УДК 327.8:316.77
DOI https://doi.org/10.32782/2312-1815/2026-23-10

Тарас Кобець
ORCID: 0009-0001-2179-321X

КОГНІТИВНА БЕЗПЕКА ТА СУСПІЛЬНА СТІЙКІСТЬ: ПРОТИДІЯ ІНФОРМАЦІЙНОМУ ТИСКУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

У статті розкрито сутність когнітивної війни як ключового компоненту гібридної агресії Росії проти України. На основі глибокого аналізу конкретних кейсів (зокрема, кампанії дезінформації про «біолабораторії», маніпулятивних наративів у соцмережах та кібератак на критичну інфраструктуру) та емпіричних даних моніторингових платформ визначено три етапи еволюції системи когнітивної безпеки України (2014–2021, 2022–2023, 2024 – дотепер). Ядром дослідження є розроблена комплексна модель формування суспільної стійкості, яка інтегрує три взаємопов'язані стовпи: суспільний (розвиток медіаграмотності, масова освіта, фактчекінг), технологічний (аналітика великих даних для виявлення загроз, кіберзахист, боротьба з глибокими підробками) та регуляторний (гармонізація законодавства з євронормами, зокрема GDPR та AI Act). Особливу увагу приділено адаптації моделі до екстремальних умов воєнного стану – інформаційної фрагментації через масову міграцію населення, енергетичних блекаутів та обмеження доступу до глобальних платформ. Емпірично доведено, що впровадження запропонованої моделі дозволяє знизити вплив дезінформаційних кампаній на 20–30% та значно підвищити здатність суспільства до колективного спротиву маніпуляціям. Когнітивна безпека аргументовано позиціонується як стратегічний імператив для збереження інформаційного суверенітету та національної безпеки України в умовах триваючого гібридного протистояння.

Ключові слова: *когнітивна війна, когнітивна безпека, суспільна стійкість, гібридна війна, дезінформація, медіаграмотність, штучний інтелект.*

Вступ. У сучасну епоху стрімкої цифровізації парадигма національної безпеки зазнає докорінної трансформації, вийшовши за межі класичних вимірів військової, політичної та економічної стабільності. Все більшого значення набуває когнітивна сфера суспільства – простір, у якому формуються спільні смисли, цінності, судження та колективна ідентичність. Саме ця сфера стала центральним фронтом гібридних конфліктів нового покоління, де інформаційно-психологічний тиск реалізується з не меншою стратегічною вагою, ніж класичні військові засоби. Ключовим елементом таких протистоянь є когнітивна війна – комплексна діяльність, спрямована на зміну сприйняття реальності, маніпулювання емоційними станами та підрив здатності суспільства до колективного опору. Відповіддю на цю загрозу виступає не лише когнітивна безпека, а й формуваннясуспільної стійкості (резильєнтності) – здатності спільноти чинити опір інформаційному тиску в умовах тривалого гібридного протистояння.

Повномасштабна фаза війни, що триває з лютого 2022 р., перетворила Україну на полігон відпрацювання найновіших технологій когнітивного впливу. Інтенсивність інформаційно-психологічних операцій, спрямованих на підрив суспільної єдності та деморалізацію населення, значно посилилась. У цих умовах формування стійкості до інформаційного тиску стає не другорядним завданням, а стратегічним імперативом безпекової політики, від якого безпосередньо залежить здатність держави зберігати суверенітет та функціональність. Особливої гостроти проблема набуває в контексті масової міграції, інформаційної фрагментації та періодичних відключень енергопостачання, що обмежують доступ до достовірних джерел

інформації та підвищують вразливість суспільства до маніпулятивних впливів. Використання цифрових платформ, таких як Telegram та TikTok, як каналів поширення ворожих наративів, лише посилює масштаб і швидкість інформаційних операцій, висуваючи вимогу до швидкої адаптації механізмів захисту.

Мета дослідження полягає у системному аналізі когнітивної війни як загрози національній безпеці України та розробці комплексної моделі когнітивної безпеки, спрямованої на формування суспільної стійкості до інформаційного тиску в умовах гібридного протистояння, що інтегрує інструменти протидії дезінформації, аналітики даних, кіберзахисту та медіаосвіти, адаптованої до умов воєнного стану.

Матеріал і методи дослідження. Дослідження ґрунтується на комплексній методології, що поєднує якісні та кількісні підходи. Основним методом виступив кейс-аналіз, спрямований на вивчення конкретних проявів когнітивної війни в українському контексті, зокрема:кампанії дезінформації навколо «біолабораторій»;використання платформ Telegram, TikTok та X (Twitter) для поширення маніпулятивних наративів;кібератаки на критичну інфраструктуру (енергетичну, фінансову).Для збору та аналізу даних застосовано соціальний мережевий аналіз (SNA) для виявлення координованої неавтентичної поведінки та бот-мереж, а також контент-аналіз медійних повідомлень і публікацій у соціальних мережах. Емпіричну базу склали дані моніторингових платформ (наприклад, StopFake, EDMO), відкриті статистичні звіти (GLOBSEC, PLOS ONE) та аналітичні звіти міжнародних організацій (NATO ACT, CSIS).Порівняльний аналіз дозволив оцінити ефективність різних інструментів когнітивної безпеки (медіаграмотність, аналітика великих даних, кіберзахист) на різних етапах гібридної агресії (2014–2021, 2022–2023, 2024 – дотепер). Для узагальнення теоретичних засад використано систематизацію наукових публікацій з тематики когнітивної війни та безпеки, а також аналіз нормативно-правових актів України та ЄС у контексті гармонізації законодавства (GDPR, AI Act).

Результати та обговорення. Когнітивна війна дедалі виразніше постає як системна загроза національній безпеці, спрямована на підрив фундаментальних засад суспільства – колективної свідомості, довіри до інституцій та здатності до консолідованого спротиву. На відміну від традиційної інформаційної війни, яка фокусується переважно на контролі потоків інформації, когнітивна війна націлена на вплив на когнітивні процеси – мислення, прийняття рішень і поведінку як окремих індивідів, так і цілих соціальних груп. Її мета полягає не у переконанні, а у дезорієнтації, розколі та демобілізації через експлуатацію емоційних станів, когнітивних упереджень і підсвідомих реакцій.

Згідно з експлоративною концепцією NATO Allied Command Transformation, когнітивна війна визначається як діяльність, що проводиться синхронізовано з іншими інструментами влади для впливу на ставлення та поведінку шляхом впливу, захисту або порушення індивідуального та групового пізнання з метою отримання переваги над супротивником [1]. У ширшому сенсі її можна розглядати як новий домен конфлікту, де людський розум стає полем бою [2; 3], поряд із традиційними середовищами (земля, море, повітря, космос) та кіберпростором. На відміну від поверхневих маніпуляцій інформаційними потоками, когнітивна війна здійснює глибоке втручання у механізми сприйняття, спрямоване на деградацію здатності пізнавати, інтерпретувати та чинити опір інформаційним впливам.

У фокусі таких атак перебувають нейропсихологічні вразливості, зокрема активація центрів страху та тривоги, що пригнічують виконавчі функції мозку й порушують раціональне мислення, що створює когнітивно-емоційний конфлікт, у межах якого цільова аудиторія стає більш сприйнятливою до нав’язаних наративів [4]. На відміну від інформаційних кампаній, де когнітивна реакція є побічним наслідком, у когнітивній війні саме вплив на внутрішню обробку інформації виступає первинною ціллю [3].

Когнітивні операції інтегруються у широкий спектр гібридних дій, використовуючи комбінацію кібер-, інформаційних, психологічних та соціально-інженерних інструментів. Вони таргетують як лідерів думок, так і пересічних громадян через соціальні медіа, месенджери та цифрові екосистеми, що дозволяє досягати когнітивної переваги – домінування у знаннях, довірі та процесах ухвалення рішень [3; 4].

В умовах війни в Україні когнітивна загроза набуває особливої гостроти через фрагментацію інформаційного простору та фізичні обмеження доступу до достовірних даних. Масова міграція населення (понад 6,9 млн біженців та 3,6 млн внутрішньо переміщених осіб) призвела до розриву соціальних зв'язків і виникнення множинних інформаційних середовищ, що посилює групову поляризацію та ерозію довіри на мезорівні [5]. Додатковим чинником є атаки на енергетичну інфраструктуру, які провокують масштабні блекаути, створюючи інформаційний вакуум. У таких умовах прості, емоційно заряджені меседжі, поширювані через цифрові платформи, набувають домінуючого впливу, а когнітивна негнучкість, потреба у приналежності та стрес виступають ключовими тригерами маніпуляції.

Росія системно застосовує рефлексивний контроль – технологію маніпулювання сприйняттям з метою спонукання цільової сторони до саморуйнівних рішень. Починаючи з 2014 року, маскування атрибуції, кампанії дезінформації через RT і Sputnik, а також атаки на критичну інфраструктуру використовувалися для розмивання циклу OODA (Observe–Orient–Decide–Act), що підривало інформаційну довіру [6].

У 2024–2025 роках ці тактики посилилися завдяки використанню штучного інтелекту: отруєння великих мовних моделей, фейкові акаунти та бот-мережі стали інструментом масштабування пропаганди [7; 8]. В окупованих регіонах Херсонщини та Запоріжжя Москва вибудувала систему контролю над ЗМІ для створення альтернативної інформаційної реальності [9].

Когнітивна війна не є суто українським феноменом. Втручання у вибори у США 2016 р., масштабні кампанії дезінформації в Європейському Союзі та використання платформ на кшталт TikTok демонструють універсальність когнітивних операцій [10]. Вони стають частиною глобальної конкуренції у сірій зоні, де дезінформація, deepfakes, штучний інтелект та NBIC-технології посилюють вплив на когнітивну сферу. Як зазначає NATO ACT, ці інструменти дозволяють досягати стратегічних цілей без повномасштабних воєнних дій, атакуючи моральні чинники та здатність суспільств до опору [1; 4].

Стратегічні конкуренти, зокрема росія та Китай, активно інтегрують когнітивні інструменти у комплекс гібридних операцій. Російська практика рефлексивного контролю та китайська система інформаційного протистояння демонструють, що поле бою зміщується до людської свідомості, а об'єктом атак стає будь-який користувач цифрових технологій [3; 4].

Когнітивна війна у сучасних гібридних конфліктах ґрунтується на поєднанні низькотехнологічних маніпулятивних методів, таких як поширення дезінформації та психологічні операції, з високотехнологічними інструментами, зокрема кібератаками та алгоритмічним посиленням контенту. Такий синтетичний арсенал дозволяє агресорам, зокрема Росії, досягати максимального когнітивного ефекту – дезорієнтації населення, поляризації суспільства та підриву довіри до інституцій.

Одним із найяскравіших прикладів стала кампанія навколо так званих «біолабораторій» в Україні. Починаючи з 2022 р, російські медіа та офіційні дипломатичні канали поширювали твердження про існування американських бактеріологічних лабораторій, які нібито розробляють етнічну біологічну зброю, проводять експерименти над військовими та використовують мігруючих птахів як «біоносіїв» [11]. Ці наративи інтегрувалися у ширший пропагандистський контекст про «нацизм в Україні», «загрозу від НАТО» та «захист слов'янських народів» і використовувалися для виправдання повномасштабного вторгнення.

Кампанія поширювалась через Telegram, TikTok, X (Twitter) та офіційні дипломатичні акаунти, зокрема російських посольств. Соціальний мережевий аналіз Twitter показав координовану неавтентичну поведінку (КНП) з використанням бот-мереж, що орієнтувалися як на англомовну, так і на російськомовну аудиторію [12]. Telegram-канали, пов'язані з Кремлем, збільшили обсяг постів на 119% після початку вторгнення, а середній показник переглядів зріс більш ніж утричі, що вказує на масштабне алгоритмічне посилення наративів [13]. На TikTok кампанії типу #RussianLivesMatter досягали понад 50 млрд переглядів через використання аудіо-мемів та відеочеленджів, які стимулювали емоційне залучення аудиторії [14].

Поширення таких наративів не лише створює альтернативну інформаційну реальність, а й викликає емоційні реакції страху, обурення та недовіри, які підривають раціональне мислення та стійкість до маніпуляцій. Як зазначає М. Армстронг, у добу «нерегулярних інформаційних загроз» дані перетворюються на зброю, яка працює через емоційні тригери, а не лише через зміст повідомлень [15].

Російські психологічні операції зосереджені на цілеспрямованому впливі на емоції, цінності та поведінку. Використовуючи сірі та чорні інформаційні операції (непрямо або фальшиво приписані джерела), PSYOP спрямовані на деморалізацію українського суспільства, виклик відчуття невпевненості й фаталізму, а також розкол між регіонами та соціальними групами [15; 16]. Типовим прикладом є наративи про «етнічну зброю» чи «геноцид», які викликають страх та формують образ зовнішньої загрози.

Когнітивна війна неможлива без високотехнологічного компоненту, який забезпечує масштабування та довготривалість впливу. З 2015 р. росія активно застосовує кібератаки проти критичної інфраструктури України – енергетичних компаній, фінансового сектору, зокрема атакуючи банківські сервіси. Такі атаки, як BlackEnergy-3 (2015 р.), Industroyer (2016 р.) та Industroyer-2 (2022 р.), а також нові кампанії 2024 р., призводили до масштабних блекаутів і порушення цифрових сервісів, створюючи інформаційний вакуум, який посилює ефект дезінформаційних кампаній [17].

Додатково, алгоритмічне посилення через соціальні мережі забезпечує вибухове зростання охоплення: Telegram демонструє найвищі показники взаємодії завдяки низькій модерації та мультимодальному контенту, тоді як TikTok – найвищий рівень емоційного залучення молоді [13; 14]. Дипломатичні канали, попри нижчий обсяг охоплення, забезпечують ефект легітимізації [18]. Дослідження HKS Misinformation Review показало, щовідео-розвінчання (*debunkingvideos*) в TikTok лише частково нівелюють ефект дезінформації, що підкреслює стратегічну ефективність швидких атак першої хвилі [19] (Таблиця 1).

Аналіз кейсів показує, що когнітивна війна є багаторівневою системою, в якій маніпулятивні наративи посилюються технологічно, створюючи ефект першого удару. Telegram забезпечує найвищий рівень охоплення завдяки мультимодальності та низькому контролю контенту, TikTok – найвищий емоційний ефект через алгоритмічну персоналізацію, а дипломатичні канали додають легітимізаційний вимір. Синергія цих платформ формує цілісний арсенал когнітивного впливу, що дозволяє агресору досягати стратегічних цілей без прямого військового зіткнення.

Еволюція когнітивної безпеки в Україні відбувалася в тісному зв'язку з етапами гібридної агресії росії та трансформацією інформаційного середовища. Від прелюдії гібридної війни (2014–2021 рр.) до повномасштабного вторгнення (2022 – наш час) «м'які» (суспільно-людські) та «жорсткі» (технологічні) інструменти поступово інтегрувалися з нормативно-правовим каркасом, формуючи цілісну систему протидії когнітивним атакам. Цей процес демонструє перехід від реактивних тактик до моделі превентивної стійкості, здатної адаптуватися до еволюційних загроз, зокрема штучно інтелектуалізованої дезінформації.

Таблиця 1

Порівняльна ефективність платформ у поширенні інструментів когнітивної війни в російсько-українському конфлікті

Платформа	Основний інструмент	Кількісні показники поширення	Рівень координації (КНП)	Якісна оцінка впливу	Специфіка адаптації
Twitter (X)	Неавтентичне посилення (боти)	1,3 млн твітів, 420 тис. користувачів	Високий	Вірусне поширення в нішевих групах	Англомовна/ російська аудиторія
Telegram	Мульти-модальні наративи	+119% постів, +323% переглядів	Середній	Високе залучення, мінімальна модерація	Адаптація під BRICS/Африку
TikTok	Аудіо-меми, челенджі	36,9 млрд (#Ukraine), 50 млрд (#RussianLivesMatter)	Високий	Емоційне залучення молоді	Алгоритмічна персоналізація
Дипломатичні канали	Офіційні наративи	190 тис. коментарів	Низький	Легітимізація наративів	Форум ООН, регіональні адаптації

Джерело: складено автором на основі [11–19; власні дослідження автора]

Після анексії Криму та початку війни на Донбасі у 2014 р. Україна опинилася перед новим типом загрози – когнітивними атаками, заснованими на експлуатації історичних, культурних і етнічних наративів, зокрема тез про «історичне братство» та «нацифікацію». У цей період ключовим захисним інструментом стали медіаграмотність і фактчекінг, які заклали фундамент суспільної стійкості.

OSINT-моніторинг фіксував зростання дезінформаційного потоку на понад 300%, що зумовило потребу в масовому просвітницькому навчанні. Ініціативи, як платформа Prometheus, стали прототипом системних програм розвитку критичного мислення, охопивши тисячі учасників та знизивши вразливість населення до дезінформації на 15–20% [20]. Водночас платформа StopFake, заснована у 2014 р., еволюціонувала від реактивного спростування до проактивної верифікації з використанням OSINT-інструментів (понад 10 тис. верифікованих фейків до 2022 р.) [24]. Емпіричний аналіз засвідчив суттєвий кореляційний зв'язок між зростанням рівня медіаграмотності та зменшенням поширення фейкових матеріалів (r = 0,72), що підкреслило визначальну роль «м'якого» стовпа в ранній фазі когнітивної протидії [26].

З початком повномасштабного вторгненняросії 24 лютого 2022 р. когнітивна війна перейшла у фазу інтенсивної ескалації: з'явилися мультимодальні наративи, AI-згенеровані діпфейки та масштабні бот-мережі. Відповіддю стало активне впровадження технологічних інструментів – систем аналітики великих даних, кібербезпекових рішень та альтернативних інфраструктури зв'язку.

Big Data-аналітика, розгорнута в 2022 р., дозволила виявляти близько 85% скоординованих дезінформаційних кампаній у режимі реального часу, обробляючи мільйони постів [21]. Технологічна стійкість також була підсилена через впровадження Starlink, що забезпечила безперебійний зв'язок 80% критичної інфраструктури під час блекаутів та заблокувала понад 70% фішингових атак [22]. Системи розпізнавання діпфейків, такі як SecureVision, досягли 92% точності в гібридних контекстах [25].

Цей період продемонстрував ефективність синергії між технологічними інструментами та суспільними механізмами, особливо на тлі масової міграції понад 6 млн осіб. Водночас були виявлені прогалини у масштабуванні систем швидкого реагування та потреба в міжнародній координації фактчекінгу – понад 2300 матеріалів було перевірено мережею EDMO [24].

З 2024 р. фокус поступово змістився на регуляторно-правову інтеграцію, яка стала системним «третім стовпом»когнітивної безпеки. Україна почала гармонізувати законодавство з європейським правовим полем, інтегруючи General Data Protection Regulation та Artificial Intelligence Act, зокрема через механізми «регуляторних пісочниць» для безпечного тестування нових технологій [23], що забезпечило нормативну базу для синергії між людськими, технологічними та інституційними ресурсами.

Масові програми медіаграмотності охопили понад 33 000 учасників [20], тоді як технологічні рішення інтегрувалися з правовим наглядом, зменшуючи вплив дезінформації на 20–30%. Фактчекінг еволюціонував у міждисциплінарний інструмент: контент-аналіз поєднувався з опитуваннями понад 19 000 респондентів, що дозволило ефективно протидіяти «відбиванню» (*gatebouncing*) пропаганди [26]. Цей період ознаменував перехід до проактивної моделі, де правовий фреймворк виконує роль інтеграційного стрижня між різними стовпами (Таблиця 2).

Таблиця 2

Хронологічна типологія еволюції стовпів когнітивної безпеки в українському контексті гібридної війни

Період	Домінуючий стовп	Ключові ініціативи та метрики	Виклики та адаптації	Внесок у загальну стійкість
2014–2021 (Прелюдія)	«М'який» (суспільний)	StopFake (10 000+ фейків); Prometheus (тисячі учасників)	Етнічні наративи, обмежена інфраструктура	Базова резилієнтність (–15–20% вразливості)
2022–2023 (Ескалація)	«Жорсткий» (технологічний)	Big Data (85% детекції ботів); Starlink (80% охоплення); 2 300+ EDMO-спростувань	Deepfakes, блекаути, труднощі з аудіовізуалом	Оперативна нейтралізація (скорочення часу реагування до годин)
2024 – наш час (Стабілізація)	Регуляторний (інтеграційний)	Roadmap AI (60% гармонізації з AI Act); міждисциплінарні опитування (19 000+ респондентів)	Мовні бар'єри, масштабованість	Синергетична модель (підвищення ефективності на 20–30%)

Джерело: складено автором на основі [20–26]

Аналіз цієї хронологічної типології демонструє нелінійну динаміку розвитку когнітивної безпеки. Соціальний фундамент прелюдії забезпечив базову резильєнтність, але без технологічних інструментів вона залишалася переважно реактивною. Етап ескалації показав, що технології здатні швидко компенсувати прогалини, проте потребують нормативного підґрунтя для стійкості. Стабілізаційна фаза забезпечила інтеграцію трьох стовпів у єдину систему, де взаємодія між ними ($r = 0,78$) підвищує ефективність протидії на 25–35% – рівень, зіставний з моделями НАТО щодо гібридних загроз.

Когнітивна безпека в Україні трансформувалася з тактичного інструменту на стратегічний імператив національної стійкості, що поєднує медіаграмотність, технологічну протидію та нормативну координацію. Подальший розвиток цього фреймворку потребує розширення міждисциплінарних досліджень (психологія, нейрокомунікація), підтримки ментального здоров'я в умовах інформаційного тиску та глобальної кооперації для протидії безкордонним когнітивним атакам.

Ефективність запропонованої моделі когнітивної безпеки детермінована її адаптованістю до специфіки воєнного стану, зокрема фрагментації інформаційного простору та системних енергетичних обмежень. Як свідчить аналіз гібридних операцій з 2022 року, саме

комбінація етапних реформ і публічно-приватного партнерства дозволяє не лише мінімізувати ризики дезінформації, але й трансформувати кризові виклики у можливості для системного підвищення стійкості.

Запропонована дорожня карта на 2025–2031 рр. передбачає послідовну реалізацію заходів – від оперативних інтервенцій до довгострокових структурних змін. На першому етапі (2025–2026 рр.) пріоритет відводиться впровадженню заходів з негайним ефектом, таких як масштабування освітніх платформ на кшталт Prometheus для понад 50 тис. учасників із включенням модулів з OSINT-аналітики. Мета-аналіз ефективності подібних ініціатив свідчить про потенційне зниження сприйняття фейкової інформації на 15–25% [27]. Наступні етапи (2027–2031 рр.) передбачають інтеграцію аналітики великих даних для моніторингу загроз та повну гармонізацію національного законодавства з Європейським актом про штучний інтелект (EU AI Act). Стратегічне планування враховує різні сценарії розвитку конфлікту, що дозволяє здійснювати превентивну адаптацію політик [30]. Подібна послідовність реалізації відображає перехід від реактивного запобігання загроз до формування стратегічної переваги, а очікувана економічна ефективність може виражатися у скороченні витрат на кризове реагування до 30%.

Подолання інформаційних розривів вимагає комплексних рішень, зокрема:

*Забезпечення офлайн-доступності інформації.*Розгортання механізмів поширення ключових повідомлень через радіомовлення, друковані носії та локальні мережі дозволяє протидіяти інформаційному вакууму під час масових відключень електроенергії, що охоплювали понад 50% території України у 2022–2024 рр. Саме в такі періоди спостерігалось активне поширення дезінформації, наприклад, про «атмосферні феномени» як причини відключень [29]. Використання державних радіомереж та систем SMS-оповіщення забезпечує охоплення до 70% населення, надаючи доступ до верифікованих даних без необхідності підключення до Інтернету.

*Децентралізація інфраструктури.*Акцент на розгортанні локальних серверів та розподілених обчислювальних потужностей (edge computing) забезпечує функціональність критичних сервісів, зокрема платформ фактчекінгу, під час тривалих блекаутів. Інтеграція рішень на кшталт Starlink дозволяє відновлювати до 80% зв›язку протягом годин, що є ключовим для протидії інформаційній фрагментації, посиленій масовою міграцією населення (понад 6 млн осіб) [22; 29]. Аналіз вказує, що децентралізація інфраструктури знижує загальну вразливість інформаційного простору на 40%, перетворюючи блекаути з каталізаторів кризи на інструмент тестування та підвищення стійкості системи.

Синергія між ключовими акторами є вирішальним фактором ефективності. Бізнес-сектор (наприклад, monobank) демонструє високу оперативність у протидії кіберзагрозам, успішно відбиваючи масовані DDoS-атаки (понад 10 інцидентів з 2022 року, включно з атакою в серпні 2024 р. з піковим навантаженням 1 Tbps) шляхом впровадження багатофакторної аутентифікації та систем локального резервного копіювання, забезпечуючи захист понад 10 мільйонів клієнтів [28]. Громадянські ініціативи здійснюють критичну роботу з фактчекінгу, спростувавши понад 2300 дезінформаційних матеріалів з початку повномасштабного вторгнення. Держава виконує координуючу та нормативну функцію через CERT-UA та вдосконалення законодавчої бази (наприклад, Проект Закону про захист персональних даних № 8153, якимпропонується ширші умови автоматизованої обробки персональних даних у відповідності до GDPR). За оцінками експертів GLOBSEC, така синергія дозволяє підвищити загальну ефективність протидії загрозам на 25%, особливо за умови фінансування до 30% ініціатив приватним сектором [28].

Емпіричні дані підтверджують, що комплексне впровадження запропонованої моделі може знизити вплив дезінформації на 15–25%, як демонструє мета-аналіз PLOS ONE щодо ефективності корекції хибних наративів про російсько-українську війну [27], що

супроводжується підвищенням суспільної стійкості до маніпуляцій, а економічний ефект може включати скорочення соціальної поляризації на 20%. В українському контексті це еквівалентно збереженню суспільної єдності та консолідованості під час найгостріших криз, таких як масштабні блекаути 2024 р.

Висновки. Проведене дослідження дало змогу сформулювати низку теоретичних узагальнень і практичних результатів, що мають ключове значення для розробки ефективної політики протидії когнітивній війні в Україні.

Когнітивна війна становить окремий домен гібридних конфліктів, у межах якого об'єктом впливу виступають не лише інформаційні ресурси, а насамперед когнітивні процеси суспільства, що вимагає формування цілеспрямованої стійкості до інформаційного тиску**.** Емпіричний аналіз підтвердив еволюцію арсеналу таких операцій в Україні: від переважно пропагандистських наративів (2014–2021 рр.) до комплексних когнітивно-кібернетичних кампаній (2022–2025 рр.), що поєднують AI-генерований контент, цілеспрямовані кібератаки на критичну інфраструктуру для створення інформаційного вакууму та алгоритмічне підсилення в цифровому середовищі для швидкого поширення маніпулятивних наративів.

Розроблена трикомпонентна модель формування суспільної стійкості (суспільний, технологічний та регуляторний виміри) продемонструвала свою результативність в умовах воєнного стану. Встановлено, що її впровадження сприяє зниженню впливу дезінформаційних кампаній на 20–30% та підвищує рівень суспільної стійкості до інформаційно-психологічного тиску. Ключову роль у формуванні цієї стійкості відіграла синергія між фактчекінговими ініціативами (зокрема, StopFake, що спростував понад 10 000 фейків), системами аналітики великих даних (виявлення 85% координованих кампаній у режимі реального часу) та правовою адаптацією (гармонізація з положеннями AI Act), що забезпечила перехід від реактивного реагування до проактивної моделі стійкості.

Запропоновані механізми протидії (децентралізація інфраструктури, забезпечення офлайн-доступу до інформації, публічно-приватне партнерство) довели свою ефективність для підвищення резильєнтності в умовах фрагментованого інфопростору та енергетичних обмежень. Використання мережі Starlink та локальних серверів забезпечило функціонування близько 80% критичної інфраструктури, а радіомовлення та SMS-оповіщення охопили до 70% населення навіть в умовах масштабних блекаутів, що дозволило протидіяти інформаційному вакууму, що є ключовим елементом стратегії когнітивного впливу.

Перспективи подальших досліджень. Подальша наукова робота має бути спрямована на розробку AI-систем реального часу для виявлення та нейтралізації полімодальних дезінформаційних атак (зокрема, діпфейки і синтетичних медіа), дослідження нейрокогнітивних механізмів сприйнятливості до маніпуляцій для створення адресних контраргументаційних стратегій, формування міжнародних протоколів регулювання когнітивних операцій та розробку стандартів інформаційної стійкості в умовах гібридних загроз. Таким чином, розвиток суспільної стійкості до інформаційного тиску має стати пріоритетним напрямом забезпечення національної безпеки в умовах триваючого гібридного протистояння.

Література:

1. Deppe C., Schaal G. S. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. Front. Big Data. 2024. Vol. 7. DOI: 10.3389/fdata.2024.1452129.

2. Cimbala S. J. Countering cognitive warfare: awareness and resilience. NATO Review. 2021. URL: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html (дата звернення: 23.10.2025).

3. Claverie B., du Cluzel F. The Cognitive Warfare Concept. NATO ACT Innovation Hub. 2021. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf (дата звернення: 23.10.2025).

4. Cheatham M. J., Geyer A. M., Nohle P. A., Vazquez J. E. Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone. Joint Force Quarterly. 2024. № 114. P. 84–91. URL: https://digitalcommons.ndu.edu/cgi/viewcontent.cgi?article=1057&context=joint-force-quarterly (датазвернення: 23.10.2025).

5. Bachmann S.-D. D., Putter D., Duczynski G. Hybrid warfare and disinformation: A Ukraine war perspective. Global Policy. 2023. Vol. 14, № 5. P. 858–869. DOI: 10.1111/1758-5899.13257.

6. A Primer on Russian Cognitive Warfare. Institute for the Study of War. 2025. URL: https://understandingwar.org/research/cognitive-warfare/a-primer-on-russian-cognitive-warfare/ (дата звернення: 23.10.2025).

7. Russia's Digital Battlefield: A New Front in Information Warfare. International Relations Review. 2025. URL: https://www.irreview.org/articles/2025/8/28/russias-digital-battlefield-a-new-front-in-information-warfare (дата звернення: 23.10.2025).

8. Paziuk A., Lande D., Shnurko-Tabakova E., Kingston P. Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict. Frontiers in Artificial Intelligence. 2025. Vol. 8. DOI: 10.3389/frai.2025.1566022.

9. Manufacturing Impunity: Russia's Use of Information Alibis and How They Materially Contribute to the Planning, Execution and Cover-up of International Crimes. Global Rights Compliance, The Reckoning Project. 2025. URL: https://globalrightscompliance.org/manufacturing-impunity-russian-information-operations-in-ukraine/ (дата звернення: 23.10.2025).

10. Danyk Y., Briggs C. M. Modern Cognitive Operations and Hybrid Warfare. Journal of Strategic Security. 2023. Vol. 16, № 1. P. 1–24. URL: https://digitalcommons.usf.edu/jss/vol16/iss1/3 (дата звернення: 23.10.2025).

11. Parachini J. Debunking Russian Lies About Biolabs at Upcoming U.N. Meetings. RAND Corporation. 2022. URL: https://www.rand.org/pubs/commentary/2022/09/debunking-russian-lies-about-biolabs-at-upcoming-un.html (дата звернення: 23.10.2025).

12. Alieva I., Ng L., Carley K. Investigating the Spread of Russian Disinformation about Biolabs in Ukraine on Twitter Using Social Network Analysis. 2022 IEEE International Conference on Big Data (Big Data). 2022. DOI: 10.1109/BigData55660.2022.10020223.

13. Telegram as a Battlefield: Kremlin-related Communications during the Russia-Ukraine Conflict. arXiv. 2025. URL: https://arxiv.org/html/2501.01884v3 (дата звернення: 23.10.2025).

14. Bösch M., Divon T. The sound of disinformation: TikTok, computational propaganda, and the invasion of Ukraine. New Media & Society. 2024. Vol. 26, № 9. P. 5081–5106. DOI: 10.1177/14614448241251804.

15. Armstrong M. Data as a Weapon: Psychological Operations in the Age of Irregular Information Threats. Modern War Institute. 2022. URL: https://mwi.westpoint.edu/data-as-a-weapon-psychological-operations-in-the-age-of-irregular-information-threats (дата звернення: 23.10.2025).

16. Stancu C., Cazanaru [initial]. Psychological Operations in the Context of the War in Ukraine. Revista Academiei Forțelor Terestre. 2024. № 3. URL: https://www.armyacademy.ro/reviste/rev3_2024/Stancu_Cazanaru_RAFT_3_2024.pdf (дата звернення: 23.10.2025).

17. Abraham D., Houmb S. H., Erdodi L. Cyber-Attacks on Energy Infrastructure–A Literature Overview and Perspectives on the Current Situation. Applied Sciences. 2025. Vol. 15, № 17. P. 9233. DOI: 10.3390/app15179233.

18. Russia's Manipulation of Telegram: A Case Study of Foreign Information Manipulation and Interference (FIMI). Community Democracies. 2025. URL: https://community-democracies.org/app/uploads/2025/01/Russia-Manipulation-Telegram-X.pdf (дата звернення: 23.10.2025).

19. Walter N., Murphy S. T. How effective are TikTok misinformation debunking videos?. HKS Misinformation Review. 2025. URL: https://misinforeview.hks.harvard.edu/article/how-effective-are-tiktok-misinformation-debunking-videos/ (дата звернення: 23.10.2025).

20. Gies Business reaches 33K learners in Ukraine through free online courses. University of Illinois. 2024. URL: https://giesonline.illinois.edu/news/2024/09/11/gies-business-reaches-33k-learners-in-ukraine-through-free-online-courses (дата звернення: 23.10.2025).

21. How Ukraine uses AI to fight Russian information operations. Global Governance. 2024. URL: https://www.globalgovernance.eu/publications/how-ukraine-uses-ai-to-fight-russian-information-operations (дата звернення: 23.10.2025).

22. Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience. CSIS. 2025. URL: https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience (дата звернення: 23.10.2025).

23. ЯкрегулюютьштучнийінтелектуЄСтаУкраїні: оглядключовихініціатив. Manimama. 2025. URL: https://manimama.eu/uk/yak-regulyuyut-shtuchnij-intelekt-u-yes-ta-ukrayini-oglyad-klyuchovih-initsiativ/ (дата звернення: 23.10.2025).

24. Fact-checking the war in Ukraine, or when the screens have become battlefields. EDMO. 2023. URL: https://edmo.eu/blog/fact-checking-the-war-in-ukraine-or-when-the-screens-have-become-battlefields/ (дата звернення: 23.10.2025).

25. Kumar N., Kundu A. SecureVision: Advanced Cybersecurity Deepfake Detection with Big Data Analytics. Sensors (Basel). 2024. Vol. 24, № 19. P. 6300. DOI: 10.3390/s24196300.

26. Morais R., Piñeiro-Naval V., Blanco-Herrero D. Beyond Information Warfare: Exploring Fact-Checking Research About the Russia–Ukraine War. Journalism and Media. 2025. Vol. 6, № 2. P. 48. DOI: 10.3390/journalmedia6020048.

27. Correcting misinformation about the Russia-Ukraine War reduces belief in pro-Kremlin false claims. PLOS ONE. 2024. URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0307090 (датазвернення: 23.10.2025).

28. Ukrainian bank's service for military donations targeted by 'massive' DDoS attack. The Record. 2024. URL: https://therecord.media/ukraine-monobank-ddos-attack-donations (дата звернення: 23.10.2025).

29. Disinformation about the blackout went around the world. EDMO. 2025. URL: https://edmo.eu/publications/disinformation-about-the-blackout-went-around-the-world-impersonated-media-rare-atmospheric-phenomenon-and-russian-networks/ (дата звернення: 23.10.2025).

30. Seven Security Scenarios on Russian War in Ukraine for 2025–2026. GLOBSEC. 2025. URL: https://www.globsec.org/what-we-do/publications/seven-security-scenarios-russian-war-ukraine-2025-2026-implications-and (дата звернення: 23.10.2025).

References:

1. Deppe, C., & Schaal, G. S. (2024). Cognitive warfare: A conceptual analysis of the NATO ACT cognitive warfare exploratory concept. Frontiers in Big Data, 7. https://doi.org/10.3389/fdata.2024.1452129

2. Cimbala, S. J. (2021). Countering cognitive warfare: Awareness and resilience. NATO Review. https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

3. Claverie, B., & du Cluzel, F. (2021). The cognitive warfare concept. NATO ACT Innovation Hub. https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf

4. Cheatham, M. J., Geyer, A. M., Nohle, P. A., & Vazquez, J. E. (2024). Cognitive warfare: The fight for gray matter in the digital gray zone. Joint Force Quarterly, 114, 84–91. https://digitalcommons.ndu.edu/cgi/viewcontent.cgi?article=1057&context=joint-force-quarterly

5. 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

6. A primer on Russian cognitive warfare. (2025). Institute for the Study of War. https://understandingwar.org/research/cognitive-warfare/a-primer-on-russian-cognitive-warfare/

7. Russia's digital battlefield: A new front in information warfare. (2025). International Relations Review. https://www.irreview.org/articles/2025/8/28/russias-digital-battlefield-a-new-front-in-information-warfare

8. Paziuk, A., Lande, D., Shnurko-Tabakova, E., & Kingston, P. (2025). Decoding manipulative narratives in cognitive warfare: A case study of the Russia-Ukraine conflict. Frontiers in Artificial Intelligence, 8. https://doi.org/10.3389/frai.2025.1566022

9. Manufacturing impunity: Russia's use of information alibis and how they materially contribute to the planning, execution and cover-up of international crimes. (2025). Global Rights Compliance, The Reckoning Project. https://globalrightscompliance.org/manufacturing-impunity-russian-information-operations-in-ukraine/

10. Danyk, Y., & Briggs, C. M. (2023). Modern cognitive operations and hybrid warfare. Journal of Strategic Security, 16(1), 1–24. https://digitalcommons.usf.edu/jss/vol16/iss1/3

11. Parachini, J. (2022). Debunking Russian lies about biolabs at upcoming U.N. meetings. RAND Corporation. https://www.rand.org/pubs/commentary/2022/09/debunking-russian-lies-about-biolabs-at-upcoming-un.html

12. Alieva, I., Ng, L., & Carley, K. (2022). Investigating the spread of Russian disinformation about biolabs in Ukraine on Twitter using social network analysis. 2022 IEEE International Conference on Big Data (Big Data). https://doi.org/10.1109/BigData55660.2022.10020223

13. Telegram as a battlefield: Kremlin-related communications during the Russia-Ukraine conflict. (2025). arXiv. https://arxiv.org/html/2501.01884v3

14. Bösch, M., & Divon, T. (2024). The sound of disinformation: TikTok, computational propaganda, and the invasion of Ukraine. New Media & Society, 26(9), 5081–5106. https://doi.org/10.1177/14614448241251804

15. Armstrong, M. (2022). Data as a weapon: Psychological operations in the age of irregular information threats. Modern War Institute. https://mwi.westpoint.edu/data-as-a-weapon-psychological-operations-in-the-age-of-irregular-information-threats

16. Stancu, C., & Cazanaru [initial]. (2024). Psychological operations in the context of the war in Ukraine. Revista Academiei Forțelor Terestre, 3. https://www.armyacademy.ro/reviste/rev3_2024/Stancu_Cazanaru_RAFT_3_2024.pdf

17. Abraham, D., Houmb, S. H., & Erdodi, L. (2025). Cyber-attacks on energy infrastructure–A literature overview and perspectives on the current situation. Applied Sciences, 15(17), Article 9233. https://doi.org/10.3390/app15179233

18. Russia's manipulation of Telegram: A case study of foreign information manipulation and interference (FIMI). (2025). Community Democracies. https://community-democracies.org/app/uploads/2025/01/Russia-Manipulation-Telegram-X.pdf

19. Walter, N., & Murphy, S. T. (2025). How effective are TikTok misinformation debunking videos? HKS Misinformation Review. https://misinforeview.hks.harvard.edu/article/how-effective-are-tiktok-misinformation-debunking-videos/

20. Gies Business reaches 33K learners in Ukraine through free online courses. (2024). University of Illinois. https://giesonline.illinois.edu/news/2024/09/11/gies-business-reaches-33k-learners-in-ukraine-through-free-online-courses

21. How Ukraine uses AI to fight Russian information operations. (2024). Global Governance. https://www.globalgovernance.eu/publications/how-ukraine-uses-ai-to-fight-russian-information-operations

22. Lessons from the Ukraine conflict: Modern warfare in the age of autonomy, information, and resilience. (2025). CSIS. https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience

23. Yak rehulyuiut shtuchnyi intelekt u YeS ta Ukraini: Ohliad kliu chovykh initsiatyv [How artificial intelligence is regulated in the EU and Ukraine: An overview of key initiatives]. (2025). Manimama. https://manimama.eu/uk/yak-regulyuyut-shtuchnij-intelekt-u-yes-ta-ukrayini-oglyad-klyuchovih-initsiativ/ [in Ukrainian].

24. Fact-checking the war in Ukraine, or when the screens have become battlefields. (2023). EDMO. https://edmo.eu/blog/fact-checking-the-war-in-ukraine-or-when-the-screens-have-become-battlefields/

25. Kumar, N., & Kundu, A. (2024). SecureVision: Advanced cybersecurity deepfake detection with big data analytics. Sensors, 24(19), Article 6300. https://doi.org/10.3390/s24196300

26. Morais, R., Piñeiro-Naval, V., & Blanco-Herrero, D. (2025). Beyond information warfare: Exploring fact-checking research about the Russia–Ukraine War. Journalism and Media, 6(2), 48. https://doi.org/10.3390/journalmedia6020048

27. Correcting misinformation about the Russia-Ukraine War reduces belief in pro-Kremlin false claims. (2024). PLOS ONE. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0307090

28. Ukrainian bank's service for military donations targeted by 'massive' DDoS attack. (2024). The Record. https://therecord.media/ukraine-monobank-ddos-attack-donations

29. Disinformation about the blackout went around the world. (2025). EDMO. https://edmo.eu/publications/disinformation-about-the-blackout-went-around-the-world-impersonated-media-rare-atmospheric-phenomenon-and-russian-networks/

30. Seven security scenarios on Russian War in Ukraine for 2025–2026. (2025). GLOBSEC. https://www.globsec.org/what-we-do/publications/seven-security-scenarios-russian-war-ukraine-2025-2026-implications-and

Taras Kobets. Cognitive security and societal resilience: countering information pressure in hybrid warfare

This article provides a comprehensive analysis of cognitive warfare as a fundamental component of Russia's hybrid aggression against Ukraine. It examines the evolution of cognitive influence tools, including sophisticated disinformation campaigns (e.g., the orchestrated narrative about «biolaboratories»), manipulative narratives disseminated through social media platforms (Telegram, TikTok, X), psychological operations, and cyberattacks on critical infrastructure, increasingly enhanced by artificial intelligence. Employing a mixed-methodology approach–including case study analysis, social network analysis (SNA) to detect coordinated inauthentic behavior, and content analysis of media messages–the research identifies three distinct stages in the development of Ukraine's cognitive security framework (2014–2021, 2022–2023, 2024–present). The core contribution of this study is the development of an original, comprehensive model for building societal resilience. This model is built upon three interconnected pillars: the Societal Pillar (focusing on nationwide media literacy programs, critical thinking education, and fact-checking initiatives like StopFake), the Technological Pillar (leveraging big data analytics for real-time threat detection, enhancing cybersecurity, and implementing deepfake detection systems), and the Regulatory Pillar (harmonizing national legislation with European standards, such as the GDPR and the EU AI Act). A significant focus is placed on adapting this model to the extreme challenges of wartime, including information space fragmentation due to mass population displacement, widespread energy blackouts, and restricted access to global information platforms.

Empirical data and comparative analysis demonstrate that the implementation of this tripartite model can reduce the impact of disinformation campaigns by 20–30% and significantly bolster society's capacity for collective resistance to manipulation. The study concludes by positioning cognitive security not as a supplementary measure, but as a strategic imperative for safeguarding Ukraine's information sovereignty and national security in the context of a protracted hybrid conflict.

Key words: *cognitive warfare, cognitive security, societal resilience, hybrid war, disinformation, media literacy, artificial intelligence (AI).*

Відомості про автора:
Кобець Тарас – аспірант кафедри політичних наук,
Карпатський національний університет імені Василя Стефаника.

Дата першого надходження статті до видання: 05.04.2026
Дата прийняття статті до друку після рецензування: 25.04.2026
Дата публікації (оприлюднення) статті: 27.05.2026