Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально – науковий інститут економіки
Фінансово-економічний факультет
Кафедра міжнародних відносин і аудиту

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента/студентки Пічуріної Ірини Вадимівни
(ПІБ)
академічної групи 291м-24-1
(шифр)
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
(код і назва спеціальності)
за освітньо-професійною програмою «Міжнародні відносини, суспільні комунікації та регіональні студії»
(офіційна назва)

на тему: «Еволюція інформаційних війн крізь призму дилеми безпеки»
(назва за наказом ректора)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Керівник роботи	**Кулик Т.В.**	**100**	
Рецензент	**Ротаєнко С. В.**	**100**	
Нормоконтроль	**Кулик Т.В.**	**100**	

Дніпро
2025

ЗАТВЕРДЖЕНО:
завідувачка кафедри
міжнародних відносин і аудиту
_____ Пашкевич М.С.
(підпис) (прізвище, ініціали)
«_01_» _10____ 2025 року

ЗАВДАННЯ

на кваліфікаційну роботу

ступеню роботи ступеню магістра

Студенту __Пічуріній І.В._____ **академічної групи**__291м-24-1____
(прізвище та ініціали) (шифр)
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
спеціалізації «Міжнародні відносини, суспільні комунікації та регіональні студії»
за освітньо-професійною програмою «Міжнародні відносини, суспільні комунікації та регіональні студії»
на тему: «Еволюція інформаційних війн крізь призму дилеми безпеки»

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ №_____

Розділ	Зміст	Термін
1	Формування простору конфліктності європейського регіонального комплексу безпеки	01.10.25-19.10.25
2	Придністровський конфлікт: структурні параметри та динаміка	20.10.25-03.11.25
3	Конфліктогенність Придністров'я в позиціях ключових акторів	04.11.25-20.11.25

Завдання видано _____ __Кулик Т.В._____
(підпис керівника) (прізвище, ініціали)

Дата видачі 01.10.2025

Дата подання до екзаменаційної комісії 08.12.2025

Прийнято до виконання _____ __Пічуріна І.В.__
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна робота Пічуріної І.В. магістра кафедри міжнародних відносин і аудиту, фінансово-економічного факультету НТУ «Дніпровська політехніка» складається зі 116 с., 85 літер. Об'єктом дослідження є дилема безпеки як системна властивість міжнародного порядку. Предметом дослідження є еволюція інформаційних війн крізь призму дилеми безпеки в умовах трансформації інформаційного середовища. Мета дослідження полягає у комплексному аналізі еволюції інформаційних війн як чинника формування та відтворення дилеми безпеки, а також у з'ясуванні ролі невизначеності інформаційного середовища у сучасних безпекових процесах. Методологічною основою дослідження є принципи системності, об'єктивності, історизму, комплексності та міждисциплінарності. Застосовано структурно-функціональний підхід, методи аналізу - факторний, контент, івент, аналіз динаміки, аналіз взаємозв'язків, синтез. Отримані результати можуть бути використані в аналітичній, експертно-консультативній та освітній діяльності у сфері міжнародної безпеки, а також у процесі розроблення підходів до інформаційної політики, стратегічних комунікацій і міжнародної координації в умовах сучасних конфліктів.

Перелік ключових слів: ДИЛЕМА БЕЗПЕКИ, ІНФОРМАЦІЙНІ ВІЙНИ, ІНФОРМАЦІЙНІ ОПЕРАЦІЇ, НЕВИЗНАЧЕНІСТЬ, СТРАТЕГІЧНА КОНКУРЕНЦІЯ ІНТЕГРОВАНЕ СТРИМУВАННЯ.

RESUME

The qualification research of I. Pichurina, a master's student of the Department of International Relations and Audit, Faculty of Finance and Economics, NTU «Dnipro University of Technology», comprises 116 pages and includes 85 bibliographic sources. The object of the study is the security dilemma as a systemic property of the international order. The subject of the study is the evolution of information warfare viewed through the prism of the security dilemma under conditions of transformation of the information environment. The purpose of the research is to provide a comprehensive analysis of the evolution of information warfare as a factor shaping and reproducing the security dilemma, as well as to clarify the role of uncertainty in the information environment in contemporary security processes. The methodological framework of the study is based on the principles of systemacity, objectivity, historicity, complexity, and interdisciplinarity. The research applies a structural-functional approach and a set of analytical methods, including factor analysis, content analysis, event analysis, dynamic analysis, relational analysis, and synthesis. The obtained results can be used in analytical, expert-consultative, and educational activities in the field of international security, as well as in the development of approaches to information policy, strategic communications, and international coordination in the context of contemporary conflicts.

Keywords: SECURITY DILEMMA; INFORMATION WARFARE; INFORMATION OPERATIONS; UNCERTAINTY; STRATEGIC COMPETITION AND INTEGRATED DETERRENCE.

ЗМІСТ

ВСТУП

Тривала присутність інформаційних впливів у міждержавному протиборстві свідчить про їх перехід від допоміжного інструмента політики до стійкого елементу безпекової взаємодії. Зміна масштабів, швидкості та наслідків інформаційних операцій зумовлює необхідність аналізу тих структурних ефектів, які вони продукують у сфері міжнародної безпеки. Одним із таких ефектів є посилення невизначеності щодо намірів акторів, меж допустимої поведінки та характеру загроз, що безпосередньо впливає на процеси взаємного сприйняття й ухвалення рішень. Дилема безпеки, як теоретична модель, що описує відтворення недовіри та страху навіть за відсутності агресивних намірів, надає можливість пояснити, яким чином еволюція інформаційних війн змінює сутність та динаміку безпекової взаємодії. Аналіз інформаційних війн крізь призму дилеми безпеки дозволяє виявити їхню роль у формуванні стабільних патернів напруженості, що не зводяться до окремих криз або конфліктних епізодів.

Еволюція інформаційних війн відображає глибинну трансформацію механізмів безпеки в міжнародному середовищі, пов’язану зі зростанням ролі інформації як чинника формування загроз, сприйняття намірів і ухвалення політичних рішень. Інформаційні операції перестали обмежуватися епізодичним супроводом військових або дипломатичних дій і набули характеру безперервного процесу, в межах якого здійснюється вплив на когнітивні, інституційні та соціальні основи безпеки, що ускладнює визначення меж між миром і конфліктом, оборонною активністю та наступальним тиском, легітимною комунікацією та навмисним маніпулюванням.

Традиційні підходи до аналізу безпеки виявляються недостатніми для пояснення стабільності напруженості та повторюваності кризових ситуацій за відсутності відкритої ескалації. Дилема безпеки набуває нових вимірів у просторі інформаційних війн, оскільки ключовим джерелом загроз стає

невизначеність, що формується через контроль інтерпретацій, конкуренцію наративів і обмежену можливість надійної атрибуції дій. Інформаційне середовище посилює структурну проблему інтерпретації намірів, на якій ґрунтується дилема безпеки, трансформуючи її з наслідку матеріального нарощування сил у продукт системного впливу на сприйняття. Навіть дії з обмеженим масштабом або оборонною мотивацією можуть розглядатися як елементи ширшої наступальної стратегії, що стимулює запобіжні кроки та відтворює логіку взаємної підозри. Технологічне прискорення, автоматизація поширення інформації та глобальна циркуляція повідомлень знижують часові горизонти для оцінки ризиків і підвищують імовірність помилкових рішень.

Інформаційні війни дедалі більше вписуються в механізм відтворення дилеми безпеки, де напруженість зберігається без чітко окреслених порогів, сигналів завершення або стабілізації. Відсутність усталених норм інтерпретації інформаційних впливів ускладнює вироблення спільних уявлень про допустиму поведінку та підвищує ризик кумулятивної ескалації. Аналітичне осмислення еволюції інформаційних війн крізь призму дилеми безпеки дозволяє пояснити, чому навіть за відсутності прямого застосування сили формується стійкий стан стратегічної напруги, що не знімається окремими актами стримування або деескалації.

Новизна дослідження полягає в концептуалізації інформаційних війн як середовища відтворення дилеми безпеки, а не лише як інструмента впливу або окремого типу конфліктної діяльності, що розширює теоретичні межі аналізу інформаційної безпеки. Такий підхід дозволяє поєднати дослідження інформаційних операцій із класичними теоріями міжнародної безпеки, виявляючи їхні трансформації в умовах цифрової епохи.

Практичне значення роботи полягає у можливості застосування отриманих висновків для формування підходів до інформаційної безпеки в умовах сучасних конфліктів, спричинених діями ревізіоністських акторів, які використовують інформаційні та технологічні інструменти для підриву довіри, політичної стабільності та міжнародного правопорядку. Для України результати

дослідження створюють аналітичну основу для розуміння інформаційних впливів як частини ширшого механізму відтворення безпекової невизначеності, що поширюється як на державу-об’єкт агресії, так і на її міжнародних партнерів. Це відкриває можливості для більш чіткого визначення пріоритетів у сфері інформаційної політики, стратегічних комунікацій і міжнародної координації з метою зменшення ефектів дилеми безпеки в інформаційному просторі.

Проблематика еволюції інформаційних війн крізь призму дилеми безпеки формується на перетині кількох теоретичних полів міжнародних відносин і безпекових студій, кожне з яких має власну традицію осмислення природи загроз, механізмів їх сприйняття та умов відтворення конфліктності. Стан дослідженості проблеми характеризується наявністю ґрунтовних напрацювань щодо онтології дилеми безпеки, феномену невизначеності, розвитку концепту інформаційної війни та сучасних підходів до стримування, водночас їх поєднання в єдину аналітичну рамку залишається фрагментарним.

Досліджень, присвячені онтологічним засадам дилеми безпеки та механізмам її формування включають класичні та неокласичні підходи до осмислення дилеми безпеки представлені у роботах K. Booth і N. Wheeler [7], M. Hollis та S. Smith [28], R. Jervis [33–35], які заклали підґрунтя для розуміння дилеми безпеки як структурної умови міжнародної системи, пов’язаної з інтерпретацією намірів і невизначеністю. Значний внесок у розвиток цього напряму зробили також G. Allison [1, 2], J. H. Herz [25, 26], C. L. Glaser [20] і B. Posen [56], які розширили аналіз дилеми безпеки, зосередившись на ролі сприйняття, оборонно-наступального балансу та стратегічних виборів держав.

Другий напрям досліджень стосується феномену невизначеності як системоутворюючого чинника міжнародної безпеки. У працях J. J. Mearsheimer [50, 51], H. Bull [11], M. Wight [68] і K. W. Deutsch [16] невизначеність розглядається як наслідок анархічної структури міжнародної системи, обмеженості інформації та складності прогнозування поведінки акторів. Ці підходи створюють теоретичне підґрунтя для аналізу того, як невизначеність впливає на стратегічні рішення та підсилює логіку запобіжних дій. Питання

відтворення та поглиблення дилеми безпеки у динаміці міжнародних відносин отримали розвиток у працях K. N. Waltz [64], L. Gosling [21], M. Weisbrot [67] і B. Williams [69], де увага зосереджується на механізмах самопідтримуваної недовіри, ескалаційних спіралях та обмеженій здатності акторів вийти за межі структурно заданих страхів навіть за відсутності безпосередніх загроз.

Окремий пласт літератури формує дослідження інформаційної війни як елементу багатовимірної стратегічної взаємодії. Еволюція поняття «інформаційна війна» простежується у працях J. F. C. Fuller [30], H. D. Lasswell [39], P. M. A. Linebarger [44], T. P. Rona [57], R. J. Bunker [12], а також у фундаментальних роботах M. Libicki [40, 41], які заклали основи сучасного розуміння інформаційних операцій як інструмента стратегічного впливу, що виходить за межі суто пропагандистських практик. Практичні виміри застосування інформаційних війн висвітлюються в колективних та міждисциплінарних дослідженнях, зокрема в The Handbook of European Communication History [3], роботах «Феномен пропаганди та антипропаганди у сучасному світі» [85], «Війни інформаційної епохи: міждисциплінарний дискурс» [75], а також у працях C. Walton [65], J. J. Garstka [19] і T. Withington [70], де аналізуються конкретні практики інформаційного впливу, їх технологічна еволюція та політичні наслідки. Моделі впливу інформаційних операцій на суспільні та політичні процеси розробляються у працях J. L. Groh [22], D. J. Holbrook [27], а також у дослідженнях українських авторів – Д. В. Дубова [78], Т. Кулика [72, 79], П. Лисянського [82], які акцентують увагу на когнітивному, інституційному та поведінковому вимірах інформаційного впливу. Інформаційні операції як чинник відтворення дилеми безпеки дедалі частіше розглядаються у межах концепції стратегічної конкуренції. У цьому контексті важливими є роботи B. N. Fultz і A. G. Utuk [18], дослідження RAND Corporation [14, 54, 55], праці H. Brands [9], S. D. Bachmann, D. Lee та A. Dowse [4], у яких інформаційний простір постає як середовище тривалої конкуренції, що ускладнює сигналювання, підвищує ризики хибної інтерпретації та

підтримує стан перманентної напруженості.

Окремий напрям становлять дослідження інтегрованого стримування та міждоменних підходів до безпеки, представлені у працях J. Lindsay [43], дослідженнях RAND Corporation [48, 49], роботах P. K. Huth [29], P. M. Morgan [52], монографії *Cross-Domain Deterrence: Strategy in an Era of Complexity* [15], а також у працях K. Mallory [45], M. Johnson і T. K. Kelly [37], S. P. Larkin [38]. У цих дослідженнях інформаційний вимір стримування розглядається як важливий, але здебільшого допоміжний елемент ширших стратегічних конструкцій.

Попри значний обсяг наукових напрацювань, у сучасній літературі залишається недостатньо висвітленим питання системного зв'язку між еволюцією інформаційних війн і відтворенням дилеми безпеки. Наявні дослідження або зосереджуються на теоретичних засадах дилеми безпеки без урахування трансформацій інформаційного середовища, або аналізують інформаційні війни переважно як інструмент впливу, не розкриваючи їх ролі у підтриманні структурної невизначеності та стратегічної напруженості. Недостатньо опрацьованими залишаються механізми, через які інформаційні операції ускладнюють інтерпретацію намірів, впливають на логіку реагування та закріплюють самопідтримуваний характер дилеми безпеки в умовах інформаційної епохи. З огляду на це завданням даного дослідження є концептуальне осмислення еволюції інформаційних війн крізь призму дилеми безпеки, виявлення ролі невизначеності як ключового механізму її відтворення, а також визначення місця інформаційних операцій у сучасних безпекових процесах. Робота спрямована на заповнення наявної аналітичної прогалини шляхом поєднання теорії дилеми безпеки з дослідженням інформаційних війн, що дозволяє запропонувати цілісне бачення їхнього впливу на стабільність міжнародного середовища безпеки.

Об'єктом дослідження є дилема безпеки як системна властивість міжнародного порядку.

Предметом дослідження є еволюція інформаційних війн крізь призму

дилеми безпеки в умовах трансформації інформаційного середовища.

Мета дослідження полягає у комплексному аналізі еволюції інформаційних війн як чинника формування та відтворення дилеми безпеки, а також у з'ясуванні ролі невизначеності інформаційного середовища у сучасних безпекових процесах. У відповідності до поставленої мети у роботі сформульовано такі дослідницькі завдання:

- вивчити онтологічні засади дилеми безпеки та її місце в теоретичних моделях міжнародного порядку.
- дослідити трансформацію невизначеності в основних теоріях міжнародної безпеки та її вплив на поведінку акторів.
- охарактеризувати фактори системної вразливості, що сприяють відтворенню та поглибленню дилеми безпеки.
- проаналізувати еволюцію поняття «інформаційна війна» у провідних теоретичних напрямах та практиках застосування.
- розкрити основні моделі впливу інформаційних операцій на політичні, інституційні та когнітивні процеси.
- встановити зв'язок між невизначеністю інформаційного середовища та механізмами відтворення дилеми безпеки.
- виявити потенціал інтегрованого стримування в інформаційному просторі як інструмента обмеження ескалаційних ризиків.

Методологічною основою дослідження є принципи системності, об'єктивності, історизму та комплексності, які забезпечують цілісне, неупереджене та послідовне осмислення еволюції інформаційних війн у контексті трансформації дилеми безпеки. Принцип системності дозволяє розглядати дилему безпеки та інформаційні війни як взаємопов'язані елементи міжнародного безпекового середовища, що функціонують у межах складних багаторівневих структур. Принцип об'єктивності забезпечує аналіз теоретичних підходів і практик інформаційного протиборства з урахуванням різних наукових позицій та без нормативних оцінок. Принцип історизму дає змогу простежити

еволюцію уявлень про інформаційні війни та трансформацію механізмів дії дилеми безпеки в різні історичні періоди. Принцип комплексності забезпечує інтеграцію політичних, безпекових, комунікаційних і технологічних вимірів досліджуваної проблематики.

Зазначені принципи реалізовано через поєднання загальнонаукових і спеціальних методів дослідження. Методи аналізу, синтезу та узагальнення використано для систематизації теоретичних підходів до дилеми безпеки та інформаційних війн, а також для формування цілісних висновків. Системний метод застосовано для дослідження інформаційних операцій як складової міжнародного безпекового середовища та механізму відтворення дилеми безпеки. Структурно-функціональний метод дозволив виявити ролі та функції інформаційних впливів у процесах формування невизначеності та інтерпретації загроз. Факторний аналіз використано для ідентифікації ключових чинників, що впливають на ескалаційні ризики в інформаційному просторі. Порівняльний метод застосовано для зіставлення різних теоретичних моделей інформаційних війн і підходів до стримування в інформаційному вимірі. Елементи контент-аналізу використано для дослідження наративних структур і інтерпретаційних рамок, що формують сприйняття безпекових загроз.

Джерельну базу дослідження становлять офіційні стратегічні та доктринальні документи у сфері безпеки й оборонного планування, що відображають еволюцію уявлень про інформаційні операції, стримування та управління ескалаційними ризиками в сучасному міжнародному середовищі. Основну групу джерел складають нормативні акти, концепції та стратегічні документи США, а також матеріали, розроблені в рамках діяльності НАТО та Європейського Союзу, які задають загальні орієнтири для демократичних держав у сфері інформаційної безпеки. До ключових джерел належать директиви та меморандуми Міністерства оборони США, зокрема DoD Directive TS3600.1, Memorandum of Policy No. 30 (1993) та стратегічний документ Joint Staff «A Strategy for Peace: The Decisive Edge in War» (1996), що фіксують ранні підходи до інформаційного виміру воєнного планування. Важливе місце посідає Joint

Doctrine for Information Operations (JP 3-13) (1998 році), яка систематизувала підходи до інформаційних операцій у межах військової доктрини. Аналіз сучасного етапу представлений такими документами, як The National Defense Strategy of the United States of America, The 2022 Nuclear Posture Review, The 2022 Missile Defense Review, а також Joint Concept for Integrated Campaigning, підготовлений Об'єднаним комітетом начальників штабів США. Залучення зазначених джерел зумовлене їхньою аналітичною цінністю для дослідження механізмів формування стратегічних уявлень про інформаційні операції, невизначеність та стримування, а також їхнім впливом на міжнародні безпекові практики загалом. Використання документів США, НАТО та ЄС дозволяє простежити домінантні підходи в межах західної безпекової парадигми, не зводячи аналіз до національного рівня, а розглядаючи їх як частину ширшого транснаціонального нормативного та стратегічного середовища.

Структура роботи відповідає поставленій меті та розв'язанню основних завдань дослідження й складається зі вступу, трьох розділів (які в свою чергу поділяються на підрозділи), висновків, списку використаних джерел та літератури. Загальний обсяг - 116 с., список використаних джерел та літератури складає 85 найменувань.

РОЗДІЛ 1. ДИЛЕМА БЕЗПЕКИ ЯК СИСТЕМНА ВЛАСТИВІСТЬ МІЖНАРОДНОГО ПОРЯДКУ

1.1 Онтологія дилеми безпеки

Дилема безпеки постає як проблема стратегічної взаємодії між державами та іншими акторами, у межах якої зусилля однієї сторони щодо зміцнення власної безпеки неминуче трансформуються в джерело потенційної загрози для іншої. Її природа формується як дворівнева стратегічна дилема, що складається з дилеми інтерпретації та дилеми реагування, які у взаємодії створюють складну когнітивно-стратегічну матрицю вибору для осіб, відповідальних за ухвалення рішень. На першому рівні виникає необхідність інтерпретувати мотиви, наміри й матеріальні можливості інших суб'єктів, причому кожна з альтернативних інтерпретацій здається водночас раціональною та небезпечною, адже невизначеність міжнародного середовища не дозволяє достеменно відрізнити оборонні зусилля від потенційно наступальних. Невизначеність створює усвідомлену екзистенційну ситуацію, коли рішення має бути ухвалене за відсутності повної інформації, а отже із неминучим ризиком хибної інтерпретації сигналів. Дилема інтерпретації полягає в тому, що сприйнята військова модернізація іншої держави може бути водночас переконливо пояснена потребою забезпечити власну вразливість у непередбачуваному середовищі та амбіцією скористатися сприятливою кон'юнктурою для перегляду статус-кво на власну користь. Оскільки жодна зі сторін не може перевірити істинні мотиви іншої, саме припущення про їхній характер стає визначальним чинником того, якою буде подальша стратегія.

На рівні дилеми реагування ухвалюється рішення щодо того, як відповідати на раніше сформовану інтерпретацію, незалежно від того, наскільки вона наближена до фактичних намірів іншого актора. Особи, які приймають рішення, мають обрати між стратегією рішучості, що передбачає демонстрацію готовності віддзеркалити політику іншої сторони задля стримування, та стратегією

заспокоєння, яка покликана зменшити напруженість шляхом акцентування мирних намірів. Обидві траєкторії містять значну частку ризику, оскільки їх успішність безпосередньо залежить від того, чи збігається інтерпретація з реальними намірами іншого суб'єкта. Якщо вибір на користь жорсткої відповіді ґрунтується на хибному припущенні про ворожість іншого, то підсилення оборонних спроможностей, дипломатична непримиренність і демонстрація готовності до силового реагування можуть ненавмисно породити конфронтаційну динаміку, якої жодна сторона не прагнула, але яка поступово загострюється внаслідок взаємної підозри. Неправильна інтерпретація у протилежному напрямку, тобто необґрунтоване припущення про доброзичливі наміри іншого, може призвести до надмірної довіри й стратегічної вразливості, відкриваючи простір для примусу або маніпулятивного використання слабкості тих, хто намагається уникнути ескалації. Дилема реагування виступає логічним продовженням дилеми інтерпретації, оскільки помилка на першому рівні неминуче множиться на другому, задаючи траєкторію взаємодії, у межах якої навіть незначні прорахунки можуть набувати структурного характеру та формувати довготривалу недовіру [7, pp. 4-5].

Динаміка дилеми безпеки зумовлюється комплексом взаємопов'язаних чинників, які зазвичай класифікують як переважно матеріальні та переважно психологічні. Матеріальний вимір пов'язаний із феноменом «двозначної символіки» озброєнь і їхнього розміщення, що позначає структурну неможливість однозначно відрізнити оборонні наміри від наступальних навіть у випадках, коли сторони декларують прагнення до стабільності [7, p. 42]. Психологічний вимір ґрунтується на тому, що науковці окреслюють як проблему «чужих розумів» – фундаментальну неможливість достеменно пізнати наміри іншого актора, що неминуче породжує інтерпретаційну невизначеність і схильність до гіперчутливого сприйняття потенційної загрози [28, pp. 171-172].

Ідея двозначності зброї добре відома дослідникам контролю над озброєннями, хоч і не завжди під цим терміном, адже практична відмінність між наступальними та оборонними системами часто виявляється проблематичною

або суто умовною. Хрестоматійне припущення про те, що характер зброї визначається позицією того, «хто тримає на спусковому гачку», лише поверхово передає складність стратегічної логіки, оскільки в реальному міжнародному середовищі функціональне навантаження озброєнь залежить від контексту застосування, оперативних концепцій та взаємного сприйняття. Навіть у випадках, коли окремі види озброєнь можуть видаватися однозначно наступальними (меч) чи оборонними (щит), їх реальна стратегічна природа визначається не інструментальною формою, а сполученням із іншими засобами та місцем у загальній військово-стратегічній доктрині. Так, у військовому мистецтві щит може виконувати критичну наступальну функцію, якщо його застосування інтегрується в маневрову або проривну операцію, що робить просте дихотомічне розрізнення концептуально неспроможним.

Наприклад, концепція «щита і меча» (shield & sword), що слугувала підґрунтям змін до Стратегічної концепції НАТО у 1952 р. розмежовувала роль європейських конвенційних наземних сил, які підтримувались тактичною авіацією і військово-морськими силами як «щита», покликаного стримувати та зв’язувати противника, та роль американських стратегічних ядерних сил як «меча», що мав забезпечити вирішальний удар [71, с. 137]. З цього приводу образно висловився Б. Г. Ліддел Гарт: «вживання слова «меч» для характеристики засобу стримування, який забезпечується головним чином американською стратегічною авіацією, і слова «щит» для характеристики сухопутних військ НАТО. Цей «меч» не може бути практично використаний без того, щоб не призвести до обопільного знищення. Він нагадує старий церемоніальний японський меч, яким роблять харакірі. Старе слово «щит» не припускає захисту від нових форм агресії, які жалять і роз'їдають тіло країни, і які стали зараз більш ймовірними, чим удари меча. Щит не може захистити ні від ос, ні від пожеж» [42, p. 55].

У дискусіях щодо розгортання систем протиракетної оборони США прихильники десятиліттями наполягали, що такі системи мають переважно оборонний характер, оскільки спрямовані на захист території США від

обмеженого ракетного удару з боку держав, які розглядаються як «ізгої». Натомість критики вказували, що в умовах першого ядерного удару по потенційному противнику, здійсненого наступальними силами США, протиракетна оборона може виконувати роль «другого щита», мінімізуючи наслідки відповіді значно ослабленого противника. У цій інтерпретації оборонна система перетворюється на елемент наступальної стратегії, а її розгортання – на серйозний чинник дестабілізації стратегічного балансу, що суттєво підсилює динаміку дилеми безпеки.

Питання «що не є зброєю в руках іншого?», – відбиває фундаментальну проблему невизначеності щодо намірів і стратегічних уподобань потенційного опонента. Це запитання не втратило актуальності й у XXI столітті, адже характер політичного лідерства та репутація ключових акторів можуть істотно загострювати сприйняття загрози. Коли у 2017 році президентом США перший раз став Д. Трамп, його імідж особи з непередбачуваним стилем ухвалення рішень викликав відчутне занепокоєння серед партнерів і противників, посилюючи двозначність сигналів зовнішньої політики. Ще драматичнішим виявився випадок із маніпулятивним використанням стратегічної невизначеності з боку путіна напередодні та після початку російського повномасштабного вторгнення в Україну у 2022 р., коли свідоме нагнітання двозначності щодо намірів, масштабів та потенційного застосування ядерної зброї стало інструментом психологічного тиску, спрямованого на підрив політичної волі інших держав.

Ці приклади висвітлюють центральний психологічний вимір дилеми безпеки, пов’язаний із проблемою «чужих розумів», тобто з об’єктивною неможливістю достеменно реконструювати мотивації, страхи, очікування й стратегічні цілі осіб, які ухвалюють рішення в інших державах. Політичні лідери та аналітики змушені робити висновки про чужі наміри на основі неповної інформації, неоднозначних сигналів і часто суперечливих індикаторів, а рівень упевненості в цих оцінках має бути максимально високим, оскільки ціна

помилки в питаннях національної безпеки є надзвичайно високою. Хибна інтерпретація може призвести не лише до неефективного розподілу ресурсів, втрати міжнародного авторитету чи стратегічних переваг, але й до катастрофічних наслідків — від масових людських втрат до поразки й навіть окупації. Саме тому психологічний аспект невизначеності становить не периферійне, а структурно визначальне підґрунтя дилеми безпеки.

Проблема «чужих розумів» стає особливо наочною, коли розглянути численні приклади хибного сприйняття в міжнародній історії, які демонструють системний характер помилок у реконструкції мотивів та інтенцій зовнішніх акторів. Протягом століть як політичні лідери, так і аналітики здійснювали помилки різного масштабу – від неправильного трактування сигналів під час дипломатичних переговорів до некоректної інтерпретації розвідувальних даних, що у найкритичніших випадках призводило до неспроможності передбачити ворожі дії чи належно оцінити ймовірність ескалації конфлікту. Р. Джервіс, який зробив визначальний внесок у вивчення психологічних вимірів міжнародної політики, наголошує, що поширене інтуїтивне припущення про здатність осіб, які ухвалюють рішення, «зазвичай сприймати світ досить точно», а всі випадки хибного сприйняття трактувати як випадкові відхилення, є концептуально хибним. На його думку, хибні інтерпретації не є винятком із правила, а радше відображають структурні обмеження людського мислення, інформаційного середовища та політичного контексту, в якому відбувається ухвалення рішень [33, p. 3].

Дилеми, що випливають із проблеми «чужих розумів» та неоднозначного символізму озброєнь, супроводжують міждержавні відносини від витоків міжнародної історії й залишаються актуальними у сучасних стратегічних дебатах. Вважається, що перший ґрунтовний аналіз війни в західній традиції належить історику і полководцю Фукідіду, в якому він фактично окреслив сутність дилеми безпеки як ключовий рушій ескалації. Описуючи причини Пелопоннеської війни, Фукідід наголошував, що її породило зростання

могутності Афін і страх, який це викликало у Спарти. На стратегічному рівні лідери обох полісів зіткнулися з необхідністю одночасного вирішення дилеми інтерпретації (визначення намірів і потенціалу іншої сторони) та дилеми реагування (вибору оптимальної лінії поведінки за умов невизначеності). Двоетапне когнітивно-стратегічне напруження, властиве дилемі безпеки, демонструє безперервність проблеми між довірою та страхом у міжнародній політиці протягом двадцяти семи століть [1, 2015, p. 2].

Концепція «пастки Фукідіда» (Thucydides trap), розроблена Ґ. Алісоном (G. Allison) описує високий ризик війни між висхідною державою та державою домінуючою, що відчуває виклик своїй перевазі. Г. Аллісон запропонував сучасне теоретичне осмислення цього феномену як структурної властивості міжнародної системи, що виникає в ситуації, коли держава-претендент прагне переглянути існуючий баланс сил, тоді як домінантна держава намагається його зберегти. У межах порівняльного дослідження Г. Аллісон проаналізував шістнадцять історичних випадків зіткнення між гегемонами та висхідними державами й виявив, що у дванадцяти з них суперництво завершилося великою війною. На цій підставі він дійшов висновку, що «пастка Фукідіда» становить системну та повторювану загрозу стабільності міжнародного порядку [1, 2015, p. 4]. Центральним питанням його досліджень стало з’ясування того, чи здатні США і Китай у XXI столітті уникнути логіки силового зіткнення, властивої багатьом історичним аналогам. На думку Г. Аллісона, запобігання ескалації потребує цілеспрямованого стратегічного управління суперництвом, зокрема інституціоналізованого діалогу, дипломатичної гнучкості та стриманості у демонстрації сили [2]. Поширення цього підходу в аналітичних колах стало особливо помітним на тлі стрімкого зростання потуги Китаю та відповідного посилення стратегічної тривоги у США. До російського вторгнення в Україну 2022 року саме тайванське питання вважалося найбільш імовірною точкою виникнення конфлікту між великими державами – «війни переходу влади», яку низка аналітиків розглядала як майже неминучу за відсутності активних

механізмів стримування ескалації [2].

Дилеми інтерпретації систематично ставлять перед особами, відповідальними за формування національної безпекової політики, складні аналітичні завдання, розв'язання яких передбачає оцінку суперечливих сигналів, неоднозначних намірів і стратегічних можливостей інших акторів. Проблеми виразно проявлялися у відносинах між наддержавами під час холодної війни, у міжетнічних конфліктах на Балканах у 1990-х роках, а також у сучасній еволюції стратегічної взаємодії між Китаєм та США. Особи, які формують політику, опиняються перед необхідністю визначити, чи свідчать військово-технічні новації та доктринальні зміни потенційних суперників про намагання зміцнити власну безпеку і зберегти статус-кво, чи вони є індикатором ревізіоністських амбіцій, спрямованих на його перегляд. Додаткову складність становлять ситуації, коли заходи, мотивовані потребами захисту, на практиці підвищують вразливість інших держав, стимулюючи тим самим конфронтаційну динаміку. Хоча з аналітичної точки зору дилема реагування постає лише після того, як сформовано інтерпретацію намірів і потенціалу іншої сторони, на практиці обидва виміри дилеми безпеки (інтерпретаційний та реактивний) відбуваються паралельно й переплітаються в процесі ухвалення рішень. Дилема реагування ставить перед політичним керівництвом вибір між двома базовими стратегічними підходами. Перший передбачає спробу продемонструвати заспокоєння шляхом сигналів, риторики та поведінкових кроків, які знижують напругу та мінімізують ризик ескалації. Другий полягає у формуванні стримувальних сигналів, що мають на меті продемонструвати рішучість реагувати на потенційно загрозливі тенденції у військовій політиці та практиці іншої сторони [34, pp. 58-111].

Дилема безпеки фактично зникає лише тоді, коли дилема інтерпретації отримує остаточне рішення на користь позиції, згідно з якою інша держава однозначно кваліфікується як загроза національній безпеці і тому визначається як «ворог»; у такому випадку невизначеність щодо мотивів та намірів зовнішнього актора нібито усувається, оскільки питання інтерпретації набуває

остаточної форми, а інша сторона переходить у категорію «стратегічного виклику» (strategic challenge). Проте ця трансформація невизначеності є лише ілюзорною: зміна статусу від дилеми до виклику не знімає фонового ризику, а переформатовує його, замість проблеми розпізнавання намірів постає інший набір невизначеностей (uncertainty), пов'язаних із наслідками консолідованого визначення противника, зокрема з імовірністю гонки озброєнь, поглибленням протистояння та підвищеним ризиком фактичного збройного конфлікту. Можливо, визначення «стратегічного виклику» виявиться помилковим: заходи іншої сторони, які мають суто оборонний характер (або пояснюють як оборонний) мотив, можуть бути інтерпретовані як агресивні або потенційно ревізіоністські. У такому випадку відповідь, яка базується на хибній інтерпретації, здатна породити небажану ескалацію. Отже, перехід від невизначеності інтерпретації до певності в ідентифікації загрози формально ліквідовує один різновид невизначеності, але водночас відкриває інший, тобто невизначеність щодо траєкторії і наслідків конфронтаційних заходів. Таким чином з'являється парадокс безпеки (security paradox) [7, p. 9].

Концептуальна помилка міститься в ототожненні дилеми безпеки з парадоксом безпеки. Парадокс постає як наслідок динаміки дилеми безпеки, що проявляється у спіралі зростання незахищеності, яку генерує взаємне та взаємозалежне хибне трактування оборонних намірів іншої сторони як потенційно загрозливих. Відповідно, парадокс безпеки визначається як ситуація, у якій два або більше акторів, які прагнуть виключно посилення власної безпеки через певні політичні чи військові дії, фактично провокують зростання напруженості та зниження рівня безпеки для всіх учасників [7, pp. 6-10]. Концепт парадоксу безпеки отримав інтелектуальний імпульс від спіральної моделі Р. Джервіса, в основі якої лежить припущення, що політичні лідери та стратегічні планувальники не здатні визнати, що їхні власні дії можуть бути інтерпретовані іншими як загрозливі, а також переконання, що ворожі кроки іншої сторони зумовлені її агресивністю, а не реактивністю або страхом [33, 75]. Невміння побачити загрозу у власних діях і схильність трактувати дії інших як ворожі

запускає спіралеподібну ескалацію недовіри. Страх, у такій конфігурації, виступає визначальним рушієм міжнародної поведінки, оскільки він живить стратегічну обережність, недовіру та схильність до секретності. Анархічність міжнародної системи, побудованої за принципом самодопомоги (self-help), підсилює цю динаміку: держави побоюються втрати престижу, внутрішньополітичних викликів їхній легітимності у випадку проявів слабкості, а також потенційного тиску чи прямої агресії з боку інших акторів. Для деяких політичних еліт страх стає не лише фоном стратегічного мислення, а фундаментальним фактором формування зовнішньої політики.

У концептуальній традиції Д. Герца (J. H. Herz) страх має ще більш первинний статус. Він стверджував, що основне питання, яке лежить в основі соціального життя протягом усієї людської історії, полягає у дихотомії «вбити або загинути» («kill or perish») [25, p. 3]. Така світоглядна установка формує потужну структуру міжгрупової недовіри та потенційного конфлікту, що постає не лише з матеріальних факторів, а з базового екзистенційного відчуття небезпеки. Страх, у тлумаченні Герца, конструює той тип взаємодії, у межах якого дилема безпеки легко перетворюється на парадокс безпеки.

Перегляд власної концепції Д. Герц здійснив у статті 1981 року, в якій він демонструє суттєве поглиблення розуміння та осмислення дилеми безпеки. З’являється якісно інший контекст – глобальної взаємозалежності, ядерної взаємної уразливості та зростання проблем, що виходять за межі традиційного розуміння національної безпеки. Ризики, які раніше діяли як міждержавні, тепер набувають універсального, системного характеру: страх, що був рушійною силою дилеми безпеки у її класичному вигляді, став фактором дестабілізації окремих регіонів чи локальних балансів сил, який перетворився на потенційний детонатор глобальної катастрофи. Дилема безпеки, яка була насамперед описом механізму міждержавної взаємної недовіри, відтепер постає як феномен, що одночасно репродукується на кількох рівнях між державами, їх союзами, світовими центрами сили та, зрештою, між сенсом силового мислення та

колективного виживання людства [26, p. 1].

Класична структура самодопомоги, яка нібито забезпечує державі автономію, у світі глобальних екзистенційних загроз починає діяти у зворотному напрямку. Традиційна логіка накопичення сили та зосередження на вузьких вимірах національних інтересів уже не гарантує безпеки, а навпаки підсилює системну вразливість. Те, що раніше було раціональною стратегією виживання, тепер може бути системно ірраціональним у довгостроковій перспективі. Проблема національного інтересу більше не може розглядатися у відриві від глобальних інтересів, оскільки національна безпека більше не може бути забезпечена виключно інструментами, спрямованими на посилення власної потужності, оскільки масштаб і характер загроз робить виживання однієї держави нерозривно пов'язаним із виживанням усіх. Відбувається трансформація дилеми безпеки, бо вона перетворюється на динаміку, де вузько орієнтовані силові практики окремої держави чи групи держав створюють загрози для глобальної стабільності і тим самим для власного існування [26, p. 2].

Автор вводить поняття «реалістичного лібералізму» як спроби інтегрувати у стратегії безпеки як структурні обмеження анархії, так і необхідність пом'якшення страху та взаємної недовіри шляхом інституціонального та політичного врівноваження короткострокових силових імперативів довгостроковою логікою виживання. Це є принциповим моментом, оскільки Д. Герц фактично пропонує шлях пом'якшення дилеми безпеки без руйнування основних положень реалізму: визнаючи неможливість повного усунення структурної невизначеності намірів, він одночасно стверджує необхідність стримування тих форм поведінки, які перетворюють страх на самовідтворювану спіраль глобального масштабу. Таким чином, дилема безпеки є міждержавним феноменом та внутрішньою суперечністю самих стратегій безпеки, які за умов зростаючої взаємозалежності можуть вступати у конфлікт із власними довгостроковими цілями. Центральним елементом цього переосмислення залишається страх як структурний імпульс, який формує практики держав і який

в умовах ядерної сили (nuclear power) перетворюється з локальної проблеми на системний ризик. Виникає необхідність переходу до універсального бачення безпеки, яке визнає, що запобігання глобальним катастрофам є необхідною умовою забезпечення національних інтересів. Дилема безпеки постає як багаторівнева система взаємозалежних страхів і взаємних обмежень, де межа між раціональністю та небезпекою все більше розмивається [26, p. 2].

Ментальні установки, які визначають політику національної безпеки, формуються під впливом страху, очікування суперництва та орієнтації на найгірші можливі сценарії, отже будь-якій державі з оборонною мотивацією надзвичайно складно здійснити переконливе сигналізування мирних намірів, оскільки адресат інтерпретує повідомлення не через фактичний зміст, а через призму власних підозр, історичного досвіду та стратегічних припущень. Неможливість «сигналізувати свій тип» (signal type) означає, що жодна держава не здатна забезпечити сприйняття своїх дій як однозначно ненаступальних, а отже певний рівень невизначеності та страху є структурно невідворотним навіть у сприятливі періоди міждержавних взаємодій. Фундаментальна пастка політичного й стратегічного сигналізування полягає в тому, що результат залежить не від того, хто надсилає сигнал, а від способу, яким інша сторона його інтерпретує, і саме ця асиметрія сприйняття створює глибокі перешкоди для передачі миролюбних мотивів [20, p. 7-8]. Якщо держави не можуть передати мирний намір із майже стовідсотковою впевненістю, тоді певний ступінь невизначеності та страху не можна уникнути навіть у найкращі часи у відносинах між такими державами.

Ретроспективні спроби реконструювати державні наміри дають ілюзію зрозумілості, однак навіть історики, маючи доступ до ширших джерел і працюючи з аналітичною дистанцією, часто не можуть погодитися щодо справжніх мотивів лідерів минулого. За умов хронологічного віддалення та інформаційного надлишку інтерпретації залишаються суперечливими, отже складність, із якою стикаються сучасні особи, відповідальні за національні рішення, є «нерозв’язною дилемою» (irreducible dilemma). Вони мають

оцінювати наміри інших в умовах гострого дефіциту часу, браку ключової інформації, високої цінності потенційної помилки та масштабів можливих людських і матеріальних втрат. Дилема безпеки набуває найбільш драматичного характеру, оскільки необхідність ухвалення рішень під тиском невизначеності та страху робить навіть найобережніші інтерпретації потенційно фатальними, а спроби уникнути конфлікту – джерелом його ненавмисної ескалації.

1.2 Трансформація невизначеності в теоріях міжнародної безпеки

Невизначеність постає як екзистенційна умова людських відносин і становить неминучу складову реальності, у якій функціонують як окремі індивіди, так і соціальні групи. Вона може виявлятися нерівномірно, адже різні актори відчувають, інтерпретують і реагують на неї по-різному. Історичний досвід демонструє, що існували періоди, у яких одні держави або суспільства мали більш захищене становище порівняно з іншими. Зокрема, інституціолізована міждержавна співпраця або наявність усталених практик довіри в межах безпекових спільнот здатні забезпечувати високий рівень безпеки навіть у середовищі державної системи, де невизначеність повністю не зникає. Майбутня невизначеність надає міжнародним відносинам характеру пастки незахищеності, тому виникає необхідність обережності з боку тих, хто відповідає за безпеку держави та її населення, оскільки держави «повинні припускати найгірше», оскільки «найгірше є можливим» [56, p. 28].

У концептуалізації дилеми безпеки, яку запропонував Д. Герц, невизначеність відіграє визначальну роль. Автор окреслив дилему як стан, у якому «групи чи особи, які повинні турбуватися про свою безпеку, захищаючись від нападу, підкорення, домінування або знищення іншими групами та особами» [25, p. 157]. Хоча Герц відкинув радикальну тезу про те, що «кожен індивід, ізольований, завжди виступає та діє як ворог для всіх інших», він наполягав на існуванні «фундаментальної соціальної констеляції», яка охоплює «взаємну

підозру та взаємну дилему» [25, p. 158]. Дилему безпеки він описував як «порочне коло», що не має очевидного виходу, першопричина якого полягає «не в тому, чи є людина «за природою» мирною та схильною до співпраці, чи агресивною та домінуючою». Визначальним чинником виступає невизначеність щодо намірів інших, що занурює акторів у фундаментальну дилему і перетворює її на стрижневий факт соціального життя [25, p. 158]. Екзистенційна умова невизначеності, яку Герц визначив як «фундаментальну соціальну констеляцію», дозволяє розглядати дилему безпеки як найбільш суттєву дилему міжнародних відносин. Вона спонукає держави враховувати можливість незахищеності навіть у тих ситуаціях, коли загроза не виглядає безпосередньою. За таких умов уряди прагнуть сигналізувати іншим акторам свої мирні або оборонні наміри. Проте для тих, чия стратегічна культура формується під впливом тіні майбутньої невизначеності, міждержавна політика постає як потенційна або фактична «система війни», навіть якщо всі сторони щиро переконані у мирному характері власних намірів та оборонній спрямованості військових приготувань. Безпекове суперництво у міжнародних відносинах осмислюється через три підходи, кожен з яких пропонує різне пояснення його природи та меж подолання.

Фаталістичний підхід виходить із переконання, що уникнення безпекового суперництва неможливе за визначенням. Основою такого бачення є уявлення про незмінність людської природи та анархічного середовища міжнародної системи, де держави змушені покладатися лише на власні ресурси. Будь-яка група людей, об’єднана в політичну спільноту, неминуче існуватиме у світі суперництва, недовіри та конфлікту. Раціональна поведінка держави полягає у нарощуванні потужності, насамперед військової, оскільки довіряти іншим у довгостроковій перспективі не можна. Співпраця можлива лише тоді, коли вона прямо збігається з вузько трактованими національними інтересами. Держави постають раціональними егоїстами, які надають пріоритетне значення власній безпеці та не вважають добробут інших самодостатньою цінністю. Раціональна поведінка сприяє недовірі до інших урядів та отриманню будь-якої переваги, яку можна використати для збільшення власної могутності. Співпраця не виключається, але

за умови, що вона відповідає безпосереднім власним інтересам. Держави розглядаються як «раціональні егоїсти», де актори надають «першочергового значення власній безпеці... і не дуже дбають про добробут інших» [35, p. 364].

Проявом фаталістичного підходу в сучасній теорії міжнародних відносин є «наступальний реалізм» та його представник американський дослідник Дж. Міршаймер (J. J Mearsheimer), який пропонує власне бачення ролі гегемонії у міжнародній політиці і пояснює поведінку великих держав як структурно зумовлену боротьбу за перевагу. На його переконання, міжнародне середовище історично постає жорстким, непередбачуваним і небезпечним, і ця характеристика не є тимчасовою відхиленням, а відтворюється впродовж усієї історії міждержавних відносин. Великі держави, навіть у періоди відносного зниження напруженості, зберігають взаємний острах і змушені постійно конкурувати за владу й вплив. Їхня амбіція не обмежується прагненням бути найсильнішими серед інших великих держав; стратегічною метою стає досягнення домінування в системі, тобто становлення єдиним гегемоном, якому ніхто не може кинути виклик. Пояснюючи витоки такої поведінки, Д. Міршаймер наголошує, що держави можуть прагнути лише до забезпечення власної безпеки, однак сама структура міжнародної системи, анархія, відсутність гарантій миру та неможливість бути певним у намірах інших, змушує їх діяти наступально й нарощувати потужність, навіть у випадках, коли агресивні наміри відсутні. У результаті формується ситуація, яку ніхто цілеспрямовано не створює, але яка неминуче штовхає держави до поведінки, що породжує конкуренцію, страх і загострення суперництва. Сам Д. Міршаймер визначає цю ситуацію як справді трагічну, бо її походження не в аморальності держав, а в системі, що примушує навіть оборонно налаштованих акторів діяти агресивно [50, p. 2–3].

У подальших роботах Д. Міршаймер уточнює, що здобуття статусу регіонального гегемона є ключовою довгостроковою метою великої держави, оскільки саме регіональне домінування забезпечує найвищий рівень безпеки та стратегічної автономії. Гегемон володіє здатністю формувати правила

регіонального порядку, стримувати потенційних суперників і мінімізувати зовнішні ризики. Ця мета випливає з анархічної структури міжнародної системи, яка позбавляє держави зовнішніх гарантій захисту. У такому баченні гегемонія є прямим продовженням розуміння суперництва великих держав як постійної структурної характеристики міжнародної політики, де боротьба за владу, вплив і домінування становить фундаментальний імператив міждержавної взаємодії (Mearsheimer 2023).

Поміркований підхід містить набір припущень, що безпекове суперництво може бути зменшене, хоча й не остаточно усунуте. Ключовими його проявами є концепції «безпекових режимів» (security regime) [35] та «міжнародного суспільства» (international society) [11], які формують навички та практики безпекової співпраці, спрямовані на тривале пом'якшення небезпек суперництва в умовах міжнародної анархії, визначеної як відсутність верховного органу влади над державами. Поміркований підхід визнає анархічність міжнародної системи, однак це не означає, що анархія є синонімом хаосу чи постійного насильства. Концепція «безпекових режимів» визначає режими, які через взаємне навчання та інституціолізацію прагнуть запровадити елементи передбачуваного порядку у відносини між державами [35, p. 368]. Концепція «міжнародного суспільства» (також відома як «Англійська школа») наголошує на формуванні суспільства держав через розвиток інститутів міжнародного права [11] та практик поміркованої дипломатії [68]. Метою є забезпечення взаємної безпеки через механізми співпраці та зміцнення довіри, отже міжнародний порядок постає більш передбачуваним, а дилема безпеки стає пом'якшеною, хоча й не усуненою повністю.

Поміркований підхід ставить під сумнів фаталістичне припущення про неможливість зрозуміти зустрічний страх іншого. У 1980-х роках концепція «спільної безпеки» (common security) акцентувала увагу на необхідності зменшення найнебезпечніших характеристик суперництва наддержав у період «холодної війни». Ключовою була ідея безпеки з іншими, а не проти інших, що передбачала здатність сторін до певного рівня розуміння страхів одна одної. На

практиці це найповніше втілюється в «чутливості до дилеми безпеки» (security dilemma sensibility) – розумінні того, як власні дії можуть підсилювати взаємну недовіру і створювати ризик втрати контролю над ескалацією. Чутливість до дилеми безпеки полягає у здатності побачити роль страху у сприйнятті й військовій поведінці інших, а також усвідомити, яким чином власні кроки можуть цей страх провокувати [7, p. 7].

Трансцендентний підхід ґрунтується на переконанні, що соціальний, політичний та економічний устрій людського співіснування не є жорстко детермінованим історичними обставинами. На відміну від попередніх бачень, акцент зроблено на здатності людей і політичних спільнот до цілеспрямованої дії, що дозволяє переосмислювати та трансформувати наявні реалії. Хоча структурні обмеження залишаються значущими, вони не визначають можливості змін вичерпним чином. Тому політичні актори здатні поступово формувати середовище, в якому умови безпеки стають стабільнішими та менш конфліктогенними. Трансцендентний підхід пропонує як ширший спектр напрямків, так і включення більш обнадійливих шляхів взаємодії з дилемою безпеки. Деякі з цих напрямків є реформістськими, інші – революційними. Серед реформістських напрямків особливе значення має концепція «безпекових спільнот» (security communities). Революційні напрямки включають повалення капіталізму, скасування патріархату та ліквідацію анархії, з переконанням, що незахищеність є наслідком однієї фундаментальної причини. Усі вони поділяють віру в те, що можливо, хоча й надзвичайно важко, побудувати радикально інші світові порядки, у яких загроза або застосування сили буде радикально знижена.

Найбільш розробленою та практично впливовою концепцією в межах трансцендентного підходу є теорія «спільноти безпеки». Її найпомітнішим політичним втіленням став проєкт післявоєнної інтеграції в Західній Європі, започаткований наприкінці 1940-х років, що був спрямований на забезпечення стабільного миру, економічного розвитку та запобігання відновленню міждержавних конфліктів у регіоні. У цьому емпіричному прикладі, який згодом

охопив ширший простір, військове суперництво між державами-учасницями було поступово усунене. Проте, невизначеність щодо майбутніх взаємин не зникла повністю, оскільки жодна форма співпраці не може усунути її цілковито. Крім того, члени спільноти безпеки можуть з обережністю ставитися до намірів держав, які перебувають поза межами цього об'єднання. Повномасштабне вторгнення росії в Україну у 2022 р. чітко продемонструвало, що зменшення інтенсивності безпекових дилем усередині певної групи держав може супроводжуватися їх загостренням для інших. Те, що російське керівництво інтерпретувало як «експансію НАТО», яка нібито підвищує загрози для росії, для країн Центральної та Східної Європи означало посилення колективної безпеки та створення умов передбачуваності.

За оцінками прихильників цієї концепції, європейська спільнота безпеки характеризується стійкими зразками співробітництва на міждержавному та суспільному рівнях, інституціолізованими механізмами довіри та відсутністю підготовки до війни одна проти одної. Війна між її членами вважається практично виключеною. У класичному визначенні К. Дойча спільнота безпеки – це група людей, яка стала інтегрованою. Під інтеграцією (integration) мається на увазі досягнення на певній території почуття спільноти, а також формування інститутів і практик, достатньо стійких і поширених, щоб забезпечити надійні очікування мирних змін. Під «почуттям спільноти» (sense of community) розуміється переконання, що спільні соціальні проблеми повинні та можуть вирішуватися шляхом мирних змін. Під мирними змінами (peaceful change) – вирішення соціальних проблем, зазвичай за допомогою інституціолізованих процедур, без вдавання до масштабного фізичного насильства [16, p. 5].

Теоретично ця модель може бути поширена і на ширше міжнародне середовище, але на практиці її глобальне відтворення залишається малоймовірним. Деякі аналітики вважають, що війна росії проти України суттєво ускладнила перспективи просування до такого світового порядку, оскільки актуалізувала процеси ремілітаризації та посилення військово-політичних

союзів. Водночас історичний досвід свідчить, що значні кризи нерідко ставали каталізаторами подальших інституційних трансформацій, як це відбулося після світових воєн або під впливом травматичного досвіду Голокосту, що сприяв формуванню концепції універсальних прав людини.

Кожен із трьох підходів формує власні орієнтири для майбутньої безпекової політики. Деякі аналітики вважають, що наступальний реалізм забезпечує найбільш дієві гарантії безпеки для найсильніших акторів, однак його довгостроковий ефект полягає у відтворенні історичної та потенційно ще більш руйнівної «військової системи», загостреної появою дедалі небезпечнішого озброєння. Підхід безпекових режимів пропонує механізми пом'якшення напруженості, але історичний досвід свідчить, що більшість режимів містять «насіння власного знищення», оскільки залежать від мінливої політичної волі держав. Серйозною перевагою англійської школи є її фокус на можливостях для політиків будувати довготривалий міжнародний порядок, спираючись на спільні інтереси, норми та цінності. Проте її практична реалізація часто блокується тим, що державні лідери ставлять імперативи національних інтересів вище за зобов'язальні міжнародно-правові норми та інституції.

З позицій трансцендентного підходу найперспективнішою відповіддю на дилему безпеки є поширення безпекових спільнот. Їхній розвиток демонструє, що хоча шлях є тривалим і нерівномірним, він відкриває можливість формування середовищ, у яких застосування сили втрачає раціональність у внутрішніх відносинах. Приклад ЄС підтверджує складну, але реалістичну траєкторію становлення безпекової спільноти. Сприятливі та кризові періоди змінювали одне одного, однак після російського вторгнення в Україну у 2022 році відбулася значна консолідація бачення та цінностей ЄС. Очевидно, що розбудова будь-якої безпекової спільноти, заснованої на багаторівневій координації та міцній довірі між державами й суспільствами з різними мовами, культурами й історичним досвідом є проєктом масштабу поколінь.

Теорія і практика безпекових спільнот ставлять під сумнів усталені припущення про природу міжнародної системи суверенних держав. Хоча члени

такої спільноти не усувають дилему безпеки повністю, вони значною мірою змінюють баланс між невизначеністю та передбачуваністю: їхня поведінка і ставлення формуються у контексті стабільної інституційної взаємодії та високого рівня довіри. У межах ЄС символічні сигнали, пов'язані зі збройними силами, втрачають двозначність, оскільки внутрішнє військове планування не відбувається за логікою потенційного конфлікту. «Проблема інших розумів» тут більше стосується нормальної політики суспільного розвитку, а не екзистенційної боротьби за виживання. Зовнішні відносини спільноти з державами та недержавними акторами, які не поділяють її норм і практик, залишаються в рамках традиційної, значно менш безпечної культури міжнародних відносин. Отже, дослідження формування довіри, взаємної впевненості та інституційного переплетення є ключовими як для аналітиків, так і для практиків, що прагнуть подолати обмеження сучасної міжнародної системи.

Таким чином, можемо зробити висновки, що невизначеність у міжнародній безпеці є структурною умовою, що робить неможливим повне пізнання намірів інших акторів і створює постійну вразливість, з якої випливає безпекова дилема.

Три провідні підходи пропонують різні способи концептуалізації цієї невизначеності та різні рамки дій у відповідь на неї. Наступальний/традиційний реалістичний підхід розглядає невизначеність як нездоланну та екзистенційно небезпечну, вважаючи раціональним максимізацію сили, недовіру та готовність до превентивних дій. Дилема безпеки є неминучою й самостійно підсилювальною. Поміркований (англійська школа) визнає структурні обмеження невизначеності, але стверджує, що вони можуть бути частково пом'якшені через норми, правила, інституції та розвиток спільних очікувань. Невизначеність не усувається, але стає керованою, а безпекова дилема – менш гострою. Трансцендентний підхід трактує невизначеність як змінну соціально-політичну умову, яку можна істотно перетворити через довгострокове інституційне зближення, зміну колективних уявлень та формування безпекових

спільнот. Системні обмеження не є фатальними, а альтернативні порядки можливі.

Всі три підходи окреслюють спектр можливостей – від фаталістичної логіки виживання до реформістських та трансформаційних стратегій співіснування. Вони демонструють, що характер невизначеності та її наслідки залежать від прийнятої теоретичної перспективи та практики взаємодії. Від того, яку з цих рамок обирають політики та суспільства, залежить, чи стане невизначеність джерелом нездоланної загрози, керованим ризиком або відправною точкою для глибоких політичних трансформацій.

1.3. Фактори системної вразливості: відтворення та поглиблення дилеми безпеки

«Зараження» (contagion) або розповсюдження дилеми безпеки набуває дедалі більшої ваги, оскільки властива цьому феномену динаміка, ймовірно, поширюватиметься впродовж найближчих десятиліть. Міжнародна система входить у фазу, яку можна означити як епоху багаторівневої незахищеності, що одночасно проявляється на локальних і глобальних рівнях. Майбутні виклики, які окреслюються в дослідженнях міжнародної безпеки, формуватимуть широкий спектр невизначеностей у разі відсутності належного колективного реагування. За таких умов дилеми безпеки здатні генерувати підвищену міжнародну тривожність, стимулювати песимістичні інтерпретації глобальних тенденцій і спричиняти ризик перетворення стабільного миру на дилеми безпеки, дилеми – на структурні виклики безпеці, виклики – на ще масштабніші та глибші загрози. Війна росії проти України є і тривалий час залишатиметься огидним та різким, але важливим нагадуванням про те, що міжнародний порядок не гарантує інерційності та передбачуваності, а базові припущення щодо «завтрашнього дня» можуть виявитися хибними та руйнівними.

Дослідники у сфері міжнародної безпеки виділяють чотири ключові фактори, що окреслюють простір міждержавних і транскордонних взаємодій, де дилема безпеки вже діє або має потенціал до виникнення: суперництво великих держав (Great Power Rivalry); розповсюдження ядерної зброї (Nuclear Weapons Proliferation); регіональна небезпека (Regional Insecurity) та тероризм (Terrorism). Аналіз цих факторів свідчить, яким чином характерні для дилеми безпеки механізми поглиблюють страх, формують або посилюють недовіру та звужують спектр можливостей для розвитку співпраці, узгодження інтересів і накопичення довіри. Вони становлять головну загрозу для стабільності міжнародної системи, оскільки здатні зумовлювати небажану ескалацію, відтворювати конфліктогенність поведінки та ускладнювати інституційну адаптацію глобальних і регіональних акторів.

Суперництво великих держав залишається одним із найбільш критичних чинників, що формують ризики «зараження» дилеми безпеки в сучасній міжнародній системі. У теоретичних дослідженнях вже тривалий час наголошується на інституційній та стратегічній нестабільності, пов’язаній із переходами влади (power transitions) між державами, що демонструють зростаючу потужність, та державами, чий відносний вплив зменшується. Найбільш суттєвою зоною занепокоєння виступають відносини між Китаєм і США, оскільки саме їхнє стратегічне суперництво має найбільший потенціал структурувати майбутню систему безпеки. Попри наявність спільних інтересів (торговельних, екологічних, регіонально-стабілізаційних) між США і Китаєм зберігається значний перелік потенційних точок конфлікту. Особливо небезпечними вважаються Тайванська протока та Південно-Китайське море, які вже характеризуються високим рівнем мілітаризації та присутністю силових засобів у безпосередній близькості від зон, які обидві сторони трактують як сфери життєво важливих інтересів. За таких обставин ризик ескалації істотно зростає, атмосфера недовіри посилюється через конкретні військові дії й розвиток технологій, що мають стратегічне значення: можливості протиракетної оборони, мілітаризацію космосу, а також поширені в окремих політичних колах

припущення, що перевага у ядерній ескалації може стати визначальним чинником у разі кризи. Якщо КНР та США продовжать діяти, виходячи з припущень найгіршого сценарію, інтерпретуючи військові інструменти один одного як потенційні загрози, а наміри як стратегічно ворожі, то кожна зі сторін відчуватиме структурний примус шукати безпеки за рахунок іншої. За таких умов їхня взаємодія неминуче набуватиме рис нової «холодної війни», що супроводжуватиметься підвищеною невизначеністю, конфліктними наративами, посиленою тривогою та потенційно катастрофічними наслідками, властивими цьому типу міжнародної конфронтації.

Розповсюдження ядерної зброї залишається однією з найбільш критичних тенденцій, що здатні посилити динаміку дилеми безпеки у глобальному масштабі. Одним з перших чинників є руйнування режиму нерозповсюдження, ще до початку російської агресії проти України, оскільки міжнародні аналітики фіксували зростання сумнівів щодо довгострокової стабільності Договору про нерозповсюдження ядерної зброї та його здатності стримувати появу нових ядерних держав. Після початку війни ці занепокоєння значно посилилися, спричинені інтенсивним використанням російським керівництвом риторики, що припускає можливість військового застосування ядерної зброї, виходячи за межі суто стримування. Таким чином відновлюється уявлення про ядерну зброю як інструмент примусу й стратегічного шантажу, що підриває фундаментальні норми ядерної стабільності.

Другим чинником стала поширена хибна інтерпретація досвіду України, яка нібито втратила свій ядерний статус після підписання Будапештського меморандуму 1994 р., що відповідно спричинило вразливість до російської агресії. Насправді Україна не володіла автономним оперативним контролем над ядерними силами, розміщеними на її території, оскільки системи управління залишалися під юрисдикцією радянського, а згодом російського командування. Крім того, в Україні усвідомлювали, що Будапештський меморандум не містив дієвих інструментів, отже не міг вважатись документом, що гарантує захист в разі агресії й це він був наслідком прийняття рішення щодо володіння ядерною

зброєю, а не навпаки. Проте незалежно від фактичної історичної реальності деякі держави можуть дійти протилежного висновку, інтерпретуючи український випадок як підтвердження тези, що відмова від ядерної зброї підвищує ризики зовнішньої агресії. Така позиція створює можливість формування «ядерного каскаду» - ланцюгової реакції розповсюдження, яка вже тривалий час викликає занепокоєння в дослідників, за винятком окремих прихильників стабілізуючого плюралізму, серед яких найвідомішим є К. Уолтс [64].

Додаткову напругу створює розширення доступу до чутливих компонентів «цивільних» ядерних програм. Це загострює побоювання щодо можливості прихованої диверсифікації у напрямі створення військових ядерних можливостей під виглядом мирного атома. Показовим прикладом стала ініціатива AUKUS (2021), яка передбачає передачу Австралії технології ядерних реакторів для підводних човнів. Хоча декларативною метою було посилення регіональної обороноздатності, у низці держав виникло занепокоєння, що такий технологічний трансфер може створити передумови для розвитку автономної військової ядерної інфраструктури у майбутньому [21]. Якщо уряди інтерпретуватимуть сигнали один одного у сфері ядерних технологій через призму підозри, це може стимулювати превентивні кроки, спрямовані на «страхування» від потенційного колапсу режиму ДНЯЗ. Така інтерпретація самозахисту здатна сформувати низку системних ризиків: збільшення ймовірності несанкціонованого або випадкового застосування ядерної зброї, появу загроз, пов’язаних із втраченими чи нелегально переміщеними боєголовками, залучення недержавних акторів до ядерного підприємництва, а також швидку та небезпечну ядерну ескалацію в регіональних кризах, де держави не володіють розвинутими системами командування і контролю.

У сучасному середовищі додатковим ускладнюючим фактором виступає вплив соціальних мереж на процес прийняття рішень під час ядерних криз. Інформаційне перевантаження, ненадійність джерел, швидке поширення недостовірних даних і політично мотивованих інтерпретацій можуть підвищувати ризики стратегічних прорахунків. Це створює додаткову взаємодію

між технологічною невизначеністю та традиційною дилемою безпеки. Крім того, важливим, але системно недооціненим параметром залишається роль випадковості у перебігу ядерних криз. Дослідження Карла Р. Шервіна та інших авторів щодо Карибської кризи 1962 року демонструють, що запобігання катастрофі значною мірою було зумовлене набором контингентних обставин, які могли скластися інакше. Цей історичний досвід підкреслює фундаментальну тезу: ядерна стабільність є не тільки результатом раціональної стратегії, але й відображенням неконтрольованих змінних, що підвищує загальну вразливість міжнародної системи [67].

Регіональні конфлікти, що тривають десятиліттями, формують складні конфігурації дилеми безпеки, здатні запускати нові перегони озброєнь та підвищувати ризики ескалації на локальному й глобальному рівнях. У низці таких регіональних систем присутні держави, що володіють ядерною зброєю, значним арсеналом конвенційних сил і високим рівнем стратегічної недовіри, що створює багатовимірні та взаємопов'язані загрози. Південна Азія є одним із найбільш чутливих регіональних вузлів. Динаміка індійсько-пакистанського суперництва у сфері озброєнь значною мірою визначається пакистанським занепокоєнням щодо конвенційної переваги Індії. Водночас Індія вимушена розподіляти свою увагу між Пакистаном та Китаєм, який не лише є її власним ядерним конкурентом, але й відіграв ключову роль у становленні пакистанської ядерної програми. Стратегічне середовище додатково ускладнюється тим, що пакистанські військові та розвідувальні структури, згідно з оцінками багатьох аналітиків, підтримують ісламістські групи, здатні здійснювати атаки проти індійських цілей, що створює ризик неконтрольованої ескалації. У відповідь Індія розбудовує потенціал швидкого конвенційного реагування з метою стримування та точкового силового впливу. В умовах взаємної недовіри обидві сторони схильні тлумачити дії опонента за сценаріями найгіршого випадку, що посилює сприйняття загрози.

Особливо гострим залишається ризик регіональних перегонів озброєнь на Близькому Сході, де невизначеність навколо ядерного потенціалу Ірану є

ключовим джерелом стратегічної напруги. Іранська програма цивільної ядерної енергетики розглядається багатьма державами як потенційна ширма для розроблення ядерної зброї. Якщо Іран досягне ядерного статусу або навіть якщо регіональні актори повірять, що він наближається до цього, Саудівська Аравія, Туреччина та інші держави можуть ініціювати власні програми, запускаючи ефект ланцюгової реакції. В умовах конкуренції за регіональне домінування та відсутності міцних механізмів довіри не можна виключити сценарії превентивних ударів як інструменту стримування і примусу. Таким чином, регіональні конфліктні зони залишаються важливими каталізаторами стратегічної нестабільності. Вони асоціюються з високою ймовірністю хибної інтерпретації намірів, неконтрольованої ескалації та виникнення локальних криз, здатних перерости у конфлікти ширшого масштабу, особливо за наявності ядерних компонентів та зовнішніх покровителів.

Тероризм як фактор «зараження» дилеми безпеки проявився особливо різко після атак «Аль-Каїди» на Сполучені Штати 11 вересня 2001 р., коли адміністрація Д. Буша оголосила глобальну «війну з терором», фактично інституціоналізувавши транснаціональний вимір терористичної загрози. У наступні роки терористична тактика активно застосовувалася в Європі, руйнівні інциденти відбувалися на Близькому Сході, в Африці та Азії. Міжнародний тероризм продовжує спиратися на локальні соціально-політичні кризи, але дедалі частіше функціонує в синергії з ширшими регіональними та глобальними протистояннями, що ґрунтуються на культурних, релігійних та ідентифікаційних поділах. Відбувається перетворення терористичних ризиків на багаторівневі й глобалізовані: від індивідуальних атак у публічних місцях до загроз застосування «брудних» бомб, біологічних агентів та потенційних масштабних акцій, спрямованих на відтворення ефекту подій 11 вересня. Такі видовищні напади мають на меті масові жертви, масштабні соціальні порушення та політичні наслідки, що формують довготривалу атмосферу страху.

Одним із найбільш показових проявів «зараження» дилеми безпеки є феномен «внутрішнього терориста», коли підозра і страх перед насильницьким

екстремізмом переноситься на співгромадян. За умов, у яких є ймовірність, що насильство може бути ініційоване окремим індивідом, зокрема із застосуванням суїцидальної тактики, дилема безпеки індивідуалізується та глобалізується. Страх стає частиною повсякденного досвіду, змушуючи людей упереджено інтерпретувати поведінку інших і підвищувати рівень недовіри навіть у відносно стабільних суспільствах. Поширенню такого стану сприяють дві ключові структурні характеристики сучасності, які суттєво посилюють невизначеність. Першою з них є феномен «всеохоплюючої омнікризи» - системний комплекс взаємопов'язаних глобальних викликів, включно з кліматичними змінами, деградацією біосфери, конкуренцією за невідновлювані ресурси, масовими міграційними потоками, міжкультурними та міжрелігійними конфліктами, продовольчою та водною незахищеністю, зростанням нерівності та демографічними дисбалансами. Другою характеристикою є радикально посилена боротьба за уми людей, зумовлена стрімкістю та всепроникністю сучасних інформаційних технологій. Її проявами стали операції під чужим прапором, конспірологічні наративи, фейкові новини, постправда, інформаційні війни, мережі ботів, дезінформаційні кампанії та клікбейт-активізм. Контроль над знанням і визначенням «правди» дедалі більше перетворюється на ресурс політичної влади та інструмент конкуренції. Проте, правдивість, точність та «щирість» є складовими безпекової спільноти, оскільки уможливлює спільне використання цінностей, розбудову інститутів, необхідних для взаємної довіри, та багаторівневу довіру для їх підтримки [69].

Сучасна дилема безпеки набуває форми всеохопної невизначеності, яка підсилює глобальні ризики. Попри те що наприкінці 1950-х років Д. Герц охарактеризував дилему безпеки як таку, що досягла «найвищої гостроти», подальший розвиток міжнародної системи лише загострив її прояви. Якщо у добу «холодної війни» головним джерелом небезпеки було суперництво наддержав і перспектива неконтрольованої ядерної ескалації, то сучасна епоха відзначається більш широкою, комплексною та багаторівневою невизначеністю. Динаміка дилеми безпеки, яка раніше була зосереджена переважно у

міждержавних взаємодіях, нині стала глобалізованою та водночас індивідуалізованою, її ефекти проявляються одночасно на рівні міжнародних структур і повсякденних соціальних практик.

Концепція «чутливості до дилеми безпеки» передбачає здатність політичних акторів усвідомлювати власні страхи та враховувати дзеркальні побоювання іншої сторони, що відкриває можливість руйнувати фаталістичні очікування, переорієнтовувати інтерпретації символіки сили та формувати переконливі сигнали мирних намірів. Можливість не є гарантією, оскільки ефективність сигналізування залежить не лише від чесності та майстерності відправника, але й від когнітивних установок, політичних контекстів та стратегічної культури отримувача. Крім того, додається структурний ризик, що страх може комбінуватися з амбіціями, оскільки деякі лідери залишаються стійкими до довіри, не сприймають заспокійливі сигнали або взагалі демонструють поведінку, яка виходить за межі стримування.

Аналіз сучасної міжнародної системи свідчить, що людство не наблизилося до подолання військового сенсу безпеки, а концептуалізація «абсолютної безпеки» виглядає непридатною через нездоланність потенціалу насильства у людських взаємодіях. Проте, ідея безпекових спільнот пропонує найбільш реалістичний шлях до формування альтернативної архітектури міжнародного порядку. Усунення насильства як можливості не передбачається, проте завдяки тривалому інституційному розвитку, взаємній довірі та внутрішній інтеграції війна між членами такої спільноти може стати політично немислимою. За відсутності дієвих підходів майбутня невизначеність, характерна тривога та страх здатні спричинити відновлення деструктивних стратегій, які неодноразово приводили міжнародну систему до кризових станів. Небезпека полягає у поверненні до технологічного оптимізму як способу вирішувати дилеми безпеки силовими або автоматизованими засобами, що знову відтворює «хибне уявлення про останній хід». Паралельно можливе посилення націоналістичного егоїзму, який робить міждержавні відносини заручниками гасла «моя країна понад усе», а також закріплення фаталістичних уявлень про

природу міжнародної політики, у межах яких страх визначає поведінку. Комбінація факторів може відтворити ті самі умови, які неодноразово спричиняли стратегічні катастрофи.

Таким чином, дилема безпеки є структурною характеристикою міжнародного порядку, за якої зусилля держави щодо посилення власної безпеки неминуче сприймаються іншими як потенційна загроза. Онтологічно дилема безпеки має дворівневу структуру, що складається з дилеми інтерпретації та дилеми реагування. Динаміка дилеми безпеки визначається поєднанням матеріального та психологічного вимірів. Парадокс безпеки є наслідком її динаміки і проявляється у спіралі зростання незахищеності, коли дії, спрямовані на підвищення власної безпеки, знижують рівень безпеки для всіх учасників. Фундаментальною складовою дилеми безпеки є проблема стратегічного сигналізування. Держави не здатні переконливо сигналізувати мирні наміри, оскільки сигнали інтерпретуються не за змістом, а через призму підозр, історичного досвіду та стратегічних припущень адресата.

Невизначеність у міжнародній безпеці є структурною умовою, що робить неможливим повне пізнання намірів інших акторів і створює постійну вразливість, з якої випливає безпекова дилема. Три провідні підходи пропонують різні способи концептуалізації цієї невизначеності та різні рамки дій у відповідь на неї: наступальний/традиційний реалістичний підхід, поміркований й трансцендентний. Всі три підходи окреслюють спектр можливостей – від фаталістичної логіки виживання до реформістських та трансформаційних стратегій співіснування.

Дилема безпеки в сучасній міжнародній системі має тенденцію до «зараження» та поширення за межі окремих міждержавних відносин, формуючи багаторівневу й взаємопов’язану вразливість. Чотири ключові фактори поглиблюють і відтворюють дилему безпеки у сучасних умовах: суперництво великих держав, розповсюдження ядерної зброї, регіональна нестабільність та тероризм. Комбінація системних факторів може спричиняти повернення до фаталістичних уявлень про міжнародну політику, відтворення конфліктогенних

стратегій і загострення глобальної нестабільності. Відсутність ефективних відповідей перетворюватиме невизначеність на стійке джерело безпекових криз і масштабних загроз.

РОЗДІЛ 2. ІНФОРМАЦІЙНА ВІЙНА В СИСТЕМІ БАГАТОВИМІРНОЇ СТРАТЕГІЧНОЇ ВЗАЄМОДІЇ

2.1 Еволюція поняття «інформаційна війна» у провідних теоретичних напрямах

Інформаційна війна постає як структурно складний, поліфункціональний та концептуально мінливий феномен, що перебуває у центрі дослідницької уваги теоретиків міжнародних відносин, комунікаційних студій та безпекових наук. Її поліваріантність зумовлена як багатовимірністю інформації як ресурсу влади, так і розширенням інструментарію, що застосовується державними та недержавними акторами з метою модифікації сприйняття, впливу на поведінку та трансформації стратегічного середовища. У науковому дискурсі сформувалися декілька аналітичних підходів до інтерпретації цього явища, кожен з яких пропонує власний кут зору щодо природи інформаційних протиборств, їх функцій у системі міжнародної безпеки та механізмів досягнення політичних результатів.

Широке використання поняття «інформаційної війни» у дослідженнях політичних комунікацій зумовлене тим, що інформаційні операції, на відміну від ізольованих комунікативних актів, здатні забезпечити системне, довготривале та стратегічно орієнтоване формування сприйняття соціальних і політичних процесів. Інформаційні повідомлення, будучи розрізненими, не створюють стійкого масиву комунікаційної присутності держави чи політичного актора в публічному просторі, а отже не здатні забезпечити відтворюваність і масштабування смислів, необхідних для досягнення політичних цілей. Постійне, інтенсивне та ретельно скоординоване інформаційне підкріплення може сформувати ті комунікаційні структури, що відтворюють політико-ідеологічні наративи та забезпечують їхнє закріплення. Ефективність інформаційної війни як формату організації політичної взаємодії зумовлена також тим, що традиційні форми державної інформаційної політики часто виявляються ресурсно

затратними, інерційними та недостатньо адаптивними до динаміки сучасного інформаційного середовища. На противагу, технології інформаційного впливу дозволяють досягати стратегічних ефектів із меншими витратами, забезпечуючи при цьому гнучкість, швидкість і здатність до транснаціональної проєкції сили.

Формування концепту інформаційної війни значною мірою було обумовлене тим, що теоретики, які працювали на перетині військових та політичних наук, надавали перевагу категоріям ширшого філософського та стратегічного порядку. У міру того як політико-дипломатичні, економічні та військові форми протиборства у другій половині XX століття набували дедалі більш системного, комплексного та скоординованого характеру, інформаційний вимір цих процесів перетворювався на ключовий інтегративний елемент. Інформаційне протиборство поступово пронизало всі форми міжнародної конкуренції, від дипломатії й економіки до збройних конфліктів, залишаючись відносно автономним феноменом зі своєю власною логікою. Стратегічна мета полягає у деморалізації суспільства, руйнуванні когнітивної стійкості та паралізації волі політико-військового керівництва супротивника, що уможливлює досягнення політичних цілей без прямої ескалації до широкомасштабних бойових дій.

Формування поняття інформаційної війни не було одномоментним інтелектуальним проривом, а являло собою тривалий процес поступової концептуалізації нематеріальних інструментів впливу у збройних конфліктах. Витоки концепту сягають доінформаційного етапу й зосереджені в межах психологічно-пропагандистського напряму, що ґрунтується на розумінні інформації як засобу впливу на масові установки, сприйняття та поведінку, тобто як інструмента формування когнітивного середовища противника. У цій традиції інформаційне протиборство розглядається передусім як боротьба за контроль над процесами переконання, мотивації та інтерпретації реальності, де ключовими механізмами виступають пропаганда, психологічні операції та маніпуляція комунікаційними потоками.

Початок процесу концептуалізації інформаційного впливу як складника воєнного протиборства простежується ще у міжвоєнний період. Британський історик та військовий теоретик Дж. Ф. К. Фуллер (J. F. C. Fuller), аналізуючи досвід Першої світової війни, вперше використав термін психологічна війна (psychological warfare*)* для позначення системного впливу на моральний стан і поведінкові настанови противника. Запропоноване ним поняття фіксувало новий вимір боротьби, що виходив за межі матеріального ураження й демонструвало усвідомлення того, що масштабні війни XX століття виявили залежність результату бойових дій від ефективності роботи з інформацією, сприйняттям і настроями сторін, що стало відправною точкою подальшого теоретичного розвитку. Він передбачав трансформаційний зсув, де звичайні методи ведення війни можуть бути витіснені формою війни психологічним характером. У цьому гіпотетичному сценарії традиційна зброя та протистояння на полі бою поступилися б місцем іншому виду війни – тій, яка прагне не використовувати зброю чи захоплювати території, а маніпулювати людським інтелектом та порушувати моральні та духовні основи нації через вплив, який використовується іншим, щоб зрештою забезпечити тріумф з мінімальними втратами [30].

Розвиток психологічно-пропагандистського напряму пов’язаний із роботами Г. Лассуелла (Lasswell H. D.), який у міжвоєнний та повоєнний періоди заклав засадничі принципи дослідження політичної комунікації та пропаганди. Г. Лассуелл розглядав пропаганду як інструмент стратегічного управління громадською думкою у війні й мирі, наголошуючи на її ролі у формуванні колективних уявлень, мобілізації суспільства і підриві моральної єдності супротивника. Його підхід інституціоналізував розуміння інформаційного впливу як системної діяльності, що спирається на аналіз аудиторії, контроль каналів комунікації та вироблення цілеспрямованих повідомлень, тобто на ті принципи, які стали базовими для пізніших теорій інформаційних операцій [39].

Значний внесок у формування практичного виміру цього напряму зробив П. Лайнбаргер (Linebarger P.M.A.) автор фундаментальної праці «Psychological

Warfare» (1948), яка стала першою комплексною доктриною сучасних психологічних операцій. П. Лайнбаргер трактував психологічну війну як організований вплив на настрої та переконання противника через пропаганду, дезінформацію, чутки, маніпуляцію символами та використання емоційних наративів. Він розробив принципи планування, проведення та оцінювання психологічних операцій, поєднавши теоретичні положення з військовою практикою. У його інтерпретації інформаційний вплив поставав засобом досягнення стратегічних ефектів без прямого насильства — і саме ця логіка стала одним з концептуальних підмурків для подальшого осмислення інформаційної війни як інструмента безсилового примусу [44].

Цілісним підходом до структурування психологічного впливу як окремої сфери військової діяльності було виокремлення трьох взаємопов'язаних форм психологічної війни: стратегічну, тактичну та консолідаційну, кожна з яких охоплювала власний рівень впливу на свідомість, поведінку та мотивацію цільових груп. Стратегічний рівень був спрямований на трансформацію політичних переконань і моральної стійкості широких мас, тактичний - на безпосереднє послаблення боєздатності противника через вплив на його війська в зоні бойових дій, а консолідаційний - на стабілізацію й керованість населення після захоплення території [44, p. 22-23]. Запропонована структура стала важливою інтелектуальною ланкою між пропагандистськими практиками першої половини XX століття та подальшим оформленням інформаційної війни як багаторівневого процесу впливу на когнітивне середовище супротивника. Його концепція показала, що інформаційне протиборство не зводиться до розповсюдження повідомлень, а включає керування мотиваційними й поведінковими механізмами, інтегрованими у військове планування. Операційна складова як вплив на сприйняття задля досягнення матеріальних результатів стала одним із фундаментальних інтелектуальних підмурків, на яких у подальшому вибудовувались сучасні концепції інформаційної війни.

Поступове розширення арсеналу інформаційного впливу у другій половині XX століття спричинило зміщення фокусу від виключно когнітивних механізмів

до технологічних основ функціонування сучасних систем управління та зв'язку. Якщо психологічно-пропагандистський напрям зосереджувався переважно на впливі на переконання, емоції та поведінку, то розвиток електронних комунікацій, радіотехніки й автоматизованих систем ухвалення рішень поставив на порядок денний питання вразливості технічної інфраструктури, яка забезпечує можливість ведення війни. Формується техніко-інженерний напрям осмислення інформаційного протиборства, що трактує інформацію як матеріальний ресурс і одночасно як критичну складову військової потужності, доступ до якої може бути порушений, спотворений або знищений.

У межах цього підходу вперше з'являється уніфіковане поняття «інформаційної війни», яке було системно обґрунтоване в дослідженнях інженера-аналітика Т. Рони (T. P. Rona), чия робота стала концептуальним зрушенням від психологічних схем до технічної логіки інформаційного ураження. У технічному звіті для компанії Boeing «Weapons Systems and Information War» (1976) Т. Рона вперше вводить у науковий і політичний обіг сам термін, але й формулює його у спосіб, що виокремлює інформацію як самодостатній ресурс протиборства, здатний перетворюватися на чинник стратегічної переваги. Підхід був нетиповим для тогочасного оборонного аналізу, який зосереджувався переважно на матеріальних компонентах сили, зокрема озброєнні, логістиці, промислових можливостях. Т. Рона наголошував, що в умовах стрімкого розвитку цифрових технологій і розширення залежності держав від інформаційної інфраструктури, вирішальне значення набуває не стільки здатність завдати фізичного удару, скільки можливість порушити, обмежити чи маніпулювати інформаційними потоками, що забезпечують функціонування систем управління, комунікації та прийняття рішень. Ключовою тезою було твердження, що структурна вразливість США в інформаційному домені зростатиме пропорційно до технологічної модернізації економіки й оборонної сфери, отже інформаційна інфраструктура (мережі зв'язку, системи обробки даних, канали прийому й передачі сигналів) повинна розглядатися як потенційний театр ведення війни на рівні з традиційними середовищами. Він

підкреслював, що уразливість цих систем є двоякою: з одного боку, від можливих атак противника у воєнний час, а з іншого – від маніпулятивного чи деструктивного впливу навіть у мирний період, коли стратегічний ефект може бути досягнутий без прямого застосування сили. Таким чином, Т. Рона запропонував радикальне розширення уявлення про війну, наголошуючи, що конфлікт переміщується у сферу, де решта форм сили стають вторинними щодо контролю за інформацією як критичною інфраструктурою [57].

Сучасні системи озброєнь, зазначав Т. Рона, стають дедалі більш залежними від зовнішніх комунікаційних ланок, зокрема каналів управління й контролю, навігаційної інформації та сенсорних систем. Усі ці елементи виявлялися вразливими до ураження, і саме боротьбу за їхнє збереження або компрометацію він окреслював як «інформаційну війну». Його розуміння «інформації» мало інженерний характер і ґрунтувалося на інформаційній теорії К. Шеннона (C. Shannon's). Дослідник визначав інформацію як електричні, оптичні, акустичні або гідравлічні сигнали, що «передають стан певної підсистеми або дані, доступні їй, іншим підсистемам» [57, p. 11]. Інформація постає в нього як вхідний параметр для прийняття рішень як людиною, так і автоматизованими системами, у яких сигнал опрацьовується відповідно до наперед визначених правил і породжує відповідний вихід, отже визначення охоплює також аналогові електронні схеми. В умовах «інформаційної війни» атака могла передбачати введення людини в оману, підміну чи придушення сигналу або фізичне знищення технічного засобу [57, p. 32].

у другій половині XX століття держави почали інституціоналізувати роботу з інформацією як невід'ємний компонент оборонного планування. Подальший розвиток продемонстрував потребу у формалізації, стандартизації та доктринальному закріпленні інформаційних інструментів у структурі збройних сил, що привело до становлення інституційно-доктринального напряму, у межах якого інформаційна війна почала розглядатися як стратегічно організований компонент військової діяльності. У 1990-х роках провідні оборонні інституції

США, зокрема Міністерство оборони та Об'єднаний комітет начальників штабів, заклали основи концептуального розуміння інформаційної війни, перетворивши його на елемент офіційних доктрин, оперативних процедур і політичних документів. Цей підхід сформував рамку, у якій інформація стала стратегічним ресурсом, а інформаційний вплив - об'єктом системного військового управління.

Міністерство оборони США інституціоналізувало концепт інформаційної війни у 1992 р. через ухвалення класифікованої DOD Directive TS3600.1, яка започаткувала формальне використання цього терміну в оборонному плануванні. Хоча сама директива містила лише загальні орієнтири, її подальші інтерпретації формувалися поступово через дослідження, військові ігри та міжвідомчі обговорення, що компенсували обмежений доступ до її змісту. Перший змістовний публічний опис інформаційної війни з'явився лише у Щорічному звіті Міністра оборони США за 1994 рік. У ньому інформаційна війна визначалася як комплекс дій, спрямованих на збереження цілісності власних інформаційних систем і водночас на експлуатацію, руйнування або компрометацію інформаційних систем противника з метою досягнення інформаційної переваги у застосуванні сили. Цей підхід чітко підкреслював дуальність — оборонний та наступальний виміри інформаційного протиборства і презентував інформаційну війну як інтегративну стратегію, що підвищує рішучість дій військ і зменшує супутні ризики та втрати [17, p. 97].

Подальше доктринальне розгортання концепту відбулося у документі Joint Staff «A Strategy for Peace: The Decisive Edge in War» (1996), де інформаційна війна постає як інструмент, релевантний усім рівням ведення війни й усім спектрам військових операцій. У цьому контексті її оборонна складова визначається як комплекс заходів із захисту інформації та інформаційних систем, тоді як наступальна - як вплив на інформацію та інформаційні можливості противника. Важливим структурним елементом доктрини став концепт Command and Control Warfare (C2W), визначений у CJCS Memorandum of Policy No. 30 (1993) як інтегроване застосування OPSEC, військової дезінформації, психологічних операцій, електронної боротьби та фізичного ураження,

підкріплених розвідкою, для позбавлення супротивника можливості здійснювати ефективне командування й управління. У спільній доктрині C2W розглядався як підсистема ширшої інформаційної війни, спрямована на паралізацію інтелектуально-організаційного ядра військових структур супротивника й руйнування його здатності до координації сил [17, p. 98].

Доктринальний зсув від технологічного окреслення інформаційної війни до концептуалізації кіберпростору як самостійного операційного виміру, у якому інформаційний вплив набуває маневрового характеру відбувся з появою досліджень представника Міністерства оборони США Р. Дж. Банкера (Bunker R. J.). Він запропонував одну з перших системних спроб інтегрувати уявлення про кіберпростір у структуру майбутніх військових доктрин. Його аналіз здійснювався на тлі трансформації Збройних сил США, які переходили від доктрини холодної війни до концепції Force XXI, орієнтованої на мережево-центричні технології та інформаційну перевагу. Традиційне уявлення про поле бою як про фізично окреслений простір стверджувалось як не достатнє, оскільки вирішальне значення набувають інформаційні потоки, цифрові мережі й автоматизовані системи управління. Він вводив поняття «розширеного поля бою» (advanced battlespace), у межах якого інформаційний вимір є не допоміжним елементом, а структурною складовою військової діяльності, здатною визначати темп, характер і результат операцій [12, p. 5].

Ключовим нововведенням його підходу стало поняття «кіберманевру» (cybermaneuver), що здійснюється у віртуальному просторі, через вплив на інформаційні системи й цифрову інфраструктуру супротивника. На думку Р. Банкера, здатність здійснювати такі маневри формує нову логіку конфлікту, де перехоплення, викривлення або знищення інформаційних потоків набуває того ж значення, що й контроль над фізичною територією. Кіберманевр розглядався як інструмент, здатний паралізувати командування, порушити логістичні ланцюги або позбавити супротивника ситуаційної обізнаності без прямого застосування вогневих засобів. Іншою концептуальною лінією було трактування кіберпростору як п’ятого театру воєнних дій, поряд із сушею, морем, повітрям і

космосом. Така класифікація підкреслювала не лише автономність інформаційних процесів, але й їхню інтегрованість у всі рівні сучасних операцій від стратегічного до тактичного. Він стверджував, що інформаційні атаки та інформаційний захист не можуть більше розглядатися як допоміжні функції; вони становлять окрему форму військового впливу, що вимагає власних інструментів, доктрин і процедур планування. Підсумковим внеском Р. Банкера було формування інтелектуального підґрунтя для подальшого закріплення в офіційних документах Пентагона розширеного трактування інформаційних операцій, яке охоплювало технічні аспекти захисту мереж й керовану діяльність у кіберсфері з метою здобуття оперативної переваги. Його ідеї сприяли переходу від вузького розуміння інформаційної війни як захисту комунікацій до ширшої доктрини, що охоплює маневрування в інформаційному та кібернетичному просторі як невід'ємний елемент сучасного конфлікту [12, p. 6-7].

У тому ж 1996 році Міністерство оборони замінило інструкцію з інформаційної війни новим документом, у якому пріоритет було перенесено на поняття «інформаційних операцій». Зміна відображала прагнення розширити відповідальність за інформаційну діяльність на інші урядові інституції та, водночас, зняти побоювання, що Пентагон намагається здійснити надмірну мілітаризацію Інтернету й суміжної цифрової інфраструктури [66].

Перша спільна доктрина інформаційних операцій (Joint Doctrine for Information Operations, JP 3-13) була оприлюднена у 1998 р., що стало ключовим кроком у формалізації та стандартизації американського підходу до інформаційного протиборства. Доктрина закріпила перехід від вузького трактування інформаційної війни як окремого набору дій до більш широкої концепції інформаційної операції (information operations), визначивши їх як діяльність, спрямовану на вплив на інформаційно-обумовлені процеси - людські чи автоматизовані. Поняття «інформаційна війна» було переосмислено як окремий випадок інформаційних операцій, що здійснюються в умовах кризи або конфлікту. Доктрина постулювала, що «інформаційна війна» – це інформаційні операції, що проводяться під час кризи або конфлікту для досягнення або

просування конкретних цілей над конкретним супротивником або супротивниками», а також що «Спеціальні інформаційні операції» – це інформаційні операції, які через свій конфіденційний характер та потенційний вплив чи вплив, вимоги безпеки чи ризик для національної безпеки США потребують спеціального процесу розгляду та затвердження» [36, p. I-11]. Йшлося про весь спектр процедур, залежних від інформації: від стратегічного ухвалення рішень на рівні національного командування до автоматизованого контролю критичної комерційної інфраструктури на кшталт енергетичних систем або телекомунікацій.

Ключовим концептом доктрини стало поняття «інформаційного середовища» сукупності індивідів, організацій та систем, що збирають, обробляють і поширюють інформацію, а також самої інформації як об'єкта впливу [36, p I-9]. Це визначення демонструвало усвідомлення того, що інформація існує одночасно як технічний ресурс і як соціальний конструкт, а тому потребує комплексного підходу до її захисту та використання. Попри те, що на той момент ще не існувало сучасного Інтернету, доктрина 1998 року прямо визнавала атаку на комп'ютерну мережу («computer network attack») - операції з порушення, заборони, погіршення якості або знищення інформації, що знаходиться в комп'ютерах та комп'ютерних мережах, або в самих комп'ютерах та мережах [36, p. I-9] одним із ключових інструментів інформаційних операцій, поряд з операційною безпекою, військовою дезінформацією, психологічними операціями, електронною боротьбою, фізичним ураженням та спеціальними інформаційними операціями. Така класифікація засвідчувала розуміння зростання ролі цифрового простору як нового театру протиборства.

Визначення «інформації» було запозичене з військового словника Міністерства оборони США і мало двоскладову природу, що охоплювала як машинну, так і людську обробку. «Інформація» визначалася, по-перше, як факти, дані чи інструкції в будь-якій формі або носії; по-друге, як значення, що людина надає даним відповідно до правил їх репрезентації [36, p. I-10]. Така подвійність підкреслювала інтеграцію технічного та когнітивного вимірів інформаційного

середовища, роблячи інформаційні операції одночасно технологічною, психологічною та організаційною категорією. Показово, що у Доктрині відсутнє окреме визначення поняття даних («data»), тоді як поняття інформації подане у розширеній формі, яка охоплює як матеріальні носії фактів та інструкцій, так і значення, що їх інтерпретує людина. Така термінологічна асиметрія відображає перехідний характер доктринального мислення кінця 1990-х, коли технічне розуміння інформації ще не було концептуально відокремлене від когнітивного, а інформаційні операції трактувалися крізь призму цілісного впливу на будь-які інформаційно залежні процеси.

Паралельно з техніко-інженерними та інституційно-доктринальними підходами у США сформувався окремий аналітико-стратегічний напрям, зосереджений на інтелектуальному концептуальному моделюванні інформаційної війни та її місця в архітектурі сучасних конфліктів. Його відмінність полягає не стільки в описі конкретних технологій або процедур, скільки у вибудовуванні системних теоретичних рамок: визначенні природи інформаційного простору, типологізації форм впливу, виявленні закономірностей, за якими інформаційні дії змінюють баланс сил. Цей напрям не є прикладним, його завданням була розробка стратегічної граматики інформаційних конфліктів, що дозволяє оцінити їх логіку, межі, потенціал ескалації та взаємозв’язок з іншими формами воєнної сили. У межах цього напряму найпослідовнішою і найвпливовішою постаттю став М. С. Лібіцкі (M. Libicki), який систематизував інформаційну війну як багаторівневий, багатовекторний феномен, що виходить за межі чисто технологічних підходів і претендує на статус самостійної стратегії.

Дослідження «What Is Information Warfare?» (1995) М. С. Лібіцкі стало одним з найвпливовіших спроб систематизувати інформаційну війну як багатовимірний і внутрішньо диференційований феномен. На відміну від техніко-інженерних підходів, що концентрувалися переважно на інфраструктурних вразливостях, або доктринальних документів, орієнтованих на практичне регламентування інформаційних операцій, М. Лібіцкі

запропонував стратегічну рамку, у якій інформаційна війна постає як сукупність різнорідних, але структурно пов’язаних форм впливу. Він наголошував, що інформація має не лише технологічний, а й поведінковий, організаційний, епістемічний та політичний виміри, і тому жодне вузьке визначення не може повністю охопити складність взаємодій, що формують інформаційний конфлікт. У своїй концепції автор виходив із того, що інформаційна війна не є єдиним типом операцій, а радше парасольковим поняттям, яке включає низку відмінних за природою напрямів, що працюють у різних середовищах і переслідують різні стратегічні цілі. Він окреслював їх як відносно автономні домени впливу: від втручання у процеси командування й управління до маніпуляції когнітивними установками, від боротьби за перевагу в розвідувально-аналітичних циклах до впливу на електромагнітний спектр чи інформаційну інфраструктуру економіки. Об’єднувало ці домени не технічне споріднення, а логіка стратегічного змагання за контроль над інформаційними потоками та механізмами, які перетворюють дані на знання і рішення. Такий підхід дозволив М. Лібіцкі показати, що інформаційна війна не зводиться ані до кіберпростору, ані до психологічних операцій, а проявляється як системна конкуренція за умови, в яких противник сприймає, обробляє та використовує інформацію [40].

Одним із найважливіших внесків М. Лібіцкі стало розмежування інформаційної війни та кібернетичної війни. Він підкреслював, що кібероперації становлять лише один сегмент ширшої інформаційної боротьби, і хоча вони можуть бути високо експресивними, їхній вплив стає стратегічно значущим лише тоді, коли вони інтегруються з іншими формами інформаційного впливу. Він розглядав інформаційну війну як поліструктурний простір, де технічні, психологічні, організаційні й економічні засоби взаємодіють у спосіб, що змінює поведінку систем управління, інституцій і соціальних груп [41]. Таким чином, його концепція відійшла від традиційного уявлення про інформацію як допоміжний елемент бойових дій і запропонувала бачення інформації як самостійної складової сили, що формує нову конфігурацію стратегічного середовища. Вплив М. Лібіцкі полягав не лише в типологізації форм

інформаційної війни, а й у запропонованому ним способі мислення, який виявився важливим для американського стратегічного дискурсу кінця 1990-х і початку 2000-х років. Він допоміг пов’язати еволюцію доктринальних документів Міністерства оборони США з ширшими дебатами щодо природи конфлікту в інформаційну епоху, а також забезпечив теоретичний міст між технічними інноваціями, операційним досвідом і стратегічним аналізом. Завдяки цьому М. Лібіцкі став одним із небагатьох авторів, хто не лише описав інформаційну війну, але й запропонував цілісну інтелектуальну архітектуру, в межах якої вона може бути осмислена та порівняна з іншими формами воєнної сили.

Таким чином, інформаційна війна утверджується як автономний, але інтегрований вимір сучасних міжнародних протиборств, що пронизує політичні, економічні та військові взаємодії. Її стратегічна ефективність полягає у здатності досягати політичних цілей через трансформацію когнітивного та комунікаційного середовища, зменшуючи потребу у прямій силовій ескалації.

2. 2. Інформаційні війни в практиках застосування

Доцифровий етап включав психологічні операції та пропагандистські практики Першої світової війни, яка стала ключовою точкою становлення модерних інформаційно-психологічних впливів як системної складової ведення війни. В умовах тотальної мобілізації і зростання ролі масової політики комунікація перетворилася на інструмент, здатний визначати стійкість тилу, готовність армії до тривалих бойових дій, рівень легітимності уряду та сприйняття конфлікту на міжнародній арені. Застосування пропаганди вперше набуло індустріального масштабу, що дозволяє говорити про формування перед-цифрових (pre-digital) механізмів інформаційного протиборства, які згодом стали фундаментом для концептуалізації «інформаційної війни» у другій половині XX століття.

На стратегічному рівні держави Антанти й Четверного союзу незалежно

одна від одної прийшли до висновку, що керування масовою свідомістю не є другорядним інструментом, а являє собою самостійний театр воєнних дій. Поширення газет із фронтовими зведеннями, контроль за телеграфом, масоване використання плакатів, а також маніпуляції з даними про втрати й успіхи армій стали базовою практикою інформаційної мобілізації суспільства. Уперше були формалізовані спеціалізовані структури від німецьких пропагандистських бюро до Комітету громадської інформації у США, які працювали за принципами плановості, цільової спрямованості й сегментації аудиторії. Технічний контекст початку XX століття обумовлював особливу форму цих операцій. Радіомовлення лише зароджувалося, але телеграф забезпечував безпрецедентну швидкість поширення повідомлень між столицями, а друкована преса стала головним каналом як для мобілізації власного населення, так і для дискредитації противника. Сторони активно використовували підривну інформацію: поширювали чутки про моральний занепад, економічне виснаження чи політичну нестабільність ворога; проводили кампанії демонізації, спрямовані на виправдання ескалації бойових дій перед населенням; фальсифікували документи або підмінювали контекст реальних подій для досягнення психологічного ефекту. Психологічний вплив на війська противника став окремим напрямом. Масове скидання листівок із закликами до дезертирства, перебільшеними описами втрат та нібито невідворотної поразки мало на меті підірвати бойовий дух та ускладнити командуванню підтримання дисципліни. Уперше було апробовано тактику розмежування цільових груп: солдатам адресували одні меседжі, цивільному населенню - інші, нейтральним державам – треті [3, p. 99].

Особливістю інформаційних практик цієї доби було поєднання довготривалих пропагандистських стратегій із тактичними психологічними операціями на конкретних ділянках фронту. Це створювало своєрідний інформаційний контур війни, де керування наративами, приховування або вибіркове оприлюднення фактів, формування образу «справедливої боротьби» або «жорстокого ворога» прямо впливали на військово-політичні рішення. Низка

інновацій, що з’явилася в цей період, як от централізовані прес-бюро, планові інформаційні кампанії, координація пропаганди між союзниками, спроби оцінювати ефективність впливу, - стала передумовою розвитку інституцій та методологій, які у другій половині XX століття отримали доктринальне оформлення як психологічні операції та інформаційні операції.

Уряди європейських держав швидко усвідомили, що поряд із традиційними військовими силами колосальну роль відіграватиме інформаційна та ідеологічна складова війни. На прикладі Великої Британії початкова система організації пропаганди у 1914 р. лише формувалася, долаючи перешкоди міжвідомчої конкуренції, зашкарублих традицій взаємин уряду та підпорядкованих структур. Проте потреба впливу на громадську думку змусила відповідальні підрозділи швидко перейти до конструктивної діяльності, концентруючи зусилля на створенні образу ворога, перш за все Німеччини, що забезпечувало внутрішню мобілізацію суспільства та переконання нейтральних держав у доцільності вступу до війни на боці Антанти. Найефективнішу роботу здійснювали Бюро воєнної пропаганди (War Propaganda Bureau) та Національний комітет для воєнних цілей (National War Aims Committee), заснований у 1917 році як міжпартійна парламентська структура. Перше фокусувалося на зовнішній пропаганді та контрпропаганді, особливо для США, друге опікувалося внутрішньою мобілізацією. У 1918 році Міністерство інформації (Ministry of Information) стало координатором діяльності цих структур, розподіляючи функції між відділами внутрішньої та зовнішньої пропаганди, публікацій, роботи з окремими іноземними особами, а також формуванням візуальних матеріалів для широкої аудиторії. Заснування Бюро воєнної пропаганди означало перехід від аматорства до професійної системної роботи. Вироблення змісту та методів впливу вимагало значних інтелектуальних ресурсів, тоді як технічне виконання забезпечувала команда клерків і машиністок. Основними темами пропаганди були німецькі злочини у Бельгії, порушення міжнародного права, а також демонстрація міжсоюзницької гармонії. Особлива увага приділялася залученню США до війни: підготовка американської громадської думки до можливого

вступу країни у конфлікт стала пріоритетом Бюро. Важливим елементом стратегічного інформаційного впливу були також комітети під егідою Міністерства внутрішніх справ та Foreign Office, які забезпечували доступ іноземних журналістів до офіційної інформації, водночас залишаючи їм свободу інтерпретації. Для ефективності цього процесу використовувалися щоденні телеграми зі спеціальними новинами, що надсилалися дипломатичним та консульським представникам за кордон. Окрему увагу приділяли візуальній пропаганді, яка дозволяла оперативно впливати на широку аудиторію та формувати сприйняття війни в нейтральних та союзних країнах [73, сс. 101-103].

Таким чином, досвід Великої Британії демонструє, що вже на початку XX століття держави усвідомили стратегічне значення інформації та психологічного впливу, заклавши основи для подальшого розвитку психологічно-пропагандистського напрямку в інформаційній війні. Формування професійних бюро, координація діяльності між органами та використання різноманітних каналів комунікації забезпечили комплексний підхід до управління масовою свідомістю як критичного ресурсу у військових конфліктах. Перша світова війна виступає історичним прикладом масової пропаганди, ранньою лабораторією інформаційного протиборства, де були напрацьовані ключові принципи боротьби за контроль над масовою свідомістю, моделювання наративів та використання технологічних можливостей для досягнення стратегічних переваг.

Період Холодної війни став етапом інтенсивної формалізації інформаційних практик, коли боротьба за вплив на свідомість, канали комунікації та інформаційні потоки набула стратегічного характеру, співставного з ядерним стримуванням. Інформація у цей час перестала бути допоміжним інструментом і перетворилася на самостійний ресурс національної потужності, покликаний формувати політичну поведінку, легітимність режимів і геополітичні орієнтації. У цей період інформаційні дії набувають системного характеру, а конкуренція між США та СРСР створює двополярний інформаційний простір, у якому пропаганда, контрпропаганда, дезінформація та психологічний вплив застосовуються як повноцінні інструменти державної політики.

Стратегія стримування, що лежала в основі військово-політичного протистояння двох систем, доповнювалася широкою системою інформаційного впливу. США та СРСР паралельно використовували радіомовлення, кіно, пресу, дипломатичні канали та культурні програми для демонстрації власної політичної моделі і дискредитації опонента [Висоцький]. Американські програми «м'якої сили» на зразок *Voice of America*, *Radio Free Europe* і *Radio Liberty* були ключовими інструментами створення альтернативних інформаційних просторів у країнах соцтабору. Вони мали завдання не лише поширювати доступ до інформації, але й транслювати політичні норми, стилі життя, уявлення про свободу, ринок та демократію як противагу радянському дискурсу. СРСР, зі свого боку, вибудував потужну систему зовнішньої інформаційної проєкції через *Radio Moscow*, інформаційні агентства та партійну дипломатію. Інформаційні кампанії використовувалися для легітимізації радянської зовнішньої політики, просування антиколоніального дискурсу, а також для підриву довіри до західних інститутів. Холодна війна стала періодом, коли інформація функціонувала як чинник стримування, здатний впливати на політичні рішення, формувати союзницькі мережі й дестабілізувати внутрішню ситуацію в країні-опоненті.

У цей період інформаційний вплив уперше набуває рис системно проєктованих операцій, що поєднували психологічні дії, дипломатичний тиск, технологічні засоби масової комунікації та спецоперації. СРСР розгорнув масштабні дезінформаційні програми, відомі під назвою «активні заходи» (*active measures*), які включали поширення фальшивих документів, легендованих витоків, фабрикацію новин, вербування журналістів і вплив на міжнародні організації. Одним із найвідоміших прикладів стала операція «Інфекція» — кампанія зі звинувачення США у створенні ВІЛ/СНІД як біологічної зброї [65, p. 61].

США у відповідь розвивали ідеологічні програми, а також інвестиції в дослідження комунікацій, включно з розвитком моделей масової пропаганди, маніпуляцій, соціальних експериментів та опрацюванням психологічних механізмів впливу на аудиторії різного типу. Пропаганда у цей період стає

об’єктом наукової раціоналізації. Розробляються методики таргетування, сегментації аудиторій, створення контенту, здатного викликати довіру, а також засоби подвійного впливу - одночасно демонстративного і прихованого. Крім того, триває технологізація інформаційного впливу: телебачення стає центральним медіумом формування політичної свідомості, зростає роль інформаційних агенцій, створюються перші глобальні інформаційні мережі, які здатні миттєво транслювати події у світовому масштабі. Інформація перетворюється на поле боротьби не лише за смисли, але й за інфраструктури доступу до смислів [85, с. 148-150].

Наприкінці «холодної війни» формується передумова для подальшої кібернетизації концепту інформаційних конфліктів. Створення перших комп’ютерних систем управління, автоматизованих мереж зв’язку, розвідки та раннього попередження, а також глобальних комунікаційних систем супутникового типу породжує новий вимір уразливості. З’являються перші епізоди втручання у мережі, електронних зламів, перехоплень даних, електронного придушення та маніпуляції сигналами. Американські програми супутникового спостереження та SIGINT (signals intelligence) RADAR-типу, радянські системи радіоелектронної боротьби, комп’ютеризовані пункти управління ядерними силами – усе це підводить до усвідомлення того, що інформація не лише впливає на поведінку людей, а й управляє інфраструктурами, на які можна здійснювати кібервплив. Наприкінці 1970–1980-х років поступово формується нова рамка: інформаційний простір стає суміжним із технічним простором, а інформаційні атаки – потенційним інструментом стратегічної дестабілізації [75, с. 78].

Упродовж 1980–1990-х років змінюється сутність інформаційного простору й відбувається поява цифрових технологій і мережевої взаємозалежності. Якщо для попередніх десятиліть була характерна домінанта пропаганди, радіомовлення та таємних операцій впливу, то в останній чверті XX століття інформація набуває інфраструктурного статусу. Розвиток обчислювальної

техніки, поява глобальних комп'ютерних мереж, стрімке поширення цифрових телекомунікацій і залежність економіки від технологічно складних систем управління створили новий вимір вразливості держав. Інформаційне середовище більше не обмежувалося мас-медіа: воно включало системи енергетики, транспортні логістики, авіаційні диспетчерські вузли, супутникову навігацію, банки даних і мережі оборонного управління. Унаслідок цього політична й військова конкуренція стала охоплювати не лише контроль над свідомістю, але й контроль над потоками даних, цифровими системами та алгоритмами, що визначали функціонування критичної інфраструктури.

Зростання цієї взаємозалежності виявило низку структурних вразливостей. Однією з перших резонансних подій став інцидент «Cuckoo's Egg» 1986 року, коли група німецьких хакерів, пов'язаних із радянськими спецслужбами, змогла проникнути до мереж дослідницьких лабораторій і оборонних установ США, використовуючи некомпетентно налаштовані системи UNIX із низьким рівнем захисту. Розслідування К. Столла викрило те, що раніше не сприймалося як стратегічна загроза: мережеві структури могли бути непомітно порушені сторонніми акторами, а інформація могла витікати системно, без жодної можливості оперативного виявлення [23]. Через два роки, у 1988-му, черв'як Морріса паралізував значну частину мереж ARPANET та пов'язаних університетських систем, показавши не тільки технологічну недосконаліть раннього інтернету, а й нездатність державних та наукових інституцій адекватно реагувати на автоматизовані атаки [6]. Ці два епізоди разом сформували перше чітке усвідомлення того, що інформаційна інфраструктура є новим театром потенційних бойових дій.

Трансформацію поглядів виявила й практика Пентагону. Міністерство оборони США ще з кінця 1970-х років активно інвестувало в системи супутникової навігації, цифрову обробку розвідданих і комп'ютеризацію командування військами. У 1980-ті роки формується концепція, яку пізніше назвуть «мережево-центричною війною»: інтеграція всіх елементів бойового простору від розвідки до логістики через мережі передачі даних, що

забезпечують швидкість ухвалення рішень і точність розподілу вогневих засобів. Інформація розглядається як фактор, що визначає можливість випереджального маневру, який робить противника повільнішим і менш ефективним навіть за наявності значного потенціалу живої сили чи техніки [19, p. 30].

Першим масштабним випробуванням цих технологічних і концептуальних інновацій стала війна в Перській Затоці 1991 року, зокрема операція «Буря в Пустелі» (Dessert Storm) у ході якої коаліційні сили продемонстрували, що цифрові інструменти здатні перетворити хід операцій. Іракська армія, попри чисельність і бойовий досвід, виявилася нездатною адаптуватися до швидкості та точності ударів, які забезпечували супутникова навігація GPS, високоточні авіаційні платформи та системи електронної розвідки. Коаліція створила безперервну «інформаційну картину» поля бою: супутникові знімки, сигнали електронної розвідки та дані з літаків-розвідників інтегрувалися в єдиний цикл ухвалення рішень, що значно скоротило часові лаги між виявленням цілі та нанесенням удару. Так само важливим компонентом стала електронна війна. Придушення іракських радарів і комплексів ППО через радіоелектронні перешкоди та цілеспрямоване руйнування систем зв'язку позбавило іракське командування можливості координувати дії військ. Унаслідок цього більшість ударів завдавалися в умовах повної дезорієнтації противника. До цих технологічних інструментів додався інформаційно-психологічний компонент: масоване радіомовлення, спрямоване на деморалізацію іракських військових, розповсюдження листівок, а також демонстративна прозорість медійної кампанії коаліції, яка контролювала інтерпретацію подій у глобальних медіа. Інформаційне середовище стало одночасно зброєю, щитом і каналом легітимації операцій [70]. Таким чином, «Буря в пустелі» стала першим конфліктом, що показав реальне поєднання цифрової інфраструктури, інформаційної переваги та військової сили. Виявилося, що контроль над даними й можливість забезпечити високу швидкість циркуляції інформації може бути не менш вирішальним фактором, ніж контроль над територією. Цей досвід заклав основи подальшого доктринального оформлення інформаційних операцій і став відправною точкою

для розвитку кіберстратегій 1990-х і 2000-х років.

Перехід до мережево-центричних конфліктів на межі тисячоліть означав якісне переосмислення ролі інформації у війні, відтак інформація перестала бути лише доповненням до кінетичних дій і стала автономним чинником оперативної й стратегічної переваги, інтегрованим у сам цикл планування та виконання операцій. Розвиток високошвидкісних комунікацій, поширення інтернет-інфраструктури та вдосконалення систем командування і керування створили умови, за яких швидкість збору, обробки й розповсюдження даних визначає темп і результативність військових дій. Унаслідок цього почався перехід від поодиноких комп'ютерних інцидентів до скоординованих кампаній, у яких технічне порушення інфраструктури поєднується з маніпуляцією інформаційного поля з метою послабити опір супротивника, підривати його легітимність та впливати на політичні процеси. Еволюція цього процесу очевидна при зіставленні ранніх мережевих інцидентів із випадками початку 2000-х: із прагматичних втручань у роботу систем як таких виникли операції, що мали чітко політичну спрямованість і були інтегровані у загальні плани застосування сили. У таких кампаніях технічні заходи, від тимчасового відключення критичних сервісів до цілеспрямованого впровадження шкідливого коду, виступали як засіб, що створює інформаційну та організаційну слабкість, яку супроводжувала активна інформаційна робота з аудиторіями: дискредитація керівництва, деморалізація особового складу, створення відчуття хаосу й неминучої поразки. Це поєднання техніки й наративу знаменувало собою перший етап справжньої інтеграції кібер- та інформаційних операцій у мережево-центричні [19, 32].

Яскравими емпіричними ілюстраціями такого поєднання стали події 2007 та 2008 років. Протягом атак проти Естонії 2007 р. значні збитки завдали масовані DDoS-кампанії проти державних, банківських і медійних ресурсів, що паралізувало критичні сервіси і створило інформаційний вакуум, у якому політичні повідомлення та інтерпретації подій могли бути нав'язані як внутрішній, так і зовнішній аудиторії. Реакція на ці інциденти

продемонструвала, що навіть без прямого застосування сили кіберкампанія може спричинити параліч функціонування держави і підштовхнути політичні рішення [Ottis]. У 2008 році під час збройного конфлікту в Грузії кібероперації супроводжувалися наземними й повітряними діями, під атакою були урядові сайти й комунікаційні мережі, що ускладнило координацію та інформаційне управління, одночасно посилюючи ефект від класичних військових ударів [13]. Отже, поєднання кібернетичних втручань із фізичними діями посилює сумарний ефект і створює нові форми критичного тиску на противника.

Водночас досвід конфліктів на Близькому Сході продемонстрував іншу важливу динаміку: тут кібер- і інформаційні інструменти застосовувалися як частина довготривалих кампаній, що включали пропаганду, контрпропаганду та операції зі створення й контролю інформаційних наративів для міжнародної й внутрішньої аудиторії. У цих операціях технічне ураження інфраструктури, наприклад порушення каналів зв'язку чи компрометація систем спостереження, ставало тригером для широких інформаційно-психологічних операцій: урядові заяви, повідомлення в медіа і соціальних мережах, цілеспрямовані кампанії впливу на групи населення та міжнародних партнерів. Така практична інтеграція засвідчила, що технічний і психологічний ефекти при відповідній координації конвергують у посилення стратегічного тиску [10].

Війна в Афганістані стала одним із найпоказовіших прикладів обмеженої придатності мережево-центричної парадигми в умовах затяжного асиметричного конфлікту. Попри безпрецедентне застосування супутникових систем, безпілотних платформ, автоматизованих засобів управління та високоточної зброї, обіцяне NCW прискорення циклів ухвалення рішень і створення інформаційної переваги не трансформувалося в стійкий стратегічний ефект. Основна причина полягала в тому, що технологічно орієнтована модель була розрахована на супротивника з визначеною структурою сил і зрозумілою логікою маневру, тоді як Талібан діяв у форматі розпорошених мобільних осередків, інтегрованих у місцеві соціальні й ландшафтні умови. Малочисельні групи, що маневрували в горах, пустельних районах і селах, залишалися

фактично невидимими для органів технічної розвідки, а більшість їхніх бойових дій відбувалася в середовищах, де супутникові або БПЛА-орієнтовані методи виявлення давали мінімальний тактичний результат [61, p 13-14].

На практиці це означало структурний розрив між збором даних і їх використанням: навіть у разі успішного спостереження не існувало гарантії швидкої передачі інформації до підрозділів, які діяли у віддалених чи комунікаційно ізольованих районах. Локальні мережі зв'язку залишалися нестабільними, а різнорідність технічних систем між сухопутними силами, авіацією та розвідкою ускладнювала координацію. Таким чином, ключове припущення NCW про безперервну інтеграцію сенсорів, платформ і командних структур не реалізувалося в умовах географічно фрагментованого театру бойових дій, де тактична децентралізація противника руйнувала передбачуваність мережевої взаємодії. Провал NCW-підходу в Афганістані проявився також у інформаційній сфері. Хоча США прагнули досягти домінування в інформаційному просторі, Талібан ефективно використав дешеві та доступні засоби комунікації (мобільні телефони, радіомережі, а згодом і соціальні платформи) для поширення власної пропаганди, мобілізації прихильників і підриву довіри до афганського уряду та коаліційних сил. Американські інформаційні операції, що ґрунтувалися на технологічних можливостях, але недостатньо враховували локальні культурні коди та соціальну структуру, виявилися малоефективними. Технічна перевага США не конвертувалася в контроль над інформаційною динамікою на місцях, тоді як Талібан компенсував брак технологій високою адаптивністю, соціальною вкоріненістю й гнучкими каналами комунікації. Таким чином, афганський кейс продемонстрував, що мережево-центрична модель, сформована на уявленні про прозорий, повністю підконтрольний інформаційний простір, стикається з фундаментальними обмеженнями в умовах партизанської війни, де мобільність, локальні мережі взаємодії й соціальна інтегрованість противника системно нівелюють ефективність високотехнологічних інструментів [61, p 15].

Перехід до мережево-центричних конфліктів не був автоматичною

функцією технологічного прогресу; він вимагав доктринального й організаційного переосмислення того, що вважати за головну ціль у протиборстві. Військові й політичні органи почали все частіше розглядати інформацію як ресурс, контроль над яким дає не лише оперативну, а й стратегічну перевагу; а отже, виникла потреба в нових процедурах інтеграції кіберзусиль, розвідки та стратегічних комунікацій. Це, своєю чергою, породило виклики — від питання пропорційності й юридичної визначеності до проблеми розпізнавання джерел атак і необхідності створення механізмів захисту критичної інфраструктури.

Таким чином, за кібер-операціями закріпився статус інструмента політичного впливу, що функціонує в єдиному полі з інформаційно-психологічними засобами. Нова якість полягала в тому, що технічне ураження вже не розглядалося як самоціль; воно набувало значення лише у комбінації з операціями з контролю над інформаційними наративами, маніпуляцією увагою й легітимністю акторів. Такий синтез відкрив простір для гібридних методів ведення конфліктів, у яких межа між «кібер» і «інформацією» стала принципово розмитою, а втручання в мережі ставало невід'ємною складовою комплексних стратегій впливу.

2.3 Моделі впливу інформаційних операцій

Розширення практик інформаційної війни у цифрову добу зумовило появу низки моделей, спрямованих на пояснення різних механізмів інформаційного впливу в сучасних війнах, які виникали як відповідь на практичні зміни у способах ведення протиборства: зростання ролі мережевих структур управління, залежність військових і цивільних систем від інформаційних технологій, а також розширення впливу на когнітивну й поведінкову сфери суспільства. Відбувається перехід від застосування окремих інформаційних операцій до цілісних способів організації впливу, що поєднують технічні, організаційні та психологічні інструменти. Мережево-центрична війна ґрунтується на принципі

безперервної інформаційної взаємодії між елементами системи управління та бойовими підрозділами; концепція кібервійни фокусується на ураженні інформаційної інфраструктури; інформаційно-психологічні та когнітивні підходи зосереджуються на трансформації сприйняття, установок і моделей поведінки; гібридні інформаційні операції інтегрують ці елементи в межах комплексних стратегій впливу. Аналіз зазначених моделей дозволяє простежити розширення змісту інформаційного протиборства та формування похідних концепцій, що конкретизують різні рівні й механізми інформаційної дії та основні парадигми інформаційних впливів, які визначають сучасне розуміння інформаційної війни.

Мережево-центрична війна (network-centric warfare) сформувалася як відповідь на зростаючу залежність військових операцій від інформаційних потоків і здатності інтегрувати розрізнені елементи збройних сил у єдину систему управління. Її поява була зумовлена не стільки технологічними інноваціями як такими, скільки усвідомленням того, що інформаційна взаємодія між суб'єктами бойових дій здатна радикально змінювати характер застосування сили. Ключовим чинником бойової ефективності натомість окремого виду озброєння чи підрозділу, стає здатність системи забезпечувати обмін даними, синхронізацію дій та швидке перетворення інформації на управлінські рішення. Мережево-центрична модель передбачає інтеграцію сенсорів, засобів управління, виконавчих елементів і підтримки в єдине інформаційне середовище, що дозволяє скорочувати часові розриви між виявленням загрози, ухваленням рішення та його реалізацією. У такому середовищі інформація перестає бути допоміжним ресурсом і перетворюється на системоутворюючий елемент, від якого залежить ефективність усієї операційної архітектури. Мережево-центричний підхід змінює уявлення про командування, замінюючи ієрархічні, лінійні моделі управління більш розподіленими формами координації, у межах яких підрозділи зберігають автономність дій, але функціонують у спільному інформаційному контурі [22, pp. 324-325].

Подальший розвиток цієї парадигми супроводжувався трансформацією

командно-управлінських підходів від класичних моделей С2 до складніших систем С4ISR та спільних розвідувально-інформаційних структур. Зміщення акценту від централізованого контролю до інтегрованої ситуаційної обізнаності сприяло тому, що інформаційна перевага почала розглядатися не лише як технічна характеристика, а як передумова оперативної гнучкості й стратегічної ініціативи. Водночас зростання складності мережевих систем підвищило їхню вразливість, що зробило інформаційну інфраструктуру самостійним об'єктом ураження.

Подальший розвиток мережево-центричної війни в практиках НАТО засвідчив, що ефективність мережевих принципів управління безпосередньо залежить від здатності інтегрувати розвідувальні, спостережні та аналітичні ресурси в єдину систему підтримки ухвалення рішень. Формування концепції об'єднаної розвідки, спостереження та рекогносцировки (Joint Intelligence, Surveillance and Reconnaissance, JISR) НАТО стало відповіддю на структурні обмеження класичних моделей С4ISR, виявлені під час реальних операцій Альянсу. Досвід операцій НАТО наприкінці 1990-х - 2010-х років продемонстрував, що сама наявність технологічних засобів збору інформації не гарантує формування цілісної оперативної картини без належних механізмів інтеграції, обміну та синхронізації даних між різними компонентами сил. Операція «Allied Force» у 1999 році стала показовим прикладом раннього застосування мережево-центричних підходів, водночас виявивши їхні обмеження. Недостатній рівень розвідувально-спостережного забезпечення ускладнював виявлення мобільних і розосереджених засобів протиповітряної оборони противника, що негативно впливало на точність ураження та призводило до підвищених побічних ризиків. Аналогічні проблеми простежувалися й у подальших операціях НАТО, зокрема в Афганістані та Лівії, де розрив між повітряними, морськими та наземними компонентами, а також між національними контингентами союзників, ускладнював створення спільної ситуаційної обізнаності. У цих умовах мережево-центрична модель виявила свою залежність не лише від технологій, а й від інституційної спроможності

забезпечити обмін інформацією та координацію дій.

Особливо показовим став досвід Афганістану, де наявність засобів безперервного спостереження та передачі даних у реальному часі суттєво вплинула на процес ухвалення рішень, зокрема через залучення політичних і правових чинників до оперативного управління. Це виявило критичну потребу в системному підході до об'єднання розвідувальних ресурсів, що виходив би за межі окремих платформ або відомчих структур. Реакцією на ці виклики стало формування концепції JISR як механізму інтеграції національних і союзницьких можливостей у спільну, синхронізовану систему підтримки операцій на всіх рівнях [79, сс. 101-103]. Таким чином, розвиток JISR у межах НАТО відображає еволюцію мережево-центричної війни від технологічної моделі управління до складної організаційно-інформаційної системи, орієнтованої на формування спільного інформаційного простору. Водночас цей досвід засвідчив, що мережево-центричні підходи не є універсальним рішенням і залишаються вразливими до інституційних, організаційних і політичних обмежень, що зумовлює їх подальше переосмислення в контексті сучасних моделей інформаційного протиборства.

У рамках мережево-центричної війни інформаційний вплив виходить за межі підтримки бойових дій і набуває маневрового характеру, оскільки порушення зв'язків, спотворення даних або деградація інформаційного середовища здатні дезорганізувати систему навіть за збереження матеріальної переваги. Це зумовило поступове зближення мережево-центричних підходів із кібероперaціями та інформаційно-психологічними засобами, які спрямовуються не лише на технічні компоненти системи, але й на процеси ухвалення рішень. Мережево-центрична війна стала однією з ключових парадигм, що поєднала технологічний, організаційний і когнітивний виміри інформаційного протиборства та створила основу для подальшого розвитку похідних концепцій інформаційної війни.

Формування кібервоєнної моделі стало логічним наслідком зростаючої залежності держав і збройних сил від цифрових інформаційно-комунікаційних

систем, які перетворилися на самостійний простір протиборства. На відміну від мережево-центричної війни, де інформаційні технології слугують засобом підвищення ефективності управління та координації, кібермодель фокусується на безпосередньому ураженні інформаційної інфраструктури противника як способі досягнення стратегічних і політичних цілей. Кіберпростір постає окремим доменом ведення війни, у межах якого здійснюється вплив на функціонування держави, економіки, військових систем і суспільства загалом.

Інформаційне протиборство розгортається в цифровому середовищі як специфічний різновид асиметричної війни, у якому ураження інформаційних систем і мереж поєднується з політичною невизначеністю відповідальності та наслідків. Кібероперації можуть бути спрямовані як на приховане заволодіння інформацією з подальшим використанням її в інтересах суб'єкта нападу, так і на безпосереднє порушення функціонування або виведення з ладу елементів критичної інфраструктури. У першому випадку ключовою особливістю є латентність впливу: факт компрометації часто стає відомим лише після використання вразливостей, що позбавляє сторону-об'єкт можливості своєчасного реагування та захисту. У другому, наслідки можуть мати не лише інформаційний або економічний, а й фізичний вимір, створюючи загрозу життєзабезпеченню населення. У кіберпросторі відсутні чіткі пороги застосування сили, що ускладнює як правову кваліфікацію дій, так і формування зрозумілих механізмів відплати. Стримування втрачає характер передбачуваного інструмента безпеки й поступається логіці постійної взаємної вразливості [72, сс. 189-190].

Особливості зумовлюють зсув акценту від реактивних до превентивних і системних підходів, зокрема до всеосяжного захисту інформаційної інфраструктури та підвищення кіберстійкості. Навіть формалізовані механізми колективної безпеки стикаються з обмеженнями, пов'язаними з політичною та правовою неоднорідністю інтерпретацій кіберзагроз. Сучасні підходи до кіберзахисту дедалі більше орієнтуються на посилення спільної ситуаційної обізнаності, адаптивності та здатності мінімізувати шкоду від кіберзагроз, що

відображає трансформацію кібервоєнної моделі з інструмента прямого протиборства на складову ширших стратегій стримування та управління ризиками [72, с. 193].

Подальший розвиток кібервоєнної моделі супроводжувався її поступовою політизацією та включенням до комплексних стратегій безпеки провідних держав і міжнародних організацій. Кібероперації почали розглядатися як інструмент довготривалого впливу, спрямованого на підрив довіри до державних інститутів, створення відчуття нестабільності та формування сприятливого інформаційного середовища для досягнення політичних цілей. Таким чином, межа між суто технічним ураженням і інформаційно-психологічним впливом у кіберпросторі поступово розмивалася. Важливою особливістю кібервоєнної моделі є її асиметричний характер, що дозволяє державам і недержавним акторам із відносно обмеженими ресурсами здійснювати вплив на значно потужніших опонентів. Анонімність, складність атрибуції та низький поріг входження сприяють використанню кіберзасобів у «сірій зоні» між війною і миром, де дії не завжди досягають рівня відкритого збройного конфлікту, але мають кумулятивний стратегічний ефект [78, с. 61].

Таким чином, кібервоєнна модель розширює зміст інформаційної війни, трансформуючи її з набору допоміжних технічних дій у самостійну форму стратегічного протиборства, що демонструє зсув акценту з управління інформаційними потоками до цілеспрямованого впливу на цифрові основи функціонування сучасних суспільств, що робить кіберпростір ключовим елементом сучасних парадигм інформаційних впливів.

Інформаційно-психологічні операції та когнітивна модель інформаційної війни. Інформаційно-психологічні операції (PSYOP) традиційно розглядаються як одна з базових форм інформаційної війни, спрямована на цілеспрямований вплив на сприйняття, емоційні реакції та поведінку мас через контроль і модифікацію інформаційного середовища. На відміну від суто технічних моделей інформаційного протиборства, у межах яких інформація розглядається передусім як ресурс управління або ураження інфраструктури, PSYOP

орієнтовані на соціально-психологічний вимір конфлікту, тобто формування установок, переконань і моделей політичної поведінки, що відповідають стратегічним інтересам суб'єкта впливу. У сучасних умовах інформаційні війни суттєво виходять за межі класичних пропагандистських практик, що зумовило трансформацію інформаційно-психологічних операцій у складніші форми впливу. Якщо традиційні PSYOP зосереджувалися переважно на зміні ставлення або поведінки аудиторій через цілеспрямовані повідомлення, то новітні підходи дедалі частіше спрямовані на вплив на самі когнітивні механізми сприйняття реальності. Формується когнітивна модель інформаційної війни, у межах якої об'єктом впливу стає інформаційний простір й логіка інтерпретації подій, процеси прийняття рішень і здатність суспільства до критичного осмислення інформації [82, с. 66].

Когнітивна війна ґрунтується на створенні та закріпленні альтернативних інтерпретацій реальності, викривленні причинно-наслідкових зв'язків й підміні фактів маніпулятивними наративами. Її метою є довготривала трансформація уявлень, що впливає на політичні орієнтири, рівень довіри до інститутів влади та здатність суспільства до колективної мобілізації або опору. Таким чином, когнітивний вимір інформаційної війни забезпечує кумулятивний ефект, результати якого можуть проявлятися поступово й залишатися малопомітними в короткостроковій перспективі [82, с. 67]. Поєднання інформаційно-психологічних операцій із когнітивними стратегіями розмиває межу між інформаційним впливом і ширшими формами політичного та соціального протиборства. Інформаційна війна функціонує переважно в «сірій зоні» між війною і миром, де вплив не досягає порога відкритого збройного конфлікту, але системно змінює умови його можливості. Асиметричний характер когнітивних і психологічних впливів дозволяє як державним, так і недержавним акторам із відносно обмеженими ресурсами здійснювати стратегічний тиск на значно потужніших опонентів.

Таким чином, інтеграція інформаційно-психологічних операцій і когнітивної моделі засвідчує подальше розширення змісту інформаційної війни

від інструменту підтримки військових дій до самостійної форми стратегічного протиборства. Ключового значення набуває контроль над інформаційними потоками й вплив на ментальні та когнітивні основи функціонування сучасних суспільств, що визначає нові підходи до розуміння конфлікту, стримування та безпеки в цифрову добу.

Гібридні інформаційні операції як інтегрована модель сучасного інформаційного протиборства сформувалися як відповідь на фрагментацію класичних підходів до інформаційної війни та необхідність інтеграції різнорідних інструментів впливу в межах єдиних стратегій. На відміну від окремих моделей, що акцентують технічний, організаційний або когнітивний вимір інформаційного протиборства, гібридний підхід поєднує їх у комплексні конфігурації, адаптовані до конкретного політичного, соціального й безпекового контексту. Інформаційна війна перестає бути сукупністю ізольованих операцій і набуває характеру багаторівневого процесу, в якому різні форми впливу взаємно підсилюють одна одну. Ключовою ознакою гібридних інформаційних операцій є синхронізація технічних, інформаційно-психологічних і когнітивних інструментів у межах єдиного замислу. Кібероперації, вплив на інформаційну інфраструктуру, маніпуляція медіапростором, використання соціальних мереж, а також психологічний і когнітивний тиск застосовуються як елементи взаємопов’язаної системи впливу. Такий підхід дозволяє досягати ефекту, що перевищує суму окремих дій, і створює умови для тривалого ослаблення здатності держави або суспільства до ефективного управління та колективної дії [31, p. 21].

Гібридна модель інформаційних операцій функціонує переважно в умовах стратегічної невизначеності, де складно провести чітку межу між миром і війною, внутрішніми та зовнішніми джерелами загроз, легітимними інформаційними практиками й ворожими впливами. Інформаційні дії можуть маскуватися під звичайну політичну комунікацію, громадську активність або медіавиробництво, що ускладнює їх своєчасне виявлення та правову кваліфікацію. Традиційні механізми реагування виявляються малоефективними,

а стратегія протидії зміщується у бік підвищення стійкості інформаційного середовища та суспільства загалом. Важливою характеристикою гібридних інформаційних операцій є їхня адаптивність і контекстуальність. На відміну від уніфікованих доктринальних підходів, гібридні стратегії конструюються з урахуванням соціальних розколів, історичних наративів, рівня довіри до інститутів влади та особливостей медіасистеми конкретної держави. Це дозволяє здійснювати вплив із мінімальними витратами ресурсів, водночас забезпечуючи довготривалий кумулятивний ефект, що проявляється у зміні політичних орієнтацій, норм суспільної поведінки та уявлень про легітимність влади [27].

Гібридні інформаційні операції репрезентують завершальний етап еволюції моделей інформаційної війни, у межах якого поєднуються мережево-центричні підходи, кібервоєнні інструменти та інформаційно-психологічні й когнітивні стратегії. Ця модель відображає перехід від розуміння інформаційної війни як допоміжного елементу збройного протиборства до усвідомлення її як самостійної форми стратегічного впливу, здатної визначати політичні результати без прямого застосування військової сили. Саме гібридний характер сучасних інформаційних операцій окреслює ключові виклики для національної та міжнародної безпеки в умовах цифрової трансформації.

Таким чином, інформаційна війна постає як структурно складний і концептуально мінливий феномен міжнародної безпеки, зумовлений багатовимірністю інформації як ресурсу влади та розширенням інструментів впливу на сприйняття, поведінку й стратегічне середовище. У науковому дискурсі сформувалося кілька аналітичних підходів до її інтерпретації, які по-різному окреслюють природу інформаційних протиборств, їхні функції та механізми досягнення політичних результатів. Еволюція інформаційних війн відображає поступову трансформацію інформаційних і психологічних впливів від допоміжних інструментів воєнного протиборства до самостійного та структурно інтегрованого виміру стратегічної конкуренції у міжнародній безпеці. Розширення практик інформаційної війни у цифрову добу зумовило появу низки моделей, спрямованих на пояснення різних механізмів

інформаційного впливу в сучасних війнах, які виникали як відповідь на практичні зміни у способах ведення протиборства й відображали перехід від фрагментарного застосування інформаційних засобів до комплексних способів організації стратегічного впливу на технічні, управлінські та когнітивні основи безпеки.

РОЗДІЛ 3. ІНФОРМАЦІЙНІ ОПЕРАЦІЇ ЯК ЧИННИК ВІДТВОРЕННЯ ДИЛЕМИ БЕЗПЕКИ В УМОВАХ СТРАТЕГІЧНОЇ КОНКУРЕНЦІЇ

3.1. Концепція стратегічної конкуренції в інформаційному вимірі

Сучасний міжнародний порядок ґрунтується на системі правил і норм, сформованих після Другої світової війни, які передбачають передбачуваність поведінки держав, наявність наслідків за порушення усталених принципів та обмеження спектра допустимих дій у міжнародних відносинах. Водночас цей порядок дедалі активніше оскаржується з боку ревізіоністських держав, недержавних акторів та транснаціональних мереж, що ставить під сумнів стабільність і ефективність існуючої системи міжнародної безпеки. Стратегічна конкуренція постає не як винятковий стан, а як домінантна форма взаємодії між ключовими акторами міжнародної системи. Конкуренція не є новим явищем у міжнародних відносинах: держави завжди прагнули захищати та просувати власні інтереси з метою досягнення стратегічних переваг. Однак специфікою сучасного етапу є те, що головні виклики чинному міжнародному порядку походять від потужних держав-ревізіоністів, передусім КНР та росії, що зумовлює поширене трактування нинішньої ситуації як етапу загостреної стратегічної конкуренції між провідними центрами сили [18].

У сучасному міжнародному середовищі безпеки стратегічна конкуренція суттєво ускладнюється стрімким розвитком і поширенням цифрових комунікаційних технологій, зокрема інтернету, Інтернету речей та соціальних мереж. Сьогодні практично будь-який актор, державний чи недержавний, має змогу миттєво поширювати інформацію в глобальному масштабі, використовуючи широкий спектр платформ і каналів комунікації. Така трансформація інформаційного середовища докорінно змінює умови стратегічної взаємодії, оскільки надає опонентам безпрецедентний доступ до громадян інших держав і відкриває широкі можливості для здійснення

цілеспрямованого впливу [62, p. 8]. У практичному вимірі це проявляється в численних прикладах спроб зовнішніх акторів впливати на внутрішньополітичні процеси інших держав, зокрема на виборчі кампанії, поширювати дезінформацію щодо пандемії COVID-19 або навмисно провокувати поляризацію суспільств навколо чутливих і конфліктних тем, таких як расові відносини, контроль за обігом зброї, аборти, безпека вакцинації чи міграційна політика. Таким чином, інформаційне середовище, що постійно розширюється, формує майже необмежений простір для стратегічної конкуренції, в якому межі між зовнішньою та внутрішньою безпекою стають дедалі більш розмитими [54, p. 3].

Використання інформації для досягнення конкурентних переваг має принципові відмінності порівняно з іншими елементами національної могутності – дипломатичними, економічними та військовими. Особливо показовими є відмінності між конкуренцією в інформаційному середовищі та діями в традиційних просторових військових доменах. На відміну від суходолу, моря, повітря чи космосу, інформаційне середовище не є фізичним простором, у якому можна безпосередньо перебувати або який можна чітко локалізувати. Але воно має матеріальний вимір, що охоплює інфраструктуру зберігання, обробки, передавання та приймання інформації – комп'ютери, мобільні пристрої, сервери, маршрутизатори та інші технічні засоби. Фізичний вимір інформаційного середовища іноді може ставати об'єктом безпосереднього впливу, зокрема шляхом знищення обладнання або фізичного переривання потоків даних. Проте, у переважній більшості випадків основними цілями є не технічні системи, а людські сприйняття та моделі поведінки. У цьому контексті ідеї виступають своєрідною «зброєю», тоді як норми, переконання та традиції виконують функцію «захисту». Така специфіка інформаційного середовища зумовлює принципово інший характер операцій, що в ньому здійснюються [54, pp. 4-5].

Наслідки для операцій в інформаційному середовищі (operations in the information environment, OIE) є очевидними, особливо якщо розглядати конфлікт як поєднання засобів і волі до ведення боротьби, то традиційні домени війни

здебільшого пов’язані із забезпеченням матеріальних засобів, тоді як інформаційне середовище спрямоване передусім на формування та зміну волі до дії. Вплив на рішення, мотивацію та поведінку опонента стає центральним завданням інформаційних операцій у межах стратегічної конкуренції.

Операції в інформаційному середовищі в умовах конкуренції та конфлікту додають нові рівні складності до вже наявних викликів стратегічної взаємодії. Інформаційні операції залишаються фундаментальним компонентом військової діяльності в усьому спектрі взаємодії: від співпраці через конкуренцію і до відкритого конфлікту. Надмірна орієнтація на кінетичні засоби ведення бойових дій часто призводить до недооцінки ролі інформації та OIE, унаслідок чого вони сприймаються як допоміжний інструмент, релевантний передусім для роботи з цивільним населенням або в умовах нерегулярних конфліктів. Крім того, проблематика операцій в інформаційному середовищі має безпосереднє значення і для «гарячої» фази конфлікту, особливо на стику між стратегічною конкуренцією та збройним протистоянням. У цій зоні OIE переходять від відносно стабільного конкурентного фокусу, зосередженого на наративах, контрпропаганді, стримуванні, сигналюванні та формуванні сприятливих умов для власних сил, до виконання безпосередніх завдань воєнного часу. До них належать підрив волі противника до боротьби, втручання в процеси ухвалення рішень і системи командування та управління, а також приховування планів і переміщень власних сил. Отже, операції в інформаційному середовищі стають невід’ємним елементом стратегічної взаємодії, що поєднує конкуренцію і конфлікт в єдиному безпековому континуумі [55, с. 15].

Однією з базових узгоджених концептуальних позицій у сучасному аналізі стратегічної конкуренції є розуміння того, що вона розмиває чітку межу між миром і війною та розгортається не в дискретних станах, а на континуумі взаємодії. Цей континуум охоплює весь спектр від співпраці через конкуренцію до конфліктів різної інтенсивності. Такий підхід заперечує традиційне уявлення про міжнародну безпеку як послідовність чітко відмежованих фаз і натомість підкреслює поступовість, гібридність і взаємопроникнення різних форм

взаємодії між державами [9, p. 6].

Пов’язаною з уявленням про континуум конкуренції є концепція порогів (thresholds), яка має принципове значення для розуміння сучасної стратегічної поведінки держав. Виходячи з критики хибної дихотомії між миром і війною, дослідники наголошують, що агресивні дії в умовах стратегічної конкуренції часто навмисно конструюються таким чином, щоб залишатися нижче порогу війни. Одна з ключових особливостей конкуренції між великими державами полягає в тому, що ревізіоністські актори прагнуть змінити окремі елементи міжнародного порядку, не вдаючись до відкритого збройного конфлікту і не провокуючи відповідь, яка могла б призвести до ескалації до рівня війни. Стратегічна конкуренція ґрунтується на постійному балансуванні між дією і стримуванням, де центральним завданням є досягнення змін без перетину формальних або неформальних «червоних ліній». При цьому агресивна поведінка в межах «сірої зони» (gray zone) нерідко має на меті уникнути військової відповіді й залишитися нижче порогу сприйняття. У таких випадках одна зі сторін конкуренції може навіть не усвідомлювати, що відбуваються поступові, але системні зміни, які впливають на розподіл впливу, контроль над просторами або формування сприятливих стратегічних умов для опонента [14, pp. 5-7].

Важливим для розуміння порогів у стратегічній конкуренції є те, що вони не є фіксованими або однозначно визначеними. Пороги мають плинний і динамічний характер, що робить їх об’єктом постійної інтерпретації, маніпуляції та стратегічних розрахунків. Хоча в політичному дискурсі вони часто подаються як чітко окреслені «червоні лінії», перетин яких автоматично має викликати відповідь і ескалацію, на практиці такі лінії рідко функціонують у настільки жорсткий спосіб. Концепти «розтягування порогів» (threshold stretching) та «експлуатації порогів» (threshold exploitation), які активно використовуються в межах агресії в сірій зоні. Під розтягуванням порогів розуміють застосування заходів, що формально не досягають рівня війни, але спрямовані на поступову зміну самого характеру порогу з метою здобуття більшого регіонального впливу,

доступу та контролю. Експлуатація порогів, своєю чергою, полягає у використанні нездатності конкурента забезпечити дотримання проголошеного або неформально встановленого порогу, а також у розрахунку на його помилкову оцінку ризиків ескалації до повномасштабного конфлікту [14, p. 7].

У цій зоні особливої стратегічної значущості набувають операції в інформаційному середовищі, які майже завжди сприймаються як недостатньо провокативні для перетину порогу війни, що робить їх привабливим інструментом стратегічної конкуренції. Завдяки властивій їм амбівалентності такі операції часто здійснюються не лише нижче формального порогу війни, а й нижче порогу сприйняття або, принаймні, нижче порогу атрибуції. Це означає, що навіть за наявності підозр щодо зовнішнього впливу, відповідальність за конкретні дії залишається розмитою, що суттєво ускладнює ухвалення рішень про відповідь. Операції в інформаційному середовищі органічно вписуються в умови стратегічної конкуренції, заснованої на управлінні невизначеністю та маніпулюванні порогами. Вони дозволяють ревізіоністським акторам поступово змінювати стратегічні умови, не провокуючи відкритої ескалації, водночас підриваючи здатність опонента чітко інтерпретувати події та своєчасно реагувати на них. Комбінація розмитих меж, плинних порогів і навмисної багатозначності створює сприятливе середовище для відтворення невизначеності як структурної характеристики стратегічної конкуренції [55, p. 11].

У межах стратегічної конкуренції інформаційні операції, спрямовані на підрив політичної єдності держави-конкурента, будуються навколо цілеспрямованого втручання в процеси внутрішньої політичної комунікації. Йдеться передусім про системну роботу з інформаційними потоками, які формують уявлення про легітимність влади, узгодженість дій політичних інститутів та спільність базових політичних орієнтирів. Через інформаційні операції ці уявлення піддаються ерозії шляхом навмисного підкреслення розбіжностей між гілками влади, політичними партіями, регіональними та центральними елітами, а також між державними інституціями й суспільством.

Механізм такого впливу ґрунтується на інтенсифікації вже наявних ліній напруження, використовується селективне висвітлення політичних рішень, виривання окремих подій або заяв з контексту та їх подальше вбудовування в альтернативні інтерпретаційні рамки. Політичні розбіжності починають сприйматися як ознака системної неспроможності або внутрішнього розпаду, що підриває довіру до здатності держави діяти узгоджено. Окрему роль у підриві політичної єдності відіграє фрагментація публічного простору, яку посилюють інформаційні операції. Через одночасне просування взаємовиключних наративів для різних аудиторій руйнується спільне поле політичного сенсу, в межах якого можливе досягнення компромісів, що призводить до ситуації, коли різні групи суспільства оперують несумісними уявленнями про політичну реальність, що ускладнює формування консолідованих позицій щодо внутрішніх і зовнішніх викликів. Причина ефективності таких інформаційних операцій полягає в тому, що політична єдність є процесуальною характеристикою, яка потребує постійного відтворення через комунікацію та взаємне визнання легітимності. Втручання в ці комунікативні процеси не викликає негайних кризових ефектів, однак поступово знижує рівень узгодженості політичної системи. У стратегічному вимірі це створює для держави-конкурента ситуацію внутрішньої розбалансованості, що обмежує її здатність послідовно реалізовувати власні інтереси та реагувати на зовнішній тиск.

Конкретним прикладом використання інформаційних операцій у межах стратегічної конкуренції держав є втручання росії в інформаційний простір Сполучених Штатів під час президентської виборчої кампанії 2016 року. Масштабна багатоканальна діяльність була спрямована на підрив довіри до демократичних інститутів загалом. Через соціальні мережі та онлайн-платформи поширювалися суперечливі й взаємовиключні повідомлення щодо виборчого процесу, легітимності результатів голосування та чесності політичних еліт. Ці інформаційні дії були спрямовані на довгостроковий ефект щодо послаблення внутрішньої політичної згуртованості та підвищення рівня суспільної поляризації, що об’єктивно знижувало стратегічну стійкість держави-

конкурента [46].

Іншим показовим прикладом є використання інформаційних операцій під час пандемії COVID-19, коли низка держав цілеспрямовано поширювала дезінформацію щодо походження вірусу, ефективності вакцин та здатності демократичних урядів управляти кризами. У цьому випадку інформаційні операції були інтегровані в ширший контекст стратегічної конкуренції, оскільки вони впливали на громадську думку та спроможність держав ухвалювати та реалізовувати політичні рішення в умовах надзвичайної ситуації. Посилення недовіри до офіційних джерел інформації та державних інституцій безпосередньо ускладнювало управління кризою та створювало додаткові внутрішні вразливості, які могли бути використані у подальшій міждержавній взаємодії [4]. Отже, в умовах стратегічної конкуренції інформаційні операції застосовуються як інструмент непрямого впливу, спрямований на зміну внутрішніх умов функціонування держави-конкурента без формального порушення миру та без переходу до відкритого збройного протистояння.

Інформаційні операції, спрямовані на вплив на процеси ухвалення рішень у державі-конкуренті, фокусуються на викривленні інформаційного середовища, в якому функціонують політичні та адміністративні еліти. Відбувається створення таких інформаційних умов, за яких керівні актори змушені ухвалювати рішення на основі неповної, суперечливої або навмисно спотвореної інформації. Втручання здійснюється безпосередньо в когнітивний вимір управління, впливаючи на оцінку ризиків, альтернатив і можливих наслідків політичних дій. Механізм впливу реалізується через перенасичення інформаційного простору взаємовиключними сигналами, суперечливими інтерпретаціями подій та штучно створеними інформаційними приводами, що ускладнює пріоритизацію проблем і концентрацію уваги на стратегічно важливих питаннях. Процес ухвалення рішень зміщується від довгострокового планування до реактивного реагування на інформаційні імпульси, що постійно змінюються, що підвищує ймовірність помилкових оцінок, затримок у прийнятті рішень або вибору оптимальних стратегій. Інформаційний тиск чиниться на інституційні процедури ухвалення

рішень через публічні інформаційні кампанії, витоки даних або навмисне загострення медійної уваги до окремих аспектів політики створюється ситуація, за якої формальні процедури втрачають стабільність і передбачуваність. Політичні рішення ухвалюються в умовах постійної необхідності враховувати репутаційні ризики, очікування зовнішніх аудиторій або загрозу внутрішньої дестабілізації, що обмежує автономію стратегічного вибору. Ефективність інформаційних операцій полягає в тому, що процеси ухвалення рішень є чутливими до інформаційного контексту та часових обмежень. Навіть без прямого втручання в інституційні механізми зміна інформаційного фону здатна суттєво вплинути на процес прийняття політичних рішень. У стратегічній перспективі це дозволяє державі-ініціатору ускладнювати реалізацію політики конкурента й непрямо спрямовувати його дії в бажаному напрямі, не вдаючись до відкритого примусу або ескалації.

Прикладом інформаційного втручання в процеси ухвалення рішень є публікація викраденого дипломатичного листування та внутрішніх документів західних урядів через платформи WikiLeaks у 2010–2011 рр. Масове оприлюднення матеріалів Державного департаменту США відбулося в момент активної зовнішньополітичної діяльності та безпекових операцій безпосередньо вплинуло на внутрішні процеси ухвалення рішень. Американський та союзницькі уряди були змушені переглядати дипломатичні підходи, канали комунікації та процедури обміну інформацією не внаслідок зміни стратегічних інтересів, а через інформаційний тиск, спричинений публічним розголосом. У цьому випадку інформаційна операція вплинула на поведінку державних інститутів, звузивши простір для автономного прийняття рішень [47].

Іншим показовим прикладом є інформаційний супровід російських дій під час анексії АР Крим у 2014 р. Паралельно з військово-політичними кроками здійснювалась інтенсивна кампанія з поширення суперечливих повідомлень щодо присутності збройних формувань, легітимності місцевої влади та характеру подій. Створена інформаційна невизначеність ускладнила процес ухвалення рішень як в Україні, так і серед західних держав, зокрема щодо

масштабів і темпів реагування. Умови неповної та суперечливої інформації призвели до затримок у формуванні узгодженої відповіді, що дало ініціатору інформаційної операції часову та стратегічну перевагу [32].

Ще одним прикладом є дезінформаційні кампанії навколо застосування хімічної зброї в Сирії після 2013 року. Поширення альтернативних версій подій, сумнівів щодо джерел доказів і відповідальності сторін безпосередньо впливало на процеси ухвалення рішень у Раді Безпеки ООН та в урядах західних держав. Інформаційний тиск істотно ускладнював досягнення політичного консенсусу та відкладав практичні дії, що мало прямі наслідки для перебігу конфлікту [58]. Таким чином, інформаційні операції здатні впливати на процеси ухвалення рішень шляхом створення інформаційної невизначеності, часових затримок і репутаційних ризиків, змінюючи умови, в яких державні інститути здійснюють стратегічний вибір.

У стратегічній конкуренції між державами інформаційні операції, спрямовані на зниження довіри до інститутів, орієнтовані на підрив сприйняття їхньої легітимності, компетентності та неупередженості. Об’єктом такого впливу виступає комплекс органів публічної влади, виборчі органи, судова система, правоохоронні структури, державні регулятори та офіційні джерела інформації, які через репрезентуються як корумповані, контрольовані вузькими групами інтересів або нездатні діяти в інтересах суспільства. Застосовують різноманітні інструменти зниження довіри, систематичне поширення наративів, що ставлять під сумнів процедурну коректність інституційної діяльності. Акцентується увага на поодиноких помилках, конфліктах або переривання роботи інститутів із подальшим узагальненням їх до рівня структурної неспроможності. Окремі рішення або дії подаються як доказ цілковитої дискредитації інституції, незалежно від їхнього реального масштабу чи контексту, тобто формуються стійкі уявлення про те, що інститути не заслуговують на довіру як джерела рішень або інформації. Особливий та специфічний вплив спрямований на підрив авторитету інституцій, відповідальних за виробництво та верифікацію знань, зокрема експертних, наукових і аналітичних структур шляхом просування

взаємовиключних інтерпретацій, псевдоекспертних оцінок і альтернативних «фактів» таким чином, що знецінюється сама ідея інституційної експертизи. Суспільство дедалі менше сприймає інституційні позиції як обґрунтовані, що ускладнює реалізацію політики навіть за формальної наявності правових повноважень. Дієвість заходів зумовлена тим, що довіра до інститутів має кумулятивний характер і формується в довгостроковій перспективі, тоді як її руйнування може відбуватися поступово й непомітно. Послідовне зниження довіри не обов'язково призводить до негайної кризи управління, але створює умови, за яких інституційні рішення сприймаються як нелегітимні або нав'язані. У стратегічному вимірі це зменшує спроможність держави діяти узгоджено, мобілізувати ресурси та підтримувати політичну стабільність у ситуаціях зовнішнього тиску.

Наприклад, після збиття рейсу MH17 інформаційний вплив був спрямований на підрив довіри до самої здатності міжнародних слідчих інституцій встановлювати об'єктивну істину. Ключовим інструментом стала навмисна множинність взаємовиключних версій: у публічний простір одночасно вкидалися твердження про український винищувач, помилковий пуск українського ЗРК, змову західних спецслужб, маніпуляції з радарними даними, а також версії про «провокацію» з використанням уже пошкодженого літака. Взаємна несумісність цих наративів не розглядалася як проблема, оскільки їхнє завдання полягало не в переконанні в одній версії, а у створенні відчуття, що «правду встановити неможливо». Ефект посилювався поширенням псевдотехнічних експертиз, які імітували мову професійного розслідування: використовувалися фрагментарні радіолокаційні дані, комп'ютерні візуалізації, вибіркові цитати з авіаційних регламентів або військово-технічних характеристик. Такі матеріали подавалися як рівноцінні офіційним висновкам, попри відсутність доступу до повного масиву доказів, методологічної прозорості та незалежної верифікації. У публічному сприйнятті стиралася межа між інституційним розслідуванням і довільною інтерпретацією. Персональні атаки на слідчих та експертів Спільної слідчої групи, яких зображували як політично

заангажованих, пов'язаних з урядами зацікавлених держав або такими, що свідомо ігнорують «незручні» докази. Фокус переносився з процедур, стандартів доказування та інституційної відповідальності на особисту мотивацію конкретних учасників розслідування, що дозволяло підмінити критику результатів сумнівом у доброчесності самого процесу. Сукупність застосування інструментів сформувала уявлення про міжнародні слідчі інституції як такі, що не здатні або не мають наміру встановлювати факти, а лише відтворюють політично задані висновки. Таким чином, під сумнів ставилася не конкретна справа MH17, а сама можливість існування нейтрального, доказового та інституційно гарантованого встановлення істини [60].

3.2. Невизначеність інформаційного середовища і відтворення дилеми безпеки

У сучасній літературі з проблематики стратегічної конкуренції сформувався стійкий консенсус щодо центральної ролі невизначеності як чинника, що визначає поведінку акторів у міжнародному середовищі безпеки. Невизначеність розглядається як функціональний ресурс, який дозволяє акторам уникати однозначної інтерпретації власних дій, відкладати або розпорошувати реакцію опонентів та утримувати стратегічну ініціативу та виконує роль механізму управління ризиками ескалації, водночас створюючи сприятливі умови для поступового перерозподілу стратегічних переваг. Невизначеність в інформаційному середовищі формується як через приховування фактів, так і через контроль над способами їх інтерпретації. Операції в інформаційному середовищі дозволяють навмисно ускладнювати відповідь на базові запитання безпеки: що саме відбувається, які дії мають ворожий характер, чи є вони умисними та хто несе за них відповідальність. Навіть за наявності доступної емпіричної інформації інформаційні операції здатні розмивати причинно-наслідкові зв'язки, підмінювати ієрархію загроз і створювати конкуренцію між альтернативними пояснювальними моделями [55, p. 17].

Невизначеність формується через маніпуляцію інформаційними сигналами, наративами та інтерпретаційними рамками. Систематичне продукування багатозначності, за якої дії актора можуть водночас виглядати як легітимні, випадкові або ворожі залежно від точки спостереження. Багатозначність ускладнює процес атрибуції та позбавляє опонента можливості швидко й упевнено класифікувати подію як загрозу, що потребує відповіді. Інформаційне середовище є особливо сприятливим для такого типу впливу, оскільки воно характеризується високою швидкістю циркуляції повідомлень, множинністю каналів комунікації та відсутністю єдиного авторитетного механізму верифікації. Держави змушені ухвалювати рішення в умовах конкуренції версій, неповної атрибуції та ризику помилкової інтерпретації намірів іншої сторони, що безпосередньо впливає на здатність відрізнити оборонні дії від наступальних, рутинну активність – від підготовки до ескалації.

Невизначеність в інформаційному середовищі безпосередньо пов’язується з відтворенням дилеми безпеки. Інформаційні операції підсилюють фундаментальну проблему інтерпретації намірів, яка лежить в основі дилеми безпеки, оскільки навіть обмежені або оборонні дії можуть сприйматися як прихована загроза. Спроби реагування в умовах невизначеності здатні самі по собі генерувати додаткові сигнали тривоги для іншої сторони, запускаючи ланцюг взаємних підозр і запобіжних кроків. Таким чином, невизначеність у інформаційному середовищі виступає структурною умовою, що підтримує нерозв’язність дилеми безпеки. Операції в інформаційному середовищі формалізують цю невизначеність, перетворюючи її на стабільний елемент стратегічної взаємодії. Дилема безпеки відтворюється через інформаційні практики, які унеможливлюють досягнення однозначного взаємного розуміння навіть за відсутності відкритого конфлікту.

Невизначеність, що системно відтворюється в інформаційному середовищі, безпосередньо актуалізує дилему безпеки через ускладнення двох взаємопов’язаних процесів - інтерпретації та реагування. По-перше,

інформаційні операції посилюють дилему інтерпретації, оскільки підривають можливість однозначного тлумачення намірів іншого актора. За умов інформаційної багатозначності держави стикаються з ситуацією, коли одні й ті самі дії можуть бути витлумачені як оборонні, експериментальні або підготовчі до ескалації. Відсутність стабільних інтерпретаційних орієнтирів змушує виходити не з перевірених фактів, а з припущень щодо прихованих намірів, що підвищує роль підозри як основи стратегічного аналізу. Інформаційне середовище підсилює цю проблему тим, що воно не лише передає сигнали, а й активно конкурує за їх пояснення. Альтернативні наративи, псевдодоказові інтерпретації та взаємовиключні версії подій створюють ситуацію, за якої держава не може бути впевненою, чи має вона справу з реальною загрозою, чи з навмисно сконструйованим образом загрози. Навіть стримані або реактивні дії іншої сторони можуть сприйматися як частина ширшої наступальної стратегії.

По-друге, з дилеми інтерпретації безпосередньо випливає дилема реагування. Умови інформаційної невизначеності унеможливлюють вибір оптимальної відповіді, оскільки будь-яке рішення несе асиметричні ризики. Обмежене або відкладене реагування може бути витлумачене як слабкість або мовчазна згода, тоді як активна відповідь як непропорційна ескалація. За відсутності впевненості у намірах опонента держава змушена балансувати між ризиком надмірної реакції та ризиком стратегічної інерції. Інформаційні операції додатково ускладнюють цей вибір, оскільки самі реакції стають частиною інформаційного простору та можуть бути переінтерпретовані, вирвані з контексту або використані для формування нових наративів. Таким чином, рішення, ухвалене з міркувань стримування, може бути подане як агресивне, тоді як спроби деескалації як підтвердження вразливості. Це створює самопідтримувальний цикл, у якому кожна сторона коригує свою поведінку, виходячи не з намірів іншої сторони, а з очікувань щодо її можливих інтерпретацій. Інформаційна невизначеність не просто супроводжує дилему безпеки, а виступає механізмом її постійного відтворення, оскільки через ускладнення інтерпретації та реагування інформаційні операції закріплюють

структурну недовіру як базову умову стратегічної взаємодії. Таким чином, навіть за відсутності матеріального нарощування загроз інформаційне середовище здатне підтримувати стан взаємного страху та запобіжних дій, які лежать в основі дилеми безпеки.

Таким чином, невизначеність інформаційного середовища виступає структурною умовою сучасної стратегічної взаємодії, яка цілеспрямовано відтворюється через інформаційні операції. Вона ускладнює атрибуцію дій і тлумачення намірів, що посилює дилеми інтерпретації та реагування й підтримує самопідтримувальний цикл недовіри та запобіжних дій. Отже, інформаційне середовище стає ключовим механізмом відтворення дилеми безпеки навіть за відсутності відкритого збройного конфлікту.

3.3. Інтегроване стримування в інформаційному просторі стратегічної конкуренції

У відповідь на ускладнення стратегічної конкуренції та розширення простору конфліктності за межі традиційних військових доменів формується концепція інтегрованого стримування, яка поєднує різні інструменти державної потуги в запобігання ескалації. Інтегроване стримування виходить із визнання того, що сучасні загрози проявляються одночасно у військовій, економічній, технологічній та інформаційній сферах, а отже ефективна відповідь потребує координації дій у цих вимірах. Інформаційний простір розглядається як повноцінний домен стратегічної взаємодії, у межах якого стримування набуває специфічних форм. Інформаційне стримування як складова інтегрованого підходу ґрунтується на управлінні сприйняттям, очікуваннями та оцінками витрат і вигод потенційного опонента. Формування передбачуваності реакцій, підвищення вартості інформаційних атак та зменшення їх стратегічної доцільності обумовлює потребу в інформаційному стримуванні, орієнтованому на вплив на процес ухвалення рішень ще до моменту реалізації інформаційних операцій, закріплюючи уявлення про їх обмежену ефективність або небажані

наслідки. Включення інформаційного виміру до інтегрованого стримування відкриває перспективи для розвитку міжнародних підходів до регулювання та запобігання інформаційним війнам. Хоча формалізовані режими контролю в цій сфері залишаються обмеженими, дедалі більшого значення набувають практики встановлення норм відповідальної поведінки, підвищення прозорості інформаційної діяльності та координації між союзниками. Таким чином, інтегроване стримування створює рамку, в межах якої інформаційні операції розглядаються не ізольовано, а як елемент ширшої системи управління стратегічною стабільністю в умовах зростаючої невизначеності.

Поняття інтегрованого стримування розуміється в теорії міжнародної безпеки як намір досягати стримувального ефекту шляхом всебічної та стратегічно спроєктованої інтеграції національних інструментів влади. Центральним операційним процесом залишається саме стримування, тоді як концепція інтегрованого стримування передусім стосується характеру та поєднання засобів, за допомогою яких цей ефект досягається.

Аналіз стримування як практики державної політики ґрунтується на двох ключових вихідних положеннях. По-перше, об’єктом стримувального впливу є процес ухвалення рішення про ініціювання агресії в уявленні потенційного агресора – конкретного лідера або вузького кола осіб, які здійснюють стратегічний вибір. Політичні лідери та уряди оцінюють ризики й можливості застосування сили у спосіб, що часто є ідіосинкратичним і формується під впливом глибоко вкорінених переконань, уявлень та сприйняття реальності. По-друге, стримування за своєю суттю є передусім політичним, а не технічним феноменом. Воно залежить від інтересів, влади, інформації та рішучості, так само як і рішення про війну є політичним судженням, а не раціоналізованим розрахунком балансу сил [43, p. 14]. Ці обставини істотно ускладнюють практику стримування. Хоча класична теорія стримування формувалася як відповідь на технологічний виклик, пов’язаний із появою ядерної зброї, у реальній політичній практиці стримування не функціонує як лінійна шкала об’єктивно вимірюваних

параметрів, які можна механістично коригувати, а являє собою складний процес формування суб'єктивних уявлень і впливу на політичні судження, що за своєю природою є нестабільними та важко передбачуваними. Стримування означає зусилля, спрямовані на запобігання здійсненню небажаної дії з боку іншого актора, яким у сфері безпеки є зазвичай держави або недержавна збройна група. Отже, стримування принципово відрізняється від спорідненого поняття примусу, яке означає застосування тиску з метою змусити іншу сторону здійснити певну дію [49, p. 5].

Держави можуть прагнути стримувати інших акторів від здійснення широкого спектра дій. В сучасних умовах поняття стримування певною мірою втратило аналітичну чіткість, оскільки його дедалі частіше використовують як універсальну політичну відповідь на будь-яку поведінку або потенційну подію, що сприймається як загроза національним інтересам. Однак, стримування за своєю суттю передбачає, принаймні частково, наявність переконливих загроз відплати, здатних накласти такі витрати, які істотно змінюють розрахунок ризиків з боку опонента У випадку багатьох дій конкурентів, що здійснюються нижче порогу збройного конфлікту, сформувати заздалегідь подібні переконливі загрози вкрай складно. Поведінка агресора в таких ситуаціях часто не є достатньо відверто ворожою або неприйнятною, щоб виправдати серйозні погрози у відповідь: відповідні дії можуть не порушувати міжнародне право, не виглядати агресивними або створювати надмірні ризики ескалаційних спіралей. У сукупності це означає, що погрози жорстко покарати дії, які не досягають порогу війни, є складними з погляду їхньої переконливості та ефективності За таких умов у значній частині повсякденної конкурентної взаємодії держави змушені зосереджуватися не стільки на стримуванні відповідних дій, скільки на пом'якшенні їхніх наслідків або на активній конкуренції у відповідних сферах. Отже, під час формулювання будь-якого стримувального виклику чи політики принципово важливо враховувати низку ключових розрізнень, які визначають характер стримувальних зусиль [48, p. 82].

По-перше, будь-яка політика стримування насамперед визначається тією

ворожою дією, якій вона має запобігти. У класичному розумінні поняття стримування зазвичай застосовується до відносно вузької категорії потенційних дій – масштабної агресивної війни [29]. Зростання ролі відносно агресивних дій нижче порогу війни, зокрема кібератак або інформаційного примусу, призводить до того, що дедалі частіше йдеться про необхідність стримування окремих, особливо демонстративних та конфронтаційних форм такої діяльності. Мається на увазі обмежене коло дій нижче порогу війни, які, попри відсутність формального збройного конфлікту, характеризуються значним військовим або квазі-військовим ефектом та виразним ворожим наміром. Інший підхід до концептуалізації форм стримування пов'язаний із розрізненням за масштабом і характером інструментів державної політики, що застосовуються для досягнення стримувальних цілей. Частина теоретиків наполягає на вузькому тлумаченні «інструментарію стримування», розглядаючи його передусім як використання військових погроз для запобігання військовим діям з боку опонента [48, с. 3–5].

Другий підхід до розуміння стримування полягає в розширенні набору інструментів, за допомогою яких може формуватися стримувальний ефект. У цьому випадку стримування не обмежується виключно військовими погрозами, а включає застосування невійськових засобів у відповідь на військову агресію, зокрема економічні санкції, політичну ізоляцію, інформаційний або інші форми державного тиску. Такий підхід виходить з припущення, що загроза значущих немілітарних витрат може впливати на розрахунки потенційного агресора так само, як і загроза прямого військового протистояння [49, с. 6].

Третє, ще ширше, розуміння стримування виходить за межі виключно загрози та включає механізм поєднання стримування і заспокоєння. В межах цього підходу вважається, що для запобігання агресії необхідно враховувати базові безпекові побоювання потенційного противника та, за певних умов, адресувати їх через обмеження власної поведінки, переговори, компроміси або публічні гарантії. Мазар підкреслює, що сама по собі загроза може бути недостатньою для ефективного стримування, а в окремих випадках дії,

спрямовані на посилення стримування, можуть мати протилежний ефект, оскільки вони поглиблюють відчуття загрози у іншої сторони та стимулюють ескалаційну логіку [52, p. 52].

Класична типологія форм стримування залежно від механізму впливу на рішення агресора визначає стримування шляхом відмови (deterrence by denial) та стримування шляхом покарання (deterrence by punishment). Стримування шляхом відмови спрямоване на унеможливлення досягнення агресором бажаних цілей, зокрема через створення ефективної оборони та демонстрацію готовності її застосувати. Стримування шляхом покарання ґрунтується на загрозі ширших, часто непрямих наслідків агресії, які завдають шкоди агресору поза межами конкретного театру дій. Хоча ці два підходи не є взаємовиключними і можуть застосовуватися паралельно, треба уникати спрощеного уявлення про їх ефективність. Здатність стримування шляхом відмови або покарання впливати на поведінку агресора значною мірою залежить від його сприйняття, упереджень та інтерпретацій, а не від об’єктивно вимірюваних показників. Отже, стримування не є лінійною моделлю, в якій можна точно визначити поріг достатності, а залишається політично й психологічно зумовленим процесом.

Четвертий аспект характеру стримування, стосується часу та масштабу. Безпосереднє (immediate) стримування означає найбільш відому, короткострокову й конкретно спрямовану форму стримування, зосереджену на запобіганні безпосередній загрозі агресії. У ситуаціях, коли існують ознаки неминучого нападу, і стримувальні заходи спрямовані на вплив на конкретне рішення про початок агресивних дій. Дії держави, спрямовані на посилення загроз або демонстрацію готовності до відповіді, є складовими політики безпосереднього стримування. Загальне (general) стримування має більш довгостроковий і контекстуальний характер й полягає у формуванні стійкого співвідношення витрат і вигод у сприйнятті одного або кількох потенційних агресорів, що в цілому знижує їхню схильність до агресивної поведінки. Загальне стримування не орієнтоване на конкретну кризу чи загрозу, а функціонує як постійний фон стратегічної взаємодії [49, p. 7].

П’ятий фактор стосується об’єкта стримування. Центральне стримування передбачає зусилля держави, спрямовані на запобігання нападу безпосередньо на неї саму. Розширене (extended) стримування, своєю чергою, означає стримування агресії проти третіх сторін і ґрунтується на готовності держави застосувати свої ресурси для захисту союзників або партнерів [49, p. 7].

Сукупність цих п’яти чинників демонструє складність встановлення простих і вимірюваних причинно-наслідкових зв’язків між окремими заходами, такими як військові інвестиції, нарощування сил, заходи у сфері безпекового співробітництва або інші політичні кроки, та фактичними результатами стримування. Один і той самий інструмент або дія може мати різні наслідки залежно від того, чи йдеться про стримування шляхом позбавлення або покарання, про безпосереднє чи загальне стримування, а також залежно від того, на якого саме потенційного агресора вони спрямовані. Як зауважує П. Морган (Morgan P. M.), у сучасному дискурсі концепт стримування дедалі частіше використовується для опису широкого спектра ситуацій і дій, спрямованих на припинення, зменшення або пом’якшення загроз національним інтересам [52, p. 52]. Якщо концепція інтегрованого стримування піде цим шляхом, вона ризикує перетворитися на синонім загальної стратегії національної безпеки, тобто на позначення інтегрованого застосування всіх інструментів державної потуги для досягнення будь-яких стратегічних цілей. Таким чином, необхідно обмежувати завдання стримувальних стратегій запобіганням масштабному застосуванню сили, передусім ядерній або конвенційній агресії, а також, за певних умов, найбільш інтенсивним і насильницьким формам дій нижче порогу війни, які передбачають значне застосування військової сили [49, p. 7].

Таким чином, сучасне розуміння стримування, окреслене через п’ять ключових вимірів: характер запобіжної дії, інструментарій, механізм впливу, часовий горизонт і об’єкт стримування, – засвідчує, що стримування більше не може розглядатися виключно як військово-технічна або кризово-орієнтована практика. Стратегія стримування дедалі виразніше набуває рис комплексної

політико-стратегічної діяльності, спрямованої на формування стійких моделей поведінки в умовах тривалої стратегічної конкуренції. Інформаційна складова стає не допоміжним, а системоутворюючим елементом стримування, оскільки саме через інформаційний простір здійснюється вплив на сприйняття намірів, витрат, ризиків і допустимих меж дій. В умовах цифровізації, зростання швидкості інформаційних потоків і розширення спектра дій нижче порогу війни стримування має враховувати та передбачати нові форми впливу, які не підпадають під класичні моделі військового протиборства, але безпосередньо впливають на стабільність міжнародної системи. Стримування постає як одна з ключових стратегій міжнародного регулювання та запобігання інформаційним війнам, спрямована не стільки на реактивне покарання, скільки на попереджувальне формування таких умов, за яких інформаційна агресія втрачає свою стратегічну доцільність.

Поняття міждоменного стримування (cross-domain deterrence) означає використання спроможностей в одному домені з метою нейтралізації загроз або комбінації загроз в іншому домені, передусім у ситуаціях, коли держава має відносну вразливість або обмежені можливості в певній сфері. Концепція міждоменного стримування сформувалася в середині 2000-х років у відповідь на зростання ролі космічного та кіберпростору у військових операціях, які поступово долучилися до традиційних операційних доменів суходолу, моря та повітря. У своєму початковому вигляді вона була зосереджена насамперед на взаємодії саме бойових доменів у контексті стримування, що робить її концептуально вужчою, ніж пізніша ідея інтегрованого стримування. Міждоменного стримування багато в чому збігається з інтегрованим підходом, а саме яким чином перетин доменів або комбінування інструментів державної влади може забезпечувати додатковий стримувальний ефект. Важливою відмінністю міждоменного стримування є те, що воно не передбачає обов’язкової глибокої інтеграції спроможностей різних сфер, а радше спирається на дискретне застосування дій в одному домені для досягнення ефекту в іншому. Тобто міждоменне стримування не є повноцінною стратегією «синхронізованого

впливу», але вже містить у собі перехресні ефекти, які згодом були розвинені в концепції інтегрованого стримування [15, p. 3].

Практика міждоменного стримування тісно пов’язана з трансформацією характеру стратегічної конкуренції. Якщо США традиційно покладалися на переваги у здатності інтегрувати повітряні, морські та космічні операції, то такі держави, як Китай, росія та Іран, дедалі активніше використовують нові технології для досягнення стратегічних переваг у тих сферах, де їхні конвенційні військові можливості є обмеженими. У відповідь на це зростає увага до немілітарних або нетрадиційних інструментів впливу, які можуть компенсувати дисбаланс сил і забезпечувати стримувальний ефект без прямого застосування військової сили. Міждоменне стримування пов’язане з підвищеними ризиками хибної інтерпретації сигналів та неконтрольованої ескалації. Перенесення дій з одного домену в інший може сприйматися опонентом як ознака розширення конфлікту, що здатне провокувати превентивні або ескалаційні кроки у відповідь. Особливо це стосується таких доменів, як кіберпростір і космос, де дії можуть бути інтерпретовані як підготовка до масштабнішого нападу. Окремі дослідження вказують на потенційний стабілізуючий ефект складної «мозаїки» міждоменних зв’язків, оскільки вона знижує вирішальність будь-якого одиничного кроку та зменшує ризик різкої ескалації в межах одного домену [45, p. 6-8].

У концепції міждоменного стримування інформаційний простір набуває значення як домен, через який можуть створюватися стримувальні ефекти, непропорційні витратам і без прямого застосування військової сили. Інформаційні операції дозволяють переносити конкуренцію з доменів, де держава має відносні обмеження, у сферу, де асиметричні інструменти впливу можуть забезпечувати відчутний стратегічний ефект. Інформаційний домен виступає як об’єктом захисту, та й активним середовищем реалізації міждоменних стримувальних стратегій. Однак, застосування інформаційних засобів у рамках міждоменного стримування ускладнює інтерпретацію намірів і сигналів. Інформаційні впливи можуть одночасно сприйматися як елемент

політичного тиску, підготовка до ширших дій або як автономна форма стратегічного протиборства, що підвищує ризики хибних оцінок і небажаної ескалації. Багатозначність інформаційного домену демонструє як його стримувальний потенціал, так і обмеження міждоменного підходу, вказуючи на потребу більш узгодженого та комплексного бачення стримування в умовах сучасної стратегічної конкуренції.

Адаптоване стримування (tailored deterrence) ґрунтується на посиленні контекстуалізації стримування та відмові від універсальних, стандартизованих стратегій на користь адаптації стримувальних заходів до конкретних акторів, ситуацій і типів загроз [37, p. 2]. Стримування розглядається як процес, що має бути налаштований під специфічні умови ухвалення рішень потенційного агресора, включно з індивідуальними особливостями лідерства, інституційною структурою влади та політичною динамікою. Ключовим елементом адаптованого стримування є орієнтація на конкретного адресата стримувального сигналу, державу, домінантного лідера, вузьке коло політичних або військових еліт чи окремі центри ухвалення рішень, які безпосередньо формують курс дій. Відповідно, стримувальні загрози, стимули та комбінація інструментів державної потуги мають бути сконструйовані таким чином, щоб максимізувати вплив саме на ці групи або осіб. Адаптоване стримування створює своєрідний міст до концепції інтегрованого стримування. Якщо інтегроване стримування визначає широкий спектр доступних інструментів і способів їх поєднання, то адаптоване стримування задає принципи їх вибору та конфігурації залежно від конкретного суперника і типу виклику. У Стратегії національної оборони США 2022 року інтегроване стримування прямо пов’язується з необхідністю адаптації до «конкретних конкурентів і викликів» [62].

Аналіз стратегічної культури потенційного агресора в межах адаптованого стримування включає історичний досвід, національну ідентичність, роль військових інституцій, домінантні уявлення про застосування сили та сприйняття ризику. Оскільки стримування є інтерактивним процесом, що значною мірою залежить від комунікації стримувальних сигналів, ефективність

таких сигналів визначається тим, як вони інтерпретуються в межах конкретної стратегічної культури. Проте, існують й обмеження цього підходу. Критики застерігають від надмірної впевненості у здатності точно ідентифікувати ключові центри формування рішень і передбачити реакцію опонента. Обмеженість розвідувальної інформації, когнітивні упередження та динамічність політичних процесів можуть призводити до хибних припущень і переоцінки ефективності індивідуально налаштованих стримувальних стратегій. Попри це, навіть у теоретичному вимірі стримування не може бути ефективним без урахування специфіки конкретних ситуацій і адресатів, що й становить базову основу адаптованого стримування [38, p. 55].

Концепція інтегрованого стримування була викладена у Стратегії національної оборони США 2022 р. [62] й передбачала узгоджене й безперервне застосування можливостей у межах різних доменів ведення бойових дій, географічних театрів, усього спектра конфлікту, а також інших інструментів національної могутності США у тісній координації з союзниками й партнерами. Додатковою опорою цієї концепції залишався безпечний, надійний та ефективний ядерний стримувальний потенціал. За визначенням колишнього міністра оборони Л. Остіна, інтегроване стримування полягає у «використанні наявних спроможностей, створенні нових та їх розгортанні у взаємопов'язаних і мережевих формах, адаптованих до регіонального безпекового середовища та реалізованих у зростаючому партнерстві з союзниками» [49, p. 13].

Сутність інтегрованого стримування відображає уявлення про те, що в умовах посилення ревізіоністських намірів потенційних супротивників США можуть найефективніше зміцнювати стримування різних форм звичайної військової агресії та високоінтенсивної діяльності в сірій зоні шляхом кращого узгодження власних інструментів впливу та поглиблення інтеграції з партнерами. Концептуальною передумовою інтегрованого стримування є визнання того, що регіональні військові тенденції протягом понад двох десятиліть розвивалися не на користь США, унаслідок чого оборонна політика потребувала переорієнтації на відновлення переконливості та дієвості

американських зобов'язань у сфері воєнної безпеки. Посилення інтеграції покликане створити синергетичні ефекти, здатні підвищити загальний стримувальний ефект [62].

Досягнення цілей інтегрованого стримування потребує двох взаємопов'язаних форм інтеграції: внутрішньої та зовнішньої. Внутрішня інтеграція стосується узгодження дій між різними елементами уряду США та Об'єднаних збройних сил, тоді як зовнішня передбачає поглиблення співпраці та взаємосумісності з союзниками й партнерами. Причинно-наслідковий зв'язок між підвищенням рівня інтеграції та посиленням стримувального ефекту становить центральну ідею документу. Зміни у військових спроможностях і амбіціях потенційних супротивників суттєво підвищили ризики для союзників і партнерів США, а також для ширших американських інтересів, унаслідок чого низка базових припущень оборонного планування пост «холодної війни» втратила актуальність. У відповідь на це ключовим завданням визначено підвищення бойової спроможності Збройних сил США таким чином, щоб вони були здатні виконувати основні воєнні місії навіть за відсутності попереднього рівня домінування. Створення більш боєздатних збройних сил розглядається як головна мета концепції інтегрованого стримування. Основний аргумент Стратегії полягає в тому, що найбільш реалістичний шлях до посилення бойової спроможності полягає у максимізації наявної бойової потужності шляхом тісного поєднання всіх її складових. Інтегроване стримування постає як теорія реалізації, оскільки ідеться про способи, за допомогою яких скоординоване державне управління дозволяє максимізувати ефект від уже наявних і запланованих можливостей. Використання синергії, як усередині американських структур, так і разом із союзниками, є найбільш перспективним шляхом зміцнення стримування. Хоча цей підхід не був повністю реалізований до початку повномасштабного вторгнення росії в Україну, подальша стратегія США щодо стримування ескалації та покарання агресії розглядалась як один із найбільш наочних емпіричних прикладів логіки інтегрованого стримування [62].

У відповідь на агресію росії проти України США поєднали зусилля з

багатьох доменів і різних сегментів державної влади з метою досягнення стримувального та карального ефекту. До цього комплексу заходів увійшли військова допомога й підготовка, обмін розвідувальною інформацією, дипломатичні дії, економічний примус і підтримка, а також багатосторонні зусилля з координації дій союзників і партнерів. Демонструючи модель справді всеосяжної національної відповіді на агресію, США створили прецедент, який може бути застосований превентивно у майбутніх конфліктах для обіцянки здатності позбавляти агресора досягнення його цілей, накладати суттєві витрати та підвищувати стійкість держави-жертви агресії. Досвід України засвідчує, що інтегроване стримування може бути концептуалізоване щонайменше на двох рівнях. Перший, вужчий рівень має тактико-операційний характер і зосереджується на створенні синергії між різними ефектами. Другий, ширший рівень має геостратегічний вимір і передбачає застосування загальнодержавних підходів («whole-of-government») до стримування та конфлікту загалом. У межах вузького підходу акцент робиться на ініціативах із посилення внутрішньої інтеграції, зокрема таких як спільне у всіх доменах командування та контроль (Joint All-Domain Command and Control (JADC2)), а також на операційній взаємосумісності з союзниками й партнерами. Ширше розуміння інтегрованого стримування виходить за межі суто військових питань і охоплює поєднання військових, економічних, політичних та інформаційних інструментів, які можуть використовуватися для погроз, стримування і, за необхідності, покарання агресорів у більш комплексний і взаємопосилювальний спосіб. Заходи з нарощування спроможностей розглядаються як один із ключових елементів інтегрованого стримування, оскільки вони безпосередньо зміцнюють здатність США до ефективного ведення бойових дій у межах ширшого багатовимірного стримувального підходу. Водночас центральний меседж Стратегії 2022 р. полягав в тому, що окремі покращення спроможностей, хоч і є необхідними, самі по собі не є достатніми для досягнення ключових стримувальних цілей. Вони мають супроводжуватися цілеспрямованими зусиллями з інтеграції американських можливостей і видів діяльності таким чином, щоб створювати

нові форми синергії та підвищувати бойову достовірність оперативних планів США [49, p. 15].

У площині інформаційного стримування концепція інтегрованого стримування набуває форми цілеспрямованого стратегічного сигналу про неминучість відповіді на агресивні дії, незалежно від домену, в якому вони здійснюються. Центральним елементом такого сигналу є публічне й інституційно закріплене повідомлення, зафіксоване у стратегічних документах США, про те, що ревізіоністська поведінка не залишатиметься без наслідків. Це повідомлення не зводиться до конкретних погроз чи сценаріїв застосування сили, а формує стійке очікування, що будь-яка агресія, включно з діями в інформаційному просторі або іншими формами підпорогового примусу, буде включена до ширшого розрахунку покарання. Інформаційна складова інтегрованого стримування працює як самостійний інструмент формування уявлень потенційного агресора про структуру ризиків і як допоміжний канал комунікації. Донесення думки про стримування через покарання принаймні буде застосоване у разі провалу стримування через відмову, створює для ревізіоністських акторів ситуацію принципової невизначеності щодо меж допустимого. Вони не можуть з упевненістю розраховувати на безкарність дій у «сірих» або інформаційних доменах, оскільки відповідь може бути відкладеною, асиметричною та реалізованою через поєднання військових, економічних, політичних і інформаційних засобів. Таким чином, інформаційне стримування в межах інтегрованого підходу не обмежується попередженням або контрнаративами, а виконує системоутворюючу функцію: пов’язує окремі дії агресора в єдину рамку стратегічної відповідальності, що є ключовим чинником стримування в умовах сучасної стратегічної конкуренції, де межі між війною і миром, військовими та немілітарними діями, інформаційним впливом і силовим примусом є принципово розмитими.

Ключове, хоча й не завжди прямо артикульоване, припущення концепції інтегрованого стримування полягає в тому, що саме глибша інтеграція інструментів державної влади США, у поєднанні з діями союзників і партнерів,

є найбільш перспективним засобом посилення стримувального ефекту в сучасних умовах. Проте, трансформація характеру війни у бік мережево-технологічних форм ведення операцій об'єктивно вимагає більш комплексної інтеграції. За відсутності такої інтеграції США не зможуть суттєво підвищити бойову переконливість власних сил. Стратегія національної безпеки визначає інтегроване стримування як «безшовне поєднання можливостей з метою переконати потенційних супротивників, що вартість їхніх ворожих дій перевищує очікувані вигоди». При цьому наголошується, що інтегроване стримування передбачає ефективнішу координацію, мережування та інновації, аби будь-який конкурент, який прагне здобути перевагу в одному домені, усвідомлював можливість відповіді в багатьох інших. Такий підхід не скасовує традиційної ролі переконливих конвенційних і стратегічних спроможностей, а підсилює їх, дозволяючи точніше формувати сприйняття ризиків і витрат потенційним агресором у будь-який момент і в будь-якому домені. Відповідно, «ядром інтегрованого стримування» прямо визначено розвиток, поєднання та координацію наявних переваг для досягнення максимального ефекту [62].

Концепція інтегрованого стримування відрізняється від попередніх уявлень про міждоменне стримування тим, що в сучасному технологічному та геополітичному середовищі ефективність стримування залежить від системної синергії різних можливостей, тобто комплексне поєднання військових, політичних, економічних, інформаційних та інших інструментів. У суто військово-операційному вимірі, в умовах мережевої війни та зростаючої ролі інформації й автоматизації, різні форми інтеграції стають не додатковою перевагою, а передумовою ефективності. Саме посилення синергій розглядається як спосіб досягти більш негайного і водночас стійкішого стримувального ефекту.

Попри концептуальну привабливість інтегрованого стримування, дослідники звертають увагу на низку структурних і практичних обмежень, які ускладнюють його реалізацію в умовах сучасної стратегічної конкуренції. Інтегроване стримування істотно підвищує складність комунікації

стримувальних сигналів. Чим більш багатовимірною є стратегія, з поєднанням військових, економічних, дипломатичних та інформаційних інструментів, тим важче забезпечити однозначне сприйняття намірів і «червоних ліній» потенційним противником. В інформаційному середовищі це підвищує ризик шуму, суперечливих сигналів і помилкових інтерпретацій, що може не посилювати, а послаблювати стримувальний ефект. Надмірний оптимізм щодо керованості сприйняття противника, оскільки концепція інтегрованого стримування значною мірою спирається на припущення, що держава-ініціатор здатна досить точно зрозуміти, як її дії інтерпретуються конкретним лідером або елітною групою. В умовах інформаційної асиметрії, культурних відмінностей і навмисної дезінформації це припущення є вразливим. Інформаційний простір лише посилює цю проблему, оскільки наративи можуть бути переосмислені, спотворені або використані самим противником для внутрішньої мобілізації. Ризик хибної впевненості, коли формалізовані інтегровані підходи можуть створювати ілюзію контролю над ескалацією та ефективністю сигналів, проявляється у вірі, що правильно скоординовані повідомлення, санкції та демонстрації спроможностей автоматично транслюються у бажаний ефект. Проте, стримування залишається політичним процесом, а не технічною процедурою, і не піддається повній оптимізації.

Інтегроване стримування стикається з проблемою внутрішньої координації, сутність якого полягає в тому, що поєднання численних інструментів і акторів (від військових структур до дипломатії та інформаційних інституцій) ускладнює узгодження повідомлень і дій. Для інформаційного стримування це означає ризик фрагментованого сигналювання, коли різні елементи державної політики транслюють несумісні або взаємно нівелюючі меседжі. Обмеження ефективності інтегрованого стримування також пов’язане з ескалаційною невизначеністю. Інтеграція дій у різних доменах може непередбачувано підвищувати ставки, особливо коли інформаційні операції перетинаються з військовими або кібердіями. У такій ситуації противник може інтерпретувати інтегровані сигнали як підготовку до ширшого конфлікту, навіть якщо намір полягає у стримуванні,

що підриває стабілізуючу функцію стратегії.

Асиметрія застосування інтегрованого стримування проявляється в тому, що авторитарні режими з централізованим контролем над інформаційним простором можуть легше координувати інтегровані дії, ніж відкриті суспільства, де інформаційне середовище є плюралістичним і менш керованим, що створює структурний виклик для інформаційного стримування з боку демократичних держав. До того ж, з'являється ризик концептуального розмивання. Якщо інтегроване стримування охоплює надто широкий спектр дій - від військового планування до інформаційної політики загалом, - воно може перетворитися на узагальнену метафору державної активності, в разі чого стримування перестає бути чітко артикульованим механізмом запобігання агресії, зокрема в інформаційному просторі. Отже, у сукупності ці зауваження дозволяють зробити висновок, що інтегроване стримування створює важливі можливості для розвитку інформаційного стримування, але водночас висуває підвищені вимоги до якості комунікації, розуміння сприйняття противника та контролю ескалації. В інформаційному вимірі ці обмеження проявляються найбільш гостро, що робить його водночас ключовим елементом і найбільш уразливою складовою інтегрованих стримувальних стратегій.

Таким чином, Стратегічна конкуренція в інформаційному вимірі постає як безперервний процес взаємодії, що розгортається на континуумі між миром і війною та характеризується розмитістю порогів, амбівалентністю дій і системним використанням інформаційних операцій як інструменту непрямого впливу.

Стратегічна конкуренція в інформаційному вимірі розгортається в умовах плинних і навмисно маніпульованих порогів, де «червоні лінії» рідко мають чітко визначений характер, а простір «сірої зони» стає основним середовищем взаємодії між державами. У межах такої конкуренції інформаційні операції системно реалізуються за трьома взаємопов'язаними напрямами: підрив політичної єдності держави-конкурента, вплив на процеси ухвалення рішень її політичними та адміністративними елітами та зниження довіри до ключових

інститутів шляхом дискредитації їхньої легітимності, компетентності та неупередженості.

Невизначеність інформаційного середовища постає цілеспрямовано відтворюваною умовою стратегічної конкуренції, що суттєво трансформує класичну логіку дилеми безпеки. Відтворення дилеми безпеки відбувається через одночасне загострення дилем інтерпретації та реагування, за яких будь-яка дія або бездіяльність набуває потенційно ескалаційного значення. Інформаційні операції закріплюють структурну недовіру як стабільний елемент стратегічної взаємодії, створюючи самопідтримувальний цикл підозр і запобіжних кроків навіть за відсутності відкритого конфлікту чи матеріального нарощування загроз. Отже, інформаційне середовище перетворюється на ключовий простір, у якому дилема безпеки не лише проявляється, а й постійно відтворюється як наслідок керованої невизначеності.

Інтегроване стримування у сучасних умовах охоплює нові форми впливу, зокрема інформаційне стримування, яке розглядається як перспективний інструмент міжнародного регулювання та запобігання інформаційним війнам у межах багатовимірної стратегічної конкуренції. Розширення спектра дій нижче порогу війни зумовило еволюцію стримування у бік міждоменних та інтегрованих форматів, у межах яких стримувальний ефект може досягатися через використання спроможностей в одному домені для впливу на поведінку опонента в іншому. Інформаційний простір виступає як системоутворюючий елемент інтегрованого стримування, через який здійснюється сигналювання, інтерпретація «червоних ліній» і вплив на процеси ухвалення рішень.

Концепція інтегрованого стримування стикається з низкою суттєвих обмежень, які особливо загострюються в інформаційному середовищі. Багатовимірність і складність інтегрованих стратегій ускладнюють комунікацію стримувальних сигналів, підвищують ризик суперечливого сигналювання та хибних інтерпретацій намірів. Надмірна впевненість у можливості керувати сприйняттям противника, проблеми внутрішньої координації, асиметрія інформаційних середовищ і ризик ескалаційної невизначеності обмежують

стабілізуючий потенціал інтегрованого стримування. Проте, у підсумку, інтегроване стримування створює важливі можливості для розвитку інформаційного стримування, але водночас робить інформаційний домен найбільш уразливою та критичною складовою сучасних стримувальних стратегій.

ВИСНОВКИ

Дилема безпеки є структурною характеристикою міжнародного порядку, за якої зусилля держави щодо посилення власної безпеки неминуче сприймаються іншими як потенційна загроза. Онтологічно дилема безпеки має дворівневу структуру, що складається з дилеми інтерпретації та дилеми реагування. Дилема інтерпретації полягає в неможливості достовірно встановити мотиви, наміри й стратегічні цілі іншої сторони, а також однозначно відрізнити оборонні дії від наступальних. Дилема реагування полягає у виборі між стримуванням і заспокоєнням, причому будь-який вибір за умов хибної інтерпретації може спричинити ескалацію або стратегічну вразливість.

Динаміка дилеми безпеки визначається поєднанням матеріального та психологічного вимірів. Матеріальний вимір пов’язаний із двозначною символікою озброєнь, коли їх стратегічне значення залежить від контексту, доктрини та взаємного сприйняття. Психологічний вимір ґрунтується на проблемі «чужих розумів», тобто принциповій неможливості достовірно пізнати наміри інших, що породжує страх, підозру та схильність до найгірших сценаріїв.

Дилема безпеки не тотожна парадоксу безпеки. Парадокс безпеки є наслідком її динаміки і проявляється у спіралі зростання незахищеності, коли дії, спрямовані на підвищення власної безпеки, знижують рівень безпеки для всіх учасників. Центральним механізмом цієї спіралі є страх, підсилений когнітивними обмеженнями та анархічною логікою самодопомоги.

Фундаментальною складовою дилеми безпеки є проблема стратегічного сигналізування. Держави не здатні переконливо сигналізувати мирні наміри, оскільки сигнали інтерпретуються не за змістом, а через призму підозр, історичного досвіду та стратегічних припущень адресата. Неможливість «сигналізувати свій тип» означає, що певний рівень невизначеності та страху є структурно невідворотним, навіть за відсутності наступальних намірів.

Невизначеність у міжнародній безпеці є структурною умовою, що робить неможливим повне пізнання намірів інших акторів і створює постійну

вразливість, з якої випливає безпекова дилема. Три провідні підходи пропонують різні способи концептуалізації цієї невизначеності та різні рамки дій у відповідь на неї. Наступальний/традиційний реалістичний підхід розглядає невизначеність як нездоланну та екзистенційно небезпечну, вважаючи раціональним максимізацію сили, недовіру та готовність до превентивних дій. Дилема безпеки є неминучою й самостійно підсилювальною. Поміркований підхід (англійська школа) визнає структурні обмеження невизначеності, але стверджує, що вони можуть бути частково пом'якшені через норми, правила, інституції та розвиток спільних очікувань. Невизначеність не усувається, але стає керованою, а безпекова дилема – менш гострою. Трансцендентний підхід трактує невизначеність як змінну соціально-політичну умову, яку можна істотно перетворити через довгострокове інституційне зближення, зміну колективних уявлень та формування безпекових спільнот. Системні обмеження не є фатальними, а альтернативні порядки можливі.

Всі три підходи окреслюють спектр можливостей – від фаталістичної логіки виживання до реформістських та трансформаційних стратегій співіснування. Вони демонструють, що характер невизначеності та її наслідки залежать від прийнятої теоретичної перспективи та практики взаємодії. Від того, яку з цих рамок обирають політики та суспільства, залежить, чи стане невизначеність джерелом нездоланної загрози, керованим ризиком або відправною точкою для глибоких політичних трансформацій.

Дилема безпеки в сучасній міжнародній системі має тенденцію до «зараження» та поширення за межі окремих міждержавних відносин, формуючи багаторівневу й взаємопов'язану вразливість. Її динаміка проявляється одночасно на локальному, регіональному та глобальному рівнях, створюючи умови для накопичення страху, підозри та песимістичних інтерпретацій намірів інших акторів. За відсутності належного колективного реагування дилеми безпеки здатні трансформуватися у структурні виклики, що підривають передбачуваність міжнародного порядку та посилюють міжнародну тривожність. Війна Росії проти України засвідчила крихкість усталених

припущень щодо стабільності та неможливість інерційного відтворення безпеки.

Чотири ключові фактори поглиблюють і відтворюють дилему безпеки у сучасних умовах. Суперництво великих держав посилює стратегічну недовіру, стимулює інтерпретацію дій опонентів через призму найгірших сценаріїв та підвищує ризики небажаної ескалації. Розповсюдження ядерної зброї підриває режими нерозповсюдження, відновлює уявлення про ядерні засоби як інструмент примусу та створює передумови для ланцюгових реакцій і стратегічної нестабільності. Регіональна небезпека, пов'язана з тривалими конфліктами та слабкими механізмами довіри, формує локальні конфігурації дилеми безпеки, здатні масштабуватися за межі регіонів. Тероризм розширює дію дилеми безпеки, розмиваючи межі між зовнішніми й внутрішніми загрозами та індивідуалізуючи страх у повсякденних соціальних практиках.

За умов, коли невизначеність не пом'якшується інституційними та політичними механізмами, дилема безпеки набуває самопідсилювального характеру. Страх і недовіра звужують простір для співпраці, ускладнюють сигналізування мирних намірів і підвищують імовірність стратегічних прорахунків. Комбінація системних факторів може спричиняти повернення до фаталістичних уявлень про міжнародну політику, відтворення конфліктогенних стратегій і загострення глобальної нестабільності. Відсутність ефективних відповідей перетворюватиме невизначеність на стійке джерело безпекових криз і масштабних загроз.

Інформаційна війна постає як структурно складний і концептуально мінливий феномен міжнародної безпеки, зумовлений багатовимірністю інформації як ресурсу влади та розширенням інструментів впливу на сприйняття, поведінку й стратегічне середовище. У науковому дискурсі сформувалося кілька аналітичних підходів до її інтерпретації, які по-різному окреслюють природу інформаційних протиборств, їхні функції та механізми досягнення політичних результатів. У межах психологічно-пропагандистського напряму досліджень поняття інформаційної війни еволюціонувало від розуміння інформації як інструмента впливу на мораль, переконання та поведінку мас через пропаганду

й психологічні операції до усвідомлення системного керування когнітивним середовищем супротивника як складника досягнення стратегічних цілей без прямого насильства. У техніко-інженерному напрямі інформаційна війна була переосмислена як боротьба за контроль над інформаційною інфраструктурою, сигналами та системами управління і зв'язку, де інформація постає матеріальним ресурсом, уразливість якого здатна визначати результат воєнного протиборства. В інституційно-доктринальному напрямі поняття інформаційної війни трансформувалося у формалізований елемент військового планування, що поєднує оборонні й наступальні дії щодо захисту та ураження інформаційних систем і згодом було включене до ширшої рамки інформаційних операцій. В аналітико-стратегічному напрямі інформаційна війна набула трактування як багатовимірної, поліструктурної форми стратегічної конкуренції за контроль над інформаційними потоками, процесами ухвалення рішень і умовами перетворення даних на знання, що виходить за межі суто технічних або психологічних підходів.

Еволюція інформаційних війн відображає поступову трансформацію інформаційних і психологічних впливів від допоміжних інструментів воєнного протиборства до самостійного та структурно інтегрованого виміру стратегічної конкуренції у міжнародній безпеці. Доцифровий етап інформаційних війн характеризувався формуванням системних пропагандистських і психологічних практик, які в умовах масової мобілізації та розвитку політичної комунікації перетворили керування свідомістю на повноцінний вимір воєнного протиборства. Велика війна (перша світова війна) стала історичною лабораторією модерних інформаційно-психологічних впливів, у межах якої пропаганда набула індустріального масштабу, інституційного оформлення та стратегічного значення для підтримання тилу, легітимації війни й деморалізації противника. У період «холодної війни» інформаційні війни були формалізовані як довгострокові, системно спроєктовані кампанії, що функціонували поряд із ядерним стримуванням і слугували інструментом ідеологічної конкуренції, дестабілізації та впливу на політичні орієнтації держав і суспільств.

Кібернетизація концепту інформаційних конфліктів наприкінці XX століття зумовила усвідомлення інформації не лише як носія смислів, але й як технічної інфраструктури, втручання в яку створює нові форми стратегічної вразливості та дестабілізації. Перехід до мережево-центричних конфліктів означав інтеграцію інформаційних, кібернетичних і військових дій у єдиний цикл планування й застосування сили, в якому контроль над потоками даних, швидкістю ухвалення рішень і наративним середовищем став визначальним чинником оперативної та стратегічної переваги.

Розширення практик інформаційної війни у цифрову добу зумовило появу низки моделей, спрямованих на пояснення різних механізмів інформаційного впливу в сучасних війнах, які виникали як відповідь на практичні зміни у способах ведення протиборства й відображали перехід від фрагментарного застосування інформаційних засобів до комплексних способів організації стратегічного впливу на технічні, управлінські та когнітивні основи безпеки. Мережево-центрична модель розглядає інформаційний вплив як системоутворюючий чинник, у межах якого ефективність воєнних і політичних дій визначається здатністю інтегрувати інформаційні потоки, скорочувати часові лаги ухвалення рішень і забезпечувати координацію в єдиному інформаційному просторі. Концепція кібервійни фокусується на ураженні цифрової інфраструктури як самостійного домену протиборства, де вплив на інформаційні системи створює стратегічну вразливість, розмиває межі між миром і війною та підриває традиційні механізми стримування. Інформаційно-психологічна модель зосереджується на цілеспрямованому впливі на установки, емоції та поведінку суспільств, розглядаючи інформаційне середовище як простір формування політичної лояльності, мобілізації або деморалізації. Когнітивний підхід розширює логіку психологічного впливу, зміщуючи об’єкт протиборства до самих механізмів сприйняття й інтерпретації реальності, що забезпечує довготривалу трансформацію уявлень, норм і моделей політичного мислення.

Гібридні інформаційні операції інтегрують мережево-центричні, кібернетичні, психологічні та когнітивні елементи в єдині адаптивні стратегії, у

межах яких синхронізований вплив на різні рівні соціальної та політичної організації дозволяє досягати кумулятивних стратегічних ефектів без прямої силової ескалації.

Стратегічна конкуренція в інформаційному вимірі постає як безперервний процес взаємодії, що розгортається на континуумі між миром і війною та характеризується розмитістю порогів, амбівалентністю дій і системним використанням інформаційних операцій як інструменту непрямого впливу.

Стратегічна конкуренція в інформаційному вимірі розгортається в умовах плинних і навмисно маніпульованих порогів, де «червоні лінії» рідко мають чітко визначений характер, а простір «сірої зони» стає основним середовищем взаємодії між державами. У сірій зоні конфлікту інформаційні операції набувають особливої привабливості як інструмент дії нижче порогу війни та, водночас, часто нижче порогу атрибуції і сприйняття, що дозволяє поступово змінювати стратегічні умови без провокування відкритої ескалації. У межах такої конкуренції інформаційні операції системно реалізуються за трьома взаємопов’язаними напрямами: підрив політичної єдності держави-конкурента, вплив на процеси ухвалення рішень її політичними та адміністративними елітами та зниження довіри до ключових інститутів шляхом дискредитації їхньої легітимності, компетентності та неупередженості. Сукупний ефект цих впливів полягає не у швидкому досягненні тактичних результатів, а у довготривалому відтворенні невизначеності, внутрішньої розбалансованості та зниженні стратегічної стійкості, що робить інформаційні операції одним із центральних механізмів сучасної стратегічної конкуренції та важливим чинником формування дилеми безпеки.

Невизначеність інформаційного середовища постає цілеспрямовано відтворюваною умовою стратегічної конкуренції, що суттєво трансформує класичну логіку дилеми безпеки. Через маніпуляцію сигналами, наративами та інтерпретаційними рамками інформаційні операції системно ускладнюють атрибуцію дій і тлумачення намірів, підриваючи можливість відмежування оборонної поведінки від прихованої загрози. Невизначеність не зменшується з

накопиченням інформації, а поглиблюється через конкуренцію пояснень і навмисне розмивання причинно-наслідкових зв'язків. Відтворення дилеми безпеки відбувається через одночасне загострення дилем інтерпретації та реагування, за яких будь-яка дія або бездіяльність набуває потенційно ескалаційного значення. Інформаційні операції закріплюють структурну недовіру як стабільний елемент стратегічної взаємодії, створюючи самопідтримувальний цикл підозр і запобіжних кроків навіть за відсутності відкритого конфлікту чи матеріального нарощування загроз. Отже, інформаційне середовище перетворюється на ключовий простір, у якому дилема безпеки не лише проявляється, а й постійно відтворюється як наслідок керованої невизначеності.

Інтегроване стримування у сучасних умовах охоплює нові форми впливу, зокрема інформаційне стримування, яке розглядається як перспективний інструмент міжнародного регулювання та запобігання інформаційним війнам у межах багатовимірної стратегічної конкуренції. Інтегроване стримування постає як відповідь на трансформацію стратегічної конкуренції, в умовах якої загрози дедалі частіше реалізуються нижче порогу відкритої війни та одночасно охоплюють кілька доменів, включно з інформаційним. Класична теорія стримування, сформована в ядерну епоху, виходила з уявлення про стримування як політичний процес впливу на рішення потенційного агресора через загрозу неприйнятних витрат або позбавлення можливості досягти бажаних цілей, проте вона ніколи не була суто технічною моделлю, а ґрунтувалася на сприйняттях, очікуваннях і суб'єктивних інтерпретаціях, що зумовлює її обмежену передбачуваність у складному інформаційному середовищі.

Розширення спектра дій нижче порогу війни зумовило еволюцію стримування у бік міждоменних та інтегрованих форматів, у межах яких стримувальний ефект може досягатися через використання спроможностей в одному домені для впливу на поведінку опонента в іншому. Міждоменне стримування заклало основу для розуміння перехресних ефектів між військовими, кібернетичними та інформаційними сферами, але залишалося

концептуально обмеженим, оскільки не передбачало глибокої системної інтеграції інструментів влади. В інформаційному вимірі інтегроване стримування ґрунтується на формуванні стійких очікувань щодо неминучості відповіді на агресивні дії незалежно від домену їх здійснення й спрямоване на вплив на розрахунки потенційного агресора шляхом підвищення вартості, зниження доцільності та посилення невизначеності результатів інформаційної агресії. Інформаційний простір виступає як системоутворюючий елемент інтегрованого стримування, через який здійснюється сигналювання, інтерпретація «червоних ліній» і вплив на процеси ухвалення рішень.

Концепція інтегрованого стримування стикається з низкою суттєвих обмежень, які особливо загострюються в інформаційному середовищі. Багатовимірність і складність інтегрованих стратегій ускладнюють комунікацію стримувальних сигналів, підвищують ризик суперечливого сигналювання та хибних інтерпретацій намірів. Надмірна впевненість у можливості керувати сприйняттям противника, проблеми внутрішньої координації, асиметрія інформаційних середовищ і ризик ескалаційної невизначеності обмежують стабілізуючий потенціал інтегрованого стримування. У підсумку, інтегроване стримування створює важливі можливості для розвитку інформаційного стримування, але водночас робить інформаційний домен найбільш уразливою та критичною складовою сучасних стримувальних стратегій.

СПИСОК ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Allison, G. The Thucydides Trap. Are the U.S. and China Headed for War? // The Atlantic. September 24, 2015. URL: https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/Allison%2C%202015.09.24%20The%20Atlantic%20-%20Thucydides%20Trap.pdf (дата звернення 11.10.2025)
2. Allison, G. et al. The Great Tech Rivalry: China vs the US. Belfer Center for Science and International Affairs. 2021. URL: https://www.belfercenter.org/sites/default/files/pantheon_files/GreatTechRivalry_ChinavsUS_211207.pdf (дата звернення 11.10.2025)
3. Arnold K., Preston P., Kinnebrock S. The Handbook of European Communication History. John Wiley & Sons, Inc. 2019. P. 520. URL: https://onlinelibrary.wiley.com/doi/chapter-epub/10.1002/9781119161783.fmatter (дата звернення 12.11.2025).
4. Bachmann S. D., Lee D., Dowse A. COVID Information Warfare and the Future of Great Power Competition // The Fletcher Forum of World Affairs. Vol. 44. No. 2. 2020. P. 11-18. URL: https://www.jstor.org/stable/48599306 (дата звернення 19.11.2025).
5. Blannin P. Modelling Information Warfare // Journal of Information Warfare. Vol. 20. No. 3. .Summer 2021. P. 90-107. URL: https://www.jstor.org/stable/27125001 (дата звернення 19.11.2025).
6. Boettger L. The Morris Worm: How It Affected Computer Security and Lessons Learned by It. Global Information Assurance Certification Paper. December 20. 2000. URL: https://www.giac.org/paper/gsec/405/morris-worm-affected-computer-security-lessons-learned/100954 (дата звернення 14.11.2025).
7. Booth K., Wheeler N. J. The Security Dilemma: Fear, Cooperation and Trust in World Politics. London: Palgrave Macmillan. 2008. P. 364
8. Bouchard R. M. Information Operations in Iraq. U.S. Army War College. 1999. URL: https://apps.dtic.mil/sti/tr/pdf/ADA363160.pdf (дата звернення 14.11.2025).
9. Brands H. Paradoxes of the gray zone. Foreign Policy Research Institute. 2016. URL: https://www.fpri.org/article/2016/02/paradoxes-gray-zone/ (дата звернення: 25.09.2025).
10. Berman I. I. The Middle East As Informational Battlefield // The Jerusalem Strategy Tribune. April 11, 2025. URL: https://www.afpc.org/publications/articles/the-middle-east-as-informational-battlefield (дата звернення: 05.11.2025).
11. Bull H. The Anarchical Society: A Study of Order in World Politics. Published by Palgrave Macmillan. Third Edition. 2002. P. 365
12. Bunker R. J. Advanced Battlespace and Cybermaneuver Concepts: Implications for Force XXIImplications for Force XXI // The US Army War College Quarterly: Parameters 26. # 3 (1996). URL: https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1786&context=parameters (дата звернення 12.11.2025)

13. Chincharadze K. From Georgia to Ukraine: Seventeen Years of Russian Cyber Capabilities at War // The Modern War Institute. 07.30.25. URL: https://mwi.westpoint.edu/from-georgia-to-ukraine-seventeen-years-of-russian-cyber-capabilities-at-war/ (дата звернення 12.11.2025)
14. Connable B., Campbell J. H., Madden D. Stretching and Exploiting Thresholds for High-Order War: How Russia, China, and Iran Are Eroding American Influence Using Time-Tested Measures Short of War. RAND Corporation. 2016. URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1003/RAND_RR1003.pdf (дата звернення: 05.10.2025).
15. Cross-Domain Deterrence: Strategy in an Era of Complexity / Lindsay J. R., Gartzke E. ed. Oxford University Press. 2019. URL: https://www.researchgate.net/publication/334510592_Cross-Domain_Deterrence_Strategy_in_an_Era_of_ComplexityStrategy_in_an_Era_of_Complexity (дата звернення 22.11.2025).
16. Deutsch K.W. Political Community in the North Atlantic Area. Princeton, NJ: Princeton University Press. 1968. P. 227
17. Fredericks B. E. Information Warfare at the Crossroads // Joint Force Quarterly. National Defense University. Summer 1997. URL: https://apps.dtic.mil/sti/pdfs/ADA529170.pdf (дата звернення 12.11.2025)
18. Fultz B. N., Utuk A. G. The Competition Continuum. Intelligence support to operations in the information environment // Marine Corps Gazette. September 2020. URL: https://www.mca-marines.org/wp-content/uploads/The-Competition-Continuum-1.pdf (дата звернення 18.11.2025)
19. Garstka J. J. Network Centric Warfare: An Overview of Emerging Theory // Phalanx. Vol. 33. No. 4. December 2000. P. 28-33. URL: https://www.jstor.org/stable/43962778 (дата звернення 18.11.2025)
20. Glaser C.L. Rational Theory of International Politics. Princeton, NJ: Princeton University Press. 2010. URL: https://www.researchgate.net/publication/287634280_Rational_theory_of_international_politics_The_logic_of_competition_and_cooperation (дата звернення 11.10.2025)
21. Gosling L. Deterring at a Distance: The Strategic Logic of AUKUS. Lowy Institute. 2024. URL: https://www.lowyinstitute.org/publications/deterring-distance-strategic-logic-aukus (дата звернення: 13.10.2025).
22. Groh J. L. Network-Centric Warfare: Leveraging the Power of Information / Theory of War and Strategy. Chapter 21. 2008, P. 323-338. URL: https://www.jstor.org/stable/resrep12115.24 (дата звернення 23.11.2025)
23. Harris J. The Cuckoo`s Egg Tracking a Spy Through the Maze of **Computer** Espionage // The new York Times. November 26, 1989. URL: https://archive.nytimes.com/www.nytimes.com/books/99/01/03/specials/stoll-egg.html (дата звернення: 13.11.2025).
24. Haukkala H., Wetering C., Vuorelma J. Trust in International Relations. Rationalist, Constructivist, and Psychological Approaches. Routledge. Taylor & Francis Group. 2018. URL:

https://library.oapen.org/bitstream/handle/20.500.12657/102100/9781351807845.pdf?sequence=1&isAllowed=y (дата звернення 11.10.2025)
25. Herz J. H. Idealist Internationalism and the Security Dilemma // World Politics. Vol. 2. No. 2. Jan., 1950. P. 157-180. URL: https://www.jstor.org/stable/2009187 (дата звернення 11.10.2025)
26. Herz J. H. Political Realism Revisited: Response // International Studies Quarterly. Vol. 25. No. 2. Symposium in Honor of Hans J. Morgenthau. Jun., 1981. P. 201-203. URL: https://www.jstor.org/stable/2600352 (дата звернення 11.10.2025)
27. Holbrook D. J. Information-Age Warfare and Defence of The Cognitive Domain. Australian Strategic Policy Institute, 13 December 2018. URL: https://www.aspistrategist.org.au/information-age-warfare-and-defence-of-the-cognitive-domain/ (дата звернення 21.11.2025)
28. Hollis M., S. Smith. Explaining and Understanding International Relations. Oxford: Clarendon Press. 1990. URL: https://bayanbox.ir/view/6537647487787180404/Explaining-and-Understanding-IR-Martin-Hollis-and-Steve-Smith-libre.pdf (дата звернення 08.10.2025)
29. Huth P. K. Deterrence and International Conflict: Empirical Findings and Theoretical Debates // Annual Review of Political Science. Vol. 2. No. 1. 1999. URL:https://web.archive.org/web/20050511094300id_/http://www.eng.auburn.edu:80/~agarwra/comp8700/annurev.polisci.2.1.pdf (дата звернення 23.11.2025)
30. Ibrahim F., Rhode S., Daseking M. A Systematic Review Of Cognitive And Psychological Warfare // The Defence Horizon Journal. December 1, 2023. URL: https://tdhj.org/blog/post/cognitive-psychological-warfare/ (дата звернення 12.10.2025)
31. Information Warfare Operations in the Cyber Domain / The Use of Cyberspace in the Context of Hybrid Warfare: Means, Challenges and Trends. 2020. pp. 20-28. URL: https://www.jstor.org/stable/resrep25102.8 (дата звернення 19.11.2025)
32. Jaitner M., Mattsson P. A. Russian Information Warfare of 2014. NATO CCD COE Publications. Tallinn. 2015. URL: https://www.ccdcoe.org/uploads/2018/10/Art-03-Russian-Information-Warfare-of-2014.pdf (дата звернення 11.11.2025)
33. Jervis R. Perception and Misperception in International Politics: New Edition. Princeton University Press. 1976. P. 544. URL: https://www.jstor.org/stable/j.ctvc77bx3 (дата звернення 11.10.2025)
34. Jervis R. Cooperation Under the Security Dilemma // World Politics. Vol. 30, No. 2. 1978. pp. 167-214. URL: https://www.jstor.org/stable/2009958?origin=JSTOR-pdf (дата звернення 08.10.2025).
35. Jervis R. Security Regimes // International Organization, Vol. 36. No. 2. International Regimes. Spring, 1982. P. 357-378. URL: https://www.jstor.org/stable/2706526 (дата звернення 11.10.2025).
36. Joint Doctrine for Information Operations. 1998. URL: https://www.c4i.org/jp3_13.pdf (дата звернення 12.11.2025).
37. Johnson M., Kelly T. K. Tailored Deterrence: Strategic Context to Guide Joint Force 2020 // Joint Force Quarterly. Vol. 74. No. 3. 2014. URL: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-74/jfq-74_22-29_Johnson-

Kelly.pdf (дата звернення 22.11.2025).
38. Larkin S. P. The Limits of Tailored Deterrence // Joint Force Quarterly. Vol. 63. No. 4. 2011. P. 47-57.URL: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63.pdf (дата звернення 22.11.2025).
39. Lasswell H. D. The Theory of Political Propaganda. The American Political Science Review. Vol. 21. No. 3. Aug., 1927. P. 627-631. URL: https://www.jstor.org/stable/1945515 (дата звернення 12.11.2025).
40. Libicki M. C. What Is Information Warfare? Center for Advanced Concepts and Technology Institute for National Strategic Studies. National Defense University. 1995. URL: https://apps.dtic.mil/sti/tr/pdf/ADA367662.pdf (дата звернення 12.11.2025)
41. Libicki M. C. Conquest in Cyberspace: National Security and Information Warfare. Cambridge University Press. 2007. https://assets.cambridge.org/97805216/92144/frontmatter/9780521692144_frontmatter.pdf (дата звернення 12.11.2025)
42. Lidell Hart B.H. Deterrent or Defense: A Fresh Look at the West's Military Position. New York: Frederick A. Praeger, 1960. P. 208.
43. Lindsay J. R. Information Technology and Military Power. New York : Cornell University Press, 2020. URL: https://www.jstor.org/stable/10.7591/j.ctvq2w0mp (дата звернення 22.11.2025).
44. Linebarger P.M.A. Psychological Warfare // Naval War College Information Service for Officers. Vol. 3. No. 7. March, 1951. P. 19-47. URL: https://www.jstor.org/stable/44792590 (дата звернення 12.11.2025).
45. Mallory K. New Challenges in Cross-Domain Deterrence. RAND Corporation Expert Insights. 2018. URL: https://www.rand.org/pubs/perspectives/PE259.html (дата звернення 20.11.2025).
46. Masters J. Russia, Trump, and the 2016 U.S. Election // Council on Foreign Relations. February 26, 2018. URL: https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election (дата звернення 18.11.2025)
47. Maurer T. WikiLeaks 2010: A Glimpse of the Future? Belfer Center for Science and International Affairs. Harvard Kennedy School. Discussion Paper #2011-10. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/maurer-dp-2011-10-wikileaks-final.pdf (дата звернення 18.11.2025)
48. Mazarr M. J., Cheravitch J., Hornung J. W., Pezard S. What Deters and Why: Applying a Framework to Assess Deterrence of Gray Zone Aggression. RAND Corporation RR-3142-A. 2021. URL: https://www.rand.org/pubs/research_reports/RR3142.html (дата звернення 22.11.2025).
49. Mazarr M. J., Ke I. Integrated Deterrence as a Defense Planning Concept. RAND Corporation Expert Insights. Jun 4, 2024. URL: https://www.rand.org/pubs/perspectives/PEA2263-1.html (дата звернення 22.11.2025).
50. Mearsheimer, J. The Tragedy of Great Power Politics. New York: W. W. Norton & Co. 2001. P. 555.

51. Mearsheimer, J. Great Power Rivalries: the case for realism. Le Monde diplomatique. 2023. URL: https://mondediplo.com/2023/08/02great-powers
52. Morgan P. M. The Past and Future of Deterrence Theory / Lindsay J. R., Gartzke E. Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press. 2019. P. 50-65. URL: https://www.researchgate.net/publication/334510592_Cross-Domain_Deterrence_Strategy_in_an_Era_of_ComplexityStrategy_in_an_Era_of_Complexity (дата звернення 22.11.2025).
53. Ottis R. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. 2007. URL: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf (дата звернення: 13.11.2025).
54. Paul C., Clarke C. P., Triezenberg B. L., Manheim D., Wilson B. Improving C2 and Situational Awareness for Operations in and Through the Information Environment. RAND Corporation Research. 2018. URL: https://www.rand.org/pubs/research_reports/RR2489.html (дата звернення: 18.11.2025).
55. Paul C., Schwille M., Vasseur M., Bartels E. M., Bauer R. The Role of Information in U.S. Concepts for Strategic Competition. RAND Corporation Research. Oct 25, 2022. URL: https://www.rand.org/pubs/research_reports/RRA1256-1.html (дата звернення: 18.11.2025).
56. Posen B. The Security Dilemma and Ethnic Conflict. // Survival. 1993. № 35(1). P. 27-47.). URL: https://www.rochelleterman.com/ir/sites/default/files/posen-1993.pdf (дата звернення 08.10.2025).
57. Rona T. P. Weapon Systems and Information War. Office of the Secretary of Defense. Washington DC. 1976. URL: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf (дата звернення 12.10.2025).
58. Simons G. Syria: Propaganda as a Tool in the Arsenal of Information Warfare / The SAGE Handbook of Propaganda. SAGE Publications. 2020. DOI: https://doi.org/10.4135/9781526477170.n27 (дата звернення 18.11.2025)
59. Thomas M.A. Unleashing the U.S. Military's Thinking about Cyber Power // War on Rock. November 4, 2021. URL: https://warontherocks.com/2021/11/unleashing-the-u-s-militarys-thinking-about-cyber-power/?utm_source=chatgpt.com (дата звернення 12.11.2025).
60. Tracing Five Years of Pro-Kremlin Disinformation about MH17 // EUvsDisinfo. July 18, 2019. URL: https://euvsdisinfo.eu/tracing-five-years-of-pro-kremlin-disinformation-about-mh17/ (дата звернення 11.11.2025)
61. Tunnell H. Task Force Stryker Network-Centric Operations in Afghanistan. Center for Technology and National Security Policy. National Defense University. 2011. URL: https://ndupress.ndu.edu/Media/News/Article/1229178/dtp-084-task-force-stryker-network-centric-operations-in-afghanistan/ (дата звернення 02.11.2025).

62. U.S. Department of Defence. The National Defense Strategy of United States of America. Including The 2022 Nuclear Posture Review and The 2022 Missile Defense Review. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf
63. U.S. Joint Chiefs of Staff, Joint Concept for Integrated Campaigning. Washington, D.C. March 16, 2018. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257
64. Waltz K.N. Nuclear Myths and Political Realities // The American Political Science Review. Vol. 84. No. 3. Sep., 1990. P. 731-745. URL: https://www.jstor.org/stable/1962764 (дата звернення 12.10.2025).
65. Walton C. What's Old Is New Again: Cold War Lessons for Countering Disinformation. Texas National Security Review: Volume 5, Issue 4. 2022. P. 50-72. URL: https://tnsr.org/wp-content/uploads/2022/09/TNSR-Journal-Vol-5-Issue-4-Walton.pdf (дата звернення 13.11.2025)
66. Warner M. Notes on Military Doctrine for Cyberspace Operations in the United States, 1992-2014 // The Cyber Defense Review. Aug. 27, 2015.URL: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/ (дата звернення 12.11.2025).
67. Weisbrot R. Reviewed Work(s): Gambling with Armageddon: Nuclear Roulette from Hiroshima to the Cuban Missile Crisis, 1945–1962 by Martin J. Sherwin // Nieuwe West-Indische Gids. 2022. Vol. 96. No. 1/2. URL: https://www.jstor.org/stable/10.2307/27130504 (дата звернення 12.10.2025).
68. Wight M. International Theory: The Three Traditions. Leicester University Press. 1991. P. 286. URL: https://www.scribd.com/document/439997462/Martin-Wight-International-Theory (дата звернення 12.10.2025).
69. Williams B. Truth and Truthfulness. Princeton: Princeton University Press, 2002. P. 328.
70. Withington T. Electronic Warfare and the battle against Iraq's air defences during Operation Desert Storm. January 20, 2022 URL: https://balloonstodrones.com/2022/01/20/desertstorm30-electric-avenue-electronic-warfare-and-the-battle-against-iraqs-air-defences-during-operation-desert-storm/ (дата звернення 14.11.2025).
71. Брежнєва Т. В. Трансформація стратегії НАТО (1949-1954): сучасне бачення. Дисертація на здобуття ступеня кандидата наук. 2002. URL: https://uacademic.info/ua/document/0402U002385 (дата звернення 08.10.2025)
72. Брежнєва Т. В. Політика НАТО з кіберзахисту та співробітництво з партнерами / / Стратегічні пріоритети. 2012. № 4 (25). С. 189-195.
73. Васильчук Г.М., Маклюк О.М., Бессонова М.М. Феномен пропаганди та антипропаганди у сучасному світі: історико-політологічний дискурс. Запоріжжя: Інтер-М. 2018. 386 с. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi57/0041784.pdf (дата звернення 13.11.2025)

74. Війни – XXI: Полігібресія Росії. Центр глобалістики «Стратегія XXI». Київ.: Авега. 2017. С. 244. URL: https://geostrategy.org.ua/storage/app/public/files/nodes/1/book/1/Xa8si15867659506KcE7.pdf (дата звернення 23.11.2025)
75. Війни інформаційної епохи: міждисциплінарний дискурс: монографія / за ред. В.А. Кротюка. Харків: ФОП Федорко М. Ю., 2021. 558 с. URL: https://dspace.nlu.edu.ua/handle/123456789/19017 (дата звернення 13.11.2025)
76. Вознюк О. Інформаційна війна як інструмент міжнародної політики (досвід для України) // Історико-політичні проблеми сучасного світу: Збірник наукових статей 2024/50. URL:
77. Дубов Д. В. Кібербезпека: світові тенденції та виклики для України: аналіт. доп. / Д. В. Дубов, М. А. Ожеван. К.: НІСД, 2011. 30 с. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/kiberbezpeka-svitovi-tendencii-ta-vikliki-dlya-ukraini-analitichna (дата звернення 15.11.2025)
78. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД. 2014. С. 328
79. Кулик Т. Об'єднана розвідка, спостереження та рекогносцировка як пріоритетна сфера трансформації НАТО. Вісник Маріупольського державного університету. Серія: Історія. Політологія. Вип. 35-36, 2023. – СС. 100-110 https://visnyk.mu.edu.ua/index.php/politologia/article/view/14
80. Кундеус О., Вівчар І., Крет О. Інформаційна війна: сутність та особливості (кінець XX-початок XXI століття) // Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія. № 3(62). DOI: https://doi.org/10.21564/2663-5704.62.310919 (дата звернення 11.11.2025)
81. Курбан О. В. Теорія інформаційної війни: базові основи, методологія та понятійний апарат // Scientific Journal «ScienceRise». No11/1. (16)2015. URL: https://www.researchgate.net/publication/314551203_Theory_of_information_warfare_basic_framework_methodology_and_conceptual_apparatus (дата звернення 23.11.2025)
82. Лисянський П. Л., Саліхов А. Р., Ястребова В. А. Психологічні операції (PSYOP) як вплив на політичні процеси // Актуальні проблеми політики. 2025. Вип. 75. С. 65-72. DOI https://doi.org/10.32782/app.v75.2025.9 (дата звернення 21.11.2025)
83. Світова гібридна війна: український фронт: монографія / за заг. Ред. В.П. Горбуліна. – К.: НІСД, 2017. С. 496
84. Стадник А. Г. Основні моделі організації інформаційних війн та їх різновиди // Соціальні технології: актуальні проблеми теорії та практики. 2015. Вип. 67–68. С. 81-91. URL: http://soctech-journal.kpu.zp.ua/archive/2015/67-68/11.pdf (дата звернення 21.11.2025)
85. Феномен пропаганди та антипропаганди у сучасному світі: історико-політологічний дискурс / За наук. ред. Г.М. Васильчука, О.М. Маклюк, М.М. Бессонової. Запоріжжя : Інтер-М. 2018. С. 386. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi57/0041784.pdf (дата звернення 11.11.2025)