Політологія

УДК 32:323.2

DOI https://doi.org/10.5281/zenodo.16658818

Інформаційна війна в гібридних конфліктах: від пропаганди до кібервпливу

Кожушко Віктор Вікторович
здобувач третього (освітньо-наукового) рівня вищої освіти
кафедри політології, соціології і культурології,
Харківського національного педагогічного університету
імені Г.С. Сковороди, м. Харків, Україна,
viktorkozhusko@gmail.com,
https://orcid.org/0009-0007-8147-736X

Прийнято: 13.07.2025 | Опубліковано: 23.07.2025

Анотація. *Дослідження присвячене системному аналізу трансформаційної ролі діпфейк-технологій як ключового інструменту фабрикації реальності в сучасних інформаційних війнах, що розгортаються в умовах гібридних конфліктів. Додатковою метою є обґрунтування комплексних стратегій протидії їхньому деструктивному впливу на політичну довіру та стабільність демократичних інститутів. Досягнення поставленої мети забезпечено завдяки інтегративному застосуванню системного та порівняльного аналізу, що дозволило узагальнити концептуальні підходи до розуміння гібридних загроз, дослідити еволюцію методів інформаційного впливу та виявити якісну трансформацію, зумовлену розвитком штучного інтелекту. Використання кейс-стаді методу, зокрема на прикладі гібридної агресії Російської Федерації проти України, забезпечило глибоке вивчення прикладів*

застосування синтетичного медіа-контенту та його впливу на внутрішню й зовнішню стабільність.

Продемонстровано, що сучасні гібридні протистояння кардинально змінили парадигму конфлікту, перетворивши інформаційну сферу на стратегічний театр бойових дій. Обґрунтовано, що інформаційний вплив у таких конфліктах є самостійним, фундаментальним виміром, спрямованим на досягнення стратегічних цілей без використання традиційних військових засобів. Виявлено, що діпфейки, генеруючи гіперреалістичні сфабриковані аудіовізуальні матеріали, створюють безпрецедентну загрозу легітимності влади та суспільній злагоді, перетворюючи маніпуляцію інформацією на якісно новий рівень – фабрикацію реальності. На прикладі російсько-українського конфлікту проаналізовано стратегічний намір використання сфабрикованих відеоматеріалів для деморалізації, дезорієнтації та створення хибних наративів як всередині країни, так і для міжнародної аудиторії. Показано багатогранні ризики від комплексної дезінформації, що підриває соціальну єдність та громадську довіру. Ефективна протидія синтетичному контенту в інформаційних операціях вимагає багатовекторного та комплексного підходу, що включає розвиток технологічної асиметрії (розробка інструментів виявлення), формування суспільної стійкості (медіаграмотність та критичне мислення) та поглиблену міжнародну співпрацю в правовому полі. Дослідження підкреслює критичну важливість вивчення впливу глибинних фейків для архітектури національної та міжнародної безпеки, пропонуючи пріоритетні напрямки для розробки ефективних контрзаходів. Результати мають практичне значення для стратегій кіберзахисту та формування державних комунікацій.

Ключові слова: *гібридна війна, інформаційні операції, дезінформація, діпфейки, кіберзагрози, фабрикація реальності, національна безпека, контрзаходи.*

Information Warfare in Hybrid Conflicts: From Propaganda to Cyber Influence

Viktor Kozhushko

PhD student, Department of Political Science, Sociology and Cultural Studies

H.S. Skovoroda Kharkiv National Pedagogical University, Kharkiv,

viktorkozhusko@gmail.com,

https://orcid.org/0009-0007-8147-736X

Abstract. *This study is devoted to a systematic analysis of the transformative role of deepfake technologies as a key tool for reality fabrication in modern information warfare unfolding in the context of hybrid conflicts. An additional goal is to substantiate comprehensive strategies for countering their destructive impact on political trust and the stability of democratic institutions. The achievement of this objective was ensured through the integrative application of systemic and comparative analysis, which allowed for the generalization of conceptual approaches to understanding hybrid threats, the exploration of the evolution of information influence methods, and the identification of a qualitative transformation caused by the development of artificial intelligence. The case study method, particularly using the example of the hybrid aggression of the Russian Federation against Ukraine, provided an in-depth examination of the application of synthetic media content and its impact on internal and external stability.*

It is demonstrated that modern hybrid confrontations have fundamentally altered the paradigm of conflict, transforming the information domain into a strategic theater of operations. It is argued that information influence in such conflicts constitutes an independent, fundamental dimension aimed at achieving strategic goals without the use of traditional military means. The research reveals that deepfakes, by generating hyperrealistic fabricated audiovisual materials, pose an unprecedented threat to the legitimacy of authority and social cohesion, elevating information manipulation to a qualitatively new level – the fabrication of reality. Using the example of the Russian-Ukrainian conflict, the strategic intent behind the use of fabricated

video materials for demoralization, disorientation, and the creation of false narratives both domestically and for an international audience is analyzed. The multifaceted risks of complex disinformation that undermines social unity and public trust are highlighted. Effective counteraction to synthetic content in information operations necessitates a multi-vector and comprehensive approach, including the development of technological asymmetry (e.g., advanced detection tools), the cultivation of societal resilience (media literacy and critical thinking), and enhanced international cooperation in the legal domain. The study emphasizes the critical importance of investigating the impact of deepfakes for the architecture of national and international security, suggesting priority areas for the development of effective countermeasures. The findings have practical significance for cyber defense strategies and the formation of state communications.

Keywords: *hybrid warfare, information operations, disinformation, deepfakes, cyber threats, reality fabrication, national security, countermeasures.*

Постановка проблеми. У сучасному геополітичному ландшафті спостерігається кардинальна трансформація сутності та методів ведення військово-політичних конфліктів. Традиційні лінії фронту дедалі більше розмиваються, поступаючись місцем гібридним конфліктам, які, за визначенням багатьох дослідників, інтегрують силові, економічні, політичні, інформаційні та кібернетичні операції [23; 26; 27; 39]. Багатовекторний характер гібридних конфліктів ускладнює ідентифікацію їхніх суб'єктів, оскільки до протистояння активно залучаються окрім держав та їхніх збройних сил транснаціональні корпорації, приватні військові компанії, хакерські угруповання, медіаресурси та окремі агенти. Відтак, постає принципово нова реальність, що характеризується розмиванням меж між станом миру та війни. Це зумовлює перетворення суспільств на перманентний об'єкт цілеспрямованого впливу та маніпуляцій, значно розширюючи коло потенційних суб'єктів ураження та об'єктів агресії за межі безпосередньої зони бойових дій [2; 8; 15].

Як зазначав ще наприкінці XX ст. М. Маклюен: «Інформація є не лише засобом ведення війни, але й ставкою війни» [27]. В умовах кардинальних трансформацій цифрової епохи інформація перестає бути лише допоміжним засобом ведення війни, а дійсно набуває статусу її ключової ставки. Глобальний інформаційний простір становить динамічну арену, де створення, зберігання, обробка та поширення даних перетворюються на потужну зброю XXI століття [6; 36]. Сучасні дослідники підкреслюють, що інформаційна війна, яка історично розглядалася переважно як вторинний або допоміжний елемент військової стратегії, нині еволюціонувала до статусу самостійної та провідної складової гібридного конфлікту [1; 4; 7; 14; 17; 34]. Вона здатна формувати необхідний інформаційний фон задовго до початку збройних дій, дезорієнтувати противника та деморалізувати його населення під час активних фаз, а також підтримувати довгострокову дестабілізацію в постконфліктний період [14; 28; 31; 37]. Арсенал інформаційної війни значно розширився: від класичних методів пропаганди та психологічних операцій до високотехнологічних кібероперацій, використання масштабних ботоферм, мереж тролів, а також прогресивних технологій штучного інтелекту (ШІ) для створення діпфейків, що дозволяє маніпулювати суспільною думкою з безпрецедентною точністю та масштабом [8; 20; 24; 29; 35]. Суть інформаційної війни полягає у контролі над свідомістю, емоціями та поведінкою цільової аудиторії [5; 21; 32]. Шляхом маніпуляції інформацією, поширення відвертої дезінформації та цілеспрямованої пропаганди агресор прагне змінити сприйняття реальності, підірвати довіру до державних інститутів, посіяти соціальну напругу і, зрештою, послабити спроможність держави та суспільства до ефективного опору.

Дослідження інформаційної війни набуває критичної важливості в контексті широкого спектра гібридних загроз, що походять від сучасних автократичних режимів. Досвід України, яка нині переживає повномасштабну збройну агресію з боку Росії, беззаперечно свідчить про те, що руйнівна дія найпотужніших інформаційних кампаній співставна зі зброєю [1; 2; 18; 20; 25; 31; 37], а отже актуальність ґрунтовного дослідження цієї проблематики є

безальтернативною. Таке дослідження становить невід'ємну частину архітектури національної та колективної безпеки демократичного світу, виступаючи ключовим пріоритетом для розробки ефективних контрзаходів і зміцнення безпеки перед лицем сучасних гібридних викликів.

Аналіз останніх досліджень і публікацій. У вирі сучасних гібридних конфліктів, де інформаційний простір перетворився на ключову арену протистояння, феномен інформаційної війни привертає дедалі більшу увагу як західних, так і українських дослідників. Аналіз сутності гібридної війни, її еволюції та механізмів протидії є ключовим напрямком досліджень, що розкривається у працях провідних західних експертів, які акцентують увагу на теоретичних аспектах гібридних конфліктів, їх нелінійному характері та багатовекторності. Зокрема, значний внесок у розуміння гібридної війни зробили С.-Д. Бахманн, Д. Паттер і Г. Дучинський, аналізуючи її з української перспективи [8]. Концептуальні виклики та відповіді на «кібергібридні» загрози вивчає А. Міссіролі [28], а С. Мараренс та Й. Шрьофль зосереджуються на когнітивній перспективі гібридної війни у російсько-українському конфлікті [25]. Теоретичні засади гібридної війни також розглядаються Е. Райхборн-К'єннерудом та П. Калленом [33].

Особливу актуальність в контексті сучасної гібридної агресії набувають дослідження, присвячені впливу технологій ШІ та діпфейків на інформаційну безпеку та політичні процеси. Дж. Бота та Х. Пітерс ще у 2020 році наголошували на небезпеці фейкових новин та діпфейків для інформаційної безпеки XXI століття [12]. Роль ШІ в поширенні дезінформації розглядають Н. Бонтріддер та Й. Пуллет [11]. Деструктивний потенціал діпфейків як інструменту дезінформації та мови ворожнечі, що загрожує демократичним функціям, глибоко аналізує М. Павелець [30]. В.М. Лім досліджує діпфейки та фейкові новини в контексті інфодемії, підкреслюючи пошук істини в потоці дезінформації та малінформації [24]. Т.С. Хелмус детально розкриває роль ШІ, діпфейків та дезінформації як загроз [22]. Візуальній дезінформації в цифрову епоху присвячено синтез літератури та дослідницьку програму Т. Вайкманна та

С. Лехелера [38], а К. Ясар з колегами досліджує саму технологію діпфейків [40]. Т. Рід аналізує таємну історію дезінформації та політичної війни, що є важливим фоном для розуміння сучасних викликів [35]. Т. Солмаз досліджує гібридну війну як приклад концептуального розширення [36].

Серед вітчизняних науковців, які зробили значний внесок у дослідження проблематики інформаційних війн та їх інструментів, таких як пропаганда, дезінформація, фейкові новини, слід відзначити праці І. Дерев'янко, яка аналізує гібридну війну як різновид асиметричних дій [3], І. Патлашинської, яка досліджує сучасну російсько-українську інформаційну війну, її завдання та методи [5], та І. Фещенко, що розглядає інформаційну війну як органічну складову сучасного збройно-політичного конфлікту [7]. Ці дослідження розкривають складні механізми маніпуляції інформацією та підкреслюють необхідність розвитку критичного мислення в умовах інформаційної війни.

Виділення невирішених раніше частин загальної проблеми. Сучасна наукова думка приділяє значну увагу феномену гібридних конфліктів та інформаційної війни як їх невід'ємного компонента. Проте, попри широкий спектр існуючих досліджень, залишаються недостатньо вивченими питання, пов'язані з якісно новою природою дезінформації, зумовленою стрімким розвитком технологій штучного інтелекту. Існуючі наукові роботи часто описують діпфейки як технічний феномен або розглядають їхній вплив фрагментарно, без системного аналізу їх інтеграції у стратегічні цілі гібридної війни та без комплексного підходу до протидії.

Зокрема, бракує ґрунтовного дослідження того, як діпфейк-технології трансформують маніпуляцію інформацією на справжню фабрикацію реальності, та які механізми захисту від цього нового виміру кібервпливу є найбільш ефективними для забезпечення політичної довіри та стабільності демократичних інститутів. Необхідність подальшого дослідження цих аспектів аргументується безпрецедентною здатністю діпфейків миттєво підривати легітимність влади, сіяти паніку та дестабілізувати суспільство, що робить їх критичною загрозою національній та колективній безпеці. Ця стаття прагне заповнити існуючі

прогалини, зосередившись на системному аналізі глибинного впливу діпфейків у контексті гібридних війн, зокрема на прикладі України, та обґрунтуванні практичних рекомендацій щодо багатовекторної протидії.

Формулювання цілей статті (постановка завдання). Мета статті – системний аналіз трансформаційної ролі діпфейк-технологій як ключового інструменту фабрикації реальності в інформаційних війнах XXI століття в контексті гібридних конфліктів, а також обґрунтування комплексних стратегій протидії їх деструктивному впливу на політичну довіру та стабільність демократичних інститутів.

Для досягнення поставленої мети визначено такі завдання:

– Узагальнити сучасні концептуальні підходи до розуміння гібридних війн та ролі інформаційного компонента в них.
– Дослідити еволюцію форм та методів інформаційної війни від традиційної пропаганди до високотехнологічного кібервпливу, виокремивши якісну трансформацію, зумовлену розвитком штучного інтелекту.
– Проаналізувати унікальний потенціал діпфейк-технологій як інструменту фабрикації реальності та їхній руйнівний вплив на інститут політичної довіри.
– Вивчити практичні кейси застосування діпфейків у гібридних конфліктах, зокрема на прикладі агресії Російської Федерації проти України, та їхній вплив на внутрішню і зовнішню стабільність.
– Систематизувати та обґрунтувати ключові напрямки ефективної протидії діпфейк-контенту, включаючи технологічні, суспільні та міжнародно-правові аспекти.

Виклад основного матеріалу дослідження. Сучасне розуміння конфлікту зазнало суттєвих трансформацій, відійшовши від класичних уявлень про симетричні та лінійні протистояння між державами. У цьому контексті гібридна війна постає як ключова рамка для осмислення багатовимірних загроз XXI століття. Серед найбільш авторитетних визначень, що формують основу для

розуміння гібридних загроз, є позиція Ф. Гоффмана. У своїй роботі «Конфлікт у 21 столітті: піднесення гібридних війн» [23] дослідник стверджує, що гібридні війни інтегрують широкий спектр традиційних та нетрадиційних тактик, які розгортаються одночасно. Гоффман наголошує: «Гібридні війни включають низку різних способів ведення війни, включаючи звичайні засоби, нерегулярні тактики та формування, терористичні акти, включаючи невибіркове насильство та примус, а також кримінальні заворушення» [23, p. 8]. Розвиваючи цю думку, Р. Гленн (2009) визначає «гібридну загрозу» як «противника, який одночасно та адаптивно використовує певну комбінацію (1) політичних, військових, економічних, соціальних та інформаційних засобів, і (2) звичайних, нерегулярних, катастрофічних, терористичних та руйнівних/кримінальних методів ведення війни» [21]. Дослідники В. Мюррей та П. Мансур також підкреслюють концепцію злиття різноманітних засобів боротьби у гібридних конфліктах [29]. Однак, попри широке використання, дефініція «гібридна війна» залишається предметом інтенсивних наукових та військово-аналітичних дискусій, що свідчить про багатогранність та динамічність самого явища [36]. Узагальнюючи численні публікації та експертні дискурси, Т. Солмайз виділяє п'ять основних інтерпретацій «гібридної війни», що відображають різноманіття її проявів та підходів до визначення:

1. Використання синергетичного поєднання звичайної зброї, нерегулярної тактики, тероризму та злочинної діяльності в одному бойовому просторі.
2. Спільне застосування регулярних та нерегулярних сил під єдиним керівництвом.
3. Застосування широкого спектра військових та невійськових засобів для загрози ворогу.
4. Підпорогова діяльність, що включає будь-яке поєднання насильницьких та ненасильницьких засобів впливу.
5. Спосіб досягнення політичних цілей за допомогою ненасильницької підривної діяльності [36].

Для цілей цього дослідження, що сфокусоване на інформаційному вимірі конфліктів, особливо релевантними є інтерпретації Т. Солмайз, які підкреслюють застосування широкого спектра військових та невійськових засобів (п. 3), підпорогову діяльність (п. 4) та досягнення політичних цілей за допомогою ненасильницької підривної діяльності (п. 5), що створює широке концептуальне поле для аналізу інформаційної війни як ключового компонента сучасних гібридних загроз.

Незважаючи на наявні у наукових колах широкі дискусії щодо історичних паралелей з війнами минулого століття та термінологічної узгодженості, зокрема стосовно таких понять, як «нова війна», «війна четвертого покоління» та «асиметрична війна» [37], інформаційна війна в гібридних конфліктах XXI століття розглядається як принципово нове явище [17; 34]. Її визначальною ознакою є комплексне використання ворожою стороною некінетичних інструментів, що охоплюють кібератаки, цілеспрямовану пропаганду, дезінформацію, маніпуляцію думкою громадськості, втручання у вибори, провокування міграційних криз, економічний примус, дипломатичний тиск тощо [15; 16; 17; 18]. Ці методи органічно інтегруються з військовими засобами задля досягнення стратегічних військово-політичних цілей, а їхня ефективність значною мірою залежить від здатності впливати на суспільну свідомість. При цьому діпфейки виступають особливо потужним інструментом дезінформації та маніпуляції, що зумовлює руйнівні наслідки в сучасних інформаційних війнах.

Домінуюча роль інформаційного компоненту в гібридних конфліктах базується на глибокому розумінні природи комунікацій та суспільної свідомості, а головне – механізмів впливу на них. Видатні мислителі XX століття, такі як Е. Бернейс [10], Ж. Бодрійяр [9], М. Маклюен [27], Н. Хомський [13] та інші, заклали теоретичні основи для аналізу інформаційно-комунікаційного простору, переконливо доводячи, що пропаганда та формування громадської думки є потужними інструментами для досягнення політичних цілей. Однак у XXI столітті ці фундаментальні концепції набувають якісно нового виміру завдяки стрімкому розвитку штучного інтелекту (ШІ), що відкриває безпрецедентні

можливості для маніпуляції суспільством. Зокрема, діпфейк-технології, генеруючи гіперреалістичний сфабрикований аудіовізуальний контент, не просто посилюють існуючі методи впливу, а й втілюють ідеї про «інженерію згоди» та «гіперреальність» [27] на безпрецедентному технологічному рівні, перетворюючи їх на потужну дезінформаційну зброю.

Базуючись на теоретичних засадах розуміння інформаційного впливу, арсенал інформаційної війни зазнав якісного розширення, трансформуючись від класичних методів до високотехнологічних інструментів. Якщо традиційна пропаганда та психологічні операції XX століття, що спиралися на мас-медіа, мали обмежений масштаб та швидкість поширення, то сучасні методи охоплюють значно ширший спектр впливу та масштаб. Це включає складні кібероперації, що порушують роботу критичної інфраструктури, використання автоматизованих ботоферм та мереж інтернет-тролів для масштабування маніпулятивного контенту, а також застосування передових технологій, таких як діпфейки та алгоритми ШІ для створення переконливих, але фальшивих медіаматеріалів [12; 18; 19; 35]. Ці інструменти дозволяють реалізовувати тонкі та ефективні механізми дезінформації та цілеспрямованої пропаганди, стираючи межі між фактом і вигадкою, а їхня блискавичність та масштабованість поширення значно посилюють вплив на всіх етапах конфлікту [2; 23; 37].

Особливо руйнівним цей вплив є для інституту політичної довіри – фундаментальної основи суспільного договору між владою та громадянами. Діпфейки перетворюють маніпуляцію інформацією на справжню фабрикацію реальності, де візуальна та аудіовізуальна достовірність використовується для створення переконливих альтернативних наративів, які надзвичайно важко відрізнити від справжніх подій [27]. Це дозволяє суб’єктам інформаційної війни генерувати «медійні події», які ніколи не відбувалися, але виглядають абсолютно достовірно для пересічної аудиторії. Фальшиві звернення державних діячів, сфабриковані публічні виступи або неправдиві повідомлення від представників влади, створені за допомогою ШІ, можуть миттєво підірвати легітимність рішень, посіяти паніку, спровокувати громадянські заворушення та загалом

дестабілізувати політичну систему [12; 25; 27; 34; 38]. Ця здатність до швидкого і масштабного поширення в цифрових мережах робить діпфейки ідеальним інструментом для атак у гібридних конфліктах, де ключовим є некінетичний вплив на свідомість і волю цільової аудиторії.

Саме тому сучасні автократичні режими, використовуючи можливості цифрового інформаційного простору, отримують розширений інструментарій для здійснення пропаганди та дезінформації. Зокрема, у контексті дій Російської Федерації спостерігається послідовне використання історичних практик радянської пропаганди [15; 17; 32; 35], поширення наративів щодо загрози з боку НАТО та утисків російськомовного населення. Росія проводить цілеспрямовану діяльність з дестабілізації як всередині України, так і за її межами. Яскравим прикладом деструктивної діяльності є один з найбільш відомих діпфейків РФ – сфабриковане відеозвернення президента В. Зеленського до Збройних Сил України із закликом скласти зброю, поширене на початку повномасштабного вторгнення. Цей епізод демонструє стратегічний намір ворога підірвати бойовий дух та волю до спротиву.

Паралельно, РФ, залучаючи медійних акторів, зокрема проросійських політиків, телеграм-каналів та блогерів, здійснювала цілеспрямовану дестабілізаційну діяльність, що мала подвійну спрямованість [31; 37; 39]:

Внутрішня дестабілізація в Україні: посилення недовіри українців до влади та Збройних Сил України, сприяння поляризації суспільства та підрив національної єдності, що створює внутрішній хаос і послаблює спроможність держави до опору.

Дискредитація України за кордоном: російські діпфейки, орієнтовані на аудиторію країн ЄС та інших партнерів України, спрямовані на системну дискредитацію української влади, військових та, зокрема, українських біженців. Прикладом є численні сфабриковані матеріали, що намагаються представити українців у негативному світлі або спровокувати негативне ставлення до них у приймаючих країнах.

Таким чином, ці атаки спрямовані на кілька напрямків одночасно, щоб мати максимальний тиск, підірвати підтримку України зсередини та ззовні, і відтак підсилити військові атаки на полі бою.

У контексті агресивної гібридної війни Росії проти України, інформаційна війна виступає не просто як допоміжний інструмент, а як фундаментальний, інтегральний вимір конфлікту, спрямований на досягнення стратегічних цілей без прямого кінетичного впливу. Ключові методи ворожої інформаційної кампанії відображають глибоке розуміння когнітивного простору цільових аудиторій. Серед них виділяється стратегія деморалізації, що має на меті підірвати бойовий дух армії та суспільства, а також інспірування державної зради через цілеспрямовані психологічні операції. Паралельно розгортається масштабна кампанія зі створення фейкового медіа-образу подій, де активно формуються та поширюються альтернативні реальності – від ілюзії масової підтримки агресора на окупованих територіях до повного перекручення фактів [1; 2; 6; 8; 14; 25]. Наратив про «неонацистів» в Україні та утиски російськомовного населення є яскравим прикладом стратегічного фреймінгу, покликаного делегітимізувати українську державність, її суб'єктність на міжнародній арені та виправдати неспровоковану агресію. Ескалація з 24 лютого 2022 року лише посилила інтенсивність цих кампаній, задіявши весь спектр комунікаційних каналів – від традиційних ЗМІ до глобальних соціальних мереж та цифрових платформ, демонструючи адаптивність та багатовимірність російської інформаційної агресії.

Ризики, пов'язані з такою комплексною інформаційною війною, є багатогранними та мають довгострокові наслідки. Насамперед, існує загроза ерозії соціальної єдності в цільовій країні, підриву довіри до державних інститутів та медіа, що створює сприятливе середовище для внутрішньої дестабілізації. Для агресора, як показано, ключовим ризиком є необхідність концентрації на підтримці внутрішньої легітимності конфлікту, що веде до інтенсивного «зомбування» власного населення та формування агресивних, антизахідних настроїв. Це створює небезпечну «бульбашку реальності», яка

унеможливлює раціональний діалог і сприяє тривалій підтримці автократичного режиму. Водночас, здатність України ефективно протистояти цим викликам, забезпечуючи чітку комунікацію з власним суспільством та міжнародними партнерами, свідчить про важливість розбудови національної стійкості до дезінформації. Це включає не лише технічні можливості, а й критичне мислення громадян, що є ключовим у протидії інформаційному впливу, який прагне спотворити сприйняття дійсності та досягти політичних цілей через маніпуляції свідомістю.

Висновки. Проведене дослідження переконливо демонструє, що сучасні гібридні конфлікти кардинально змінили парадигму війни, перетворивши інформаційний простір на критично важливий театр бойових дій. У цьому контексті інформаційна війна утвердилася як невід'ємний і фундаментальний вимір конфлікту, спрямований на досягнення стратегічних політичних цілей через некінетичний, але руйнівний вплив. Центральним відкриттям цієї трансформації є поява та стрімке поширення діпфейк-технологій, які якісно змінюють природу дезінформації, перетворюючи маніпуляцію інформацією на справжню фабрикацію реальності.

Аналіз показав, що діпфейк-контент, генеруючи гіперреалістичні сфабриковані аудіовізуальні матеріали, створює безпрецедентну загрозу інституту політичної довіри та стабільності демократичних систем. Досвід агресивної гібридної війни Російської Федерації проти України яскраво ілюструє, як ці передові інструменти використовуються для деморалізації, дезорієнтації, делегітимізації та створення альтернативних реалій. Швидкість та масштабованість поширення такого контенту в цифрову епоху значно посилюють його деструктивний потенціал. У світлі виявлених загроз, стратегічна протидія діпфейк-контенту є невідкладним імперативом для національної та колективної безпеки. Вона вимагає багатовекторного та комплексного підходу:

Технологічна асиметрія: необхідна постійна розробка та впровадження високоточних, адаптивних інструментів виявлення та спростування діпфейків на

основі штучного інтелекту, що дозволить ефективно протистояти технологічним перевагам агресора.

Формування суспільної стійкості: критично важливим є системне підвищення медіаграмотності населення та розвиток критичного мислення, а також забезпечення прозорої та достовірної комунікації з боку держави. Це забезпечить суспільству здатність розпізнавати та протистояти маніпуляціям, зміцнюючи внутрішню стійкість.

Міжнародна координація та правове поле: жодна країна не може ефективно протистояти цій транснаціональній загрозі самостійно. Майбутня архітектура безпеки має ґрунтуватися на поглибленому міжнародному співробітництві, оперативному обміні інформацією, координації контрнаративів та узгодженні універсальних правових та етичних механізмів регулювання використання ШІ та синтетичного контенту. Отже, ефективна протидія гібридним викликам XXI століття та забезпечення стабільності демократичних інститутів в умовах безперервної фабрикації реальності можливі лише за умови інтеграції всіх окреслених стратегічних напрямків: від розробки та імплементації передових технологій захисту до виховання свідомого громадянського суспільства та формування міцних міжнародних альянсів.

Перспективними напрямками подальших досліджень у цій царині є розробка комплексних моделей оцінки впливу діпфейків на політичну довіру в різних суспільствах, аналіз ефективності існуючих законодавчих ініціатив у протидії кібервпливу, а також дослідження можливостей штучного інтелекту для проактивного виявлення та нейтралізації діпфейк-кампаній в умовах інформаційних війн.

Список використаних джерел

1. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові Україні*. 2015. № 1. С. 136–141. http://nbuv.gov.ua/UJRN/Vnadu_2015_1_21

2. Горбулін В. П. Світова гібридна війна: український фронт. К. : НІСД, 2017. – 496 с.

3. Дерев'янко І.П. Гібридна війна як різновид асиметричних дій. *Міжнародні відносини: теоретико-практичні аспекти*. 2023. № 11. С. 6–16. DOI:10.31866/2616-745X.11.2023.278396

4. Калініченко Б. Визначальні напрями формування стратегії протистояння інформаційній війні. *Держава і право. Серія: Політичні науки*. 2019. № 83. С. 61–73.

5. Патлашинська І. В. Сучасна російсько-українська інформаційна війна: Завдання, методи та особливості використання. *Науковий вісник Ужгородського національного університету. Серія: Політологія. Соціологія. Філософія*. 2022. № 28. С. 154–159. https://doi.org/10.32782/2663-6170/2022.28.15

6. Почепцов Г. Г. Сучасні інформаційні війни [Текст] / Георгій Почепцов. - Київ : Києво-Могилянська академія. 2015. – 495 с.

7. Фещенко. І. В. Інформаційна війна як органічна складова сучасного збройно-політичного конфлікту. *Філософія та політологія в контексті сучасної культури*. 2021. Вип. 13(1). С. 96–103. https://doi.org/10.15421/352111

8. Bachmann, S.-D. D., Putter, D., & Duczynski, G. (2023). Hybrid warfare and disinformation: A Ukraine war perspective. *Global Policy*, 14(5), 858–869. https://doi.org/10.1111/1758-5899.13257

9. Baudrillard, J. (1981). *Simulacra and Simulation*. Semiotext(e).

10. Bernays, E. L. (1928). *Propaganda*. Horace Liveright.

11. Bontridder, N., & Poullet, Y. (2021). The role of artificial intelligence in disinformation. *Data & Policy*, 3, e32.

12. Botha, J. & Pieterse, H. (2020). Fake News and Deepfakes: A Dangerous Threat for 21st Century Information Security. *Proceedings of the 15th International Conference on Cyber Warfare and Security*, 57-67. Norfolk, Virginia, USA.

13. Chomsky, N., & Herman, E. S. (1988). *Manufacturing Consent: The Political Economy of the Mass Media*. Pantheon Books.

14. Darczewska, J. (2014). The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study. *Point of View*, 42. Centre for Eastern Studies.

15. Der Spiegel. (2016). The hybrid war. Russia's propaganda campaign against Germany. *Der Spiegel*. https://www.spiegel.de/international/europe/putin-wages-hybrid-war-on-germany-and-west-a-1075483.htm l

16. EURACTIV. (2017). Tillerson: Russian vote meddling was 'hybrid warfare'. *EURACTIV*. https://www.euractiv.com/section/global-europe/news/tillerson-russian-vote-meddling-was-hybrid-warfare/

17. Fridman, O. (2018). *Russian "Hybrid Warfare": Resurgence and Politicisation.* Hurst.

18. Galeotti, M. (2016). *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military operations straight* (A New Generation Warfare Project Paper). The Jamestown Foundation.

19. Gelfert, A. (2018). Fake News: A Definition. *Informal Logic*, 38(1), 84-117.

20. Giles, K. (2016). Handbook of Russian Information Warfare. NATO Defense College.

21. Glenn, R. W. (2009). Thoughts on "Hybrid" Conflict. *Small Wars Journal*. https://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf

22. Helmus, T. C. (2022). Artificial intelligence, deepfakes, and disinformation. *Rand Corporation*, 1-24.

23. Hoffman, F. (2007). *Conflict in the Twenty-First Century: The Rise of Hybrid Warfare*. Potomac Institute for Policy Studies.

24. Lim, W. M. (2023). Fact or fake? The search for truth in an infodemic of disinformation, misinformation, and malinformation with deepfake and fake news. *Journal of Strategic Marketing*, 1-37.

25. Marahrens, S., & Schröfl, J. (2024). The Russia-Ukraine conflict from a hybrid warfare cognitive perspective. TDHJ. URL: https://tdhj.org/blog/post/russia-ukraine-hybrid-cognitive-warfare/

26. McCulloh, T., & Johnson, R. (2013). *Hybrid Warfare. MacDill Air Force Base*, Joint Special Operations University Press.

27. McLuhan, M. (1989). *The Global Village: Transformations in World Life and Media in the 21st Century*. Oxford University Press.

28. Missiroli, A. (2024). From hybrid warfare to'cybrid'threats-and back? Concepts, challenges, responses. In *Addressing Hybrid Threats* (pp. 40-56). Edward Elgar Publishin

29. Murray, W., & Mansoor, P. (Eds.). (2012). *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge University Press.

30. Pawelec, M. (2022). Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions. *Digital society*, 1(2), 19.

31. Pomerantsev, P. (2014). *Nothing is True and Everything is Possible: The Surreal Heart of the New Russia*. PublicAffairs.

32. Pomerantsev, P. (2019). *This is not propaganda: Adventures in the war against reality.* PublicAffairs.

33. Reichborn-Kjennerud, E., & Cullen, P. (2022). What is hybrid warfare?. Norwegian Institute for International Affairs (NUPI).

34. Rid, T. (2016). *Cyber war will not take place*. Oxford University Press.

35. Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare.* Farrar, Straus and Giroux.

36. Solmaz, T. (2022, February 25). 'Hybrid Warfare': A dramatic example of conceptual stretching. *Small Wars Journal*. https://smallwarsjournal.com/2022/02/25/hybrid-warfare-one-term-many-meanings/

37. Thornton, R. (2015). The Changing Nature of Modern Warfare; Responding to Russian Information Warfare. *RUSI Journal*, 160(4), 40–48.

38. Weikmann, T., & Lecheler, S. (2023). Visual disinformation in a digital age: A literature synthesis and research agenda. *New Media & Society*, 25(12), 3696-3713.

39. Weissmann, M. (2019). Hybrid warfare and hybrid threats today and tomorrow: Towards an analytical framework. *Journal on Baltic Security*, 5(1), 17–26.

40. Yasar, K., Barney, N., & Wigmore, I. (2024). What is deepfake technology? *TechTarget.* URL: https://www.techtarget.com/whatis/definition/deepfake