. Мельник І. В. Інформаційні кампанії у військових конфліктах. — Дніпро : Видавництво Дніпровського національного університету, 2019. — 204 с.

106. Мельник С. В. Феномен фейкових новин у цифровому суспільстві: причини, наслідки та шляхи протидії // Вісник Харківського національного університету імені В. Н. Каразіна. Серія “Соціальні комунікації”. – 2018. – № 85. – С. 91-104.

107. Молчанов С. В. Роль сил спеціальних операцій у гібридних конфліктах // Військова думка. 2021. № 1. С. 45-57.

108. Морозов Є. Г. Аналітичне забезпечення процесу прийняття рішень у військовому управлінні. — Львів : Видавництво Львівської політехніки, 2020. — 180 С.

109. Най, Дж. С. М'яка сила: як досягти успіху у світовій політиці / пер. з англ. — Львів : Літопис, 2004. — 240 с.

110. Найман А. Л. Проксі-війни в сучасних міжнародних відносинах // Актуальні проблеми міжнародних відносин. 2020. Вип. 141. Ч. 2. С. 72-85.

111. Петров А. І. Еволюція військової думки: від стратегії виснаження до операцій базових ефектів. — Харків : Видавництво Харківського національного університету, 2022. — 196 с.

112. Петров В. В. Кібернетична безпека об'єктів критичної інфраструктури: сучасний стан та перспективи // Безпека інформації. – 2020. – № 4(29). – С. 112-125.

113. Почепцов Г. Г. Стратегічні комунікації. — Київ : Видавничий дім "Арій", 2017. — 368 с.

114. Почепцов Г. Г. Сучасні інформаційні війни. Київ: Видавничий дім "Києво-Могилянська академія", 2017. – 496 с.

115. Райнгольд Г. Віртуальний народ: знаходження зв'язку в комп'ютерну епоху. – Київ: Ваклер, 2002. – 416 с.

116. Рассказов І. О. Інструменти гібридної війни: класифікація та особливості застосування // Стратегічна панорама. 2019. № 2. С. 130-143.

117. Резніков В. В. Інформаційна війна в умовах цифрового суспільства: теоретико-методологічний аналіз. — Київ : Центр учбової літератури, 2019. — 216 с.

118. Романенко Є. А. Інформаційна війна в контексті гібридних конфліктів // Інформаційна безпека людини, суспільства, держави. 2024. № 1(13). С. 115-129.

119. Романенко Є. А. Кібернетична війна: сучасні виклики та загрози. — Київ : Фенікс, 2024. — 216 с.

120. Рульов І.М. Співвідношення кібертероризму та кіберзлочину // Юридичний вісник. Одеса : Гельветика, 2021. № 3. С. 178–185.

121. Семенов І. П. Кількісні методи оцінки в операціях, орієнтованих на ефект. Вісник Національного університету оборони України імені Івана Черняховського. 2023. № 2(33). С. 88-101.

122. Сенченко О. Мережевий інструментарій нових війн // Вісник книжкової палати. 2017. № 1. С. 37-41.

123. Середюк П. В. Атрибуція кібератак в контексті гібридної війни // Безпека інформації. – 2019. – № 2. – С. 45-108.

124. Середюк П. В. Державне спонсорування кібертероризму як загроза національній безпеці // Право і суспільство. – 2019. – № 3. – С. 69-82.

125. Сидоренко В. М. Економічні санкції в системі інструментів національної безпеки. — Одеса : Видавництво Одеського національного університету, 2020. — 224 с.

126. Сметана С. О. Синергія інструментів гібридної війни // Наукові записки Національного університету “Острозька академія”. Серія “Військові науки”. 2024. № 2(20). С. 150-163.

127. Смирнов П. М. Стратегія непрямих дій у сучасних конфліктах. — Київ : Національна безпека, 2018. — 128 с.

128. Стейн Ф. Кібервійна: невидима загроза. – Москва: АСТ, 2001. – 320 С.

129. Стельмах В. В. Концепція операцій базових ефектів у протидії тероризму // Науковий вісник Львівського державного університету внутрішніх справ. 2019. № 4. С. 98-111.

130. Стратегія кібербезпеки України (2021–2025 роки) // Указ Президента України від 26 серпня 2021 р. № 447/2021.

131. Стронський В. В. Інформаційна політика авторитарних режимів в умовах глобалізації // Наукові записки Інституту політичних і етнонаціональних досліджень ім. І.Ф. Кураса НАН України. – 2020. – № 2. – С. 92-105.

132. Телешун С. О. Дестабілізація суспільства як мета кібератак в гібридній війні // Стратегічні пріоритети. – 2016. – № 4. – С. 102-115.

133. Телешун С. О. Стратегії інформаційної агресії Російської Федерації проти України // Стратегічні пріоритети. – 2016. – № 3(41). – С. 116-129.

134. Терещенко О. О. Вплив економічних санкцій на соціально-економічну ситуацію в країні-об'єкті. Економіка та суспільство. 2023. № 48. С. 145-158.

135. Ткаченко В. А. Економічна безпека держави в умовах інформаційної війни // Економіка та держава. – 2019. – № 1. – С. 55-91.

136. Ткаченко В. В. Система зворотного зв'язку в управлінні операціями базових ефектів. Наукові записки Національного університету "Острозька академія". Серія "Військові науки". 2024. № 1(19). С. 135-148.

137. Тоффлер, Е., Тоффлер Г. Війна і антивійна: виживання на світанку XXI століття / пер. з англ. — Київ : Україна, 1992. — 382 с.

138. Федоров М. М. Гібридні загрози в інформаційному просторі: сутність, структура та механізми протидії // Стратегічні пріоритети. – 2020. – № 1(55). – С. 47-60.

139. Фернандес-Арментос П. Інформаційна війна та зовнішня політика демократичних держав // Міжнародна безпека. – 2018. – № 3. – С. 121-134.

140. Фернандес-Арментос П. Кібербезпека критичної інфраструктури: міжнародний досвід та рекомендації для України // Міжнародна безпека. – 2018. – № 3. – С. 93-106.

141. Фернандес-Арментос П. Кібервійна та гібридні конфлікти: нові виклики для міжнародної безпеки // Міжнародна безпека. – 2018. – № 2. – С. 78-120.

142. Флоров В. М. Правове регулювання кіберпростору в Україні: сучасний стан та перспективи розвитку // Право України. – 2019. – № 7. – С. 115-128.

143. Хома Н. М. Вплив кібератак на психологічний стан населення в умовах гібридної війни // Психологія і суспільство. – 2018. – № 3. – С. 136-149.

144. Хома Н. М. Інженерія соціальних мереж як інструмент кібератак на критичну інфраструктуру // Психологія і суспільство. – 2017. – № 4. – С. 132-145.

145. Хома Н. М. Інформаційно-психологічні операції в кіберпросторі як елемент гібридної війни // Психологія і суспільство. – 2017. – № 3. – С. 128-141.

146. Хома Н. М. Кіберпсихологія: психологічні аспекти кіберзагроз та кібербезпеки. — Львів : Львівський державний університет внутрішніх справ, 2018. — 224 С.

147. Хома Н. М. Психологічні аспекти вербування в терористичні організації через кіберпростір // Проблеми екстремальної та кризової психології. – 2017. – № 20. – С. 145-158.

148. Хомчак Р. Б. Інформаційна безпека в умовах гібридної війни. // Національна безпека та оборона. 2017. № 5. С. 105-119.

149. Цимбалюк В. С. Гібридна війна Росії проти України: генезис та особливості // Стратегічна панорама. — 2017. — № 1. — С. 18–31.

150. Цимбалюк В. С. Міжнародне співробітництво у сфері протидії кіберзлочинності в умовах гібридної війни // Актуальні проблеми міжнародних відносин. – 2019. – Вип. 142(2). – С. 152-165.

151. Ярош О. Б. Психологічний вплив дезінформації на національну безпеку // Науковий вісник Львівського державного університету внутрішніх справ. – 2018. – № 2(92). – С. 77-90.

152. Ярошенко В. М. Кібергігієна як елемент протидії гібридним загрозам // Інформаційна безпека людини, суспільства, держави. – 2020. – № 1. – С. 98-111.

Інтернет-посилання:

153. Yaari E., M. Israel’s Shadow War with Iran. The Jerusalem Post. Режим доступу: https://www.jpost.com/middle-east/israels-shadow-war-with-iran-analysis-671828 (дата звернення: 10.05.2025).

154. Академія української преси. Медіаграмотність. Режим доступу: https://www.google.com/search?q=https://aup.com.ua/mediagramotnist/ (дата звернення: 10.05.2025)

155. Європейська конвенція про захист прав людини і основоположних свобод від 04.11.1950. Режим доступу:

https://www.echr.coe.int/documents/d/echr/convention_ukr (дата звернення: 10.05.2025)

156. Європейський Союз. (2022). Спільна комунікація Європейської Комісії та Високого представника Союзу з питань закордонних справ та політики безпеки щодо протидії іноземному інформаційному втручанню та маніпулюванню інформацією. Режим доступу: https://www.google.com/search?q=https://www.eeas.europa.eu/eeas/foreign-information-manipulation-and-interference_en (дата звернення: 10.05.2025)

157. Кібербезпека України. Основні поняття та терміни. Режим доступу: https://www.google.com/search?q=https://cip.gov.ua/ua/kiberbezpeka (дата звернення: 10.05.2025)

158. Національний координаційний центр кібербезпеки. Концепція мережево-центричної війни та її актуальність. Режим доступу: https://www.facОБЕok.com/ncsccUA/?locale=uk_UA (дата звернення: 10.05.2025)

159. Національний центр кібербезпеки. Аналітичні матеріали щодо інформаційних загроз. Режим доступу: https://www.google.com/search?q=https://ncscc.gov.ua/ (дата звернення: 10.05.2025)

160. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. Режим доступу: https://ips.ligazakon.net/document/MN024739 (дата звернення: 10.05.2025)

161. Стратегія кібербезпеки України (2021–2025 роки) // Указ Президента України від 26 серпня 2021 р. № 447/2021. — Офіційне інтернет-представництво Президента України. — Режим доступу: president.gov.ua/documents/4472021-40013. (дата звернення: 10.05.2025)

162. Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392/2020. Режим доступу: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 10.05.2025)

163. Сучасна діяльність приватних військових компаній. Режим доступу: https://www.cir-ps.com/post/сучасна-діяльність-приватних-військових-компаній (дата звернення: 10.05.2025)