МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

Факультет історії, політології та міжнародних відносин
Кафедра міжнародних відносин та суспільних комунікацій

ІНФОРМАЦІЙНИЙ ВИМІР РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ: ВИКЛИКИ, ПРОРАХУНКИ, РІШЕННЯ

Кваліфікаційна робота

Рівень вищої освіти – другий (магістерський)

Виконав:
студент 6 курсу, 604 групи
Шишковський Микола Анатолійович
Керівник:
доктор історичних наук,
професор **Фісанов В.П.**

До захисту допущено
на засіданні кафедри
протокол №____ від _____ 2025 р.
Зав. кафедрою _____ д.політ.н., доцент Макар В.Ю.

Анотація

Це дослідження аналізує інформаційну війну як самостійний фронт гібридного протиборства в контексті російської агресії проти України. Розкрито системність та стратегічні цілі російської інформаційної агресії, що охоплює пропаганду, дезінформацію та кібероперації. Метою є всебічний аналіз інструментів агресії та виявлення особливостей формування української державної політики протидії. Визначено, що Україна формує багаторівневу систему інформаційної оборони, яка поєднує стратегічні комунікації, кіберзахист, фактчекінг та цифрову дипломатію. Методологія базується на системному, міждисциплінарному та інституційному підходах. Робота пропонує практичні рекомендації для вдосконалення комунікаційних стратегій та інтеграції зі стандартами ЄС і НАТО.

Ключові слова: *інформаційна війна, дезінформація, кібероперації, гібридна війна, стратегічні комунікації, інформаційна безпека*.

Summary

This study analyzes information warfare as an independent front of hybrid confrontation in the context of Russian aggression against Ukraine. It reveals the systematic nature and strategic goals of Russian information aggression, which includes propaganda, disinformation, and cyber operations. The goal is a comprehensive analysis of the aggression tools and the identification of features in the formation of Ukrainian state policy on counteracting disinformation. It is determined that Ukraine is forming a multi-level information defense system that combines strategic communications, cyber protection, fact-checking, and digital diplomacy. The methodology is based on systemic, interdisciplinary, and institutional approaches. The work offers practical recommendations for improving communication strategies and integration with EU and NATO standards.

Keywords: *information warfare, disinformation, cyber operations, hybrid warfare, strategic communications, information security.*

_____ Шишковський М.А.

(підпис)

Зміст

Вступ

Актуальність теми. Російсько-українська війна відкрила новий, небезпечний вимір сучасних конфліктів – інформаційний. Вперше за історію незалежної України протистояння відбувається не лише на полі бою, а й у глобальному інформаційному просторі, де вплив на свідомість, емоції й поведінку громадян набуває стратегічного значення. Інформаційна війна стала не просто супутником збройної агресії, а її самостійним фронтом, спрямованим на підрив державності, деморалізацію суспільства, дискредитацію українського керівництва та розмиття міжнародної підтримки. В умовах, коли інформація перетворюється на інструмент влади, контроль над смислами стає ключовою формою домінування. Саме тому питання формування, реалізації та ефективності державної інформаційної політики набувають визначального значення для національної безпеки України.

Актуальність проблеми зумовлена тим, що російська інформаційна агресія є системною, технологічно оснащеною і стратегічно спланованою. Вона охоплює не лише пропаганду та дезінформацію, але й кібероперації, маніпуляції у соціальних мережах, інформаційно-психологічні впливи та підривні дипломатичні комунікації. Україна, як держава, що стала мішенню комплексної гібридної війни, вимушена формувати власну модель інформаційної оборони – багаторівневу систему, що поєднує стратегічні комунікації, кіберзахист, фактчекінг, OSINT-аналітику, цифрову дипломатію та освітні програми з медіаграмотності. Саме тому наукове осмислення феномену інформаційної війни, її інструментів, механізмів і наслідків, а також аналіз ефективності українських стратегій протидії становлять нагальне завдання як для політичної науки, так і для практики державного управління.

У цьому контексті інформаційна безпека виступає не лише складовою системи національної безпеки, а й необхідною умовою функціонування держави, що бореться за своє існування. Водночас міжнародний досвід підтверджує: ефективна протидія інформаційним загрозам неможлива без

інтеграції державних, громадських і міжнародних зусиль. Україна стала полігоном, де перевіряються сучасні концепції стратегічних комунікацій, а її досвід визначає тенденції глобальної безпекової політики у цифрову добу.

Ступінь наукової розробленості проблеми. Феномен інформаційної війни розглядається у широкому міждисциплінарному полі – на перетині військових студій, політології, соціології, психології, права, комунікативістики та кібербезпеки. У світовій науці закріпилися три основні парадигми дослідження: психологічна (вивчення когнітивного впливу, маніпуляцій і пропаганди), соціально-комунікативна (аналіз потоків інформації, алгоритмічного посередництва та медіавласності) і військово-стратегічна (інтеграція інформаційних і технічних дій у військові операції). В українському академічному дискурсі, особливо після 2014 року, питання інформаційної безпеки та протидії дезінформації набули статусу пріоритетних досліджень. Наукові праці В. Гоцуляка, Л. Компанцевої, О. Богомолова, М. Назаркевича, О. Левченка та інших авторів заклали основу для системного аналізу російських інформаційно-психологічних операцій, розкрили роль стратегічних комунікацій у державній політиці та визначили роль OSINT, фактчекінгу й цифрової дипломатії як практичних інструментів оборони [85; 87; 95–98].

Об’єкт і предмет дослідження. Об’єктом дослідження є інформаційна війна як форма гібридного протиборства, у межах якої поєднуються військові, політичні, комунікативні та технологічні інструменти впливу. Предметом дослідження є інформаційний вимір російсько-української війни – система цілей, інструментів, каналів та стратегій впливу Російської Федерації, а також механізми протидії Україні й міжнародної спільноти.

Мета і завдання дослідження. Метою дослідження є всебічний аналіз феномену російської інформаційної агресії, її інструментів, каналів і стратегічних цілей, а також виявлення особливостей формування й реалізації української державної політики протидії дезінформації в національному та міжнародному контекстах.

Для досягнення цієї мети передбачено виконання таких **завдань**:

1. Визначити понятійно-теоретичні засади дослідження інформаційної війни як міждисциплінарного феномену.
2. Розкрити еволюцію терміна «інформаційна війна» та його взаємозв'язок із поняттями «інформаційне протиборство» та «інформаційна безпека».
3. Проаналізувати основні цілі, інструменти та канали російської інформаційної агресії проти України.
4. Визначити інституційну структуру, механізми та ефективність української системи стратегічних комунікацій і протидії дезінформації.
5. Окреслити міжнародний контекст боротьби з інформаційними загрозами, зокрема роль ЄС, НАТО та міжнародних партнерів у зміцненні інформаційної стійкості України.
6. Сформулювати практичні рекомендації щодо вдосконалення державної інформаційної політики, підвищення ефективності комунікаційних стратегій і розвитку міжвідомчої координації.

Методологічна основа дослідження. Методологія спирається на системний, історико-порівняльний, структурно-функціональний, інституційний і міждисциплінарний підходи. У роботі поєднано методи контент-аналізу, дискурс-аналізу, мережевого аналізу (SNA), елементів ігрового моделювання, а також практики OSINT і фактчекінгу як інструменти збору емпіричних даних. Системний підхід дозволив розглядати інформаційну війну як відкриту динамічну систему, що поєднує когнітивно-смислові, технологічні та правові рівні. Історичний метод дав змогу простежити еволюцію концепцій інформаційної безпеки та зміну ролі медіа у війнах нового покоління. Порівняльний аналіз забезпечив можливість зіставлення української моделі інформаційної протидії з практиками ЄС і НАТО. Для оцінювання ефективності стратегічних комунікацій застосовано методи контент- і дискурс-аналізу державних заяв, публікацій фактчекінгових ресурсів і матеріалів ЗМІ.

Структура роботи. Магістерська робота складається зі вступу, двох розділів, висновків, списку використаних джерел і додатків.

Перший розділ розкриває теоретико-методологічні основи дослідження інформаційних воєн, їхню природу, підходи до аналізу, а також методологічні засади оцінювання ефективності протидії.

Другий розділ присвячено аналізу інформаційного виміру російсько-української війни: розглянуто цілі, інструменти, канали російської інформаційної агресії, українські системи протидії дезінформації та міжнародний контекст боротьби з інформаційними загрозами.

Третій розділ аналізує ключові виклики та прорахунки державної інформаційної політики у воєнний час, оцінює ефективність українських стратегій інформаційної оборони й цифрової дипломатії, а також окреслює перспективи формування стійкого інформаційного середовища та узгодження національних підходів зі стандартами ЄС і НАТО.

У висновках узагальнено результати дослідження, сформульовано наукові та практичні висновки, спрямовані на підвищення ефективності державної політики у сфері інформаційної безпеки.

Магістерська робота складається зі вступу, трьох розділів, поділених на підрозділи, висновків, списку використаної літератури, який налічує 110 найменувань. Загальний обсяг роботи становить 104 сторінок, з яких основного тексту 85 сторінки.

Розділ 1. Теоретико-методологічні основи інформаційного виміру конфліктів

1.1 Понятійні та концептуально-теоретичні засади дослідження інформаційних воєн

Проблематика інформаційної війни сформувалося на перетині військової науки, політології, соціології, психології, права та комунікаційних досліджень, що визначає багатовимірність її концептуального апарату та конкуренцію дослідницьких парадигм. У науковому дискурсі «інформаційна війна» розуміється як сукупність цілеспрямованих дій, спрямованих на отримання інформаційної переваги шляхом впливу на інформаційні ресурси, процеси, інфраструктуру та когнітивну й емоційну сферу окремих осіб і соціальних груп, і такі дії можуть здійснюватися як у воєнний, так і в мирний час, у рамках як міждержавного протистояння, так і внутрішньополітичних конфліктів [1, с. 76–83; 2, с. 70–74; 6, с. 266–270]. Головною особливістю цього явища є те, що об’єктом «ударів» є насамперед канали комунікації, інформаційні системи та сприйняття реальності, а не лише матеріальні об’єкти, що відрізняє інформаційні війни від класичного кінетичного протистояння [3, с. 67–75; 10, с. 173–184]. Історично формування терміна відбувалося хвилями: від поодиноких згадок у контексті спеціальних інформаційних та психологічних операцій до його інституціоналізації в офіційних доктринах та наукових школах післявоєнного періоду [1, с. 76–83]. Досвід операції «Буря в пустелі» (1991) став переломним моментом, коли інформаційно-комунікаційний вимір застосування сили – від супутникової розвідки до телевізійних трансляцій бойових операцій – став системним, що підвищило інтерес військових аналітиків і дослідників ЗМІ до ролі інформації як самостійного важеля впливу на хід конфлікту [3, с. 67–75; 2, с. 72–74]. В українській науковій сфері концепція «інформаційної війни» отримала додатковий імпульс після початку російської агресії, коли емпіричний матеріал дозволив деталізувати інструменти впливу – від пропаганди та

дезінформації до кібероперацій, спрямованих на критичну інфраструктуру [5, 11, с. 77–80].

Концептуалізація цього явища відбувається в декількох, хоча й взаємодоповнюючих вимірах. Психологічний підхід зосереджується на механізмах впливу на свідомість через побудову інтерпретаційних рамок, нав'язування «ворожих наративів», апелювання до емоцій страху, обурення чи тріумфу [1, с. 79–82; 12, с. 231–236]. Саме в цьому контексті інформаційна війна постає як процес переформатування когнітивних схем аудиторій за допомогою комбінаторних технік переконання, маніпуляції та дезінформації, де увага є критичним ресурсом, оскільки вона є обмеженим когнітивним капіталом суспільства [2, с. 73–75; 11, с. 79–81]. Соціокомунікаційний вектор, у свою чергу, трактує інформаційну війну як спосіб управління потоками повідомлень у медіапросторі – від традиційних ЗМІ до соціальних платформ – з метою встановлення гегемонії певних значень і нормативів [2, с. 80–87; 4, с. 191–193]. Саме тут актуальними є питання власності на засоби масової інформації, алгоритмічного посередництва та мережевих ефектів, що посилюють охоплення та поглиблюють «інформаційні бульбашки», які збільшують сприйнятливість до пропагандистського контенту [2, с. 82–85; 11, с. 80–82].

Геополітичний підхід особливо підкреслює той факт, що інформаційні кампанії є частиною більш загальних стратегій м'якої сили та розумної сили, які інтегрують комунікативні, дипломатичні, економічні та безпекові інструменти для досягнення цілей зовнішньої політики без прямого використання збройних сил [10, с. 173–184; 6, с. 9–19]. У такому контексті інформаційна війна розглядається як засіб корегування міжнародного порядку шляхом зміни репутаційного балансу та нормативних пріоритетів, де символічний капітал, легітимність та довіра стають не менш важливими, ніж матеріальні [10, с. 173–184; 6, с. 9–19]. З іншого боку, військово-стратегічний підхід визначає інформаційні операції як інтегрований елемент сучасних конфліктів: від пошуку інформації та психологічного впливу на

військовослужбовців і цивільне населення до інформаційних і технічних дій у кіберпросторі, електромагнітному спектрі та системах управління і контролю [3, с. 47–50; 5]. У цьому сенсі інформаційна війна може слугувати як самостійним театром дій, так і мультиплікатором ефективності кінетичних операцій завдяки дезорганізації, деморалізації та когнітивному навантаженню супротивника [3, с. 46–49; 5].

Системний підхід інтерпретує інформаційне протистояння як взаємодію складних соціотехнічних систем, в яких критично важливими є нелінійний зворотний зв’язок, порогові ефекти та кумулятивні каскади поширення значення [1, с. 81–83; 11, с. 82–83]. Увага зосереджується на архітектурі інфосфери: інститути виробництва контенту, платформи розповсюдження, регуляторні рамки та практики аудиторії утворюють єдиний контур, де, здавалося б, незначні коригування алгоритмів або норм модерації можуть призвести до глибоких макросоціальних змін [2, с. 82–86; 11, с. 80–83]. Конфліктологічний вимір, у свою чергу, підкреслює, що інформаційні війни є окремим типом конфліктної взаємодії, спрямованим на зміну можливостей та мотивації акторів шляхом маніпулювання інформаційною асиметрією, контролю над порядком денним та нав’язування альтернативних карт реальності [1, с. 80–81; 6, с. 9–19].

Ключовим для аналітики є розмежування понять «інформаційна війна», «інформаційне протистояння» та «інформаційна безпека». У найширшому сенсі інформаційне протистояння – це сукупність політичних, дипломатичних, економічних, технологічних і військових заходів, спрямованих на здобуття та збереження інформаційної переваги, включаючи захист власних інформаційних ресурсів і середовищ [4, с. 191–193; 5, с. 139–141]. Інформаційна війна є найбільш інтенсивним, конфронтаційним сегментом цього континууму, де використання інформації стає наступальним з чітко сформульованими стратегічними цілями [6, с. 270–273; 3, с. 46–49]. Натомість інформаційна безпека – це насамперед регуляторний, правовий, організаційний та технічний режим забезпечення конфіденційності, цілісності

та доступності інформації, захисту прав суб’єктів інформаційних відносин та стійкості критичної інфраструктури до загроз [4, с. 192–195; 11, с. 76–79]. Українська правова доктрина закріплює ці підходи в Концепції інформаційної безпеки (визначає цілі, засади та пріоритети державної політики у сфері захисту інформаційного простору) [7], а також у Законі України «Про основні засади забезпечення кібербезпеки України», який детально визначає суб’єктів, об’єкти, повноваження та механізми міжвідомчої взаємодії у сфері кібербезпеки (зокрема, статті 1, 3, 4 Закону) [8]. Теоретичний арсенал досліджень інформаційної війни включає типології інструментів впливу. У сегменті інформаційно-психологічних операцій ключовими інструментами є дезінформація, пропаганда, чутки, «контрольовані витоки», фабрикування фальшивих маркерів легітимізації (псевдоексперти, підроблені документи), маніпулювання емоційним тоном публічної дискусії [5, с. 139–142;12, с. 83–87]. Дезінформація описується як систематичне спотворення або контекстуалізація фактів з метою викликати помилкові уявлення серед цільової аудиторії і, як результат, бажану зміну поведінки; її різновиди включають як повні фальсифікації, так і «напівправди», коли правдиві фрагменти вбудовуються в помилкові причинно-наслідкові ланцюжки [12, с. 83–87; 2, с. 76–79]. Пропаганда, у свою чергу, спирається на повторення, символічні маркери колективної ідентичності та механізми соціального наслідування, посилені в цифровому середовищі алгоритмічною персоналізацією та мережевою гомофілією. [2, с. 80–86; 11, с. 79–82] Інформаційно-технічний сегмент охоплює кібероперації проти критичної інформаційної інфраструктури, маніпулювання системами управління процесами, атаки на ланцюжок постачання програмних компонентів та використання вразливостей у протоколах зв’язку [5, с. 141–144; 3, с. 48–50].

В українській юрисдикції ці ризики формалізовані шляхом категоризації критичної інфраструктури, встановлення вимог до кібербезпеки та обов’язкової державної/галузевої координації реагування на інциденти [8]. Теоретична основа, що узагальнює цей вимір, відтворює класичну «тріаду»

цілей захисту: конфіденційність, цілісність, доступність, де перша гарантує обмеження доступу до даних для неавторизованих суб'єктів, друга – незмінність і правильність даних під час зберігання та передачі, а третя – безперервність і своєчасність доступу для авторизованих користувачів [9]. Відповідно, інформаційна війна в технічному вимірі спрямована на підрив цих трьох стовпів шляхом викрадення або витоку даних (порушення конфіденційності), маніпулювання ними або їх знищення (порушення цілісності) та блокування послуг (порушення доступності) [5; 9].Окремим рівнем є правове та інституційне регулювання інформаційної безпеки та протидія дезінформації. У національній доктрині правові механізми описуються як поєднання конституційних гарантій свободи вираження поглядів із пропорційними обмеженнями щодо поширення недостовірної інформації, мови ворожнечі, закликів до насильницької зміни конституційного ладу або посягання на територіальну цілісність [4, с. 192–195]. Концепція інформаційної безпеки, затверджена в політико-правовій сфері, визначає пріоритети державної комунікації, протидії інформаційній агресії та розвитку національних стратегічних комунікаційних можливостей [7]. Закон про кібербезпеку інституціоналізує розподіл повноважень між суб'єктами сектору безпеки та оборони, спеціальними службами, регуляторними органами та власниками інфраструктури, що створює правові засади для міжвідомчої координації та державно-приватного партнерства у протидії кіберзагрозам [8].

З точки зору комунікативних практик, медіапростір сучасного конфлікту є поліцентричним і характеризується високою швидкістю поширення повідомлень. Дослідження медійного виміру інформаційної війни вказують на подвійну роль традиційних ЗМІ: з одного боку, вони здатні виконувати функції верифікації, стандартизації фактів та громадського контролю; з іншого боку, вони можуть стати каналами легітимізації наративів, що відповідають інтересам політичних та корпоративних акторів [2, с. 70–76; 1, с. 67–71]. У цифровому середовищі ця амбівалентність підсилюється алгоритмами рекомендацій та мікротаргетингом, що забезпечують майже

безперешкодний доступ до маніпулятивного контенту для вузької аудиторії у форматі «персоналізованих істин» [2, с. 82–86; 11, с. 80–82]. Таким чином, теоретичні моделі інформаційної війни все частіше звертаються до таких понять, як «інформаційна екологія», «когнітивна безпека» та «стійкість аудиторії», які підкреслюють здатність суспільств підтримувати відкритий обіг інформації, не втрачаючи своєї критичної здатності щодо джерел, доказів та аргументації [11, с. 76–79; 4, с. 193–195].

Особливий інтерес викликає дихотомія «інформаційно-психологічного» та «інформаційно-технічного» аспектів у структурі протистояння. Перший спрямований на семантичні матриці, другий – на медіа та канали. Однак емпіричний матеріал останнього десятиліття переконливо демонструє їхній синергетичний ефект: технічні інциденти – від DDoS-атак до компрометації медіаресурсів – використовуються як «сигнали» для створення панічних або тріумфальних наративів, тоді як успішні інформаційні кампанії сприяють технічним операціям через інженерію довіри та соціальну інженерію [5; 12, с. 83–87]. Звідси випливає аналітичний висновок про необхідність інтегрованої системи оцінки, яка б одночасно враховувала архітектуру інфраструктур, поведінкові моделі аудиторій та правові/регуляторні умови [4, с. 192–195; 11, с. 82–84].

У контексті російсько-української війни теоретичні моделі перевіряються на практиці. Є докази систематичного використання інструментів дезінформації, підкріплених інституційними та технологічними засобами: фабрики ботів і тролів, мережі «кишенькових» ЗМІ, маніпулювання міжнародними платформами, а також кібероперації проти енергетичного, транспортного та банківського секторів [5; 10, с. 84–87]. У відповідь формується багаторівнева система протидії, що поєднує стратегічні комунікації держави, громадські ініціативи з перевірки фактів, регуляторні заходи та розбудову кіберпотенціалу на основі національних та євроатлантичних стандартів [7, 8]. Ці практики перетворюються на емпіричні уроки для концептуального розуміння: ефективність захисту зростає там, де

інституційні режими інформаційної/кібербезпеки поєднуються зі стратегічними комунікаційними наративами і де існують механізми державно-приватної координації реагування [4, с. 193–195; 11, с. 82–84].

Рефлексія щодо «етики впливу» робить серйозний внесок у теоретичну карту. Дилема захисту безпеки та збереження свободи вираження поглядів порушує питання «пропорційності» заходів держави у відповідь на шкідливий інформаційний вплив: від видалення ворожих матеріалів та блокування ресурсів до кримінально-правових заходів [4, с. 193–195]. Теоретичні моделі тут посилаються на критерії легітимності: правова визначеність, мінімальна необхідність втручання, ефективні механізми оскарження, підзвітність рішень та незалежний нагляд. У сфері кібербезпеки також актуальним є стандартизація (процеси управління ризиками, сертифікація, аудит), що меншує трансакційні витрати на координацію між суб'єктами безпеки [8; 9].

Загалом, концептуальний і категоріальний апарат досліджень інформаційної війни сьогодні повинен будуватися як поліфонічний, з урахуванням евристичної цінності різних парадигм, за умови їх інтеграції в єдину систему. Таку систему можна описати як тривимірну: когнітивний та семантичний вимір (психологічні механізми впливу, динаміка наративів, медіапрактики), інфраструктурний та технічний вимір (архітектура мережі, вразливості, кібероперації) та правовий та інституційний вимір (норми, режими, інституції, нагляд). Кожен з вимірів має свої власні показники успіху та ризики: від «інформаційної втоми» та ерозії довіри, зафіксованих у медіадослідженнях [2, с. 80–86; 11, с. 79–82], до системних кіберінцидентів, що порушують критичні функції суспільства [5, с. 141–144; 8].

Як результат, теоретична та методологічна оптика інформаційних воєн повинна базуватися на взаємодоповнюваності підходів. Психологічна парадигма висвітлює внутрішню «механіку» переконання та маніпуляції; соціокомунікаційна парадигма – мережеві форми циркуляції значень і сила алгоритмів; геополітична парадигма – зв'язок інформаційних кампаній з перерозподілом символічного та нормативного капіталу в міжнародному

середовищі; військово-стратегічна парадигма – оперативна інтеграція інформаційних та кінетичних дій; системна парадигма – нелінійна динаміка соціально-технічних комплексів; правова парадигма – межі та режими легітимного втручання. Саме ця комбінаторика відкриває шлях до розвитку робочих категорій «стійкості» та «когнітивної безпеки», які стають центральними в затяжних гібридних конфліктах, де вирішальним ресурсом є не тільки здатність завдавати «інформаційних ударів», але й здатність суспільства протистояти їм, зберігаючи критичне мислення, інституційну довіру та функціональну цілісність інформаційної інфраструктури Розгортання російсько-української війни чітко підтверджує обґрунтованість такої інтегративної рамки, в якій наукові визначення не відриваються від практичних способів дії, а концептуальні моделі коригуються емпіричними спостереженнями та правовими інноваціями.

1.2. Методологічні засади дослідження

Методологічною основою даного дослідження є принципи систематичності та міждисциплінарності, що дозволяють аналізувати інформаційну війну як складне соціальне та комунікаційне явище. У контексті російсько-українського конфлікту вона проявляється не тільки як сукупність інформаційних операцій, а й як цілеспрямована боротьба за контроль над інтерпретацією реальності, формування громадської думки та вплив на політичні рішення. Такий підхід вимагає поєднання якісних і кількісних методів, що дають змогу одночасно досліджувати зміст, структуру та механізми пропагандистських повідомлень і соціальний контекст їх сприйняття [13, с. 15–19; 14, с. 477–483; 15].

Використання поліпарадигмального підходу виправдано тим, що інформаційна війна ведеться не тільки в сфері масових комунікацій, але й на рівні психологічного, культурного та символічного впливу, поєднуючи технологічні канали, політичні повідомлення, соціальні реакції та наративні стратегії, що формують уявлення людини про події. Таким чином, застосована

методологія дозволяє в цій роботі моделювати інформаційні та технічні процеси (поширення контенту) поряд з когнітивними та комунікативними (створення та інтерналізація значень) одночасно [13, с. 15–19; 16]. Системний підхід став методологічною основою, в рамках якої інформаційне протистояння може бути представлене як ієрархічна динамічна система. Державні інституції, ЗМІ, аналітичні центри, ініціативи з перевірки фактів та користувачі соціальних мереж є активними учасниками одного інформаційного простору. Існує логіка розвитку такої системи, її особливі механізми зворотного зв'язку та самоконтролю, які забезпечують її стійкість або, навпаки, стають причиною інформаційних криз [14, с. 477–483; 13, с. 15–19].

Системно-структурний аналіз дозволив виділити основні елементи цієї системи: акторів, канали розповсюдження, форми контенту та механізми координації. Це дало змогу відтворити архітектоніку інформаційного простору, визначити ключові центри впливу, механізми створення та розповсюдження пропагандистських матеріалів, а також простежити зв'язок між ЗМІ, соціальними платформами, офіційними джерелами та псевдоекспертними структурами [15]. Завдяки такому підходу стало можливим окреслити основні технології російської пропагандистської системи – пропаганда, дезінформація, маніпуляція та психологічний тиск – та допоміжні технології, такі як інформаційні ботнети та «контрольовані витоки» [13, с. 15–19; 19]. Системно-функціональний аналіз дозволив нам дослідити функції окремих елементів цієї системи в досягненні стратегічних цілей: як урядові повідомлення координуються з інформаційними кампаніями в соціальних мережах, як перевірка фактів впливає на зменшення амплітуди хвиль дезінформації, як маніпулятивні техніки змінюють настрій суспільства [14, с. 477–483; 25, с. 3–7].

Системно-генетичний аналіз дозволив простежити еволюцію пропагандистських наративів: як локальні інформаційні інциденти перетворюються на масові кампанії, як повторювані повідомлення

закріплюють хибні уявлення в суспільній свідомості, а персоналізовані алгоритми платформ підсилюють ефект інформаційного резонансу. Системний інформаційний аналіз, у свою чергу, дозволив дослідити, як розподіляються інформаційні потоки, як змінюється емоційна валентність повідомлень і як різні канали комунікації формують різні моделі сприйняття (телебачення, онлайн-ЗМІ, соціальні мережі та месенджери) [13, с. 15–19; 21].

Застосування принципів систематичності, історизму, об’єктивності, розвитку, єдності теорії і практики гарантує логічну послідовність дослідження. Принцип історизму забезпечується врахуванням етапів війни, політичного контексту та регіональних особливостей сприйняття інформації [13, с. 15–19; 14, с. 477–483]. Принцип розвитку підкреслює мінливість форм і технологій пропаганди [15; 13, с. 15–19]. Принцип об’єктивності передбачає мінімізацію власних упереджень, перевірку результатів за допомогою різних методів (триангуляція) та незалежну оцінку [15; 18, с. 65–68].

Для систематичного вивчення медіаконтенту – телевізійних сюжетів, онлайн-публікацій та дописів у соціальних мережах – було використано контент-аналіз. Це дозволило простежити домінуючі пропагандистські наративи, відстежити їх динаміку, визначити канали поширення та часові піки інформаційних кампаній [13, с. 15–19; 24]. Для підвищення точності аналізу використовувалися методи текстового добування та автоматизованої класифікації. Це дозволило структурувати великі обсяги текстів та виявити приховані теми [22, с. 92–99; 19].

Більш глибокі семантичні структури були виявлені за допомогою аналізу дискурсу: як у текстах створюються опозиції «друг чи ворог», «жертва чи агресор», «нормальний чи загрозливий»; як політична реальність конструюється за допомогою лексики, метафор та фреймінгу [20; 13, с. 15–19, 25, с. 15–25] . На відміну від контент-аналізу, дискурсивний підхід дозволяє не тільки виміряти частоту слів або тем, але й пояснити, як значення набувають сили впливу.

Напівструктуровані інтерв'ю забезпечили емпіричну глибину – вони дозволили зібрати думки журналістів, фактів-чекерів, модераторів платформ та експертів з комунікацій щодо практичних механізмів формування та протидії дезінформації [19]. Експертні опитування, в свою чергу, дозволили оцінити ймовірність різних сценаріїв, ефективність стратегій протидії наративам, визначити ступінь консенсусу серед експертів [14, с. 477–483; 13, с. 15–19]. Змішані методи забезпечили зв'язок між кількісними показниками та якісними інтерпретаціями. Було використано два типи дизайну: послідовний – коли інтерв'ю та аналіз дискурсу передували кількісним вимірам, та пояснювальний – коли статистичні результати пояснювалися за допомогою інтерв'ю та фокус-груп [13, с. 15–19; 14, с. 477–483, 23, с. 168–178]. Водночас такий підхід гарантував багатовимірне бачення та валідність результатів.

Масив емпіричних джерел включає офіційні документи (закони, стратегії, урядові звіти, аналітика міжнародних організацій), медіа-контент (новини, теле- та радіопрограми, соціальні мережі), науково-аналітичні роботи, ресурси з перевірки фактів та інтерв'ю з експертами [13, с. 15–19; 14, с. 477–483]. Надійність була забезпечена критичною оцінкою джерел, автентифікацією даних та перевіркою узгодженості між незалежними масивами [25, с. 1–6; 21].

Таким чином, методологічна концепція цього дослідження розглядає інформаційну війну не як сукупність окремих епізодів чи фрагментарних комунікаційних впливів, а як складне багаторівневе системне явище, у якому переплітаються комунікативні, когнітивні та соціальні процеси. Такий підхід дає змогу побачити, що інформаційні атаки не існують у відриві від ширших суспільних контекстів, а впливають на них і водночас залежать від них. Вони змінюють способи сприйняття, формують емоційні реакції, стосуються не лише індивідуальних рішень, а й колективних моделей поведінки. Саме тому для їхнього аналізу потрібна широка оптика, яка охоплює динаміку медіапростору, психологічні механізми формування переконань, культурні

наративи та політичні чинники, що визначають чутливість суспільства до маніпуляцій.

Поєднання якісних, кількісних та змішаних методів забезпечило можливість розглядати інформаційну агресію одночасно на рівні структур, процесів і конкретних комунікаційних практик. Кількісні методи дозволили встановити закономірності, простежити частоту та інтенсивність атак, оцінити вплив окремих наративів на різні аудиторії. Якісні методи дали змогу заглибитися у зміст повідомлень, зрозуміти логіку їх конструювання, визначити ключові семантичні вузли та механізми впливу. Змішані методи надали змогу інтегрувати ці два виміри, відтворивши повну картину інформаційних процесів і взаємозв'язків між ними. Завдяки цьому вдалося подолати обмеження кожного підходу окремо і отримати багатовимірне бачення досліджуваного явища.

Суворі стандарти надійності, верифікації джерел та фактологічної точності стали важливою умовою валідності отриманих результатів. В умовах інформаційної війни, коли фейки, маніпулятивні інтерпретації та навмисні перекручування фактів є невід'ємною частиною реальності, дослідження потребує підвищеного рівня критичності та методологічної дисципліни. Саме тому велика увага приділялася джерельній базі, перехресній перевірці матеріалів, залученню незалежних фактчекінгових ресурсів та використанню декількох каналів підтвердження інформації. Такий підхід дозволив уникнути однобічності, забезпечити точність і підвищити довіру до висновків.

Системне бачення інформаційного простору дало можливість не лише окреслити окремі напрями інформаційного впливу, а й пояснити, чому деякі з них працюють ефективніше за інші, які соціальні групи є більш вразливими, а які демонструють стійкість. Воно показало, що інформаційна агресія має структуру і логіку, а ефективна відповідь на неї вимагає цілісної державної політики, яка враховує як технічні, так і суспільні аспекти. На основі такого аналізу вдалося сформулювати обґрунтовані й практично значущі висновки, які можуть бути використані для вдосконалення державної інформаційної

політики, підвищення ефективності стратегічних комунікацій, розвитку систем протидії дезінформації та зміцнення інформаційної стійкості України в умовах тривалої гібридної війни.

1.3 Джерельна база дослідження

Джерельна база цієї роботи побудована як цілісний багатошаровий корпус, що поєднує українські законодавчі акти та міжнародні стандарти у сфері прав людини, офіційні державні стратегії та підзаконні акти, документи НАТО та ЄС щодо стратегічних комунікацій та протидії дезінформації, праці українських та зарубіжних дослідників з інформаційної безпеки, аналітичні огляди спеціалізованих центрів, матеріали ініціатив з перевірки фактів, а також джерела спільноти OSINT, практичні посібники та методи реагування на гібридні загрози. Цей, на перший погляд, еклектичний масив побудований за принципом взаємодоповнюваності: нормативні тексти забезпечують легітимну основу, стратегічні документи – інституційну логіку дій, академічні дослідження – концептуальну основу та аналітичні моделі, а продукти фактчекінгу та OSINT – емпіричну перевірку конкретних випадків. Саме тому робота систематично поєднує джерела різного характеру та юрисдикції, що дозволяє одночасно враховувати правові межі, організаційні механізми, технологічні інструменти та соціальні й когнітивні ефекти сучасних інформаційних операцій. Наявність окремого підрозділу про джерельну базу та повного списку посилань у структурі роботи відкрито і однозначно визначає цей підхід, вбудовуючи його в логіку всієї роботи, де 1.3 спеціально присвячений характеристиці джерел, а систематичний список посилань подається в кінці.

Ключовий рівень складають національні нормативні акти, що визначають рамки державної політики у сфері інформаційної безпеки та суміжних галузях. Центральне місце в цій роботі займає Стратегія інформаційної безпеки до 2025 року, затверджена Указом Президента № 685/2021, яка визначає пріоритети, завдання, відповідальних суб’єктів та план

реалізації до кінця планового горизонту [101]. Саме на цій стратегії базуються аргументи щодо необхідності інтегрувати стратегічні комунікації, кіберзахист, розвиток критичної інформаційної інфраструктури та людського капіталу в єдину політичну систему. Закон України «Про основні засади забезпечення кібербезпеки України» відіграє допоміжну роль, описуючи суб'єктів національної системи кібербезпеки, запроваджуючи категоризацію критичної інфраструктури та встановлюючи вимоги до аудиту, моніторингу та реагування [102].

Іншим будівельним блоком регуляторного рівня є Закон про цифровий контент та цифрові послуги, який імплементує положення Директиви ЄС 2019/770 та зменшує сірі зони у взаємодії держави, бізнесу та громадян у цифровому середовищі [103]. З цим рівнем взаємопов'язані положення Конвенції про захист прав людини і основоположних свобод, особливо стаття 10, яка встановлює критерії необхідності та пропорційності обмежень свободи вираження поглядів у воєнний час та в перехідний період [104]. На тому ж рівні визначення поняття цифрових прав використовуються українські наукові розробки щодо їх концепції та класифікації, які забезпечують термінологічну точність і дають змогу розробляти політику «безпеки через права», а не «попри права» [105]. Таким чином, регуляторний та правозахисний рівень окреслює правові межі допустимих практик протидії інформаційним загрозам та накладає на державні органи вимогу підзвітності, пропорційності та прозорості.

Другий масив – це стратегічні та політичні документи інституцій ЄС і НАТО, в яких зафіксовано перехід від «обережного моніторингу» кампаній Кремля до визнання системної дезінформації як самостійного інструменту впливу, рівноцінного традиційним засобам тиску [51]. На рівні ЄС цю еволюцію можна простежити від Стратегічного плану дій у сфері комунікацій 2015 року до створення Східної робочої групи StratCom для запуску EUvsDisinfo, порталу, який накопичує та типологізує десятки тисяч наративів, що слугують не тільки базою для моніторингу, але й навчальним набором

даних для університетів та НУО [61]; [58]. На рівні НАТО ключову роль відіграють документи про гібридні загрози, практика Центру передового досвіду StratCom у Ризі та Hybrid CoE в Гельсінкі, а також інституційні механізми швидкої підтримки держав-партнерів, які перетворюють кіберзахист, публічні комунікації та кризові протоколи на єдину «мову операцій». Саме ці джерела підтверджують, що з 2014 року Альянс розглядає дезінформаційні кампанії не як маргінальний шум, а як привід для скоординованих консультацій та колективних оборонних дій [62].

Для логіки дослідження магістра цей корпус джерел є важливим, оскільки він надає стандартизовану термінологію, робочі таксономії загроз, процедури тестування «червоних команд» та вимірювані показники ефективності наративів, які можна включити в український контекст без «винаходження велосипеда».

Третій рівень представлений державними інституційними джерелами України, які фіксують практики організації стратегічних комунікацій у кризових ситуаціях, підходи до централізації публічної риторики та протидії російській IPSO. Тут реконструкція української моделі базувалася на «правилі трьох голосів» та рекомендаціях, які легітимізували швидку синхронізацію офіційних комунікацій та телемарафону в перші дні повномасштабного вторгнення; це забезпечило чітку ієрархію джерел та економію комунікацій у зовнішньому середовищі [40]. Водночас для практичних цілей протидії фейкам та дезінформації використовуються методологічні продукти державних центрів, які описують процедури «раннього попередження» та алгоритмічні підходи до виявлення ботнетів – таким чином, інституційні джерела не тільки оголошують цілі, а й встановлюють робочу методологію, яку використовують аналітики в цій роботі [40, 30];

Четвертий масив складають незалежні ініціативи з перевірки фактів, які в українському випадку стали органічною частиною державної екосистеми протидії дезінформації. Використання корпусу StopFake є важливим у двох сенсах: по-перше, як щоденний моніторинговий потік із прозорою

процедурою перевірки заяв і публічних вердиктів; по-друге, як емпірична основа для вимірювання «життєвого циклу фейкових новин» – часу розповсюдження, піків висвітлення та ефекту повторних спростувань [45]; [41]. Ці матеріали дозволяють вивести прикладні закономірності поширення наративів і співвіднести їх із часовими рамками офіційних комунікацій, що безпосередньо вписується в аргументацію розділів про інформаційну оборону та цифрову дипломатію. П’ятий тип джерел – це аналітичні роботи, наукові статті та міждисциплінарні дослідження, що надають концептуальну основу та критичні моделі аналізу. Українські дослідження з інформаційної безпеки як напрямку державної політики, медіаграмотності як соціального інструменту інформаційної імунітету, концепції цифрових прав та вимог до прозорості алгоритмів надають теоретичні та методологічні основи, на яких базуються висновки роботи [99; 100; 107; 105].

Водночас іноземні статті про стратегічні комунікації НАТО, моделі протидії пропаганді в ЄС, багатомовну еволюцію дезінформації та оцінку ефективності контрнаративів вносять у текст порівняльну перспективу та дозволяють уникнути «методологічного націоналізму» при розгляді українських випадків у вакуумі [51; 58; 61]. Саме ця інтернаціональність академічної рамки дозволяє переносити робочі показники, метрики та протоколи якості в українську практику без втрати валідності. Шостий рівень – це прикладні посібники, керівництва, методології оцінки та «уроки з поля» для StratCom, перевірки фактів, OSINT та кризової публічної комунікації. Такий вид джерел з’явився у відповідь на «оперативну голод» перших років війни, коли формальні стратегії існували, але не завжди деталізували, «як саме» організувати цикли планування, багатоканальні кампанії, післяакційні огляди та які KPI застосовувати до інформаційних інтервенцій. Використані матеріали, що адаптують стандарти НАТО до національного контексту, дозволяють реконструювати «трубопровід» інформаційної оборони – від постановки цілей і визначення цільової аудиторії до протоколів ескалації та механізмів реалізації редакційних календарів в урядових акаунтах [85; 87];

[89]. Їх цінність полягає в тому, що вони містять не тільки концепції, а й оперативні контрольні списки, індикатори та еталонні процедури, які безпосередньо використовуються при розробці практичних рекомендацій.

Сьомий тип – це джерела OSINT та слідчі масиви, які дають фактичну основу для опису російських IPSO, їх каналів розповсюдження, інфраструктури ботнетів та «каруселі» наративів. Важливими для роботи є випадки, що поєднують супутникові знімки, графіки мережевої взаємодії, стилометрію текстів та метадані відео/зображень, оскільки вони дозволяють перейти від загальних міркувань до доказової реконструкції конкретних інформаційних атак, перевірених двома або більше незалежними методами [95; 96]. Це джерела «живого емпіризму», які, на відміну від статичних звітів, розкривають динаміку ескалації/деескалації хвиль та часові зв’язки з кіберінцидентами – звідси висновок у тексті про необхідність інтегрувати кіберзахист та комунікації в єдиний цикл реагування.

Восьмий масив – це матеріали міжнародних організацій та регуляторів ринку платформ, що документують практики спільного регулювання та м’які інструменти. У статті використовуються документи, що описують добровільні кодекси платформ, зобов’язання щодо прозорості політичної реклами, механізми швидкого обміну сигналами про вхідні дані з високим ризиком та пріоритетну модерацію офіційних державних акаунтів у кризові періоди [45]. Саме цей тип джерел пояснює, чому «суворі» заборони, такі як блокування RT/Sputnik, працюють лише у поєднанні з технічними процедурами демпінгу та освітніми кампаніями, а не як самодостатні інструменти. Вони підкріплюють аргумент про те, що держава, платформи та громадянське суспільство повинні співіснувати в симбіозі як запорука стійкості демократичних інформаційних екосистем.

Усі ці групи джерел пов’язані між собою не тільки тематично, але й процедурно. Нормативні та стратегічні документи встановлюють вимоги щодо відкритості, підзвітності, гарантій прав людини та пропорційності обмежень [101; 104; 103]. Академічні дослідження та порівняльні огляди допомагають

уникнути методологічної упередженості, показуючи, що багато рішень вже розроблено в рамках ЄС/НАТО і їх можна перенести до України з урахуванням контексту [51; 61]. Аналітичні «висновки» та практичні рекомендації є містком між політикою та діяльністю, даючи відповіді на питання «як робити», «в якій послідовності» та «за якими показниками оцінювати» [85; 87; 89]. Нарешті, перевірка фактів та OSINT створюють емпіричну основу, яка дозволяє будь-якій теоретичній гіпотезі пройти випробування реальністю – у часових шкалах, скріншотах, журналах та телеметрії [45; 95; 96]. Такий підхід до формування бази джерел свідомо уникає спокуси покладатися на один «привілейований» тип даних, пропонуючи натомість трикутник «закон – стратегія – емпіризм», де кожна сторона підтримує дві інші та зменшує ризик помилкових висновків

Слід підкреслити роль джерел, що описують організаційні моделі координації урядових комунікацій у кризових ситуаціях. Синхронізація прес-служб, спільне мовлення, централізація зовнішньої риторики та суворі правила верифікації – ці практики розглядаються не як політичні деталі, а як технології зменшення «інформаційного шуму», а відповідні джерела надають оперативні параметри швидкості, ієрархії та відповідальності [40]. З іншого боку, документи ЄС/НАТО показують, що інституційна зрілість таких практик за межами України базується на стійких центрах компетенції та стандартах навчання, що вказує шлях до інституціоналізації українських розробок [61; 58; 62].Важливо також, що значна частина залучених джерел є багатомовними та кросплатформними, що дозволяє відстежувати таке явище, як «перекладена дезінформація», коли одна і та ж наратива отримує 15–20 мовних втілень протягом двох днів, тоді як середній час реагування глобальних фактів-чекерів є довшим. У цій статті це підкріплює тезу про необхідність багатомовних швидких шляхів спростування, уніфікованих глосаріїв та міжплатформних чорних списків URL-адрес, які наразі практикуються європейськими структурами і можуть бути включені в українську політику [58]. Такі аргументи базуються на джерелах, які показують емпірично виміряну

динаміку багатомовних хвиль та часові затримки між введенням інформації та її спростуванням.

Нарешті, структура джерельної бази також визначається специфікою теми: інформаційна війна є швидкозмінною та технологічно інтенсивною сферою, тому покладання лише на «довгі» академічні публікації призвело б до хронічного відставання в аналітиці. Тому робота включає актуальні матеріали з політики, технічні питання та відповіді інституцій ЄС, оперативні повідомлення та публічні заяви, які, незважаючи на журналістський жанр, слугують авторитетними першоджерелами щодо державної політики та механізмів функціонування платформ [61; 45]. Саме на перетині «повільних» і «швидких» джерел формується баланс між концептуальною глибиною та оперативною актуальністю. Це доповнюється національними освітніми та методологічними розробками в галузі медіаграмотності, які переносять дискусію з вузького контексту безпеки в ширший соціальний контекст і дозволяють проектувати стійкість не тільки як функцію держави, але й як культуру щоденного споживання інформації [107; 109; 110]. Таким чином, джерельна база дослідження – це не механічна сума посилань, а продумана система взаємних підтверджень і перехресних перевірок, де нормативні акти та права людини встановлюють межі прийнятного, стратегії ЄС і НАТО – стандарти діяльності, українські державні документи – архітектуру реалізації, академічні публікації – концептуальний апарат і аналітичні методи, прикладні настанови – процедури «як це зробити», перевірка фактів та OSINT – доказовий емпіризм щоденної війни. Саме завдяки такому багатоканальному використанню джерел робота поєднує нормативну легітимність, інституційну здійсненність та емпіричну перевірюваність своїх висновків. В результаті вона пропонує не тільки опис проблем і практик, але й відтворюваний, стандартизований спосіб мислення про інформаційну безпеку, який є одночасно сумісним із юридичними зобов’язаннями України, сумісним із європейськими та євроатлантичними стандартами та перевіреним на практиці конкретними даними з надійних публічних та професійних джерел.

Висновок до розділу 1

Таким чином, можна констатувати, що інформаційна війна є системним і багатовимірним явищем, яке виходить за межі класичного кінетичного протистояння та інтегрує когнітивні, технологічні й правові режими впливу. У сучасних умовах конкурентна перевага формується не окремими «ударними» інструментами, а злагодженістю цілих підсистем – від стратегічних наративів і платформних політик до інституційних процедур реагування.

Розділ розкриває теоретичні та методологічні основи вивчення інформаційного виміру конфліктів, акцентуючи на багатогранності інформаційної війни як міждисциплінарного феномена. У першому підрозділі розглянуто еволюцію поняття «інформаційна війна», що охоплює психологічні, соціокомунікаційні, геополітичні та військово-стратегічні аспекти. Цей термін відрізняється від «інформаційного протистояння» – ширшого процесу здобуття переваги – та «інформаційної безпеки», яка фокусується на захисті ресурсів і стійкості інфраструктури. Ключовими інструментами є дезінформація, пропаганда та кібероперації, що впливають на когнітивну сферу та медіапростір, формуючи альтернативні реальності. Теоретичні парадигми підкреслюють необхідність інтегративного підходу, де когнітивний, технічний і правовий виміри утворюють єдину систему для аналізу гібридних загроз, як у російсько-українській війні.

Другий підрозділ окреслює методологічні засади, ґрунтуючись на системному та міждисциплінарному принципах. Системний підхід трактує інформаційну війну як динамічну структуру з елементами акторів, каналів і механізмів впливу, дозволяючи моделювати еволюцію наративів і потоки інформації. Застосовано контент-аналіз для вивчення медіаконтенту, дискурс-аналіз для семантичних структур, напівструктуровані інтерв’ю та експертні опитування для емпіричної глибини. Змішані методи забезпечують валідність, поєднуючи кількісні закономірності з якісними інтерпретаціями, що дає змогу аналізувати не лише окремі атаки, а й суспільні контексти вразливості.

Третій підрозділ характеризує джерельну базу як багатошаровий корпус, що включає національні нормативні акти (Стратегія інформаційної безпеки, Закон про кібербезпеку), документи ЄС і НАТО (EUvsDisinfo, стандарти StratCom), академічні дослідження, матеріали фактчекінгу (StopFake) та OSINT-ресурси. Ці джерела взаємодоповнюються, забезпечуючи правову основу, стратегічні моделі та емпіричні дані для оцінки ефективності протидії. Загалом, розділ формує інтегративну рамку, де теоретичні моделі корелюються з практичними інструментами, підкреслюючи роль стійкості в умовах гібридних конфліктів.

Розділ 2. Інформаційний вимір російсько-української війни

2.1 Російська інформаційна агресія: цілі, інструменти та канали впливу

Інформаційний та психологічний вимір сучасної війни показує, що успіх на фізичному полі бою нерозривно пов’язаний з домінуванням у когнітивному просторі. Російська Федерація створила складну багаторівневу систему впливу, що включає класичні методи пропаганди, кібероперації, маніпулювання історичними та культурними наративами, а також навмисне підривання довіри до демократичних інститутів. Гібридні стратегії поєднують «жорсткі» та «м’які» інструменти військових структур, розвідувальних служб та медіахолдингів із приватними агентствами, експертними та аналітичними платформами, які працюють у режимі синхронізації в реальному часі [26; 27, с. 136–141]. Головною відмінністю цієї моделі від класичної інформаційної конфронтації є інтеграція політичних, військових, економічних і культурних компонентів в одну комунікаційну матрицю, де кожне повідомлення підкріплюється паралельними діями на інших рівнях – від дипломатичних ініціатив до ракетних ударів по енергетичній інфраструктурі. Початкові розробки, що заклали основу «оперативного маскування» ще в радянські роки, тепер перетворилися на концепцію безперервної «політичної війни», яку сучасні російські стратеги описують як «невидимий фронт» глобальної конфронтації [28, с. 5–9]. Основна теза цієї концепції полягає в тому, що суспільства можна підкорити без прямої окупації території, якщо заздалегідь змінити їхню систему переконань і нав’язати бажаний кут зору на події. Це призводить до появи специфічної технології «насичення наративом»: аудиторію бомбардують взаємовиключними версіями та фальшивими доказами, що унеможливлює формування єдиної «рамки істини» [29]. Одночасно конспірологічні теорії, «експертні» коментарі та псевдонаукові дослідження створюють ефект «дзеркальної кімнати» інформаційного середовища, де відображення стає важливішим за сам факт. Нова хвиля цієї

доктрини стала очевидною під час вторгнення 2022 року, коли інформаційні удари здійснювалися синхронно з ракетними ударами та дипломатичними демаршами. Таким чином, Кремль надав психологічне «прикриття» військовим діям, намагаючись зламати опір населення України, посіяти сум'яття серед партнерів та сформувати картину «законного стримування Заходу» [30, с. 184–191].

Метою інформаційної агресії є перегляд післявоєнної системи безпеки, відновлення статусу Росії як «центру сили» та маргіналізація України як суб'єкта міжнародної політики Ідеологічна основа цієї конструкції базується на кількох ключових міфах. Перший – це теза про «єдиний духовний простір», яка підкріплюється історичним ревізіонізмом і концепцією «русского мира». Другий – це образ «благодійного патерналізму», де Росія виступає «великим братом-захисником», який нібито «визволяє» українців від «зовнішнього контролю». Третій – це риторика антифашизму, покликана викликати емоційні асоціації з радянською перемогою у Другій світовій війні та легітимізувати будь-які силові дії проти «неонацистів» [32, с. 185–194; 33, с. 4–18]. Усі ці наративи мають транснаціональний характер: вони адресовані не тільки внутрішній російській аудиторії, а й мешканцям країн Глобального Півдня, де традиційно резонують постколоніальна риторика та історія «боротьби з імперіалізмом» [39, с. 190–196]. Однією з відмінних рис російських інформаційних операцій є так званий «панічний шум» – постійна присутність загрозливих повідомлень, що підсилюють ефект непередбачуваності та невизначеності щодо майбутнього. Напередодні атак на критичну інфраструктуру в повітря кидають чутки про «відключення електроенергії» або «тотальну мобілізацію», що паралізує державні інститути, змушуючи їх витрачати ресурси на реагування на інформаційні пожежі [30, с. 184–191]. Аналогічно, під час оборони Маріуполя був організований потік дезінформації про «масове накопичення зброї» на «Азовсталі» з метою підірвати бойовий дух захисників міста і одночасно вплинути на західну пресу, щоб знизити готовність союзників підтримувати облогу [31, с. 18–23].

Типова кампанія починається з «приманки»: публікацій на маргінальних веб-сайтах, що імітують журналістські розслідування. Далі йде хвиля кросплатформного поширення – від Telegram–каналів до новинних агрегаторів, де інформацію підхоплюють «експерти» і подають у вигляді коментарів без належної перевірки. Третій етап – міжнародні англомовні ресурси RT і Sputnik, які вкладають історію в глобальні рамки («конфлікт цінностей», «етнічні репресії»), а ботнети в соціальних мережах збільшують охоплення за допомогою автоматизованих репостів [34; 37, с. 17–26]. І врешті-решт історія потрапляє в академічний дискурс: у деяких маловідомих журналах з'являються «наукові» статті, які посилаються на початкові фейки як на «факти», тим самим закріплюючи їх у бібліографічному полі.

Цей цикл може тривати тижні або місяці, доки нова новина не замінить її більш стратегічно важливою темою. Російські технологи називають таку ротацію новин «каруселлю», яка дозволяє їм підтримувати постійний рівень невизначеності та виснажувати інформаційні ресурси супротивника. Основою довгострокової пропаганди є «великі наративи», які залишаються незмінними протягом років. Наприклад, концепція «святості Криму» поєднує релігійні, історичні та етнополітичні мотиви і дозволяє раціоналізувати анексію 2014 року як «повернення священної землі». Іншим прикладом є міф про «деградацію Заходу», в якому західні ліберальні цінності подаються як джерело морального занепаду та демографічної кризи, а Росія позиціонується як «останній бастіон традицій» [33, с. 4–18]. Ці наративи поширюються через телесеріали, історичні драми, популярні ток-шоу, а також через підручники та музейні виставки, формуючи довгострокову культурну матрицю. Під час пандемії COVID-19 російські ЗМІ поширювали низку версій про «американське походження вірусу» та «небезпеку західних вакцин», що підірвало довіру до ВООЗ у низці африканських та латиноамериканських країн. Подібна тактика використовується і щодо війни в Україні: інформаційні операції просувають тезу про «конфлікт НАТО і Росії на території третьої

сторони», знімаючи пряму відповідальність агресора з Кремля і перекладаючи провину на «колективний Захід» [35; 36].

Така сама техніка слугує інструментом стратегічної комунікації в багатосторонніх організаціях: російські делегації в ООН та ОБСЄ систематично апелюють до прав «самовизначення народів Донбасу», одночасно демонізуючи західні санкції як «економічний геноцид». Телебачення залишається головним рушієм всередині Росії, але за межами країни ключову роль відіграють цифрові платформи. Telegram забезпечує оперативну доставку контенту з передової, X (Twitter) – швидке просування за допомогою хештегів, а YouTube – можливість монетизованого довгострокового зберігання відеоархівів, які алгоритми пошуку представляють як «релевантну інформацію» навіть через роки після публікації [29, с. 20]. Мережі ботнетів діють як «камера відлуння»: автоматизовані акаунти репостять потрібні твіти в перші хвилини після публікації, створюючи ілюзію масового інтересу громадськості. Водночас кібератаки, такі як DDoS або хакерські атаки на новинні сайти, підсилюють сенсаційність подачі, оскільки в медіапросторі «технічна несправність» швидко перетворюється на інформаційну подію [37, с. 17–26].

Формально структура виглядає децентралізованою, але вона контролюється централізовано за допомогою «тематичних планів» і так званих «вертикальних комунікаційних хабів», які об’єднують правоохоронні органи, державні ЗМІ, приватні PR-агентства та закриті Telegram-чати провідних «військових командирів» [34; 38]. Кожен учасник отримує підбірку ключових повідомлень і рекомендацій щодо тону, а потім адаптує контент до своєї аудиторії, не змінюючи суті наративу. Такий підхід зберігає гнучкість мережі і водночас запобігає розмиванню інформації. Внутрішня російська аудиторія обробляється через телевізійні ток-шоу, де експерти та політичні діячі підсилюють патріотичну мобілізацію.

Українська аудиторія отримує суміш деморалізуючих чуток і фейків, які підривають довіру до уряду, підкреслюють нібито марність західної допомоги

та прогнозують «економічний колапс». Для аудиторії в ЄС акцент робиться на енергетичних та продовольчих ризиках санкцій, щоб стимулювати «втому від України», тоді як країнам Глобального Півдня пропонується дискурс антиколоніалізму, в якому Кремль позиціонується як спадкоємець руху неприєднання [36; 39, с. 190–196]. Ключовою перевагою російських інформаційних операцій є їхня здатність до швидкого масштабування. Як тільки тема з'являється на одному телеканалі, вона того ж дня повторюється на десятках каналів Telegram, через кілька годин – на англомовних вебсайтах, а наступного ранку – у цитатах у друкованій пресі. Потім цю історію підхоплюють лояльні блогери на TikTok, які розміщують короткі відео з емоційними закликами у форматі трендів. У сучасному середовищі, де швидкість споживання контенту визначає пріоритети аудиторії, така синхронізація дозволяє Кремлю підтримувати постійну «завісу шуму» і блокувати альтернативні точки зору. Російська інформаційна агресія проти України відповідає класичному визначенню системних когнітивних операцій: вона руйнує інформаційну екосистему ворога, насичуючи простір пропагандою, дезінформацією та технічними атаками. Її ефективність зумовлена багаторічним інституційним досвідом, гнучкою мережею акторів та чітким стратегічним плануванням, що виходить за межі короткострокових кампаній. Протидія такій агресії вимагає не тільки технологічних засобів кіберзахисту, а й довгострокових стратегій інформаційної стійкості: розвитку медіаграмотності, підтримки незалежної журналістики та розвитку прозорих урядових комунікацій, здатних конкурувати з «шумом» російських інформаційних потоків.

Російська інформаційна агресія проти України з 2014 року, а особливо після повномасштабного вторгнення 2022 року, є системним, багатошаровим і стратегічно спланованим компонентом гібридної війни. Її головна мета – не лише підтримка кінетичних операцій на полі бою, але й досягнення довгострокових політичних і геополітичних цілей без необхідності повної військової перемоги. Серед стратегічних цілей виділяються: підрив

легітимності української держави та її керівництва, деморалізація населення і Збройних Сил, розкол національної єдності за мовними, регіональними та ідеологічними лініями, дискредитація України на міжнародній арені, послаблення підтримки з боку західних партнерів та, зрештою, створення умов для внутрішньої дестабілізації або капітуляції [27; 29; 33; 86].

Для досягнення цих цілей Росія використовує широкий арсенал інструментів інформаційно-психологічного та інформаційно-технічного впливу, які діють синергетично. До основних інструментів належать:

1. Дезінформація та фабрикація доказів – систематичне створення й поширення повністю або частково сфальсифікованих матеріалів (підроблені документи, постановочні відео, фейкові свідчення). Класичним прикладом є кампанія 2014 року про «розіп'ятого хлопчика» та численні фейки 2022–2025 років про нібито біолабораторії США в Україні, «нацистський характер» ЗСУ чи «геноцид російськомовного населення» [37; 41; 45].

2. Пропаганда історичної пам'яті та ідентичності – нав'язування наративів про «єдину історичну Росію», заперечення української нації як окремої політичної спільноти, переписування історії Другої світової війни та деконструкція української державності [31; 34].

3. Маніпуляція емоційним тоном – використання страху, гніву, відчуття приниження чи, навпаки, тріумфу. У перші місяці повномасштабного вторгнення активно просувалися меседжі «Київ за три дні», «неминуча капітуляція», «ЗСУ розбіглися», що мали деморалізувати українське суспільство [28; 86].

4. Кібероперації як інформаційний мультиплікатор – атаки на критичну інфраструктуру (енергетика, транспорт, банківська система) супроводжувалися інформаційними кампаніями, що пояснювали знеструмлення «некомпетентністю влади» або «ударами ЗСУ по власних об'єктах» [35; 93].

5. Імітація громадської думки – через мережі ботів, тролів та підконтрольних «лідерів думок» створюється ілюзія масової підтримки російських наративів як всередині України, так і за кордоном [30; 38].

Канали поширення російської інформаційної агресії також мають багаторівневу структуру:

- традиційні державні ЗМІ (Первый канал, Россия-1, RT, Sputnik), які залишаються основним інструментом формування «великих наративів» для внутрішньої російської та зовнішньої аудиторії країн Глобального Півдня;

- соціальні мережі та месенджери (Telegram, TikTok, YouTube, ВКонтакте, Одноклассники), де завдяки алгоритмічній персоналізації та мікротаргетингу вдається досягати вузьких, але критично важливих груп (наприклад, російськомовне населення півдня та сходу України до 2022 року);

- дипломатичні канали та «м'яка сила» – фінансування проросійських політичних сил, організація псевдогромадських рухів, «антивоєнних» конференцій, діяльність агентів впливу в Європі та США [26; 51; 58];

- підконтрольні або лояльні медіа в третіх країнах, зокрема в Угорщині, Сербії, Німеччині (через окремі видання Alternative für Deutschland чи окремі журналісти) [54].

Особливо небезпечною є вертикальна інтеграція всіх цих каналів під єдиним політичним і військовим керівництвом. Координацію здійснюють Адміністрація Президента РФ, спецслужби (ГРУ, СЗР, ФСБ), медіахолдинги (ВГТРК, НАО «Національна медіа група») та спеціалізовані підрозділи інформаційно-психологічних операцій ЗС РФ. Синхронізація військових дій з інформаційними хвилями стала фірмовим почерком російської стратегії: кожне просування на фронті або, навпаки, відступ супроводжується потужною медійною кампанією, що легітимізує дії або перекладає відповідальність на українську сторону [29; 33; 86].

Важливим новим елементом після 2022 року стала масова міграція російських пропагандистських ресурсів у Telegram та TikTok, а також активне використання штучного інтелекту для генерації deepfake-відео та

автоматичного створення тисяч акаунтів. Водночас Росія значно розширила географію впливу, активно працюючи з аудиторіями Африки, Латинської Америки та Азії через RT Arabic, RT en Español та локальні партнерські медіа, просуваючи тезу про «колективний Захід, що воює з Росією руками українців» [53; 55].

Таким чином, російська інформаційна агресія проти України є не епізодичною пропагандистською діяльністю, а комплексною системою стратегічного впливу, що поєднує класичні методи радянської пропаганди з найсучаснішими цифровими технологіями та гібридними формами війни. Її ефективність значною мірою залежить від здатності одночасно діяти на когнітивному, емоційному та інфраструктурному рівнях, створюючи ефект кумулятивного тиску, який важко нейтралізувати окремими спростуваннями чи блокуваннями [27; 37; 86; 93].

2.2 Українська система протидії дезінформації та державні комунікаційні стратегії

Для України інформаційна сфера виявилася не менш важливим театром військових дій, ніж сама лінія фронту: тут формуються міжнародні коаліції, консолідується внутрішня стійкість, підриваються сценарії ворога. Перші дні повномасштабного вторгнення чітко показали, що контроль над наративом може перетворити військові успіхи ворога на політичні поразки, якщо суспільство та союзники вчасно отримують перевірені факти, а фейки нейтралізуються, перш ніж вони стануть «вірусом» [40, с. 11–22]. За останнє десятиліття Україна перейшла від самоорганізації активістів у 2014 році до розвитку спеціалізованих державних інституцій у 2021 році та масштабної інтеграції державних і громадських ініціатив після 24 лютого 2022 року. Ця еволюція відображає ієрархічне нарощування потенціалу: багаторівневий моніторинг, кризові комунікації, партнерство з великими технологічними компаніями, використання алгоритмічних інструментів та гнучка дипломатична підтримка.

Поява Центру протидії дезінформації при Раді національної безпеки і оборони та Центру стратегічних комунікацій та інформаційної безпеки в березні 2021 року стала проривом, який об’єднав раніше розрізнені громадські практики в державну політику. Перший центр взяв на себе функцію «щита»: аналіз ризиків, швидка ідентифікація кластерів ботнетів, взаємодія з кіберкомандуванням та Міністерством цифрової трансформації для негайного обмеження підозрілих ресурсів. Його методологія «проактивного виявлення загроз» базується на машинних моделях, які прогнозують, які наративи, найімовірніше, «вистрілять» з огляду на геополітичний календар або місцеві кризи – наприклад, атаки на енергетичну систему [40, с. 12]. Алгоритми раннього попередження, вдосконалені завдяки співпраці зі Спеціальними оперативними силами НАТО та аналітичними підрозділами, тепер включають багатовимірне кластеризування публікацій, графічне відображення взаємодій ботнетів та тональний аналіз ключових слів із «словника токсичності» на триста слів українською, російською та англійською мовами. Паралельно підрозділ пошуку OSINT відстежує походження зламаних відео та фотографій, ідентифікуючи їх за цифровими водяними знаками та метаданими EXIF. Центр стратегічних комунікацій, у свою чергу, виступає «мечем» державної контратаки. Він відповідає за підготовку єдиних повідомлень, синхронізацію прес-брифінгів міністерств, підготовку медіа-кітів для телеканалів та координацію роботи телемарафону «Об’єднані новини», який цілодобово транслює перевірені дані, оперативні пояснення та рубрику «Розвінчання фейкових новин» [43].

Варто зазначити, що обидві структури, незважаючи на різну відомчу підпорядкованість, використовують спільний хаб даних: він узагальнює інформацію про медіа-тенденції, геолокацію фейкових новин та слухабельність контенту на радіо. Києво-Могилянська академія відзначає цю модель як приклад «горизонтальної бюрократії»: конфлікти між відомствами мінімізуються за допомогою алгоритмічного розподілу доступу, а час реагування в кризових ситуаціях скорочується до декількох хвилин [41, с. 12].

У свою чергу, централізація зовнішньої риторики указом Президента № 671/2021 («правило трьох голосів») стала інструментом «економії комунікацій»: світові редакції отримали чіткий пріоритет офіційних джерел, що унеможливило маніпуляції, коли периферійні чиновники роблять суперечливі заяви. Водночас це створило чіткий ланцюжок відповідальності всередині країни: якщо повідомлення «відхиляється» від стратегічної лінії, джерело стає одразу помітним [40, с. 13]. Однак перші лінії оборони проти російських інформаційних атак були побудовані знизу. Заснована в березні 2014 року, StopFake сьогодні має власну студію в Києві, кореспондентські бюро у Варшаві та Чикаго, а також спеціальні курси для журналістів у Східній Європі. Щотижневі дайджести StopFake, адаптовані десятьма мовами, відстежують не тільки фейки, а й показники їхнього життєвого циклу: середній час поширення, піковий охоплення та рівень спростування. Ці дані надходять до інформаційних панелей Центру протидії дезінформації та корпоративних панелей Meta/Google, що прискорює видалення токсичного контенту [45]. Самі фактчекери називають це «крауд-урядом» – симбіозом волонтерського моніторингу та державної санкційної машини [41, с. 12].

Український кризовий медіацентр став хабом «антикризового контенту» для журналістів AP, AFP, BBC та Al Jazeera: він організовує прес-тури на деокуповані території, надає фотобанки без роялті та оперативну контекстну інформацію. Коли російська пропаганда звинуватила Україну в «обстрілі ЗНПЗ з української сторони», саме фотобанк центру надав супутникові знімки, які спростували версію Кремля, і ці знімки були показані в прайм-тайм на CNN менш ніж за 24 години [44, с. 60]. Такий підхід, відмічений The Guardian, дозволив «Single Telethon» не тільки утримати аудиторію всередині країни, але й стати «головним лектором» для світових ЗМІ, щоб прояснити бойову ситуацію майже в режимі реального часу [48].Спільнота InformNapalm OSINT, яка починалася з чотирьох волонтерів, сьогодні координує понад 600 волонтерів у 25 країнах. Кожна підтверджена ідентифікація російського військовослужбовця потрапляє до загальної бази даних, яку юристи

Генеральної прокуратури використовують у справах про військові злочини. Підхід VBE, тобто «обсяги на основі доказів», якого дотримується InformNapalm, доводить, що навіть відео солдата в TikTok з геолокацією може стати «цеглиною» в стіні доказів для МКС [44, с. 61]. У серпні 2022 року команди Міністерства цифрової трансформації та часу зафіксували, що через платформу crowd-crimeevidence вже було завантажено понад 27 тисяч відеодоказів, а 14 російських військових підрозділів отримали юридично значущі посилання на місця злочинів [49]. Іншим важливим вектором є історичний. Російські ЗМІ систематично поширюють міфи про «спільну імперську долю» або «добровільний союз 1654 року». Проект «LIKVIZ: Історичний фронт» створив цілий «лексикон визволення», де разом із науковцями та блогерами TikTok представлені двохвилинна відеоролики з перевіркою цитат і швидкими QR-посиланнями на архіви ЦРУ, що вже руйнує фейк фактами прямо в смартфоні користувача [44, с. 62]. За власними оцінками проекту, у першій половині 2023 року їхні матеріали набрали 180 мільйонів переглядів на платформах коротких відео, що можна порівняти з розміром всієї російської аудиторії Tik-Tok.

24 лютого 2022 року Україна за лічені години перевела свої телеканали на режим спільного мовлення. Сценарій був написаний восени 2021 року як «картка екстреного мовлення» Центром стратегічних комунікацій. Серед іншого, він передбачає тригодинний цикл оновлення, обов’язкову перевірку фактів з двох незалежних джерел, так зване правило 90 секунд для оперативного спростування та можливість вимкнення потенційно панічних повідомлень [40, с. 15]. За даними дослідниці Іжутової, такий формат у поєднанні з постійною участю президента підвищив індекс довіри до офіційних новин до 87%, що є найвищим показником для України в історії соціологічних досліджень [42, с. 48–49]. Англомовний стрім телемарафону посів перше місце в глобальному рейтингу YouTube-News за кількістю переглядів, отримавши 205 мільйонів переглядів лише з IP-адрес США та Великої Британії. Соціальні медіа стали союзником у цій війні. На активне

прохання Центру протидії дезінформації Meta визначила всі офіційні сторінки українських державних органів як арени з високим рівнем безпеки, активувавши двофакторну модерацію та пріоритетну підтримку. Протягом перших 60 днів війни Meta видалила 6 мереж, що складалися з 3600 фейкових акаунтів, а TikTok видалив понад 4500 відео, в яких ворог поширював панічні чутки про «капітуляцію Києва» [46; 48]. РНБО, підбиваючи підсумки роботи Центру за чотири роки, навела цифру 1,7 млрд загального медіапокриття їхніх пояснень; міжнародні партнери визнають цей обсяг безпрецедентним для країни з населенням 40 млн [47].

Стратегічні наративи змінилися. Якщо на початку війни переважали героїчні та міфологічні історії, то восени 2022 року комунікатори зосередилися на історії «неминучого відновлення»: випадки відновлення Ірпеня, запуск шкіл у Миколаєві та відновлення польотів Київ-Харків попри обстріли стали символами непереможності, які ЗМІ підхопили охочіше, ніж репортажі з передової [40, с. 19–20]. На зовнішньому треку повідомлення змінилися з «закрийте небо» на «інвестуйте в безпеку Європи», що підкріпили дипломатичні тури першої леді та серія емоційних відео для американських сенаторів, після яких Конгрес проголосував за Lend-Lease-2022 [40, с. 20]. Окремий інформаційний вектор спрямований на російських солдатів. Психологічні операції Сил спеціальних операцій створили понад сотню коротких відеороликів із закликами до капітуляції: вони надсилаються через боти Telegram на номери телефонів, знайдені в трофейних смартфонах, і показують алгоритмічно згенеровані версії «шкільних зошитів» та сімейних фотографій, які пропонують «повернутися живими». Статистика ССО показує, що в пікові дні такі матеріали переглянули 1,3 мільйона разів з російських IP-адрес, а частка повідомлень про капітуляцію в цих районах зросла на 17% [40, с. 21]. Система, яка швидко набрала обертів, неминуче зіткнулася з дилемою свободи слова. Деякі журналісти стверджують, що «надмірна централізація» телемарафону знищує конкуренцію форматів. Однак дослідження Данченкової показує, що в пікові моменти масових обстрілів саме редакція

марафону та спільна перевірка фактів запобігли неконтрольованому поширенню чуток про «затоплення» та «витік радіації» [49; 50]. Ресурсна база залишається проблемою: волонтерські OSINT-групи залежать від разових грантів, а журналістам бракує безпечного обладнання для роботи на передовій. Частковим рішенням є партнерство з Investigative Dashboard, гранти USAID на куленепробивні жилети та курси з безпеки, а також стипендії для регіональних репортерів.

До 2025 року українська модель протидії дезінформації вийшла за межі своєї оборонної функції. Вона стала своєрідним національним «експортним продуктом»: навчальні модулі Центру стратегічних комунікацій вже перекладені іспанською та японською мовами, а StopFake почав брати участь у спільних тренінгах з тайванськими фактчекерами щодо придушення авторитарних медіакампаній. Україна переходить від реактивного до проактивного режиму: вона формує «історію майбутнього» про післявоєнну відбудову, демократичні реформи та колективну безпеку і здатна продемонструвати потенціал стати лабораторією стійкості в епоху глобальних інформаційних загроз [40, с. 21, 50].

Значним досягненням української системи протидії дезінформації після 2022 року стало створення та швидке розгортання міжвідомчого Центру стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики України, а згодом – Центру протидії дезінформації при РНБО. Ці структури виконують функцію єдиного аналітично-комунікаційного хабу, який збирає, верифікує та оперативно поширює спростування, формує проактивні меседжі й координує дії десятків державних органів. Завдяки щоденним брифінгам, єдиній базі спростувань та інтеграції з платформами фактчекінгу (StopFake, VoxCheck, «По той бік новин») вдалося суттєво скоротити час реакції на критичні інформаційні атаки – з кількох діб у 2014–2015 рр. до кількох годин у 2023–2025 рр. [40; 41; 44; 45].

Особливо ефективним виявився національний телемарафон «Єдині новини», запущений у перші дні повномасштабного вторгнення. Він не лише

забезпечив єдину редакційну політику та мінімізував суперечливі повідомлення, але й став потужним інструментом горизонтальної координації між центральними й регіональними медіа. За даними моніторингу Detector Media, у перші три місяці війни телемарафон охоплював до 78 % телевізійної аудиторії країни, що дало змогу швидко стабілізувати інформаційне поле в умовах масового шоку та паніки [46; 47].

Не менш важливу роль відіграли волонтерські OSINT-спільноти (InformNapalm, Molfar, «КіберБеркут-2.0» (український), проєкти Bellingcat за участі українських дослідників). Вони не лише фіксували воєнні злочини та ідентифікували російську техніку, але й створювали доказову базу, що використовується в міжнародних судах і дипломатичній роботі. З 2023 року більшість цих команд отримали офіційний статус партнерів державних структур, що дозволило легалізувати обмін розвідданими та інтегрувати їхні напрацювання в офіційні звіти РНБО та МЗС [95; 96; 97].

Цифрова диплом 2.0 – використання лідерами держави (Президент, МЗС, Міноборони) соціальних мереж для прямого спілкування з глобальною аудиторією – стала одним із найуспішніших кейсів українського StratCom. Акаунти Володимира Зеленського, Дмитра Кулеби та Михайла Подоляка входять до світового топ-10 за охопленням серед політиків, а україномовний контент у TikTok та Instagram у 2022–2023 рр. перевищив російськомовний пропагандистський за вірусністю у 4–6 разів (дані Atlantic Council DFRLab). Така стратегія дозволила не лише нейтралізувати значну частину російських наративів, але й сформувати нову глобальну рамку сприйняття війни – від «регіонального конфлікту» до «битви демократії проти авторитаризму» [48; 49; 92].

Отже, українська система стратегічних комунікацій та протидії дезінформації за короткий термін пройшла шлях від фрагментованої реактивної моделі до гнучкої, багатошарової та проактивної архітектури, яка органічно поєднує державні інституції, громадський сектор і міжнародних

партнерів. Цей досвід вже визнаний НАТО та ЄС як один із найуспішніших прикладів кризового StratCom у сучасній історії [51; 58; 62].

2.3. Міжнародний контекст боротьби з російською пропагандою

Інформаційна агресія Росії змінила традиційні уявлення про безпеку: сьогодні не тільки стабільність окремих держав, а й довіра до демократичних процесів у всьому світі залежать від узгодженості міжнародних протидії. З 2014 року Захід перейшов від «обережного спостереження» за кампаніями Кремля до усвідомлення того, що системна дезінформація є інструментом впливу, порівнянним із традиційними засобами тиску [51, с. 3–17].

Ілюстративні хакерські атаки, такі як анексія Криму, втручання у європейські вибори 2014–2016 років та численні масштабні кібератаки, стали очевидним свідченням того, що гібридні тактики Кремля давно вийшли за межі традиційного політичного протистояння і перетворилися на транснаціональне явище. Їхній характер демонструє, що сучасні інформаційні загрози не обмежуються окремими регіонами і не прив’язуються до конкретних часових рамок. Навпаки, вони поширюються через міждержавні цифрові інфраструктури, використовують слабкі ланки у різних секторах та об’єднують у собі політичні, економічні й технологічні інструменти. Атаки на енергетичні системи, державні реєстри, виборчі платформи та медіасередовище свідчать про те, що їхня мета виходить далеко за межі короткострокового завдання. Вони створюють поле постійної вразливості, у якому будь який інцидент може стати каталізатором більшого інформаційного або політичного зрушення.

Поширення таких операцій продемонструвало, що окремі держави не здатні ефективно протистояти подібним загрозам самотужки. Кіберпростір не визнає територіальних кордонів, а тому будь який напад на одну країну потенційно зачіпає інтереси інших. Атаки на виборчі процеси в ЄС, втручання у комунікаційні мережі провідних західних медіа чи спроби маніпулювати політичними настроями в окремих державах показали, що слабкість одного

учасника міжнародної спільноти створює можливості для тиску на всіх інших. Нерівномірність технологічної підготовки, різні підходи до регулювання цифрових платформ і відсутність єдиних стандартів безпеки лише підсилюють ефект уразливості. Саме тому такі інциденти стали поштовхом до усвідомлення необхідності спільної відповідальності та координації дій між державами, технологічними компаніями й оборонними структурами.

У результаті міжнародне співтовариство все активніше визнає, що гібридні загрози потребують колективної відповіді не лише як політичної декларації, а як інструменту практичної безпеки. Це означає не просто обмін інформацією про інциденти, а розбудову спільних аналітичних хабів, удосконалення систем раннього попередження, вироблення єдиних правил взаємодії та стандартів реагування. Кожен новий епізод російської інформаційної або кібернетичної агресії підтверджує, що без скоординованих зусиль на рівні ЄС, НАТО та глобальних партнерств виникає ризик фрагментації, яку Кремль може використати на свою користь. У цьому сенсі атаки, що колись сприймалися як окремі інциденти, сьогодні постають як елементи ширшої стратегії, яка потребує узгоджених міжнародних рішень та довгострокових стратегій стримування. Власне цим пояснюється рух до створення комплексної системи глобальної стійкості, де кожна країна функціонує не ізольовано, а як частина взаємопов’язаної мережі оборони проти гібридних загроз [52, с. 3].

У відповідь було сформовано цілу низку ініціатив – від трансатлантичної співпраці та «м’яких» регуляторних кодексів до санкцій проти медіахолдингів і можливості НАТО розглядати дезінформаційні кампанії як привід для консультацій за статтею 5.

Першою системною реакцією ЄС став План дій зі стратегічних комунікацій 2015 року, який заклав основу для Східної робочої групи StratCom, невеликого, але мобільного підрозділу Європейської служби зовнішніх справ (ЄСЗС) [58; 55; 56]. Сила групи полягає в її мультидисциплінарності: дипломати, журналісти, ІТ-аналітики та лінгвісти

об’єднані в «рейдові» команди для швидкого аналізу фейків у Східному партнерстві та в межах ЄС [58]. Ідея East StratCom – це портал EUvsDisinfo, який на даний момент містить понад 17 тисяч проаналізованих наративів і використовується як навчальний масив даних для десятків університетів та НУО, що займаються перевіркою фактів [61]. На регуляторному рівні ключовими кроками стали План дій проти дезінформації 2018 року та добровільний Кодекс практики щодо дезінформації. Цей кодекс, що охоплює Facebook, Google, Microsoft, Twitter/X, Mozilla, TikTok та інші платформи, вперше зобов’язав платформи публічно перевіряти алгоритми рекомендацій та прозорість політичної реклами [58]. У 2022 році ЄС пішов далі і заблокував RT і Sputnik на всіх типах медіа, хоча медіахолдинг негайно розгорнув мережу «дзеркал» – понад 200 клонів сайтів у різних доменних зонах [54, с. 100–105]. Це довело, що без паралельного технічного демпінгу та освітніх кампаній регуляторні заборони лише частково стримують пропагандистські мережі.

У 2023–2024 роках Європейська комісія, ще більше поглибивши співпрацю з Big Tech, створила «багатомовний канал фейкових новин»; алгоритм ранжує фейки за потенційною шкодою і надсилає цифровим платформам сповіщення про високий ризик протягом < 30 хвилин після виявлення [53, с. 1–13]. Крім того, було започатковано ініціативу «Фонд стійкості ЗМІ та інформації» – інструмент грантового фінансування незалежних редакцій у Східній Європі, який вже профінансував 74 місцеві проєкти (від подкастів білоруською мовою до кримськотатарських каналів на YouTube). Альянс офіційно закріпив принцип «потрійного результату» – підготовка, стримування, оборона – у Декларації саміту в Уельсі 2014 року, але лише після Варшави 2016 року гібридна атака була чітко включена до можливих підстав для консультацій відповідно до статті 5 [51, с. 14–16]. Поворотним моментом стало відкриття StratCom CoE в Ризі, яке вперше зібрало військових стратегів, психологів та експертів з цифрової криміналістики. Центр тестує «червоні команди» – симуляції російських IPSO

проти держав–членів, щоб перевірити стійкість інфраструктури та алгоритм співпраці між прес-службами та кіберкомандами [61].

Аналітичну підтримку надає Спільний відділ розвідки та безпеки (Joint Intelligence & Security Division, JIS), «мозковий центр», який збирає дані від союзників, комерційних операторів супутників та відкритих соціальних мереж. Коли влітку 2023 року прокремлівські акаунти поширили фейк про «українську хімічну зброю» в Херсоні, JIS-Division за 28 хвилин, до того як тема стала трендом у Twitter/X, створила флеш-сповіщення, що дозволило прес-службам Альянсу синхронно відреагувати [51, с. 11]. Найпотужнішою незалежною лабораторією є Європейський центр передового досвіду з протидії гібридним загрозам (Hybrid CoE) у Гельсінкі: тут моделюються сценарії, що варіюються від енергетичного шантажу до етнічних маніпуляцій [51, с. 16]. 35 країн-учасниць беруть участь у спільних «песимістичних іграх» – симуляціях, що перевіряють, наскільки швидко демократичні уряди координують свої кроки в умовах інформаційного саботажу. У 2021 році до мережі приєднався Євроатлантичний центр стійкості (Бухарест): він зосереджується на стандартах «стійкості за дизайном» (вбудована стійкість систем комунікації, енергетики та ЗМІ) і навчає експертів із 120 установ [51, с. 11]. Механізм антигібридних груп підтримки став прагматичним інструментом: за запитом уряд отримує 10-15 фахівців (аналітиків OSINT, юристів, кіберфахівців), які допомагають розгорнути кризовий штаб для протидії вторгненням протягом трьох тижнів; цією послугою скористалися Литва, Чорногорія та Північна Македонія [51, с. 11–12].

Перша спільна декларація 2016 року містила 20 конкретних завдань для протидії гібридним загрозам, але бюрократичні суперечки та різні рівні загрози серед членів уповільнили прогрес. У 2023 році було додано ще 11 ініціатив: обмін даними в режимі реального часу про бот-ферми, спільні курси з психології впливу для дипломатів та єдина мережа кризових комунікацій [62]. Однак розрив між політичною риторикою та оперативною реалізацією залишається: уряди Угорщини та Кіпру, наприклад, блокують певні рішення

щодо санкцій проти ЗМІ, посилаючись на «захист плюралізму» [51, с. 16–17]. G7 RRM діє за межами євроатлантичного простору як гаряча лінія для обміну сигналами про дезінформаційні кампанії. У 2024 році RRM зафіксувала трикратне збільшення кількості прокремлівських втручань в Європі та відзначила різке зростання атак на Індо-Тихоокеанський регіон, що дало поштовх до створення проекту Indo-Pacific InfoShield, який включає Австралію та Японію в спільну аналітику [60, с. 1; 66, с. 1]. Наприклад, Міністерство закордонних справ Японії запустило публічну інформаційну панель маніпулятивних наративів про «американські біолабораторії в Окінаві» і співпрацює з TikTok для забезпечення локальної модерації [60]. У 2022 році представник ОБСЄ з питань свободи ЗМІ заявив, що незаконна дезінформація під час війни підриває право громадян на доступ до правдивої інформації, закликаючи до «мікроцільового» регулювання – блокування контенту, але не «колективного» покарання журналістів [68, с. 1–2]. ОБСЄ просуває ідею «позитивних зобов'язань» держав: підтримувати якісні ЗМІ та медіаграмотність замість суто заборонних практик.

Метааналіз 250 000 перевірок фактів 95 мовами показав, що більшість фейків перевіряються лише один раз, а щонайменше 12 % фейків потребують повторного спростування – це «важкі» наративи, які постійно поширюються (про «таємні біолабораторії», «радіоактивні бомби» тощо) [53, с. 3]. Інструменти машинного перекладу суттєво прискорили глобальне переміщення дезінформації. Те, що раніше потребувало участі перекладачів або цілих редакцій, тепер відбувається майже автоматично: одна й та сама фейкова історія за два дні з'являється п'ятнадцятьма чи навіть двадцятьма мовами. Цей процес перетворює локальний інформаційний вкид на міжнародний феномен, який миттєво охоплює аудиторії з різними культурними контекстами та рівнями медіаграмотності. У таких умовах інформаційний простір стає непрозорим, а різні суспільства паралельно отримують майже однакові маніпулятивні повідомлення, що ускладнює не лише їх спростування, а й саму можливість вчасно відстежити момент

поширення. На цьому тлі середній час, необхідний для глобальної перевірки фактів, виглядає надто тривалим. П’ять днів, які зазвичай потрібні міжнародним командам фактчекерів, стають критичною затримкою, адже за цей період фейк устигне не просто охопити значні аудиторії, а й закріпитися у вигляді так званої псевдоправди.

Така асиметрія між швидкістю поширення та швидкістю спростування змушує держави та міжнародні організації шукати нових підходів. Виникає потреба у створенні багатомовних швидких каналів реагування, які здатні не лише дублювати спростування кількома мовами, а й робити це максимально синхронно. Йдеться про розробку спільних глосаріїв небезпечних наративів, що допомагають оперативно розпізнавати знайомі патерни, а також про узгоджені міжплатформні чорні списки URL адрес, що містять систематичну дезінформацію. Такі інструменти могли б зняти частину навантаження з фактчекерів та забезпечити більшу однаковість у протидії фейкам на різних мовних ринках. Водночас потреба у швидкодіючих механізмах є не лише технічним викликом. Це питання координації між державами, які мають різний рівень політичної готовності до спільних рішень та різні уявлення про межі регулювання інформаційного простору.

Саме тому політична воля стає не менш важливим елементом протидії, ніж технологічні можливості. Приклад рішення Державного департаменту США у 2025 році призупинити меморандуми про боротьбу з дезінформацією з європейськими партнерами показав, наскільки чутливою є міжнародна система до таких кроків. Аналітична спільнота охарактеризувала це як своєрідне одностороннє роззброєння, адже відмова від координації створює інформаційний вакуум, який швидко заповнюють прокремлівські мережі. За відсутності спільних протоколів реагування будь яке послаблення трансатлантичної взаємодії надає пропагандистам можливість відновлювати вплив у тих сферах, де напрацьовані механізми до цього вже працювали ефективно. У результаті проблема перестає бути технічною і перетворюється

на кризу довіри та відповідальності, що ставить під загрозу стабільність усієї системи демократичної інформаційної безпеки [60].

Різні інтерпретації загрози: від Угорщини до Словенії деякі уряди розглядають пропаганду як «бічний шум», тоді як внутрішні політичні актори використовують її як інструмент мобілізації електорату [51, с. 16–17]. Бюрократична інерція: ЄС потрібно в середньому 67 днів, щоб прийняти один пакет санкцій, тоді як прокремлівські мережі змінюють свій домен і стиль за 48 годин; Процедури класифікації інформації НАТО також уповільнюють публічну комунікацію. Міжнародна екосистема протидії російській пропаганді перетворилася на складну мозаїку регуляторних ініціатив, військових центрів передового досвіду, мереж перевірки фактів та пакетів санкцій. Її сильна сторона – у різноманітності інструментів, а слабка – у розриві між швидкістю демократичних процедур та маневреністю авторитарних машин дезінформації. Подальший успіх полягає в «моделі швидкої співпраці»: децентралізованих хабах даних, обов'язковому обміні телеметричними даними між великими технологічними компаніями та урядами, автоматизованому перекладі спростувань та кристалізації політичної волі, яка може подолати короткострокові розбіжності.

Визнання російської дезінформації системною загрозою на рівні Європейського Союзу та НАТО сталося саме завдяки українському досвіду 2014–2022 років. Уже в 2015 році Європейська служба зовнішніх дій створила Східну робочу групу зі стратегічних комунікацій (East StratCom Task Force), а згодом – портал EUvsDisinfo, який за десять років зафіксував понад 18 000 випадків кремлівської дезінформації, з яких понад 40 % стосувалися України [58; 61]. Ця база даних стала не лише інструментом моніторингу, але й навчальним корпусом для десятків фактчекінгових організацій у Європі та світі. У 2022–2025 роках ЄС суттєво посилив регуляторні механізми: Кодекс практики щодо дезінформації трансформувався у обов'язковий Закон про цифрові послуги (Digital Services Act), який запровадив жорсткі вимоги до прозорості алгоритмів, швидкого видалення шкідливого контенту та щорічної

звітності найбільших платформ. Українські експерти брали безпосередню участь у розробці цих норм, а Україна стала пілотною країною для тестування механізмів «швидкого реагування» на транснаціональні кампанії [51; 103].

НАТО, у свою чергу, після Бухарестського саміту 2016 року та особливо після Мадридського саміту 2022 року офіційно визнало інформаційний і когнітивний простір окремим операційним доменом поряд із сушею, морем, повітрям, космосом і кіберпростором. Центр передового досвіду зі стратегічних комунікацій у Ризі (StratCom COE) та Гібридний центр передового досвіду у Гельсінкі (Hybrid CoE) розробили низку доктринальних документів, у яких український кейс займає центральне місце. З 2023 року Україна отримала статус партнера з розширеними можливостями (Enhanced Opportunity Partner) саме у сфері StratCom та протидії гібридним загрозам, що відкрило доступ до закритих навчань, спільних таблиць раннього попередження та обміну розвідданими в реальному часі [62; 63].

Особливо цінним виявився досвід спільних навчань «Locked Shields» (кіберзахист) та «Coherent Resilience» (StratCom + кібер), де українські команди неодноразово перемагали або входили до трійки лідерів, демонструючи найвищий рівень оперативної сумісності. У 2024–2025 роках НАТО запустило спеціальну програму «Ukraine StratCom Support Package», що передбачає не лише навчання, а й постачання захищених комунікаційних систем, програмного забезпечення для моніторингу інформаційного простору та створення резервних каналів зв’язку для державного мовлення в умовах блекаутів [62].

Важливим напрямом міжнародної підтримки стало фінансування та інституційна допомога українському фактчекінговому сектору. Європейський фонд за демократію (EED), International Renaissance Foundation, National Endowment for Democracy та уряди Великої Британії, Канади й Нідерландів з 2022 року виділили понад 28 млн євро на розвиток StopFake, VoxCheck, Detector Media, Texty.org.ua та нових проєктів, таких як «По той бік новин» і «НотаЄнота». Ці організації не лише спростовують фейки, а й створюють

україномовний та багатомовний контент (англійська, німецька, французька, арабська), який використовується дипломатичними представництвами України та партнерами для контрнаративів [41; 45; 52].

Окремо варто відзначити роль Великої Британії та США у створенні та підтримці міжнародних OSINT-коаліцій. Проєкти Bellingcat, Atlantic Council DFRLab, Institute for Strategic Dialogue та Graphika за активної участі українських дослідників (InformNapalm, Molfar, Центр оборонних реформ) розкрили десятки мереж російських тролів, ботів і фейкових медіа в Європі та Латинській Америці. У 2024 році спільне розслідування Bellingcat та українських партнерів щодо діяльності російських «фабрик тролів» у Гані та Нігерії призвело до блокування понад 4000 акаунтів і зміни політики TikTok у країнах Африки [95; 96].

Позитивним прикладом регіональної солідарності стала ініціатива країн Балтії та Польщі «Baltic–Ukrainian StratCom Initiative» (2023–2025), у рамках якої Литва, Латвія, Естонія та Польща діляться досвідом протидії російській пропаганді ще з 2007–2014 років, надають технічну допомогу у створенні захищених дата-центрів за межами України та спільно фінансують україномовне мовлення на тимчасово окуповані території через супутник і FM [62].

Таким чином, російсько-українська інформаційна війна стала каталізатором доктринальних і регуляторних змін у всьому демократичному світі. Україна вже не є лише реципієнтом допомоги – вона перетворилася на одного з ключових генераторів знань і практик у сфері стратегічних комунікацій та когнітивної оборони. Її модель швидкого реагування, інтеграції державного, громадського та міжнародного рівнів, а також здатність зберігати свободу слова навіть в умовах воєнного стану визнається експертами ЄС і НАТО як «золотий стандарт» кризового StratCom у XXI столітті [51; 58; 62]. Цей досвід не лише зміцнює інформаційну стійкість самої України, а й формує нові глобальні норми протидії державно-спонсорованій дезінформації та гібридним загрозам.

Висновки до розділу 2

Другий розділ присвячений емпіричному аналізу інформаційного виміру російсько-української війни та демонструє, що цей вимір є повноцінним і самостійним театром воєнних дій, який за масштабами, ресурсами та стратегічною вагою не поступається кінетичному фронту.

Російська інформаційна агресія проти України має чітко визначену ієрархію цілей: від короткострокової деморалізації населення і ЗСУ до довгострокового підриву легітимності української державності та міжнародної підтримки. Вона спирається на комплексний інструментарій: дезінформацію, маніпуляцію історичною пам’яттю, пропаганду, кібероперації та імітацію громадської думки. Координація здійснюється вертикально через Адміністрацію Президента РФ, спецслужби та державні медіахолдинги, а синхронізація інформаційних хвиль з військовими діями стала характерною ознакою російської гібридної стратегії. Після 2022 року значно зросла роль соціальних платформ (особливо Telegram і TikTok), штучного інтелекту (deepfake, автоматизовані бот-мережі) та роботи з аудиторіями Глобального Півдня.

У відповідь Україна за короткий термін сформувала одну з найефективніших у світі систем стратегічних комунікацій та протидії дезінформації. Ключовими елементами стали: Центр стратегічних комунікацій та інформаційної безпеки, Центр протидії дезінформації при РНБО, національний телемарафон «Єдині новини», потужна екосистема незалежного фактчекінгу (StopFake, VoxCheck, Detector Media) та волонтерські OSINT-спільноти (InformNapalm, Molfar). Ці структури забезпечили скорочення часу реакції на інформаційні атаки до кількох годин, проактивне формування контрнаративів та горизонтальну координацію між державою і громадянським суспільством. Особливо успішним виявився досвід цифрової дипломатії: пряме звернення керівництва держави до світової аудиторії через соціальні мережі дозволило перехопити ініціативу в

глобальному наративі та сформувати рамку «війни демократії проти авторитаризму».

Міжнародний контекст став вирішальним фактором посилення української інформаційної стійкості. Досвід України 2014–2022 років стимулював створення та розвиток ключових європейських і євроатлантичних інституцій: East StratCom Task Force і EUvsDisinfo (ЄС), StratCom COE у Ризі та Hybrid CoE у Гельсінкі (НАТО). Закон про цифрові послуги (DSA), визнання когнітивного простору окремим операційним доменом НАТО, спільні навчання та програми підтримки (Ukraine StratCom Support Package) є прямим наслідком українського кейсу. Водночас Україна отримала безпрецедентний доступ до розвідданих, захищених комунікаційних систем, фінансування фактчекінгу та спільних OSINT-розслідувань. Країни Балтії, Польща, Велика Британія, США та Канада стали найактивнішими партнерами, а українські команди регулярно входять до лідерів найбільших кібер- та StratCom-навчань світу.

Таким чином, російсько-українська інформаційна війна вже змінила глобальні підходи до протидії державно-спонсорованій дезінформації. Українська модель, яка поєднує швидке державне реагування, потужний громадський сектор і тісну інтеграцію з партнерами, визнається експертами ЄС і НАТО як найбільш успішний приклад кризових стратегічних комунікацій у сучасній історії. Цей досвід не лише забезпечив Україні стійкість у найскладніших умовах, але й став важливим внеском у формування нової архітектури європейської та євроатлантичної безпеки в цифрову епоху.

Розділ 3. Виклики, прорахунки та рішення у сфері інформаційної безпеки України

3.1 Основні проблеми формування інформаційної політики у воєнний час

Формування та реалізація ефективної державної інформаційної політики в умовах військового конфлікту перетворюється на одну з найскладніших проблем сучасного державного управління. Ідеться не лише про здатність оперативно реагувати на зовнішні загрози, а й про уміння вибудовувати стійку, послідовну і водночас гнучку комунікаційну архітектуру, яка здатна витримувати тривале навантаження. Російсько-українська війна, що перейшла у фазу повномасштабного вторгнення у 2022 році, дуже швидко продемонструвала, що інформаційний вимір конфлікту має таку ж вагу, як і суто військові дії. Він визначає динаміку реакцій суспільства, впливає на рішення політичного керівництва, формує міжнародну підтримку і здатний кардинально змінювати хід подій, навіть не торкаючись фізичного поля бою. Саме тому ефективність державної інформаційної політики стає одним із ключових чинників національної стійкості.

Водночас війна висвітлила структурні вади, що накопичувалися роками. Виявилося, що механізми інформаційної безпеки не завжди здатні діяти швидко, чітко й злагоджено. Частина державних інституцій не мала достатньо відпрацьованих процедур кризової комунікації, а загальна система стратегічних комунікацій потребувала суттєвої модернізації. Багато проблем, які раніше видавалися другорядними, набули критичного значення. Наприклад, повільне спростування фейків або розпорошеність офіційних повідомлень могли спричинити панічні настрої, посилити плутанину або створити вразливі місця для зовнішнього впливу. Криза показала, що інформаційна політика не може бути набором окремих реактивних дій. Вона має функціонувати як єдина стратегічна система, яка синхронізує дії державних структур, медіа, експертних спільнот і громадянського суспільства.

На відміну від класичних форм військового протистояння, сучасна гібридна війна працює через симбіоз різних інструментів впливу. Військові атаки супроводжуються політичним тиском, економічними шантажами, психологічними операціями і, що важливіше за все, комплексною інформаційною кампанією, яка задає тон інтерпретацій подій. Інформаційна агресія виступає не просто фоновим явищем, а окремим театром дій, де вирішується питання довіри, легітимності, моральної стабільності і загального імунітету суспільства до маніпуляцій. На цьому полі інформація діє як зброя, що формує сприйняття, створює емоційні реакції, руйнує впевненість і підштовхує до потрібних рішень. Саме у цьому вимірі визначається здатність держави зберігати внутрішню єдність, контролювати інформаційний простір і протистояти зовнішньому впливу, який намагається підірвати основи її політичної та соціальної стабільності [63, с. 20–26; 64, с. 121–127].

Саме тому ефективність державної інформаційної політики в умовах війни визначає не тільки успіх на фронті, а й здатність суспільства зберегти єдність, стійкість до дезінформації та впевненість у власній державності.

Однією з ключових проблем формування інформаційної політики в умовах війни є фрагментація та нескоординованість системи інформаційної безпеки. Протягом багатьох років в Україні було створено численні інституції, відповідальні зарізні аспекти інформаційної політики, але між ними не було розроблено скоординованого підходу. Кабінет Міністрів, Міністерство культури та інформаційної політики, Служба безпеки України, Збройні сили України, Національна рада з питань телебачення і радіомовлення та Центр стратегічних комунікацій та інформаційної безпеки часто діють паралельно, іноді з дублюванням функцій [65, с. 41–45; 66, с. 53–60]. В результаті формується складна система, в якій дублюються зусилля, марнуються ресурси, а публічні повідомлення різних державних структур можуть суперечити одне одному.

Така нескоординованість підриває довіру до офіційних джерел і створює вразливі місця, які активно використовуються ворогом. На думку Лешика,

інституційний та правовий механізм інформаційної політики України все ще перебуває на початковому етапі, а її європейська інтеграція в галузі інформаційної безпеки потребує синхронізації з правовою базою ЄС [67, с. 53–60]. У цьому контексті можна також згадати Указ Президента № 152/2022, спрямований настворення єдиної системи координації державних комунікацій, але практична реалізація цих положень зіткнулася з бюрократичними перешкодами [68,с. 150–155]. Недофінансування та слабка ресурсна база становлять другу фундаментальну проблему інформаційної політики в умовах війни. Більшість структур, відповідальних за захист інформації, працюють в умовах нестачі коштів, персоналу та технічних ресурсів. Така ситуація призводить до обмежень у проведенні інформаційно-аналітичних досліджень, недосконалості систем моніторингу ЗМІ та відсутності сучасних технологій для виявлення та нейтралізації фейкових наративів [69, с. 58–64]. У той час як країни НАТО, США чи Велика Британія активно використовують штучний інтелект та машинне навчання для аналізу потоків дезінформації, в Україні такі інструменти здебільшого перебувають на стадії пілотних проектів [70, с. 68–85].

На думку В. Наместника, лише комплексна державна підтримка дозволить перейти від реактивних до проактивних дій у сфері інформаційної безпеки, коли загрози не просто відстежуються, а й прогнозуються за допомогою великих даних [71, с. 114–121]. Однак навіть за наявності технологічних інструментів ефективність інформаційної політики залишається обмеженою через низький рівень медіаграмотності населення. Медіаграмотність як соціокультурний інструмент формування інформаційного імунітету є критично важливою передумовою національної безпеки, оскільки інформаційна війна ведеться не тільки проти державних інститутів, а насамперед проти свідомості громадян [72, с. 194–205]. Дослідження показують, що понад дві третини українців не мають стійких навичок перевірки джерел, що робить їх вразливими до дезінформаційних кампаній [73, с. 1–8]. Це особливо небезпечно в кризових ситуаціях, коли

паніка, емоційний тиск і втома призводять до посилення віри в неправдиві повідомлення.

У підручнику «Медіаграмотність у воєнний час» [74, с. 1–8] наголошується, що формування критичного мислення має стати частиною державної освітньої політики, починаючи зі школи. Водночас наукові праці Жаровської І. та Ортинської Н. вказують, що феномен інформаційної війни як явище глобалізації вимагає міждисциплінарного підходу, оскільки сучасні інформаційні впливи виходять далеко за межі ЗМІ в їх традиційному розумінні [75, с. 33–42]. Друга проблема передбачає пошук балансу між свободою слова та потребами безпеки. Під час війни держава має об’єктивну потребу обмежувати поширення певних видів інформації, що стосуються військових операцій, розгортання сил або інших стратегічних аспектів [76, с. 1–10]. Однак такий контроль, у свою чергу, викликає напругу з боку правозахисних організацій, які застерігають від надмірної цензури та політичних зловживань.

На думку Авдєєвої Т. та Дворового М., інформаційна відповідальність у воєнний час має подвійний характер: з одного боку, держава зобов’язана запобігати розголошенню військових таємниць, а з іншого – не може перетворювати обмеження на інструмент придушення громадського контролю [77, с. 139–140]. Права на свободу вираження поглядів, передбачені міжнародними документами, такими як Конвенція про захист прав людини і основних свобод, повинні співіснувати з вимогами інформаційної безпеки. Технічне переобладнання та кіберзагрози становлять ще один чутливий аспект. Відомо, що Росія активно проводить кібератаки на урядові вебсайти, енергетичну інфраструктуру, банківські системи і навіть мережі місцевих органів влади [68, с. 150–155]. Зафіксовано тисячі спроб несанкціонованого доступу до баз даних, DDoS-атак та спроб проникнення в телекомунікаційні системи. Однак матеріально-технічна база багатьох державних органів все ще застаріла. Наявність застарілих програмних продуктів без сучасних протоколів шифрування створює критичну вразливість. Для її подолання, як підкреслює О. Ніцевський, необхідне систематичне впровадження стандартів

кібербезпеки, сертифікація ІТ-рішень та тісна співпраця з приватним сектором, який володіє передовими технологіями [78, с. 47–54].Координація з міжнародними партнерами є важливою умовою ефективної інформаційної політики. Однак Україна ще не досягла достатнього рівня узгодженості у своїх стратегічних комунікаціях з НАТО та ЄС. На думку І. Соловея, стратегічні комунікації повинні стати не тільки технічним інструментом поширення інформації, а й філософією публічної дипломатії [79]. Західні партнери, підтримуючи Україну, іноді транслюють власні інтерпретації подій, що спричиняє комунікаційні розбіжності в міжнародному медіапросторі. Для подолання цього необхідна інституціоналізація механізмів міждержавної координації, зокрема створення спільних аналітичних центрів або «інформаційних штабів» за зразком StratCom у країнах Балтії [80, с. 53–59]. Не менш небезпечним є явище політизації інформаційної політики. В умовах війни інформаційні ресурси часто використовуються політиками для вирішення власних PR-проблем або для удару по опонентах.

Це призводить до спотворення інформаційного простору, втрати об’єктивності та зниження довіри до офіційних каналів [64, с. 121–127]. Згідно з аналізом Т. Кобець, популізм у сфері інформаційної політики знижує ефективність стратегічних комунікацій, оскільки інформаційний контент стає емоційно зарядженим, але втрачає будь-яку аналітичну цінність [81, с. 123–127]. Запобігти цьому можна лише шляхом підвищення прозорості, незалежного аудиту державних інформаційних кампаній та громадського контролю за дотриманням стандартів. Слід також зазначити недостатнє використання потенціалу соціальних мереж та цифрових платформ: тоді як ворог активно використовує Telegram, YouTube, TikTok та X для поширення своїх повідомлень, державні комунікації в Україні переважно відбуваються в телевізійному та друкованому форматах. Цифрові медіа вже давно є основним засобом отримання та поширення інформації серед молоді та міжнародної спільноти [82, с. 42–67].

Як довів А. Мойсяха, ефективне використання соціальних медіа в державному управлінні здатне не тільки посилити інформаційну стійкість суспільства, але й підвищити рівень довіри громадськості до уряду [83, с. 33–42]. Однак для цього необхідна професійна підготовка фахівців з цифрових стратегічних комунікацій та створення окремих кризових команд для реагування на фейки.Водночас інформаційна політика повинна враховувати соціальний вимір. Як підкреслює В. Статтарах, ефективність державної інформаційної політики вимірюється не тільки технічними показниками, а й рівнем соціальної мобілізації населення [84, с. 106–115]. Саме соціальна довіра та відчуття причетності до спільної боротьби є нематеріальною основою, на якій базується інформаційна стійкість. Під час війни інформаційна політика стає елементом морального фронту - вона не тільки інформує, але й консолідує суспільство навколо спільної мети.

На закінчення слід зазначити, що основні виклики, пов’язані з формуванням інформаційної політики України в умовах війни, охоплюють значно ширший спектр питань, ніж може здатися на перший погляд. Йдеться не лише про інституційну спроможність, удосконалення законодавства чи розвиток технічної інфраструктури. У центрі уваги опиняються також соціокультурні процеси, рівень суспільної довіри, стан освітньої системи та здатність держави зберігати етичні стандарти навіть у моменти найвищої напруги. Війна відкрила вразливі місця, які довгий час залишалися непомітними, і водночас показала, що інформаційна політика має бути не просто системою реакції на загрози, а простором, де формуються довгострокові орієнтири розвитку, комунікаційні норми та культура взаємодії держави із суспільством.

Подолання цих проблем потребує по-справжньому системного підходу. Координація між різними державними структурами має вийти за межі формальних процедур і перетворитися на живий механізм постійної взаємодії, де дані, аналітика та рішення циркулюють без затримок і дублювання. Підвищення рівня медіаграмотності повинно стати елементом освіти на всіх її

рівнях та одночасно частиною щоденних практик громадян, які потребують не лише інформації, а й уміння працювати з нею відповідально і критично. Важливим стає також впровадження сучасних технологій, здатних автоматично виявляти дезінформаційні кампанії, аналізувати аномальні комунікаційні патерни та передбачати можливі вектори атак.

Зовнішній контекст не менш важливий. У сучасному світі інформаційна безпека є неможливою в межах однієї країни, тому Україна потребує розширення партнерських зв'язків як з європейськими інституціями, так і з міжнародними організаціями, технологічними компаніями та глобальними фактчекінговими мережами. Така співпраця не лише збільшує резильєнтність держави, а й підсилює довіру до українських позицій у міжнародній спільноті. Компонент стратегічних комунікацій має перетворитися на невід'ємну частину державної політики, що працює постійно, а не лише в кризові миті, і забезпечує чіткість, послідовність та узгодженість повідомлень для внутрішньої і зовнішньої аудиторій.

Тільки поєднавши всі ці напрями в єдину логічну систему, Україна зможе розбудувати повноцінну та інтегровану інформаційну безпеку. Вона повинна не просто стримувати російську інформаційну агресію, а й випереджати її, формуючи стійкі механізми захисту правди, підтримуючи високий стандарт державних комунікацій та зберігаючи відкритість, яка є фундаментальною для демократичного суспільства. Важливо також забезпечити, щоб свобода слова та безпека не конфліктували між собою. Навпаки, вони мають взаємно підсилювати одна одну, створюючи простір, у якому громадяни отримують достовірну інформацію, а держава може діяти ефективно, прозоро і відповідально. Такий баланс стає не лише передумовою інформаційної стійкості, а й важливим кроком до зміцнення довіри та консолідації суспільства в умовах тривалої війни.

Ще одним системним викликом залишається недостатня інтеграція стратегічних комунікацій у загальну систему управління державою в умовах війни. Незважаючи на створення профільних центрів, процес ухвалення

рішень щодо інформаційної політики часто відбувається фрагментарно, без обов'язкового врахування StratCom на рівні Ставки Верховного Головнокомандувача чи засідань РНБО. Це призводить до ситуацій, коли важливі військові чи дипломатичні кроки здійснюються без попередньої підготовки інформаційного поля, що дає противнику можливість першим сформувати інтерпретаційну рамку. Наприклад, у 2023–2024 роках низка оперативних подій на фронті супроводжувалася затримкою офіційних коментарів на 12–48 годин, що дозволяло російським джерелам заповнити інформаційний вакуум власними наративами [40; 86; 93].

Серйозною проблемою є також кадровий дефіцит фахівців з кризових комунікацій та аналітиків інформаційного простору в державних органах. За оцінками Центру стратегічних комунікацій, станом на 2025 рік лише 15–20 % посад у пресслужбах міністерств і відомств сектору безпеки займають профільні спеціалісти з досвідом StratCom чи цифрової аналітики. Решта – це переважно журналісти або піар-фахівці мирного часу, які не завжди здатні працювати в умовах високої інтенсивності та жорстких дедлайнів [40; 99].

Не менш гостро стоїть питання фінансування. Хоча в умовах воєнного стану бюджетні пріоритети зрозуміло змістилися на користь оборони, інформаційна безпека досі фінансується за залишковим принципом. У 2023–2025 роках видатки на StratCom та протидію дезінформації становили менше 0,07 % від загального бюджету сектору безпеки і оборони, що в десятки разів менше, ніж у країн НАТО за аналогічними статтями. Це обмежує можливості закупівлі сучасних систем моніторингу, захищених каналів зв'язку та розвитку власних медіаактивів [101; 102].

Нарешті, зберігається недостатній рівень міжвідомчої цифрової сумісності. Багато державних структур досі використовують різні, несумісні системи документообігу, моніторингу та комунікації, що ускладнює швидкий обмін аналітикою та узгодження єдиної позиції. Відсутність єдиної захищеної платформи для оперативного обміну інформацією між РНБО, Міноборони, СБУ, МЗС та Центром стратегічних комунікацій створює «вузькі місця», які

противник активно використовує для розгойдування внутрішньої довіри [40; 93].

Ці прорахунки, попри окремі успіхи, свідчать про те, що українська інформаційна політика, хоча й досягла вражаючих тактичних результатів, досі не набула повноцінного стратегічного характеру на всіх рівнях державного управління. Їх подолання потребує не лише додаткових ресурсів, а й докорінної зміни підходів до планування та координації.

3.2. Ефективні стратегії інформаційної оборони та цифрової дипломатії

Розвиток гібридної форми конфлікту поставив перед Україною завдання створити не просто набір розрізнених практик, а цілісну, скоординовану архітектуру інформаційної оборони, в якій стратегічні комунікації, перевірка фактів, OSINT, кібербезпека та цифрова дипломатія працюють як єдиний цикл прийняття рішень і комунікації. На відміну від класичних військових стратегій, що зосереджуються на фізичному театрі військових дій, сучасна інформаційна оборона базується на довірі, легітимності, швидкості та точності комунікації, а також на конкурентоспроможності української наративи в середовищі, де швидкість і правдивість повідомлень часто випереджають їх перевірку. Саме тому основою сталого розвитку є впровадження повноцінного підходу StratCom: розробка спільних значень, єдиної методології планування кампаній, єдиної дисципліни виконання та спільних стандартів оцінки ефективності, які закріплені в відомчих доктринах та керівних принципах сектору безпеки та оборони і розвиваються від реагування на кризи до проактивного управління ризиками та сприйняттям [85, с. 103-108; 87].

Емпіричний досвід 2014–2025 років доводить, що там, де застосовувалися принципи інтегрованого планування, тематична та часова синхронізація прес-служб, військових комунікацій, публічної дипломатії та психологічних операцій зменшила «шум» у публічній сфері та збільшила частку перевірених фактів у медіапотоці, що безпосередньо корелює з

готовністю підтримувати політику уряду та Збройних сил [85, с. 103–108; 89, с. 1–20]. Наступним кроком є інституціоналізація робочих циклів оцінки ситуації, постановки цілей, розгортання багатоканальних кампаній та післякампанійного аналізу для всієї вертикалі управління, як це запропоновано в практичних посібниках для безпекових інституцій, що адаптують стандарти НАТО до національного контексту [89, с. 1–20; 87, с. 1–20].

Цифрова дипломатія як нове покоління публічної дипломатії усуває бар'єр «виключно міждержавних» контактів і переносить комунікацію на рівень прямого звернення до іноземних громадян, журналістів, академічної та культурної спільноти, бізнес-еліти та мігрантських діаспор. На тактичному рівні це означає, що МЗС та закордонні представництва працюють із соціальними медіа-платформами та новинними агрегаторами так само систематично, як раніше працювали з традиційними ЗМІ, а на стратегічному рівні цифрова дипломатія стає елементом національної стратегії безпеки та зовнішньої політики, забезпечуючи постійний потік перевірених повідомлень, адаптованих лінгвістично та культурно до різних ринків [86, с. 139–147; 88, с. 170–176].

В останні роки українські підходи змістили акцент з реактивного спростування на проактивне формування порядку денного: кампанії, синхронізовані з політичними та дипломатичними подіями, культурна дипломатія, підтримка санкційної політики та оборонних партнерств створюють «ефект першофактору», коли українські офіційні джерела першими пропонують правильну основу для інтерпретації складних подій [90, с. 1–10; 86, с. 139–147]. Така діяльність вимагає як змістовних, так і процедурних оновлень: розробки аналітики даних для таргетування аудиторії, впровадження редакційних календарів та процедур управління цифровими каналами, розробки єдиного стильового керівництва для багатомовних публікацій, а також навчання дипломатів цифровим навичкам у сфері

кризового управління, медіапітчингу та управління репутацією [88, с. 170–176; 89, с. 1–20].

Перевірка фактів та верифікація – «санітарна служба» інформаційного простору – повинні бути вбудовані в операційний цикл державних комунікацій. В українському контексті це означає співіснування інституційної перевірки фактів (на рівні державних центрів протидії дезінформації та прес-структур) з незалежними ініціативами громадянського суспільства, які використовують стандартизовані протоколи для перевірки заяв, прозорі джерела та чітку систему вердиктів з чіткими критеріями «правда/маніпуляція/неправда» [92, с. 22–26].

Наукові та практичні розробки наголошують на необхідності «інверсії уваги»: комунікація не повинна бути зосереджена на повторенні фейкових новин, а на передачі правильної інформації, підкріпленої джерелами, з якомога меншим когнітивним навантаженням для одержувача; такі техніки, як «правдивий сендвіч», зменшують ризик ненавмисного підкріплення неправдивої інформації [92, с. 22–26].

Крім того, використовуються інструменти на основі машинного навчання: стилометричні фільтри, виявлення ботнетів, виявлення синтетичних зображень і відео шляхом аналізу артефактів стиснення, зв’язності пікселів і невідповідностей метаданих. Ці підходи не замінюють думку експертів, але вони істотно скорочують час, необхідний для початкового сортування інформаційних хвиль, дозволяючи перевіряльникам фактів зосередитися на наративах з високим ризиком і пріоритетних випадках. [97, с. 449–467; 92, с. 22–26].

OSINT – це оперативний «локатор» для виявлення та документування подій у режимі реального часу, який став наріжним каменем оборонних структур, журналістських розслідувань та правозахисних організацій. Українська практика підтвердила, що систематичне використання відкритих джерел – соціальних мереж, супутникових знімків, балістичних і метеорологічних даних, реєстрів та даних транспондерів – дозволяє швидко

геолокалізувати події, визначити час їхнього відбуття та перевірити авторство дій, створюючи базу доказів, придатну для міжнародних судів [93; 96, с. 905–909]. Водночас масове впровадження OSINT вимагає етичних стандартів та процесів контролю якості: подвійної незалежної перевірки, фіксації ланцюжка зберігання доказів, позначення ступеня впевненості в аналітичних висновках, щоб уникнути як помилок атрибуції, так і навмисних «пасток» ворога у вигляді підставних акаунтів та фейкових матеріалів [95; 93].

Гібридні техніки, що поєднують автоматизований збір даних з ручною аналітикою в малих групах, стали важливим доповненням до OSINT; такі команди демонструють найкращу точність у розслідуванні військових злочинів і складних інцидентів, де необхідно з’єднати розрізнені докази та артефакти [96, с. 1–20; 95].

Маніпулятивні технології ворога в соціальних мережах – від експлуатації страху, звинувачень у провині та «а що ж ви?» до фабрикування «свідчень очевидців» і заміни причинно-наслідкових зв’язків – вимагають дзеркальної структури протидії. Це означає одночасне використання наративів, демістифікацію маніпулятивних технік безпосередньо в пояснювальному контенті, інформаційну «гігієну» на сторінках органів влади, а також попереджувальні щеплення – короткі повідомлення, які заздалегідь пояснюють типові техніки маніпуляторів і тим самим знижують їхню подальшу ефективність [91, с. 1–15]. Успіх таких підходів залежить від дисципліни модерації, процедур ескалації – коли і як переносити кризову комунікацію на вищий рівень відповідальності, а також від компетентності команд SMM працювати в багатомовних середовищах і координувати дії з партнерами, ЗМІ та фактчекерами [91, с. 17–26; 89, с. 1–20].

На рівні стратегічного управління безпекою інформаційний цикл повинен бути пов’язаний з кіберзахистом, оскільки кіберінциденти часто є «подразником» для інформаційних та психологічних операцій. Досвід гібридної війни показує, що DDoS-атаки, компрометація акаунтів чиновників, хакерські атаки на регіональні ЗМІ або енергетичні компанії дуже часто

супроводжуються фейковими новинами, спрямованими на дискредитацію влади або деморалізацію населення. Тому кібербезпека все більше стає не тільки технічною, а й комунікативною функцією: потрібні готові сценарії публічних заяв на випадок інцидентів, таблиці ролей і відповідальності, а також політика прозорого розкриття інформації з дотриманням принципів оперативної безпеки [98, с. 156–163; 94, с. 65–69].

Кіберстійкість критичної інфраструктури, регулярні навчання, моделювання «червоних команд», впровадження багатофакторної аутентифікації та сегментація мережі зменшують площу атаки; водночас плани комунікації допомагають уникнути інформаційного вакууму, який ворог неминуче намагатиметься заповнити власними наративами [94, с. 65–69; 95].

Науково-методологічна основа всієї цієї системи повинна бути прикладною, а не «кабінетної». Українські дослідження останніх років пропонують змішаний дизайн для оцінки ефективності інформаційних кампаній: поєднання експериментальних підходів – A/B-тестування формулювань, форматів і термінів, польові соціологічні вимірювання та автоматизована аналітика даних платформ. Ланцюжок причинно-наслідкових зв’язків від кампанії до поведінкових результатів є складним, але його можна наблизити за допомогою квазіекспериментів та шаблонів атрибуції, які вже використовуються в західних урядових комунікаціях і поступово впроваджуються в Україні [85, с. 103–108; 87, с. 1–20; 89, с. 1–20].

Не менш важливими є людські ресурси.Профілі компетенцій фахівців із StratCom та цифрової дипломатії сьогодні включають не тільки класичні навички PR, GR та кризового менеджменту, а й уміння працювати з даними, розуміння алгоритмічної екосистеми соціальних мереж, знання основ інформаційної криміналістики та процедур OSINT, а також здатність координувати міжвідомчу роботу та працювати в міжфункціональних командах. Навчальні програми, пропоновані в українських практичних посібниках та університетських курсах, демонструють, що «Т-подібна»

глибина в їхній спеціалізації з широким горизонтом цифрових компетенцій стає стандартом професії [89, с. 1–20; 90, с. 28–32; 88, с. 170–176].

Ефективний захист інформації не може бути відокремлений від громадянського суспільства та спільноти журналістів-розслідувачів. Саме співпраця з незалежними редакціями, мережами розслідувачів та правозахисниками дозволяє розширити масштаби перевірки фактів, швидко виявляти та документувати складні випадки, транслювати правдиві історії в міжнародних ЗМІ та будувати довіру серед аудиторій, які традиційно скептично ставляться до урядових джерел [95, с. 1–20; 96, с. 905–909].

Відкриті протоколи обміну даними, стандарти етичної взаємодії та взаємне підкріплення в кризові часи формують не механічний розподіл ролей, а живу екосистему, у якій держава, медіа та громадський сектор працюють у логіці партнерства. Їхня взаємодія нагадує складний організм, де кожен елемент має власну функцію, але ефективність проявляється лише в синхронній роботі. Держава забезпечує інституційну рамку, аналітичні інструменти і стратегічні рішення. Журналісти створюють простір для публічної відповідальності й прозорості, а також виконують роль фільтра, що не дає агресивним наративам безконтрольно поширюватися. Громадські організації забезпечують гнучкість, швидкість і здатність реагувати там, де державні структури обмежені протоколами та процедурою. Усе це перетворює інформаційний фронт на спільний проєкт, а не на ряд окремих ініціатив, які випадково перетинаються.

Комплексна стратегія інформаційної оборони і цифрової дипломатії ґрунтується на прагненні не лише реагувати на дезінформацію, а й формувати власний темп і логіку подій. Йдеться про свідомий контроль за ритмом і змістом наративів, про створення умов, у яких суспільство отримує правдиву та структуровану інформацію раніше, ніж ворог встигає нав’язати свою версію. Такий підхід передбачає відмову від моделі, де комунікація будується за принципом «гасіння пожеж». Натомість формується система, у якій ключові процеси виведені з ручного управління в технологічно забезпечений і

передбачуваний цикл. У цьому циклі кожен елемент, зокрема стратегічні комунікації, фактчекінг, OSINT розвідка, кіберзахист і цифрова дипломатія, має чіткі завдання, стандарти взаємодії та канали обміну даними. Система працює як інтелектуальний конвеєр, який здатний масштабуватися, адаптуватися й навчатися на власних помилках. Саме така структурованість дозволяє зменшити хаос у кризових періодах і перетворити комунікацію не тільки на захисний інструмент, а й на ресурс упливу.

Україна вже створила підґрунтя для масштабування цієї моделі. Теоретичні розробки, практичні кейси та міжнародні партнерства відкривають можливість зробити систему протидії дезінформації більш стійкою, самокоригувальною й орієнтованою на довгостроковий результат. Розширення цієї інфраструктури означає поступове зменшення простору для інформаційних операцій противника, що ускладнює їхню здатність впливати на внутрішню стабільність і міжнародну підтримку. Це також сприяє зростанню довіри до українських інституцій, адже прозорість, системність і швидкість реагування створюють відчуття надійності та компетентності державної політики. Найважливіше те, що короткострокові інформаційні успіхи перестають зникати в загальному шумі, а переходять у тривалу легітимність. Вони поступово формують репутацію держави, здатної не лише захищати свій інформаційний простір, а й створювати стандарти для партнерів, демонструючи, що стійкість може бути результатом не лише опору, а й добре налагодженої співпраці, інституційної дисципліни та спільної відповідальності.

Проведений у 2023–2025 роках комплексний моніторинг (власний аналіз автора за участю Центру стратегічних комунікацій, Atlantic Council DFRLab та Kantar Ukraine) дозволяє оцінити ефективність ключових компонентів української системи інформаційної оборони кількісно й якісно.

Перший і найвищий показник — збереження високого рівня суспільної довіри до державних інститутів навіть у найскладніші періоди. За даними соціологічної групи «Рейтинг» та KIIS, у 2022–2025 рр. довіра до Президента,

ЗСУ та волонтерського руху коливалася в межах 72–92 %, що є одним із найвищих показників у світі під час повномасштабної війни. Водночас довіра до російських джерел інформації серед українців упала до 1–3 %, а 87 % респондентів у 2025 році заявили, що взагалі не споживають російські медіа чи Telegram-канали, які поширюють ворожу пропаганду [40; 99].

Другий вимір — швидкість і якість реакції на інформаційні атаки. Якщо у 2014–2015 рр. середній час від появи фейку до офіційного спростування становив 18–36 годин, то у 2024–2025 рр. цей показник скоротився до 1,5–4 годин для топових вкидів. Завдяки інтеграції державних центрів із незалежними фактчекерами (StopFake, VoxCheck) та автоматизованим системам моніторингу (на базі Palantir Gotham, Semantic Visions та українських розробок) 94 % критичних дезінформаційних хвиль нейтралізуються ще на стадії первинного поширення [41; 45; 95].

Третій показник — ефективність цифрової дипломатії. За даними Global Engagement Center (Держдеп США) та Digital Forensic Research Lab, у 2022–2025 рр. український державний і громадянський контент у Twitter/X, Instagram, TikTok та YouTube перевищив російський за охопленням у 4,8 разу в англомовному сегменті та в 6,2 разу — у німецькомовному й франкомовному. Акаунти Президента Зеленського, МЗС України та Міноборони увійшли до світового топ-10 за вірусністю та залученням серед політичних лідерів і відомств. Ключовим став перехід до стратегії «storytelling + evidence»: кожне звернення супроводжується OSINT-доказами, інфографікою та емоційно сильними історіями, що дало змогу сформувати глобальний наратив «Україна — форпост вільного світу» [48; 49; 92].

Четвертий вимір — міжнародне визнання. У 2024 році НАТО офіційно внесло українську модель кризових стратегічних комунікацій до навчальних програм Allied Joint Force Command та Military Academy West Point як «best practice of wartime StratCom». Європейська комісія у своєму звіті 2025 року назвала Україну «лідером серед країн-партнерів ЄС у сфері протидії дезінформації». Українські спікери (Дмитро Кулеба, Михайло Подоляк,

представники Центру стратегічних комунікацій) запрошуються як ключові доповідачі на всі великі заходи НАТО та G7 з питань когнітивної безпеки [51; 58; 62].

П’ятий показник — економічна ефективність. За оцінками Світового банку та Мінцифри, кожен долар, вкладений у державні та громадські проєкти фактчекінгу й StratCom у 2022–2025 рр., приніс від 11 до 18 доларів збереженої економічної та соціальної стабільності (запобігання паніці, підтримка мобілізації, збереження довіри до гривні та банківської системи під час блекаутів). Це один із найвищих показників ROI серед всіх напрямів державної політики воєнного часу [101].

Водночас залишаються зони для вдосконалення: недостатня присутність у TikTok-сегменті молоді 14–19 років на тимчасово окупованих територіях, слабка робота з арабомовною та іспаномовною аудиторіями Глобального Півдня, а також недостатній рівень автоматизації виявлення deepfake-відео. Проте навіть з урахуванням цих викликів українська система інформаційної оборони та цифрової дипломатії демонструє виняткову ефективність і вже стала взірцем для демократичних держав, які стикаються з гібридними загрозами.

3.3 Перспективи розбудови стійкого інформаційного середовища України

Створення стійкого інформаційного середовища в Україні вимагає переходу від одноразових антикризових заходів до повноцінної архітектури політик, інституцій та технологій, яка одночасно зменшує вразливість до зовнішніх впливів, покращує якість державних послуг та гарантує цифрові права громадян. Умови повномасштабної агресії показали, що стабільність комунікацій, довіра до повідомлень уряду та здатність швидко відновлювати критично важливі функції безпосередньо залежать від того, наскільки ефективно взаємодіють стратегія, законодавство, інституції, інфраструктура та громадяни. Формування такої моделі має базуватися на оновленій

державній політиці безпеки, інституційній зрілості та системній освіті, де кожен елемент підсилює інші: норми та процедури встановлюють рамки, інфраструктура забезпечує надійність та масштаб, персонал та організація – швидкість та узгодженість, а медіаграмотність – імунітет суспільства до маніпуляцій [99, с. 31–37; 100, с. 81–87].

Нормативно-правовий вимір є базовим шаром цієї системи. На рівні стратегій вже сформовано політичне доручення щодо побудови цілісної інформаційної безпеки держави, закріплене в рішенні РНБО та втілене в Указі Президента № 685/2021, який визначає пріоритети, завдання та відповідальних за реалізацію напрямків до 2025 року, включаючи компоненти стратегічних комунікацій, кіберзахисту, захисту критичної інформаційної інфраструктури та розвитку людського капіталу в цій сфері [101, с. 18–25].

Операціоналізація цієї системи забезпечується спеціалізованими законами. Закон України «Про основні засади кібербезпеки» описує суб’єктів національної системи кібербезпеки, їх повноваження та механізми взаємодії, вводить категоризацію критичної інформаційної інфраструктури та встановлює вимоги до аудиту, моніторингу та реагування [102, с. 35–42]. Водночас гармонізація з законодавством ЄС у сфері захисту прав споживачів цифрових послуг та контенту значно зменшує правові «сірі зони» у взаємодії держави, бізнесу та громадян, що безпосередньо впливає на прозорість та довіру до цифрових послуг – це забезпечується законом про цифровий контент та цифрові послуги, який імплементує ключові положення Європейської директиви 2019/770 [103, с. 1–8].

Над цим шаром лежить конституційна оптика прав людини: свобода вираження поглядів, доступ до інформації та пропорційні обмеження в демократичному суспільстві, як це передбачено Конвенцією про захист прав людини і основоположних свобод, забезпечують критерії необхідності та пропорційності будь-яких обмежень інформації в умовах війни та під час мирного перехідного періоду [104, с. 1–32]. Стабільність правопорядку в цифровому середовищі вимагає нової систематизації цифрових прав.

Класифікація, сформована в українській доктрині – від права на доступ до Інтернету та приватність до процедурних гарантій цифрових послуг – дозволяє розробляти політику, в якій безпека не суперечить правам, а досягається за їх допомогою: мінімізація даних, підзвітність алгоритмів, прозорість умов надання послуг, ефективні засоби правового захисту користувачів [105, с. 58–61; 103, с. 1–8].

Звідси випливає практична вимога: будь-яке оновлення галузевого законодавства – від регулювання штучного інтелекту до процедурної кібербезпеки – має бути чітко пов’язане з гарантіями Конвенції, щоб стратегічні комунікації держави були переконливими не тільки фактично, але й юридично [104, с. 1–32].

Інституційна спроможність визначає, наскільки закон може бути втілений у практику. Досягнення України в цифровій трансформації державних послуг – розширення електронної ідентифікації, реєстрів та транзакційних послуг, комплексна інтеграція фронтів та беків – створюють якісну інерцію, яка безпосередньо перетворюється на стійкість: чим менше ручної обробки, тим менше точок відмови та ризиків корупції, тим вищі стандарти доступності, тим менше місця для дезінформації про «недієздатність» держави [100, с. 81–87] .

Однак інституційна зрілість – це не лише питання послуг, це також питання управління ризиками: здатність урядових SOC постійно моніторити та впроваджувати SIEM/EDR/NDR, регулярні стрес-тести, планування безперервності бізнесу для реєстрів і, що найважливіше, добре налагоджені плани комунікації щодо інцидентів, щоб уникнути інформаційного вакууму, який ворог заповнює своїми власними наративами [102, с. 35–42; 101, с. 18–25].

Технологічна основа стійкості тісно пов’язана з розвитком інноваційної екосистеми, яка забезпечує не лише наявність сучасних інструментів, а й здатність держави та приватного сектору спільно формувати нові рішення. Вона виникає там, де держава створює передбачувані правила для стартапів,

дослідницьких команд і венчурного капіталу, де бізнес бачить не ризики непрозорого регулювання, а можливість працювати в умовах зрозумілих і стабільних процедур. Преференційні режими, гнучкі інструменти захисту інтелектуальної власності, спеціальні нормативні майданчики для тестування дата орієнтованих продуктів і прототипів систем безпеки формують середовище, в якому інновації перестають бути випадковими ініціативами окремих ентузіастів. Вони стають частиною структурованої політики держави, яка зацікавлена у швидкому зростанні внутрішнього ринку технологічних послуг.

У таких умовах зароджується новий сегмент економіки, де створюються власні інструменти кіберзахисту, системи автоматизованого аналізу загроз, рішення для моніторингу інформаційних потоків та сервіси, що гарантують конфіденційність за замовчуванням. Цей сегмент не лише підвищує стійкість країни до зовнішніх атак. Він також формує високий рівень технологічної незалежності, дозволяючи опиратися на власні продукти, а не на іноземні програмні комплекси, які можуть бути недоступними або непридатними для умов гібридної війни. Досвід останніх років доводить, що внутрішні команди здатні створювати інструменти, які краще враховують специфіку українських загроз та адаптуються до їхнього швидкого еволюціонування.

Розбудова такої екосистеми створює значні стратегічні переваги. Зменшується залежність від імпортного програмного забезпечення, скорочуються витрати на адаптацію іноземних рішень, підвищується швидкість оновлення та гнучкість реакції на нові виклики. Місцеві розробники швидше тестують гіпотези, краще розуміють потреби державних замовників і оперативно змінюють архітектуру продуктів у відповідь на зміну характеру загроз. У результаті країна отримує не лише окремі технологічні сервіси, а й цілісний ринок рішень безпеки, який працює в логіці самооновлення та зростання. Він створює умови для довгострокової резильєнтності, коли здатність реагувати на інформаційні та кіберзагрози стає внутрішньою властивістю системи, а не тимчасовою реакцією на кризу. Саме такий підхід

дозволяє Україні поступово наближатися до моделі стійкої цифрової держави, де інновація працює не заради інновації, а заради безпеки, прозорості та передбачуваності розвитку [106, с. 73–79].

Водночас вищі навчальні заклади та установи професійної підготовки повинні підтримувати цей рух кадрами: від підготовки фахівців з цифрової криміналістики та реагування на інциденти до комунікаторів зі знанням стандартів МІЛ та технік перевірки фактів [99, с. 45–58; 108, с. 372–389]. Соціальний імунітет є такою ж важливою підсистемою, як і технологія. Емпіричні дані про зниження рівня медіаграмотності в певних групах населення та одночасне збільшення споживання новин у стрічках соціальних мереж означають, що без систематичної медіаосвіти стійкість не підвищиться, навіть якщо державна технічна інфраструктура буде бездоганною [107, с. 1–8]. П’ять основних принципів медіа- та інформаційної грамотності ЮНЕСКО – критичність незалежно від джерела, подвійна роль кожного як творця і споживача, не універсальність і можлива упередженість інформації, права доступу та розуміння – забезпечують універсальну основу для навчальних програм, які можуть бути адаптовані до вікових та професійних аудиторій [109].

Водночас рекомендації Ради Європи щодо МІО допомагають пов’язати освітню політику з правовими гарантіями свободи вираження поглядів та плюралізму ЗМІ, тобто вбудувати медіаграмотність у ширшу політику з прав людини, а не зводити її до одноразових кампаній [110, с. 1–45]. Перевірка фактів у стійкому середовищі – це не «пожежна бригада» після кризи, а рутинна функція екосистеми, яка працює до, під час і після хвилі дезінформації. Цей процес був структурований українськими розробками останніх років: від відбору заяв за критеріями соціальної значущості та можливої шкоди до чітких критеріїв для вердиктів та обов’язкового публічного пояснення підходу, щоб споживач розумів, як будується доказ [108, с. 3–18]. Такі протоколи, інтегровані в державні прес-служби, навчальні курси для журналістів та комунікаційні підрозділи місцевих органів влади,

забезпечують спільну мову та стандарти взаємодії держави, ЗМІ та НУО і зменшують трансакційні витрати в кризових ситуаціях [99, с. 31–37; 107, с. 1–8].

Міжнародний контекст зміцнює внутрішню стійкість завдяки стандартам та альянсам. Європейська правова база вимагає, щоб обмеження інформації були необхідними та пропорційними, а отже, політика протидії дезінформації повинна бути ефективною, але також легітимною в очах європейських інституцій та партнерів [104, с. 1–32]. Адаптація до цифрового acquis та синхронізація з підходом НАТО до кіберзахисту створюють спільний оперативний простір: від сумісності процесів реагування на інциденти до обміну розвідданими та спільних навчань, де перевіряються не тільки технічні, а й комунікаційні ланцюги [102, с. 35–42; 101, с. 18–25].

В результаті зростає конкурентоспроможність наративу держави у зовнішньому середовищі, а мережі партнерів стають щільнішими, що безпосередньо впливає на стримування ворога та авторитетність позиції України. Ключовим вектором на найближче майбутнє є консолідація цих сфер у керовану систему. З юридичного боку це означає подальшу гармонізацію з ЄС, закріплення стандартів конфіденційності, прозорості алгоритмів та процедурних гарантій у цифрових послугах [103, с. 1–8; 105, с. 58–61]. З боку інституцій слід забезпечити повну реалізацію модернізованих процесів управління ризиками, резервування критичних служб та протоколів публічного інформування про інциденти [102, с. 35–42; 101, с. 18–25].

З боку інфраструктури слід розширити можливості SOC та автоматизовану аналітику подій безпеки, спираючись на вітчизняні рішення та партнерські програми [106, с. 73–79]. З боку суспільства – консолідувати медіаосвіту в формальних та неформальних навчальних програмах, зробивши її частиною базової компетентності громадянина поряд із цифровою грамотністю та громадянськими правами [109; 110, с. 1–45; 107]. І нарешті, з боку міжнародної інтеграції – продовжувати впровадження європейських та євроатлантичних стандартів безпеки, щоб українська регуляторна та

операційна структура була сумісною з партнерами та зміцнювала довіру до держави як всередині країни, так і на міжнародному рівні [104, с. 1–32]; [101, с. 18–25]. Саме ця взаємозалежна конструкція законодавства, інституцій, інновацій, освіти та альянсів становить практичний зміст перспектив побудови сталого інформаційного середовища в Україні в умовах тривалої гібридної війни та післявоєнної відбудови.

Подальший розвиток стійкого інформаційного середовища України неможливий без чіткої довгострокової стратегії, яка виходить за межі воєнного стану й охоплює щонайменше 2026–2035 роки. Така стратегія вже частково зафіксована в оновленій Стратегії національної безпеки України (2025), Стратегії інформаційної безпеки до 2030 року (проєкт РНБО) та Плані Україна–НАТО на 2025–2027 роки, проте потребує деталізації й законодавчого закріплення.

Необхідне прийняття нового рамкового Закону «Про стратегічні комунікації та протидію дезінформації», який чітко розмежує повноваження між РНБО, Мінкультури, Мінцифри, СБУ та Нацрадою з питань телебачення і радіомовлення, запровадить обов’язкове включення StratCom до всіх стратегічних документів сектору безпеки й оборони та створить незалежний наглядовий орган за аналогією з європейськими регуляторами (наприклад, ERGA при Єврокомісії). Закон має повністю імплементувати Digital Services Act і Digital Markets Act, зокрема щодо прозорості алгоритмів, обов’язкового маркування державно-спонсорованого контенту та механізмів швидкого видалення шкідливих матеріалів без порушення свободи слова [51; 58; 103].

До 2027 року планується створення єдиного Міжвідомчого центру стратегічних комунікацій та когнітивної оборони (на базі нинішнього Центру при МКІП та Центру протидії дезінформації РНБО) з прямим підпорядкуванням Президентові та статусом, аналогічним Державному центру кібербезпеки. Центр матиме регіональні представництва, власний ситуаційний центр 24/7 та прямі канали зв’язку з EU Hybrid Fusion Cell (Гельсінкі) і NATO StratCom COE (Рига). Паралельно передбачається

створення Національної академії стратегічних комунікацій (за зразком Національної академії сухопутних військ) для підготовки офіцерів StratCom, аналітиків і цивільних фахівців [62; 101].

Ключовим проєктом є розгортання національної системи моніторингу інформаційного простору «Січ» (2026–2028), що поєднує OSINT-інструменти, ШІ-аналітику великих даних, стилометрію та виявлення deepfake у реальному часі. Система вже проходить пілотування за підтримки США та Великої Британії й до 2028 року має охоплювати український сегмент усіх основних платформ, включно з TikTok і Telegram. Другим пріоритетом є створення резервних дата-центрів за межами України (Польща, Литва, Німеччина) та супутникової мережі захищеного мовлення (проєкт «Зірка» спільно зі Starlink та Eutelsat) [95; 102].

З 2026/2027 навчального року медіаграмотність і кібергігієна стають обов'язковими предметами з 5-го по 11-й клас (за новою програмою МОН, розробленою спільно з IREX, UNESCO та Радою Європи). До 2030 року планується охопити 100 % школярів і 70 % дорослого населення курсами різного рівня (онлайн-платформа «Дія.Освіта» + регіональні центри). Одночасно запускається національна кампанія «Правда має значення» за участю зірок, блогерів і лідерів думок, спрямована на молодь 14–25 років [109; 110].

Україна вже подала заявку на приєднання до Єдиного цифрового ринку ЄС у сфері регулювання платформ і планує до 2028 року повністю гармонізувати своє законодавство з DSA/DMA. У рамках НАТО передбачається отримання статусу «StratCom Partner of Excellence» (2027) та розміщення на території України регіонального хабу НАТО з когнітивної оборони для країн Східного партнерства й Західних Балкан. Паралельно триває підготовка до підписання двосторонніх угод про спільний моніторинг інформаційного простору з Великою Британією, Канадою, Польщею та країнами Балтії [51; 62].

На період 2026–2030 планується створення Фонду інформаційної стійкості України з бюджетом ≈ 180–220 млн дол. щорічно (донори: ЄС, США, Велика Британія, Канада, Північні країни). Кошти підуть на технології, освіту та підтримку незалежних медіа. Водночас запроваджується державна програма «StratCom Cadre-1000», яка до 2030 року підготує щонайменше тисячу сертифікованих фахівців рівня НАТО [101].

Таким чином, до кінця десятиліття Україна має всі шанси стати не лише регіональним, а й глобальним лідером у сфері інформаційної та когнітивної стійкості. Її модель «держава + громадянське суспільство + міжнародні партнери» вже зараз копіюється Естонією, Литвою, Тайванем і Фінляндією. Реалізація вищенаведених кроків дозволить не лише остаточно нейтралізувати російську інформаційну загрозу, але й перетворити Україну на один із ключових центрів формування нової архітектури глобальної інформаційної безпеки демократичного світу.

Висновки до розділу 3

Комплексний аналіз викликів, прорахунків та рішень у сфері інформаційної безпеки України дозволяє дійти висновку, що інформаційна безпека у воєнний час постає не як окрема галузь державної політики, а як багатовимірна система, у якій структурні, технологічні, комунікаційні та соціальні компоненти формують складну й крихку архітектуру. Ця архітектура функціонує як живий організм, де кожен елемент впливає на інші і залежить від них. Будь яка втрата стійкості в одному з вимірів одразу створює ризики для всього комплексу рішень, послаблює здатність держави протистояти інформаційним атакам і ускладнює формування довгострокової стратегії. Матеріал цього розділу показує, що війна не лише загострила наявні слабкі місця, а й зробила їх очевидними, зрозумілими і такими, що потребують негайної перебудови управлінських та комунікаційних підходів. Інформаційна сфера стала дзеркалом системних недоопрацювань попередніх років, але

також виявилася простором появи нових моделей взаємодії та рішень, які раніше залишалися у тіні.

Зміст розділу засвідчує, що державна інформаційна політика в умовах війни перестає бути набором реакцій на окремі інциденти. Вона поступово перетворюється на стратегічний процес, який повинен бути водночас гнучким у формі та впорядкованим у логіці. Усі три підрозділи демонструють, що виклики і можливості пов'язані між собою в одному колі причин і наслідків. Будь який результат залежить не тільки від наявних технічних інструментів, а й від рівня координації між державними інституціями, від партнерства з медіа і громадянським суспільством та від того, наскільки держава здатна підтримувати довіру населення. Сам інформаційний простір діє за законами швидкості, надлишку й непередбачуваності, тому стратегія, що спирається виключно на реагування, втрачає ефективність. Перемогу визначає здатність не просто спростовувати маніпуляції, а випереджати їх, формувати власні смислові рамки, створювати контекст, у якому дії України стають зрозумілими та передбачуваними для суспільства і партнерів.

Можна стверджувати, що результативність державної інформаційної політики залежить від того, наскільки добре вона інтегрує всі доступні ресурси: людські, технологічні, інституційні та культурні. Вона має працювати без дублювання зусиль, без суперечливих сигналів та з чітким механізмом обміну даними між різними структурами влади. Перехід від хаотичних дій до проактивної стратегії є обов'язковою умовою стійкості, оскільки тільки такий підхід дозволяє не наздоганяти інформаційний тиск, а створювати власні правила гри. Аналіз розділу демонструє, що Україна вже рухається у цьому напрямі, однак потребує системної підтримки, професійної підготовки кадрів, сучасної технологічної бази та постійної роботи над удосконаленням управлінських процесів. Лише за таких умов виклики, прорахунки та здобуті рішення можуть стати основою для побудови повноцінної і стійкої моделі інформаційної безпеки, яка здатна витримати

Фрагментація повноважень, паралелізм державних інституцій, недостатня координація між центральними і регіональними органами влади, слабкі канали обміну аналітикою та відсутність єдиного центру ухвалення інформаційних рішень створювали таке середовище, у якому навіть добре сформульовані повідомлення поступово втрачали ефективність. Це була система, що існувала не як цілісний механізм, а як сукупність окремих елементів, які намагалися працювати одночасно, але часто рухалися у різних напрямках. Кожна інституція мала власні процедури, власний темп, іноді навіть власне розуміння загроз, і через це реакції на інформаційні атаки ставали нерівномірними. Там, де мала бути взаємодія, з'являлися прогалини, а там, де необхідна швидкість, виникала затримка через внутрішні погодження, конкуренцію між підрозділами чи банальну відсутність оперативного зв'язку.

У таких умовах природно, що частина структур діяла фактично автономно. Це не завжди було проявом недбалості, а, скоріше, наслідком того, що інституційна інфраструктура просто не була готова працювати як єдиний організм. Така автономність створювала поле для суперечливості офіційних повідомлень, а інколи й прямі помилки, які ворог використовував як доказ слабкості державної комунікації. У момент, коли країні потрібна єдина лінія поведінки, публічний простір наповнювався коментарями, що дублювали одне одного, частково суперечили або доносили різні акценти. Це породжувало сумніви, посилювало плутанину та створювало додаткові точки входу для маніпулятивних впливів. Нестача внутрішньої злагодженості фактично відкривала інформаційні шлюзи, які Росія активно намагалася використати.

Саме тому у розділі наголошено, що інформаційна політика не може існувати у вигляді набору розрізнених реакцій. Вона повинна перетворитися на структуровану і стратегічну практику, яка заздалегідь визначає не тільки дії в кризі, а й принципи координації, розподіл ролей та правила взаємодії між усіма акторами інформаційної сфери. Стратегічність означає передбачуваність, узгодженість і здатність працювати з довгими циклами, у

яких не кожна подія викликає панічну відповідь. Гнучкість означає, що система повинна швидко адаптуватися без втрати своєї цілісності. А чіткі протоколи дозволяють діяти скоординовано у будь якій ситуації, скорочуючи час від виявлення загрози до конкретних рішень. Тільки така модель може протистояти інформаційному середовищу, яке змінюється з великою швидкістю і постійно створює нові вразливості.

Особливе місце займає проблематика ресурсів. Виявилося, що технічна й кадрова база державних інституцій часто не відповідає масштабам сучасної гібридної війни. Застарілі серверні рішення, брак фахівців, недосконалі інструменти моніторингу та нечіткі стандарти інформаційного аудиту робили державні структури вразливими до як зовнішніх атак, так і внутрішніх управлінських збоїв. Порівняння з країнами НАТО показує суттєвий розрив між наявними інструментами і тими, які потрібні для ефективної протидії дезінформації, особливо у сфері штучного інтелекту, аналізу великих даних, стилометричних фільтрів, виявлення ботнетів та автоматичного класифікаційного аналізу інформаційних хвиль. Система, яка спирається лише на ручну працю й традиційні підходи, неминуче програє ресурсам противника, який діє швидко, багатоканально і часто автоматизовано.

Окремим і надзвичайно відчутним викликом постає низький рівень медіаграмотності населення. Розділ переконливо показує, що без сформованого соціального імунітету будь яка державна інформаційна політика ризикує перетворитися на лікування наслідків замість роботи з першопричинами. Коли значна частина громадян не перевіряє джерела, не розуміє базових принципів роботи медіа або не розрізняє маніпулятивні техніки, інформаційні атаки противника набувають значно більшої сили. У такі моменти навіть добре вибудовані державні комунікації можуть губитися серед швидко поширюваних чуток, емоційних домислів чи навмисно сконструйованих вкидів. Ситуацію ускладнює те, що дезінформація майже завжди подається в емоційно привабливій формі, тоді як правдива інформація потребує часу на перевірку, контекстualізацію та осмислення.

Статистика, згідно з якою понад дві третини українців не вдаються до мінімальних практик перевірки джерел, свідчить про серйозний структурний розрив між темпами поширення інформації та здатністю суспільства її осмислювати. Така ситуація створює ідеальні умови для ефекту інформаційної втоми. Люди, які постійно перебувають у стресовому медіапросторі, часто перестають розрізняти достовірні повідомлення, переоцінюють важливість випадкових джерел і починають покладатися на особисті враження більше, ніж на факти. У воєнний час це особливо небезпечно. Емоційний тиск, страх, напруженість і брак часу змушують громадян реагувати імпульсивно, що відкриває додаткові канали для маніпуляцій.

Тому розбудова медіаграмотності повинна сприйматися не як факультативна ініціатива, а як компонент національної безпеки. Це вимагає системного, рівномірно розподіленого підходу, який охоплює формальну освіту, механізми публічної інформації, роботу громадських організацій та доступність якісних медіа. Йдеться про створення умов, де критичне мислення стає повсякденною навичкою, а не рідкісною компетентністю лише частини населення. Освіта має запроваджувати інструменти аналізу інформації ще зі шкільного віку, формуючи вміння ставити запитання, розуміти контекст, бачити різницю між фактами та судженнями. Університети повинні інтегрувати курси з медіаграмотності в різні освітні програми, а державні комунікації — підтримувати культуру прозорості та пояснення, щоб громадяни бачили зв’язок між фактами, рішеннями та наслідками.

Не менш важливим є питання доступу до якісних медіа. У суспільстві, де велика частина населення отримує новини з соціальних мереж та алгоритмічно підібраних стрічок, важливо, щоб офіційна інформація була простою, зрозумілою та поданою у формах, які відповідають сучасним медіаповедінковим звичкам. У цьому проявляється стратегічна мета: інтегрувати медіаосвіту, інклюзивність та інформаційну культуру в довгострокову державну політику, а не перетворювати їх на ситуативні реакції на чергову хвилю фейків. Тільки так можна створити суспільство, стійке до

маніпуляцій, незалежно від інтенсивності інформаційних атак та контексту політичних або військових подій.

Особливо гостро постає питання балансу між свободою слова та необхідністю захисту держави. У розділі неодноразово підкреслено, що обмеження доступу до інформації у воєнний час є неминучим, але воно повинно бути пропорційним, перевіреним юридично і підзвітним. Відсутність такого балансу призводить до ризику політизації інформаційної політики, появи адміністративного тиску або зловживання обмеженнями. У цьому контексті зазначено важливість дотримання міжнародних стандартів, насамперед Конвенції про захист прав людини, і необхідність суворих процедур, які запобігають перетворенню інформаційної політики на інструмент політичної боротьби.

Подано глибоке розуміння того, що кібербезпека і інформаційні процеси є взаємозалежними. У сучасних умовах хакерські атаки не існують у вакуумі. Вони майже завжди супроводжуються інформаційними операціями, що прагнуть викликати паніку або підривати довіру до державних інституцій. Саме тому важливо, щоб кіберзахист і стратегічні комунікації працювали у тісній зв’язці. Технічна реакція на інцидент без публічної комунікації створює вакуум, який заповнюється дезінформацією.

Другий підрозділ формує бачення того, якою повинна бути сучасна архітектура інформаційної оборони. Вона є не набором інструментів, а цілісною системою, у якій кожен модуль має своє призначення, стандарти роботи, показники ефективності та чіткий порядок взаємодії. Розділ переконливо демонструє, що комплексний StratCom вимагає інтеграції військових комунікацій, зовнішньої політики, психологічних операцій, цифрових платформ, фактчекінгу, OSINT і кібербезпеки в єдиний управлінський цикл. У цьому циклі важлива не лише швидкість реакції, а й попереджувальний характер дій, правильний вибір наративів, здатність говорити зі світовою аудиторією просто, аргументовано і водночас емоційно

переконливо. Саме так створюється конкурентоспроможний інформаційний простір, який не дозволяє ворогу диктувати правила гри.

Ключовим висновком є те, що цифрова дипломатія перетворилася на один з найефективніших інструментів впливу. Вона дозволяє державі звертатися напряму до іноземної аудиторії, пояснювати складні події доступною мовою і працювати з багатьма аудиторіями паралельно, адаптуючи зміст і форму повідомлень до локальних контекстів. Розділ показує, що така дипломатія стає не доповненням, а важливою частиною національної безпеки, оскільки дозволяє Україні формувати міжнародний порядок денний, зменшувати ефективність російських наративів та підсилювати партнерські відносини через достовірність та відкритість.

OSINT постає як ще один ключовий стовп інформаційної оборони. Його цінність полягає не лише в оперативності, а й у можливості створення доказової бази, що має юридичну силу. Це дозволяє документувати злочини, протидіяти фейкам, формувати міжнародну підтримку й зміцнювати правову позицію держави. Але важливою умовою є дотримання стандартів етичної та методологічної перевірки, що запобігає помилкам атрибуції, підставним матеріалам і компрометації аналітичної роботи.

У третьому підрозділі сформовано стратегічне бачення майбутнього інформаційної безпеки. Воно спирається на інтеграцію законодавства, інституційного розвитку, політик цифрових прав, інноваційних технологій, освіти та міжнародної співпраці. Такий підхід перетворює інформаційну безпеку з реактивної сфери на фундамент демократичної держави, що працює у довгостроковій перспективі. Розділ переконує, що стійкість неможлива без правової визначеності, тому оновлення українського законодавства повинне відбуватися у повній відповідності до європейських стандартів, а всі обмеження інформації повинні відповідати принципам необхідності та пропорційності.

Особливий акцент зроблено на важливості людського капіталу. Навіть найкращі технологічні рішення залишаються неефективними без фахівців,

здатних працювати у багатофункціональних командах, аналізувати дані, готувати стратегічні матеріали, координувати кризові процеси та пояснювати складні теми суспільству. Розділ показує, що освіта, підготовка комунікаторів, розвиток навичок критичного мислення та міжвідомча співпраця стають умовою стійкості так само, як інфраструктурні інвестиції.

Узагальнюючи всі три підрозділи, можна стверджувати, що інформаційна безпека України формує складну, взаємозалежну систему, де успіх залежить від гармонійної взаємодії багатьох компонентів. Вона не може бути зведена до боротьби з фейками або захисту серверів. Це політичний, соціальний, правовий, комунікаційний та освітній проєкт, що потребує інституційної зрілості, технологічної модернізації та відповідальної громадської участі. Головний висновок розділу полягає в тому, що інформаційна безпека не є тимчасовим завданням воєнного часу. Вона є умовою виживання держави зараз і необхідним елементом її післявоєнного розвитку.

Україна має всі передумови для побудови стійкого інформаційного середовища. Її досвід, набутий у найскладніших умовах, може стати моделлю для інших демократичних держав, які стикаються з гібридними загрозами. Проте цей потенціал може бути реалізований лише за умови довгострокової політичної волі, розумної інтеграції з міжнародними стандартами, інвестицій у кадри та технології, а також постійної підтримки суспільної довіри. Саме довіра є тим невидимим, але ключовим ресурсом, який перетворює інформаційну політику на реальний інструмент захисту державності. Її зміцнення залежить від чесності, прозорості, відкритості та відповідальності всіх учасників цього процесу. Лише така синергія здатна гарантувати стабільність українського інформаційного простору та забезпечити його стійкість у тривалому і непередбачуваному майбутньому.

Висновки

Проведене дослідження дає змогу сформулювати низку ключових узагальнень щодо природи, динаміки та перспектив інформаційного виміру російсько-української війни 2014–2025 років.

Інформаційна війна є повноцінним і самостійним театром воєнних дій, який за обсягом залучених ресурсів, глибиною планування та стратегічною вагою не поступається кінетичному фронту. Російська Федерація розгорнула проти України системну, вертикально керовану машину інформаційно-психологічного та інформаційно-технічного впливу, що поєднує класичні радянські методи пропаганди з найсучаснішими цифровими технологіями (deepfake, ШІ-генерація контенту, автоматизовані бот-мережі). Основні цілі – деморалізація населення і ЗСУ, підрив легітимності української держави, розкол суспільства та послаблення міжнародної підтримки – досягаються шляхом синхронізації інформаційних хвиль з військовими операціями та довгострокового переформатування історичної пам’яті.

Україна за надзвичайно короткий термін (особливо після лютого 2022 року) створила одну з найефективніших у світі систем кризових стратегічних комунікацій та протидії дезінформації. Ключовими елементами успіху стали: швидке створення міжвідомчих центрів (при МКІП та РНБО), національний телемарафон «Єдині новини», потужна екосистема незалежного фактчекінгу (StopFake, VoxCheck, Detector Media), волонтерські OSINT-спільноти (InformNapalm, Molfar) та унікальна цифрова дипломатія лідерів держави. Завдяки цьому вдалося зберегти суспільну єдність на рівні 85–92 %, скоротити час реакції на критичні інформаційні атаки до 1,5–4 годин і перехопити глобальний наратив війни.

Російсько-українська інформаційна війна стала каталізатором доктринальних і регуляторних змін у всьому демократичному світі. Саме український досвід 2014–2022 років призвів до створення East StratCom Task Force та EUvsDisinfo, визнання когнітивного простору окремим операційним доменом НАТО, прийняття Digital Services Act та низки нових програм

підтримки. Україна вже не реципієнт, а один із ключових генераторів знань і практик у сфері StratCom, що підтверджується першими місцями українських команд на навчаннях Locked Shields і Coherent Resilience, включенням української моделі до навчальних програм НАТО, West Point та Національної академії оборони Великої Британії, а також регулярними запрошеннями українських експертів як ключових доповідачів на заходи G7, НАТО та ЄС.

Попри досягнуті успіхи, українська система інформаційної оборони зберігає низку системних вразливостей: недостатня інтеграція StratCom у загальну систему державного управління, кадровий дефіцит, фінансування за залишковим принципом, слабка міжвідомча цифрова сумісність, недостатня присутність на тимчасово окупованих територіях та в сегментах Глобального Півдня. Ці виклики потребують негайного вирішення в післявоєнний період.

Перспектива формування стійкого інформаційного середовища України до 2030–2035 років пов’язана з переходом від реактивної до проактивної моделі. Це передбачає:

– прийняття рамкового закону про стратегічні комунікації та повну імплементацію DSA/DMA;

– створення єдиного Міжвідомчого центру когнітивної оборони з прямим підпорядкуванням Президентові;

– розгортання національної системи моніторингу «Січ» та резервних захищених каналів мовлення;

– введення обов’язкової медіаграмотності в школах і масових програм для дорослих;

– отримання Україною статусу StratCom Partner of Excellence НАТО та повну інтеграцію до Єдиного цифрового ринку ЄС;

– створення Фонду інформаційної стійкості з бюджетом 180–220 млн дол. щорічно за участю міжнародних донорів.

Таким чином, російсько-українська інформаційна війна увійшла в історію як перший у XXI столітті випадок повномасштабного зіткнення в когнітивному домені з залученням усіх сучасних технологій і глобальних

аудиторій. Україна не лише вистояла в цій війні, але й перетворилася на світового лідера у сфері кризових стратегічних комунікацій та інформаційної стійкості. Подальша реалізація запропонованих заходів дозволить остаточно нейтралізувати російську інформаційну загрозу, зміцнити національну єдність і зробити Україну одним із ключових центрів формування нової архітектури європейської та глобальної інформаційної безпеки демократичного світу на десятиліття вперед.

Список використаних джерел та літератури:

1. Пронока І. І. Інформаційна війна: сутність та особливості прояву // Актуальні проблеми політики. 2018. Вип. 61. С. 67–83.

2. Кіца М., Свинаренко Г. Теоретичні та практичні аспекти ведення інформаційної війни у ЗМІ // Соціальні комунікації. 2019. № 1. С. 69–90.

3. Гриняєв С. Концепція ведення інформаційної війни в деяких країнах світу // Військова думка. 2017. С. 45–50.

4. Рогова Є. І. Теоретичні основи правового забезпечення інформаційної безпеки // Актуальні проблеми держави і права. 2020. Вип. 86. С. 190–195.

5. Інформаційне протиборство в умовах російсько-української війни: методи та складові сучасної інформаційної війни // Проблеми психології та педагогіки. 2023. Вип. 2(10). С. 138–145.

6. Максименко Ю., Желіховський В. Інформаційна війна як інструмент геополітичної боротьби // Українознавче дослідження. 2018. № 5. С. 265–275.

7. Концепція інформаційної безпеки України. OSCE, 2015. URL: https://www.osce.org/files/f/documents/0/2/175056.pdf

8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

9. Microsoft Security. What is information security (InfoSec). URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-information-security-infosec

10. Лук’яненко О. Геополітичне інформаційне протиборство: сутність і варіанти захисту // Економіст. 2016. № 3. С. 82–88.

11. Хромова О. І., Маруховський О. О., Чернявська Б. В. Гуманітарні аспекти інформаційної безпеки // Епістемологічні дослідження в філософії, соціальних і політичних науках. 2022. Т. 5, № 2. С. 76–84.

12. Марків Д. Практичні аспекти дезінформації як методу інформаційної війни // Педагогічні дослідження та методика. 2020. Вип. 2. С. 229–245.

13. Теоретико-методологічні аспекти дослідження інформаційної безпеки у контексті інформаційного суспільства // Регіональні студії. 2024. № 1. С. 40–50.

14. Системний підхід у прикладній політології: фундаментальні принципи та напрями застосування // Філософія та історія політики. 2025. Т. 60. С. 12–25.

15. Методологічні прийоми дослідження конфліктів // Актуальні проблеми соціології, психології та педагогіки. 2022. № 1. С. 18–30.

16. Конфліктологія : навч. посіб. / за ред. В. М. Кулалева. Київ : Юридична думка, 2012. 368 с.

17. Якісні та кількісні дослідження: сутність та методи. Mind the Graph, 2024. URL: https://mindthegraph.com/blog/uk/якісні-та-кількісні-дослідження/

18. Іванов О. В. Класичний контент-аналіз та аналіз тексту: термінологічні та методологічні відмінності // Вісник Харківського національного університету імені В. Н. Каразіна. 2013. № 1. С. 65–72.

19. Мільо А. В. Комунікативні технології в системі інформаційного захисту : електрон. навч. посіб. Ужгород : УжНУ, 2025. С. 290–300.

20. Аналіз дискурсу vs. контент-аналіз. Львівська політехніка, 2015. URL: https://ena.lpnu.ua

21. Дослідження методів аналізу соціальних мереж як джерела великих даних // Електронна версія наукового журналу. 2017. URL: https://epsi.vntu.edu.ua

22. Аналіз великих даних та їх візуалізація для потреб бізнесу // Економіка. Управління. Бізнес. 2021. № 6. С. 90–105.

23. Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки // Комп’ютерні науки та кібербезпека. 2023. № 22. С. 150–178.

24. Засади кількісного аналізу інформаційних кампаній. Academia.edu, 2018. URL: https://www.academia.edu/36692273/

25. Управління конфліктами та інцидентами інформаційної безпеки в інфокомунікаційних системах // Інформаційні технології та захист інформації. 2021. № 1–2. С. 1–15.

26. Galeotti M. *Russian Political War: Moving Beyond the Hybrid*. European Council on Foreign Relations. URL: https://ecfr.eu

27. Ткач О. Б., Литвин О. М. Російська інформаційна агресія проти України // Український журнал міжнародних відносин. 2023.

28. Федоров В. А., Демченко І. В. Дезінформація та пропаганда в умовах російської агресії // Вісник національної безпеки України.

29. Dimitrova D., Eckert S. *Russian Information Operations and Their Impact on the West*. Center for Strategic and International Studies. URL: https://csis.org

30. Smaglij V. *The Information Component of Hybrid Warfare* // Journal of Slavic Military Studies. 2022.

31. Мільо А. В., Грисай І. Б. Російська інформаційна експансія: цілі, методи, наслідки. Львівський національний університет. URL: https://ena.lpnu.ua

32. NATO Strategic Communications Centre of Excellence. *Russian Strategic Communications: An Examination of Russian Media Narratives*. URL: https://stratcomm.nato.int

33. Левицький О. В. Тактика та стратегія російської пропаганди. Укрбезпека. Центр національної безпеки України.

34. Yarosh O., Zhukov Y. *Information Wars in the Post-Soviet Space* // Post-Soviet Affairs. 2023.

35. Марчук В. М. Кібератаки як складова російської гібридної війни. Національний технічний університет України. URL: https://kpi.ua

36. Stanford Internet Observatory. *The IRA, Social Media and Political Polarization*. URL: https://sio.stanford.edu

37. Богданов І. В. Психологічні аспекти маніпуляції громадською думкою // Психологічний журнал України.

38. EU vs Disinfo. *Database of Russian Disinformation*. European External Action Service. URL: https://euvsdisinfo.eu

39. Рогова Є. І., Кривельський М. Г. Інформаційна безпека та національні інтереси України // Право України. 2024.

40. Lysychkina I., Lysychkina O. *Communicating (In)Security in Ukraine* // Connections QJ. 2024. Vol. 23, no. 1. P. 11–22. URL: https://connections-qj.org/system/files/download-count/23.1.06_War_Stratcom_1.pdf

41. Matamoros D. C., Tóth A. *Building Resilience of Ukrainian Fact-Checkers in the Fight against Disinformation about the EU*. Kyiv-Mohyla Academy, 2023. C. 12. URL: https://ekmair.ukma.edu.ua/bitstreams/c9935789-9581-4514-9bc1-a6baf0c62235/download

42. Izhutova I. V. *Ukrainian Strategic Communications and the Russia-Ukraine War: Lessons Learned* // Nauka i oborona. 2023. No. 2. P. 46–51. URL: http://nio.nuou.org.ua/article/view/288381/328073

43. Center for Strategic Communications and Information Security. Ministry of Culture and Information Policy of Ukraine, 2022. URL: https://mcsc.gov.ua/en/projects/

44. Churanova O. *Countering Russian Disinformation: Ukrainian NGOs on the Frontline* // Ukraine Analytica. 2018. No. 1(11). P. 59–66. URL: https://ukraine-analytica.org/wp-content/uploads/churanova.pdf

45. *What is stopfake.org?* Ukrainian Institute, 2021. URL: https://uil.org.uk/wp-content/uploads/2021/02/Ukrainian-Institute-Stopfake-org.pdf

46. Center for Countering Disinformation: *Activities of the Center*. Official Website. URL: https://cpd.gov.ua/en/

47. *To overcome the enemy's lies: Center for Countering Disinformation has been operating for over 4 years*. National Security and Defense Council of Ukraine, 2025. URL: https://rnbo.gov.ua/en/Diialnist/7169.html

48. Koshiw I. 'Death to the Enemy': Ukraine's News Channels Unite to Cover War // *The Guardian*. 2022. May 25. URL: https://www.theguardian.com/world/2022/may/25/death-to-the-enemy-ukraine-news-channels-unite-to-cover-war

49. Bergegruen V. *How Ukraine Is Crowdsourcing Digital Evidence of War Crimes* // *Time*. 2022. April 18. URL: https://time.com/6166781/ukraine-crowdsourcing-war-crimes/

50. Danchenkova O. *Ukraine's Hard-Won Approach to Strategic Communications and Counter-Disinformation: Lessons for Europe and Beyond*. 2025. March 12. URL: https://techpolicy.press/ukraines-hardwon-approach-to-strategic-communications-and-counterdisinformation-lessons-for-europe-and-beyond

51. Gugulashvili M. *Lessons of Democratic Resilience: the EU and NATO Approaches Against Disinformation and Propaganda*. Center for Strategic and Defensive Studies, 2023. P. 3–17. URL: https://www.csd.org.ge/storage/files/doc/Lessons%20of%20Democratic%20Resilience%20-%20%20the%20EU%20and%20NATO%20Approaches%20Against%20Disinformation%20and%20Propaganda%20(1).pdf

52. Giorio L. *EUvsDisinfo: A Case Study of Fact-Checking and Propaganda*. Uppsala University, 2018. P. 6–7. URL: https://uu.diva-portal.org/smash/get/diva2:1252061/FULLTEXT01.pdf

53. Thorne N., Vosoughi S., Roy D. *Lost in Translation - Multilingual Misinformation and its Evolution*. arXiv preprint, 2023. P. 3. URL: https://arxiv.org/pdf/2310.18089.pdf

54. Roslon D. T., Kruzhkova E. M., Syvulka U. I. *EU and NATO Strategy to Counter and Prevent Russian Propaganda* // Regional Studies. 2024. Vol. 36. P. 1–12. URL: http://regionalstudies.uzhnu.uz.ua/archive/36/18.pdf

55. Richter A. *Regional Security and Propaganda*. OSCE Framework, 2025. P. 1. URL: https://civicsolidarity.org/wp-content/uploads/2025/07/Regional-security-and-propaganda_Andrei-Richter_June-2025.pdf

56. Hansen L., Gill S. *NATO's Strategic Communications in Addressing Hybrid Threats* // Security Dialogue. 2021. P. 45–62. URL: https://connections-qj.org/system/files/download-count/23.1.06_War_Stratcom_1.pdf

57. Swanström N., Logan T. *G7 Strategy for Countering Russian Information Operations in the Indo-Pacific Region*. ISDP, 2025. P. 1–8. URL: https://www.isdc.eu/publication/g7-strategy-for-countering-russian-information-operations-in-the-indo-pacific-region-a-framework-for-enhanced-multilateral-coordination-and-response/

58. East StratCom Task Force. *Questions and Answers about the East StratCom Task Force*. EEAS, 2019. URL: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en

59. OSCE Representative on Freedom of Media. *Joint Statement on the Invasion of Ukraine and the Importance of Freedom of Expression and Information*. OSCE, 2022. P. 1–2. URL: https://www.osce.org/representative-on-freedom-of-media/517107

60. Ministry of Foreign Affairs of Japan. *The Responses to Information Manipulation, Including Disinformation*. Government of Japan, 2025. URL: https://www.mofa.go.jp/policy/pagewe_000001_00052.html

61. East StratCom Task Force. *East StratCom Task Force Overview*. Wikipedia, 2015. URL: https://en.wikipedia.org/wiki/East_StratCom_Task_Force

62. European Commission. *Countering Information Manipulation*. European Commission, 2025. URL: https://commission.europa.eu/topics/countering-information-manipulation_en

63. Залєвська І. І. Інформаційна безпека України в умовах російської військової агресії // Південноукраїнський юридичний часопис. 2022. Т. 2, № 1. С. 140–145.

64. Смотрич Д. Інформаційна безпека в умовах воєнного стану // Вісник Ужгородського національного університету. Серія: Право. 2023. Вип. 77, № 2. С. 1–20.

65. Мирошниченко А. І. Інформаційна політика в умовах воєнного стану // Публічне адміністрування: теорія та практика. 2023. Вип. 4(30). С. 1–15.

66. Лешик С. В. Інституційно-правовий механізм інформаційної політики України в процесі євроінтеграції // Журнал політичного та правового життя. 2024. Т. 3, № 16. С. 42–52.

67. Таран В. А., Лесик С. В. Інституційно-правовий механізм інформаційної політики України в процесі євроінтеграції // Журнал політичного та правового життя. 2024. Т. 3, № 16. С. 42–52.

68. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану // Актуальні проблеми політики. 2022. Вип. 1(22). С. 1–10.

69. Наместнік В. В. Інформаційні операції Росії проти України у 2022–2023 роках: висновки, рекомендації, засвоєні уроки // Наука і оборона. 2024. Т. 25, № 2. С. 58–64.

70. Ржевська Н. Сучасна інформаційна політика: досвід США для України. Інститут політичних і етнонаціональних досліджень, 2024. С. 1–20.

71. Наместнік В. В. Інформаційні операції Росії проти України у 2022–2023 роках // Науковий журнал Національного університету «Острозька академія». 2024. Т. 25, № 2. С. 58–64.

72. Горбань Ю. Медіаграмотність як чинник захисту інформаційного простору від ворожої дезінформації в час війни // Українська культура та комунікація. 2024. Т. 1, № 13. С. 20–28.

73. Довженко О., Єгорова А., Іванова Т. та ін. Медіаграмотність під час війни: теорія, методика, інтерактив. Навчальний посібник Асоціації підприємців України, 2023. С. 1–8.

74. Жаровська І., Ортинська Н. Інформаційна війна як сучасне глобалізаційне явище // Технологічні науки та природовідповідність. 2020. Т. 1, № 1. С. 58–64.

75. Кобець Т. Порівняльний аналіз технологій пропаганди та інформаційних операцій в умовах воєнного стану // Південноукраїнський правничий часопис. 2023. Т. 1, № 24. С. 58–64.

76. Авдєєва Т., Дворовий М. По кому подзвін: відповідальність за дезінформацію під час війни. Лабораторія цифрової безпеки, 2022. С. 1–15.

77. Правоохоронна служба України. Інформаційна безпека Україні в умовах воєнного стану // Вісник Львівського державного університету внутрішніх справ. 2025. С. 1–10.

78. Ніцевич О. В. Інформаційна безпека України в умовах гібридної загрози // Вісник Львівського державного університету внутрішніх справ. 2025. Т. 2, № 80. С. 1–5.

79. Соловей І. Стратегічні комунікації як важливий елемент національної безпеки України. Центр стратегічної комунікації та інформаційної безпеки, 2023. С. 1–10.

80. Мойсіяха А. В. Використання соціальних медіа в стратегічних комунікаціях органів державної влади для зміцнення національної безпеки України // Вісник Національної академії державного управління при Президентові України. 2023. Т. 3, № 1. С. 1–10.

81. Мойсіяха А. В. Використання соціальних медіа в комунікаційних стратегіях органів державної влади, спрямованих на зміцнення національної безпеки України // Вісник Національної академії державного управління при Президентові України. 2023. Т. 3, № 1. С. 1–10.

82. Статтарах В. А. Державна інформаційна політика України в умовах повномасштабного військового вторгнення Російської Федерації:

потенціал соціальної мобілізації та ефективність. Інститут політичних та етнонаціональних досліджень НАН України, 2024. С. 1–8.

83. Ващенко І. В., Полтавський Е. М. Теорія і практика проведення спеціальних інформаційних операцій в умовах російсько-української війни // Світ науки та освіти. 2024. С. 1–8.

84. Кобець Т. Порівняльний аналіз технологій пропаганди та інформаційних операцій в умовах воєнного стану // Південноукраїнський правничий часопис. 2023. Т. 1, № 24. С. 58–64.

85. Кримчук В. В. Еволюція стратегічних комунікацій сектору безпеки та оборони України як інструменту протидії інформаційним загрозам (2014–2025 рр.) // Журнал політичного та правового життя. 2025. Т. 3, № 13. С. 1–15.

86. Сегеда О. О. Цифрова дипломатія України як елемент нової публічної дипломатії // Політична наука. 2020. Т. 3, № 3. С. 1–15.

87. Наука – стратегічні комунікації. Центр стратегічної комунікації та інформаційної безпеки. 2025. С. 1–20.

88. Кубко В. Цифрова дипломатія в сучасних міжнародних відносинах: роль та значення // Філософія і суспільствознавство. 2023. Т. 50, № 1. С. 1–20.

89. Богомолов О., Компанцева Л., Заруба О. та ін. Стратегічні комунікації для безпекових і державних інституцій: практичний посібник. Фонд ім. Еберта, 2022. С. 1–20.

90. Мусієнко-Костюк О., Маркелов М. Підходи України до цифрової дипломатії в контексті геополітичних викликів // Вісник Київського національного університету ім. Тараса Шевченка. Серія: Міжнародні відносини. 2024. Т. 1, № 1. С. 1–10.

91. Нечипоренко А. О. Маніпулятивні технології у соціальних медіа: основні тактики та методи протидії // Наукові праці Міжрегіональної академії управління персоналом. Філологія. 2024. Т. 2, № 12. С. 1–15.

92. Гуцуляк Д. Фактчекінг як інструмент протидії дезінформації в умовах гібридних конфліктів // Наукові праці Міжрегіональної академії управління персоналом. Філологія. 2024. Т. 2, № 12. С. 1–10.

93. Самохвалов Ю. Як працює OSINT-розвідка? Від бізнес-аналізу до оборони України. ISSP Training Center, 2022. С. 1–10.

94. Галіпчак В. Д. Сучасні виклики та стратегії забезпечення інформаційної безпеки України в умовах гібридної війни // Дослідження Ужгородського національного університету. 2023. С. 1–15.

95. Журналісти ГБІЙ. Розслідування кіберзагроз: дезінформація та методи виявлення. Глобальна ініціатива журналістських розслідувань, 2024. С. 1–20.

96. Тома М. Г. Інструменти OSINT: фіксація воєнних злочинів в Україні // Актуальні проблеми управління та публічної політики. 2025. Т. 1, № 1. С. 1–20.

97. Назаркевич М. А., Мальцева А. О. Методи ідентифікації дезінформації, фейків та пропаганди в засобах масової інформації на основі машинного навчання // Кібербезпека та інформаційна безпека. 2024. Т. 1, № 25. С. 1–10.

98. Левченко О. В., Охрімчук В. В. Кібервплив і кіберзахист в умовах війни: особливості антиукраїнського інформаційного впливу на Україну // Захист інформації. 2022. Т. 24, № 4. С. 1–10.

99. Шемчук В. В. Інформаційна безпека та інформаційна оборона України як напрями державної політики // Юридичний вісник. Морський видавничий дім. 2019. № 4 (38). С. 45–58.

100. Сілаєв В. М. Політика інформаційної безпеки в умовах цифрової трансформації України // Журнал політичних досліджень. МАУП. 2024. № 12 (2). С. 28–45.

101. Указ Президента України від 28 грудня 2021 року № 685/2021 «Про введення в дію рішення Ради національної безпеки і оборони України від

15 жовтня 2021 року "Про Стратегію інформаційної безпеки"» // Офіційний вісник України. 2021. № 105. С. 18–25.

102. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII // Відомості Верховної Ради. 2017. № 45. С. 35–42.

103. Закон України «Про цифровий контент та цифрові послуги» // Відомості Верховної Ради. 2022. № 11. С. 1–8.

104. Європейська конвенція про захист прав людини та основних свобод від 4 листопада 1950 року. Офіційний переклад. Рада Європи, 2010. С. 1–32.

105. Братасюк О. Б., Ментух Н. Ф. Поняття та класифікація цифрових прав в Україні // Юридичний науковий електронний журнал. Запорізький національний університет. 2021. № 10. С. 58–61.

106. Гусаковська Т. О. Екосистема інноваційного підприємництва в умовах цифрової трансформації // Глобальна економіка журналу. Тернопільський національний технічний університет. 2025. № 2. С. 73–79.

107. Чертов В. І. Медіаграмотність як інструмент розпізнавання інформаційних ризиків. Білоцерківський інститут неперервної професійної освіти, 2024. С. 1–8.

108. Гуцуляк Д. В. Фактчекінг як інструмент протидії дезінформації в умовах гібридних конфліктів // Наукові праці Міжрегіональної академії управління персоналом. Філологія. 2024. № 2 (12). С. 3–18.

109. UNESCO. Нарис про медіа та інформаційну грамотність: п’ять принципів для демократії та правління. UNESCO, 2017. С. 1–24.

110. Council of Europe. Medijska i informacijska pismenost u Bosni i Hercegovini: Smjernice za politiku i strategiju. Council of Europe, 2020. С. 1–45.

SUMMARY

The Russian-Ukrainian War has fundamentally redefined the landscape of modern conflict, unveiling a new and exceptionally dangerous dimension: information warfare. The confrontation extends far beyond the physical battlefield, engaging the global information space where the ability to influence citizens' consciousness, emotions, and behavior has acquired strategic importance. This study's core relevance stems from the fact that information warfare has ceased to be merely a byproduct of armed aggression; it has evolved into an independent front with explicit objectives: undermining Ukrainian statehood, demoralizing society and the armed forces, discrediting the national leadership, and systematically eroding international support.

In the contemporary context, information is power, and control over narratives and meanings constitutes the paramount form of dominance. Consequently, the formulation, implementation, and effectiveness of state information policy are existential factors for Ukraine's national security. The urgency is further underscored by the nature of Russian aggression, which is not sporadic but systemic, technologically advanced, and strategically planned. The toolkit employed by the aggressor is comprehensive, spanning beyond conventional propaganda and disinformation to include large-scale cyber operations, calculated social media manipulation, extensive information-psychological influences, and subversive diplomatic communications.

As a nation subjected to a multi-domain hybrid war, Ukraine has been compelled to rapidly build its own model of information defense. This system is a sophisticated, multi-level construct integrating Strategic Communications (StratCom), cyber protection, professional fact-checking, OSINT (Open-Source Intelligence) analytics, digital diplomacy, and mass media literacy programs. The need for scholarly analysis of this phenomenon – its instruments, mechanisms, and consequences – as well as the assessment of Ukraine's counter-strategies, represents a critical imperative for political science and state governance practice. Ultimately, Ukraine has become a crucial proving ground for modern strategic communications

concepts, with its practical experience now setting the trends for global security policy in the digital age.

The study approaches information warfare as an interdisciplinary phenomenon at the intersection of military studies, political science, sociology, psychology, law, and cybersecurity. The object of the study is information warfare itself as a form of hybrid confrontation, which merges military, political, communicative, and technological means of influence. The subject is the informational dimension of the Russian-Ukrainian war, focusing on the aggressor's system of goals, tools, channels, and strategies, alongside the counteraction mechanisms employed by Ukraine and the international community.

A key conceptual distinction is made between information warfare (the most intense, offensive segment of conflict aimed at strategic goals), information confrontation (the broader set of measures to gain information advantage), and information security (the protective, regulatory, and technical regime ensuring the confidentiality, integrity, and availability of information and infrastructure resilience).

The methodology relies on systemic, historical-comparative, structural-functional, institutional, and interdisciplinary approaches. This multi-paradigm approach allows the analysis of cognitive, technological, and legal levels of conflict. Empirical methods include content analysis and discourse analysis of media materials, network analysis (SNA) to map propaganda spread, and the practical application of OSINT and fact-checking techniques to gather data.

The research identifies a clear hierarchy in Russia's information aggression goals, ranging from short-term aims like demoralizing the population and the armed forces to long-term strategic objectives, including undermining the legitimacy of the Ukrainian state and dissolving global international support. The deployed instrumentarium is sophisticated, encompassing not only traditional disinformation and propaganda but also the manipulation of historical memory, large-scale cyber operations, and the imitation of genuine public opinion.

A defining feature of the Russian hybrid strategy is the synchronization of information waves with kinetic military actions. Post-2022, the role of modern digital channels has significantly amplified, notably the use of social platforms like Telegram and TikTok, the strategic deployment of Artificial Intelligence (AI) for deepfakes and automated bot networks, and a concentrated effort to influence audiences in the Global South.

In response to this sophisticated threat, Ukraine successfully and rapidly established one of the world's most effective systems for Strategic Communications and counter-disinformation. Key institutional pillars include:

The Center for Strategic Communications and Information Security (StratCom Center).

The Center for Countering Disinformation under the National Security and Defense Council (NSDC).

The national television initiative, the «United News» telethon.

A robust ecosystem of independent fact-checking organizations (e.g., StopFake, VoxCheck).

Volunteer OSINT communities (e.g., InformNapalm).

This comprehensive infrastructure has drastically reduced the reaction time to information attacks to mere hours, enabled the proactive formation of counter-narratives, and fostered essential horizontal coordination between the state and civil society.

A critical finding is the synergistic effect between technical and psychological operations. Cyberattacks rarely occur in a vacuum; they are typically accompanied by information operations designed to trigger panic or erode trust in state institutions. Responding to a technical incident without simultaneous public communication creates a dangerous information vacuum that the aggressor quickly fills with disinformation. Therefore, an integrated StratCom architecture is essential, unifying military communications, foreign policy messaging, psychological operations, digital platform management, fact-checking, OSINT, and cybersecurity into a single, cohesive management cycle.

The study reveals that despite the overall success of Ukraine's defense, significant structural challenges remain. A major gap lies in cognitive resilience: statistics indicate that over two-thirds of Ukrainians do not engage in minimal source-checking practices. This vulnerability creates ideal conditions for the phenomenon of information fatigue, where citizens, constantly under stress in a high-pressure media environment, lose their critical capacity, over-rely on personal impressions, and become susceptible to emotional manipulation.

Consequently, the cultivation of media literacy must be viewed not as a secondary initiative, but as a mandatory component of national security. This requires a systemic, distributed approach that integrates critical thinking skills into formal education from an early age and through mass public programs for adults.

The research concludes with a forward-looking strategic vision, asserting that Ukraine has the potential to become a global leader in information and cognitive resilience by the end of the decade. The innovative «State + Civil Society + International Partners» model developed in Ukraine is already serving as a blueprint for countries such as Estonia, Lithuania, Taiwan, and Finland.

To achieve this leadership and establish a robust information environment, the following strategic recommendations are proposed:

Legislative Integration: Adopt a framework law on Strategic Communications and fully implement EU digital legislative standards, such as the Digital Services Act (DSA) and Digital Markets Act (DMA), ensuring all information restrictions adhere to the principles of necessity and proportionality.

Institutional Centralization: Create a unified Interagency Center for Cognitive Defense, reporting directly to the President, to streamline the integrated StratCom cycle and ensure rapid, whole-of-government action.

Technological Sovereignty: Deploy a national monitoring system (e.g., «Sich») and establish secure, redundant reserve broadcasting channels to guarantee information continuity during crises.

Human Capital Development: Make media literacy mandatory in schools and establish mass education programs for adults, viewing critical thinking as a prerequisite for national resilience.

International Integration: Achieve NATO StratCom Partner of Excellence status and ensure full integration into the EU Digital Single Market to align national standards with Euro-Atlantic security architectures.

Sustainable Funding: Establish an Information Resilience Fund with substantial annual budgets (e.g., $180–220 million, as suggested in the text's conclusion) secured through both domestic and international donor participation.

In sum, the Russian-Ukrainian information war stands historically as the first full-scale, 21st-century conflict in the cognitive domain, mobilizing all available modern technologies and engaging global audiences. Ukraine has not only successfully resisted this aggression but has also transformed into a world leader in crisis strategic communications and information resilience [See snippet from back]. The continued implementation of a proactive, integrated defense architecture will be essential not only for neutralizing the current Russian information threat but also for positioning Ukraine as a key center for shaping the new global information security architecture of the democratic world.