The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.18

Аналіз теорії і практики розвитку когнітивних загроз у сфері воєнної безпеки: шляхи подолання

Олександр Кінь
кандидат технічних наук, доцент
старший науковий співробітник
Дипломатична академія України імені Геннадія Удовенка
при Міністерстві закордонних справ
01001, м. Київ, вул. Велика Житомирська, 2
email: cubalibre1972@ukr.net
ORCID: 0009-0001-2196-7515

Анотація. Державна політика безпеки, військова наука та практичне військове управління досі не мають системного підходу до вивчення й протидії когнітивним загрозам. Не вироблено єдиного понятійно-термінологічного апарату, методів діагностики, моніторингу й оцінювання рівня когнітивної безпеки. Відсутність доктринальної, нормативної та науково-методичної бази унеможливлює формування ефективної системи протидії. Отже, потреба у теоретико-прикладному аналізі процесів формування, розвитку та реалізації когнітивних загроз у сфері воєнної безпеки України є вкрай актуальною, оскільки безпосередньо пов'язана з потенціалом держави до стратегічного спротиву, стійкості системи національної безпеки, збереженням управлінської цілісності та морально-психологічної готовності до оборони. Основними результатами статті є те, що в ній: сформовано хронологічну послідовність розвитку когнітивних загроз у війнах і воєнних конфліктах (історичний аспект); розкрито порядок трансформації когнітивних загроз для України з 1991 року до сьогодення; удосконалено понятійно-термінологічний апарат методології стратегічного реагування на когнітивні загрози; сформовано станом на червень 2025 року сучасні когнітивні загрози воєнній безпеці України; розроблено матрицю пріоритезації когнітивних загроз; визначено ключові інтегральні показники, які дозволяють не лише виявляти небезпеки, а й оцінювати динаміку впливу, здатність до спротиву та потенціал до попередження негативних когнітивних ефектів; наведено результати експертного опитування щодо частоти появи та рівня впливу когнітивних загроз на рівень воєнної безпеки України, а також результати розрахунку індексу когнітивного тиску станом на червень 2025 року; сформовано систему рекомендацій щодо ефективної протидії актуальним когнітивним загрозам воєнній безпеці України станом на червень 2025 року; запропоновано модель (структура) реагування на когнітивні загрози воєнній безпеці України та визначено основні показники моніторингу когнітивних загроз і заходи реагування на них. Матеріали статті можуть бути корисними військовим, аналітикам, фахівцям з безпеки, науковцям і стратегам, які займаються захистом інформаційного простору та реагуванням на сучасні когнітивні загрози у сфері воєнної безпеки України.

Ключові слова: гібридна війна, воєнні дії, воєнна безпека, збройна боротьба, когнітивні загрози, когнітивний вплив, когнітивні виклики, воєнно-політична логіка, індекс когнітивного тиску, технології війни, тактика та стратегія воєнних дій, національна безпека, глобальна стабільність, методи ведення війни, трансформація збройних конфліктів, реагування на когнітивні загрози, моніторинг когнітивних загроз, форми воєнних дій.

Вступ (Introduction)

У сучасних умовах російсько-української війни, що триває, питання щодо забезпечення воєнної безпеки України набуло критичної важливості. Поряд із традиційними формами збройної агресії, дедалі більшого значення набуває використання когнітивних загроз – цілеспрямованого впливу на свідомість, поведінку та сприйняття суспільства, військовослужбовців, керівництва держави. Цей новий вимір війни – так звана когнітивна війна – охоплює інформаційно-психологічні операції, маніпуляції у медіа-просторі, використання штучного інтелекту (ШІ), соціальних мереж і цифрових платформ для формування викривленого уявлення про реальність, дезорієнтації, деморалізації або навіть провокування дій, вигідних агресору [1–6].

Сьогодні російська федерація системно застосовує когнітивні впливи як складову своєї стратегії гібридної війни. Це проявляється у спробах підірвати довіру до державних інституцій, розмиванні суспільної єдності, деморалізації військових, дискредитації міжнародної підтримки України, створенні ілюзії невідворотності поразки чи безсенсовності спротиву. Особливо небезпечними є складноідентифіковані або латентні загрози, які маскуються під “внутрішні” дискурси або позиціонуються як альтернативна правда. Водночас державна політика безпеки, військова наука та практичне військове управління досі не мають системного підходу до вивчення й протидії когнітивним загрозам. Не вироблено єдиного понятійно-категоріального апарату, методів діагностики, моніторингу й оцінювання рівня когнітивної безпеки. Через відсутність доктринальної, нормативної та науково-методичної бази неможливо сформувати ефективну систему протидії [1–22].

Отже, потреба у теоретико-прикладному аналізі процесів формування, розвитку та реалізації когнітивних загроз у сфері воєнної безпеки України є вкрай актуальною, оскільки безпосередньо пов’язана з потенціалом держави до стратегічного спротиву, стійкості системи національної безпеки, збереженням управлінської цілісності та морально-психологічної готовності до оборони.

Дослідження цієї тематики має не лише науково-пізнавальну, а й високу практичну значущість – для розроблення національної стратегії когнітивної безпеки, удосконалення доктринального апарату, підготовки військових кадрів нового покоління, здатних протистояти не лише фізичному, а й когнітивному впливу противника.

Матеріали та методи (Materials and Methods)

У контексті формування ефективної системи стратегічного реагування на когнітивні загрози у сфері воєнної безпеки особливої актуальності набуває всебічний аналіз наукових і прикладних джерел, що розкривають природу, механізми та наслідки таких загроз. Такий аналіз дозволяє: виявити існуючі підходи до трактування когнітивних загроз та їхнього впливу; визначити наукові та методологічні прогалини в сучасному дискурсі; зіставити вітчизняні й зарубіжні дослідницькі традиції; ідентифікувати потенційно релевантні практики, які можуть бути адаптовані до умов України. У табл. 1 представлено огляд джерел, який дає змогу сформувати наукове підґрунтя для подальшого розроблення теоретико-методичних засад протидії когнітивним загрозам у секторі безпеки і оборони.

Західна література більше зосереджена на системному аналізі, прогнозуванні, технологіях когнітивного впливу. Українські джерела концентруються на практиці протидії в умовах гібридної війни з росією. Спільна тенденція – визнання когнітивної сфери як одного з основних полів воєнного протиборства в XXI столітті [1–22].

На підставі аналізу літератури за тематикою розвитку когнітивних загроз сформуємо історичний алгоритм розвитку когнітивних загроз у війнах і воєнних конфліктах, представлений у вигляді хронологічної послідовності з виокремленням ключових періодів, особливостей когнітивного впливу, методів його реалізації та основоположників нових типів

загроз (табл. 2) [1–22].

Таблиця 1. Аналіз джерел за тематикою когнітивних загроз у воєнній безпеці

Автор / Джерело	Назва або тип публікації	Короткий зміст / Основні положення
NATO Innovation Hub (2020)	*Cognitive Warfare – NATO's Sixth Domain of Operations*	Уперше вводиться концепт "когнітивної війни" як окремої домінанти. Описано використання дезінформації, соціальних медіа для впливу на мислення та ухвалення рішень. Когнітивна сфера визначена як поле сучасного конфлікту.
RAND Corporation (2019–2023)	Аналітичні доповіді: *Cognitive Security, Influence Operations, Disinformation Threats*	Поглиблено розглядається вплив інформаційних операцій на сприйняття, поведінку військових і цивільного населення. Увага на стратегіях рф і Китаю. Розглянуто методи оцінювання та протидії.
Hybrid CoE (Helsinki)	Аналітичні нотатки (2021–2024)	Вивчаються гібридні загрози, у т. ч. когнітивні. Особливу увагу приділено впливу на процеси ухвалення рішень, психологічній маніпуляції та створенню фальшивої реальності через цифрові платформи.
J. Q. Wilson, P. K. Davis	*Cognitive Domain Operations: Strategic Advantage in the Human Mind* (2021)	Підкреслено важливість когнітивного домену в концепції "multi-domain operations". Обґрунтовано важливість формування ментальної переваги для забезпечення стійкості збройних сил.
З. Манойла (НУОУ)	Монографія *Когнітивна безпека держави: теоретико-прикладні основи* (2021)	Розроблено класифікацію когнітивних впливів, визначено їхню роль у трансформації безпекового середовища. Запропоновано структуру когнітивного захисту держави.
І. Шевцов (Інститут стратегічних досліджень)	Аналітичні записки щодо інформаційної війни рф	Вказано, що когнітивні операції рф формуються на базі радянської школи маскування та сучасних інформаційно-психологічних технологій. Розглянуто приклади з війни проти України.
S. Bendett (CNA, США)	Аналітика про російські інформаційні та когнітивні підходи (2018–2023)	Детально аналізується підхід рф до когнітивних впливів як елемента "воєнно-інформаційної доктрини". Акцент на роботі з емоціями, страхом, фейками.
Збірник наукових праць "Воєнна безпека України" (НІСД, 2022–2024)	Збірка статей	Низка авторів аналізують когнітивний вплив у контексті війни з рф. Оцінюються ризики дезорієнтації населення, деморалізації військ, підриву довіри до влади.
Центр стратегічних комунікацій та інформаційної безпеки України (2021–2024)	Аналітика, доповіді	Системно досліджуються ворожі наративи, маніпулятивні кампанії в інформаційному середовищі. Створено базу прикладів когнітивних атак.
P. W. Singer, Emerson T. Brooking	*LikeWar: The Weaponization of Social Media* (2018)	Розкрито, як соціальні мережі перетворилися на інструмент ведення когнітивних бойових дій. Приклади з США, Близького Сходу, України.

Історичний розвиток когнітивних загроз демонструє поступовий перехід від інстинктивно-психологічного впливу до високотехнологічної багаторівневої когнітивної війни, в якій мета – не фізичне знищення ворога, а перехоплення його мислення, нав'язування рішень і підрив системи ідентичності. Розуміння цієї історичної логіки – ключ до розроблення ефективних стратегій захисту в умовах сучасної війни.

Таблиця 2. Хронологічна послідовність розвитку когнітивних загроз у війнах і воєнних конфліктах (історичний аспект)

Період	Особливості когнітивних загроз	Методи формування когнітивних загроз	Основоположники
Давньосхідний і Античний період (до V ст. н. е.)	Основу становили обман, дезінформація, психологічна маніпуляція через релігію, міфи, символіку, страх. Вплив здійснювався через ритуали, пророкування, демонстративні жорстокі дії.	Поширення чуток, чуттєвого залякування, використання "страху богів". Символічні дії (знищення священних артефактів, демонстрація трофеїв).	Сунь-Цзи, автор трактату *"Мистецтво війни"*, описав важливість обману і психологічної переваги. Артеміда і Александр Македонський – застосовували ритуальну демонстрацію сили й інформаційне нав'язування переваги.
Середньовіччя та Ранній Новий час (V–XVII ст.)	Інтеграція релігії та воєнної пропаганди. Когнітивний вплив через індоктринацію, фанатизм, створення образу "священного ворога".	Проповідницька війна (хрестові походи). Створення героїчних і демонічних образів через церковну пропаганду, літописи. Публічні страти, які мали когнітивний ефект покарання і страху.	Католицька церква, інквізиція – як інструменти когнітивного контролю. Мартін Лютер – започаткував реформаційні рухи, які мали потужний когнітивний вплив на світогляд народів.
Епоха Просвітництва і Національних війн (XVIII–XIX ст.)	Поява світської пропаганди, ідеологічного впливу через ідеї свободи, націоналізму, соціалізму. Когнітивна війна йде через інститути друку, школи, символіку влади.	Використання гасел ("Свобода, рівність, братерство"), памфлетів, театральних виступів. Створення культу особистості (Наполеон, Гарібальді). Нав'язування національної ідентичності через освіту.	Наполеон Бонапарт – активно використовував пропаганду як засіб контролю над масами. Французькі просвітники Вольтер, Руссо – створили інтелектуальне підґрунтя для нових когнітивних впливів.
Світові війни (1914–1945)	Широкомасштабна державна пропаганда як частина воєнної стратегії. Мілітаризація інформації та введення в оману як стратегічна зброя.	Мобілізаційна пропаганда через газети, плакати, кінематограф. Поширення фальшивих повідомлень (операції "London Black"). Використання радіо як інструменту масового впливу.	Йозеф Геббельс – творець нацистської інформаційної машини. Британський офіс воєнної інформації (MOI) – піонери психологічних операцій.
Холодна війна (1947–1991)	Формування концепції психологічної війни, стратегічної дезінформації, боротьби за уми та переконання. Війна ідеологій (капіталізм vs. комунізм).	Радіо-війни (Radio Free Europe, Голос Америки). Культурна експансія, контроль за інформаційними потоками, пропагандистські фільми. Спецоперації КДБ, ЦРУ для посилення внутрішніх конфліктів у державах супротивника.	КДБ СРСР – творці концепції активних заходів. ЦРУ США – розробники програм психологічного впливу і медійної дестабілізації.
Постмодерний етап (1991–2010)	Когнітивний вплив в умовах інформаційного перевантаження, маніпуляцій у глобальному медіа-просторі. Формування реальності через візуальні образи, масову культуру, соціальні наративи.	Використання CNN-ефекту, "інформаційного шуму", фабрикацій. Поява перших інформаційних операцій у кіберсередовищі. Цілеспрямована дестабілізація через медіа-сюжети (приклад – війна в Іраку 2003).	RAND Corporation – автори концепцій інформаційних операцій. Збігнєв Бжезинський – аналітик когнітивних і геополітичних взаємозв'язків.

Продовження таблиці 2. Хронологічна послідовність розвитку когнітивних загроз у війнах і воєнних конфліктах (історичний аспект)

Цифрова когнітивна війна – етап (2010–2014)	Масове застосування штучного інтелекту, ботів, deepfake, нейронних мереж для впливу на суспільну думку. Поняття когнітивного домену стає ключовим у концепціях нової війни (NATO Cognitive Warfare).	Мікротаргетинг через соціальні мережі (Facebook-Cambridge Analytica). Інфільтрація цифрових платформ, нав'язування "альтернативних реальностей". Глибока дезорієнтація та когнітивне виснаження суспільства.	Китайські концепції "brain-control warfare". NATO Innovation Hub – автори доктрини Cognitive Warfare. Російські структури (IRA, ФСБ) – практики інформаційної деструкції через Telegram, TikTok, YouTube.
Формативно-експериментальний етап когнітивної війни (2010–2014 рр.)	Формування передумов до масової гібридизації воєн; Акцент на інформаційно-психологічному впливі у кіберсередовищі. Спроба маніпулювання протестними наративами.	Технології впливу через ЗМІ, тролі, "ботоферми". Викиди дезінформації; Таргетована реклама в соцмережах.	рф: концепція інформаційної війни Герасимова (2013). КНР, Іран – тестування цифрових впливів.
Етап гібридизації та інституціоналізації когнітивних загроз (2014–2022 рр.)	Інституціоналізація ІПСО як воєнного інструмента (після окупації Криму і вторгнення на Донбас). Введення в обіг терміна "когнітивна війна". Масова цифровізація впливу.	Операції впливу на Facebook, Twitter; Fake news. Конспірологічні наративи; Створення медіа-кілерів.	рф: "фабрика тролів", RT, Sputnik. NATO StratCom дослідження когнітивних маніпуляцій. Cambridge Analytica.
Етап тотальної когнітивної війни та технологічної ескалації (2022–2025 рр.)	Системна когнітивна війна на тлі широкомасштабної війни в Україні. Інтеграція ШІ та Big Data в інформаційні атаки. Deepfake як масовий інструмент впливу.	Генерація фальшивих відео та заяв. Інформаційне насичення / когнітивне перевантаження. Спроби деморалізації через Telegram, TikTok.	рф: ІПСО на фронті й у тилу (через Telegram, ботмережі). Китай – гібридні експерименти у Тайванському регіоні. Захід: розвиток контрнаративів, OSINT.

До основних узагальнених трендів трансформації когнітивних загроз у період 2010–2025 років належать:

зміщення фокусу з фактів на емоції, від переконання до нав'язування альтернативної реальності, тобто тренд від інформаційної війни до когнітивної домінації;

активне використання ШІ, глибокого навчання, нейромереж, психометричних моделей для таргетованого впливу, тобто здійснюється ефект технологізації впливу;

активна глобалізація виконавців, тобто якщо раніше загрози реалізовували державні актори, то після 2014 року з'явилися квазідержавні структури, приватні фірми, IT-платформи, а після 2022 навіть автономні системи.

Results (Результати)

З моменту відновлення незалежності у 1991 році Україна послідовно стикалася з різними формами загроз, зокрема і когнітивного характеру. Спершу ці загрози мали переважно латентний, м'який характер і реалізовувалися через механізми культурного впливу, історичних наративів, медійного простору та освітніх програм, проте з плином часу вони набирали більш агресивної, організованої та системної форми, інтегруючись у загальну стратегію гібридної війни проти України.

Особливо інтенсивна трансформація когнітивних загроз спостерігається у трьох ключових періодах:

після 2014 року – із початком збройної агресії рф та активного використання інформаційної зброї;

після 2022 року – з розгортанням широкомасштабної війни та переходом рф до стратегій "ментального ураження";

станом на 2025 рік – з ускладненням загроз за рахунок штучного інтелекту, діпфейків, мікротаргетингу, багаторівневого впливу на командну єдність, національну рішучість і волю до спротиву.

У зв'язку із цим необхідність системного дослідження трансформації когнітивних загроз визначається кількома ключовими факторами:

по-перше, відсутністю єдиної хронологічної моделі еволюції таких загроз в українських умовах;

по-друге, зміною способів, інструментів і цільових аудиторій впливу з боку противника;

по-третє, зростаючим значенням когнітивної сфери як арени воєнної боротьби у XXI столітті.

Отже, у табл. 3 відображено аналітичну реконструкцію трансформації когнітивних загроз для України з 1991 року до сьогодення – з виокремленням характерних особливостей впливу, механізмів реалізації, джерел загроз і стратегічних наслідків для воєнної безпеки держави.

Таблиця 3. Трансформація когнітивних загроз для України з 1991 року до сьогодення

Період	Характер когнітивних загроз	Першопричини змін	Наслідки для України
Період 1991–2003 рр. – пострадянська дезорієнтація та інфільтрація через "русскій мір"	Насадження постколоніального світогляду: ностальгія за срср, культурна меншовартість. Масована російська культурно-інформаційна експансія (ТБ, газети, фільми, література). Формування наративу "єдиного народу", "братніх націй", "неповноцінної української державності".	Відсутність повноцінної інформаційної політики України. Внутрішній розкол ідентичностей (Захід–Схід, україноцентризм – совєтоцентризм). Продовження функціонування радянських еліт в українській політиці та медіа.	Ослаблення української національної ідентичності. Вкорінення проросійських політичних сил. Системне гальмування процесу українізації армії, освіти, церковного простору.
Період 2004–2013 рр. – системна когнітивна боротьба за геополітичний вектор	Геополітичне розщеплення України на "Європейську" і "русскую" частини. Вплив через масові ЗМІ: дискредитація Заходу, просування образу "загниваючої Європи". Підживлення концепту "зовнішнього управління", "штучності Майдану".	Помаранчева революція 2004 року як виклик для рф. Активізація російських спецслужб та експансії медійних інструментів. Відсутність консолідованої державної інформаційної політики.	Поляризація суспільства. Ослаблення довіри до інституцій. Підготовка ґрунту для анексії та вторгнення (особливо в Криму та на Донбасі).

Продовження таблиці 3. Трансформація когнітивних загроз для України з 1991 року до сьогодення

Період 2014–2021 рр. – гібридна когнітивна війна у формі постправди та інформаційного терору	Масована пропаганда рф про "громадянську війну" в Україні. Інформаційні атаки через соцмережі, тролі, боти, фейкові новини. Деструктивний вплив на Захід: викривлення образу України за кордоном. Інформаційне викривлення тем війни, втрат, героїв (атаки на УПА, ЗС України, волонтерів).	Анексія Криму та війна на Донбасі. У відповідь на європейську інтеграцію – розгортання росією гібридної агресії. Активна участь рф у глобальному інфопросторі (RT, Sputnik, YouTube, Telegram).	Часткова деморалізація суспільства, страх та апатія. Розгубленість у міжнародному дискурсі: необхідність доводити свою правоту. Водночас – зміцнення української ідентичності через спротив.
Період з 2022 р. – широкомасштабна когнітивна війна нового покоління (масштабована і цифрова)	Спроба росії зламати ментальну волю України до спротиву через інформаційне виснаження. Кампанії: "Захід втомився", "влада вас зраджує", "не має сенсу воювати", "все вирішено за вас". Масове застосування deepfake, ІІ-генерованого контенту, Telegram-операцій, психологічного терору. Присутність когнітивних атак у військовому середовищі: вкиди про "оточення", "зраду", "катастрофу".	Зрив російського плану блискавичної перемоги та переходу до затяжної війни. Український цифровий прорив: "Дія", OSINT, ІТ-спільнота – нова загроза для рф. Відсутність ефекту від традиційної пропаганди змушує рф посилювати когнітивну війну.	Постійне психологічне напруження в суспільстві. Посилення потреби у державній когнітивній обороні (аналітика, протидія дезінформації). Водночас – підвищення рівня інформаційної стійкості громадян, розвиток критичного мислення, виникнення нової когнітивної суб'єктності української нації.

З 1991 року до сьогодення когнітивні загрози для України трансформувалися від латентної культурно-лінгвістичної інфільтрації до високотехнологічної когнітивної війни нового покоління, де інформаційна атака вже дорівнює удару по системі оборони. Їхня еволюція була зумовлена як зовнішніми чинниками (російська агресія, геополітичні виклики), так і внутрішніми вадами (слабкість ідентичності, нерозвинена інформаційна політика). Відповіддю на ці виклики має стати формування національної системи когнітивної безпеки, інтегрованої у структуру воєнної стратегії.

Для ефективної протидії сучасним когнітивним загрозам, особливо в умовах гібридної та інформаційної війни, надзвичайно важливо мати чітко визначений і унормований понятійно-термінологічний апарат. Удосконалення термінології сприяє формуванню єдиного методологічного базису для аналізу, оцінювання та розроблення стратегічних заходів реагування.

Це дозволяє забезпечити уніфікованість підходів як у наукових дослідженнях, так і в практичній діяльності органів національної безпеки та оборони. Методологія стратегічного реагування на когнітивні загрози – це сукупність науково-обґрунтованих принципів, понять, процедур, механізмів і стратегій, спрямованих на ідентифікацію, передбачення, нейтралізацію та мінімізацію впливу когнітивних загроз на воєнну безпеку держави, з урахуванням інформаційного, психологічного, соціального і технологічного середовища.

У табл. 4 розкрито оновлені визначення ключових термінів, що відображають сучасні реалії розвитку когнітивних загроз і викликів, а також їхній вплив на воєнну безпеку держави. Такий системний підхід до кодифікації термінів є необхідною умовою для підвищення якості стратегічного реагування в умовах постійно зростаючої складності когнітивного простору. Деякі основні терміни методології стратегічного реагування на когнітивні загрози також розкрито у табл. 4. Усі терміни логічно інтегруються у понятійно-термінологічний апарат методології стратегічного реагування, зокрема як його науково-методичні інструменти.

Таблиця 4. Удосконалений понятійно-термінологічний апарат методології стратегічного реагування на когнітивні загрози

Термін	Визначення	Джерело
Когнітивна загроза	Маніпуляції, спрямовані на сприйняття, ухвалення рішень і поведінку людини з метою дестабілізації національної безпеки, військових операцій чи суспільної згуртованості або впливу на них.	NATO Innovation Hub (2020)
	Психологічні та інформаційні дії, що спрямовані на підрив довіри, зміну переконань або провокування ірраціональних рішень.	RAND Corporation (2021)
	Ворожі дії, спрямовані на маніпуляцію когнітивною сферою: як люди мислять, сприймають, інтерпретують і діють.	Hybrid CoE (EU/NATO)
	Інформаційно-психологічні впливи на індивідуальну чи колективну свідомість, що призводять до спотвореного сприйняття реальності, порушення ухвалення рішень або дезорганізації управління.	Українські наукові джерела (ІСЗЗІ, НІСД, НУОУ)
	Цілеспрямований, переважно прихований вплив на ментальні процеси індивіда, групи чи суспільства, що спричиняє викривлення сприйняття, дезорієнтацію, підрив раціонального мислення чи здатності ухвалювати самостійні рішення з наслідками для безпеки держави.	Авторське
Когнітивний виклик	Ментальна, комунікаційна чи інформаційна ситуація, що ставить завдання збереження ідентичності, цінностей, критичного мислення й ухвалення обґрунтованих рішень в умовах інформаційного впливу; може перетворюватися на загрозу в разі ігнорування.	Авторське
Когнітивна загроза воєнній безпеці	Прихований вплив на когнітивний простір військово-політичного керівництва, командування, військових чи населення з метою підриву здатності адекватно оцінювати ситуацію, планувати оборону, мобілізувати ресурси і зберігати спротив.	Авторське
Вплив когнітивної загрози	Зміна ментальних моделей сприйняття, оцінювання ситуації або поведінки особи / групи / нації в результаті цілеспрямованого інформаційно-когнітивного втручання.	RAND, NATO StratCom CoE, авторське уточнення
Вплив когнітивної загрози на стан воєнної безпеки	Підрив спроможності командування, військ чи оборонної інфраструктури до адекватного ухвалення рішень, ведення бойових дій чи мобілізації ресурсів.	Авторське
Вплив когнітивної загрози на стан національної безпеки	Деструктивна трансформація стратегічних комунікацій, громадської свідомості, політичної єдності, що унеможливлює ефективне функціонування держави.	НІСД, Hybrid CoE, авторське доповнення
Когнітивне середовище (когнітивний домен)	Сукупність інтелектуальних, інформаційних, комунікативних і культурних процесів, у межах яких формується сприйняття реальності, ухвалення рішень і поведінкові реакції особистості, соціуму чи держави.	Авторське

Продовження таблиці 4. Удосконалений понятійно-термінологічний апарат методології стратегічного реагування на когнітивні загрози

Когнітивна операція (операція у когнітивному домені)	Спланована діяльність, що має на меті змінити когнітивні моделі мислення противника, дезорієнтувати або нав'язати бажану картину реальності для досягнення стратегічної переваги без фізичного вторгнення.	Авторське
Когнітивна оборона	Комплекс заходів щодо виявлення, запобігання та нейтралізації когнітивних впливів через освіту, критичне мислення, кіберзахист і стратегічну комунікацію.	NATO StratCom CoE, авторське доповнення
Когнітивна вразливість	Наявність у свідомості або структурі держави слабких місць, через які можливе маніпулювання, нав'язування чужих наративів чи деморалізація.	Авторське (на основі терміну cognitive vulnerability в дослідженнях RAND)
Когнітивна стійкість	Здатність зберігати критичне мислення, психологічну рівновагу та спроможність до дій в умовах когнітивного тиску чи інформаційного терору.	NATO Resilience Concept, авторське уточнення
Когнітивне збройне втручання	Використання когнітивного впливу як інструменту досягнення політичних і воєнних цілей без прямого збройного насильства.	Авторське
Когнітивна розвідка	Системне вивчення джерел когнітивних загроз, їх поширення, впливу на свідомість та прогнозування сценаріїв їхньої еволюції.	Авторське
Реверсивна когнітивна операція	Контрвплив або нейтралізація джерела когнітивного впливу шляхом його демаскування, дискредитації або нав'язування зворотного образу.	Авторське
Методологія стратегічного реагування на когнітивні загрози	Сукупність науково-обґрунтованих принципів, понять, процедур (методів) і стратегій, спрямованих на виявлення, аналіз, запобігання та нейтралізацію когнітивних загроз у сфері безпеки.	Авторське (системне узагальнення
Метод пріоритезації когнітивних загроз в умовах невизначеності проблематики їхнього впливу	Система оцінювання та ранжування когнітивних загроз за критеріями потенційної небезпеки, ймовірності реалізації, масштабів впливу та здатності до поширення за умов неповноти інформації.	Авторське (на основі концептів decision science, risk management)
Метод ідентифікації, вибору та прогнозування впливу когнітивних загроз на стан воєнної й національної безпеки держави	Комплекс інструментів, моделей і процедур для виявлення джерел когнітивного впливу, класифікації загроз, оцінювання їхнього сценарного розвитку та прогнозування наслідків для національної стійкості.	Авторське (інтеграція підходів foresight, cognitive threat modeling, systems analysis)
Метод оцінювання ефективності заходів протидії когнітивним загрозам	Методологія вимірювання досягнутих результатів дій у відповідь на когнітивні загрози за показниками зниження їхнього впливу, підвищення обізнаності, зміцнення стійкості та недопущення повторних атак.	Авторське (на основі performance assessment, counter-influence operations)
Оцінювання ефективності протидії когнітивній загрозі	Аналіз рівня зниження когнітивного впливу, стабілізації суспільної думки, відновлення довіри та стійкості у цільовій аудиторії внаслідок захисних заходів.	Авторське

Закінчення таблиці 4. Удосконалений понятійно-термінологічний апарат методології стратегічного реагування на когнітивні загрози

Проблематика когнітивних загроз	Сукупність актуальних теоретичних, прикладних та організаційних питань, пов'язаних з виникненням, розпізнаванням, масштабуванням і нейтралізацією впливу на свідомість.	Авторське
Ефективність когнітивної загрози	Ступінь досягнення поставлених цілей атакуючою стороною шляхом когнітивного впливу, включно з рівнем дезорієнтації, деморалізації та дестабілізації.	Авторське
Пріоритезація когнітивних загроз	Процес розподілу загроз за рівнем небезпеки, впливовості, масштабом потенційних наслідків і невідкладності реагування.	Авторське
Критерії потенційних небезпек від когнітивних загроз	Показники оцінювання рівня шкоди: масштаб цільової аудиторії, тривалість впливу, стійкість до розвінчання, здатність до реплікації.	Авторське визначення
Ймовірність реалізації когнітивної загрози	Ступінь імовірності того, що ворожий когнітивний вплив буде реалізовано в конкретному середовищі з досягненням цільового ефекту.	Теорія ризику, авторське уточнення
Критерій оцінювання ефективності реалізації когнітивної загрози	Визначений показник, за яким вимірюється ступінь досягнення мети когнітивного впливу (наприклад, зниження бойового духу, зростання протестної активності).	Авторське визначення
Невизначеність в системі когнітивізму	Наявність прогалин у знаннях про джерела, шляхи впливу, характер та наслідки когнітивних загроз, що ускладнює прогнозування й ухвалення рішень.	Теорія складних систем, авторське визначення

Примітка: визначення адаптовані до реалій гібридної війни, цифрового інформаційного простору та стратегічних комунікацій. За потреби кожен термін може бути розгорнуто у підрозділ методології (наприклад, окремі моделі прогнозування, оцінювання, ідентифікації).

Станом на червень 2025 року воєнна безпека України залишається критично вразливою до багатокомпонентного когнітивного тиску з боку держави-агресора. Системність, інноваційність і багаторівневість сучасних когнітивних загроз, зокрема тих, що реалізуються через цифрові, інформаційні та психологічні канали, зумовлює необхідність їх чіткої ідентифікації, оцінювання та стратегічного прогнозування. Трансформація когнітивного впливу в умовах широкомасштабної війни призвела до появи нових типів загроз, яких раніше або не було, або їх не розглядали як фактори, здатні без фізичного ураження спричинити дезорганізацію військового управління, ерозію довіри, паніку в суспільстві або деморалізацію захисників.

У табл. 5 розкрито результати аналітичного узагальнення актуального стану когнітивного середовища воєнної безпеки України й надано сформований структурований опис, а саме: назву сучасної загрози; її змістовну характеристику (форма прояву, цільова аудиторія, спосіб впливу, стратегічна мета); оцінку ймовірності реалізації протягом найближчих шести місяців (на основі експертного оцінювання, з урахуванням наявних трендів і намірів противника). Необхідність такого аналізу зумовлена: потребою адекватного пріоритезування заходів реагування в умовах обмежених ресурсів; підготовкою системи стратегічного моніторингу загроз когнітивного типу; формуванням оперативного планування заходів інформаційної та психологічної безпеки в органах оборонного управління. Отже, табл. 5 виконує роль інструменту стратегічного аналізу та ухвалення рішень, спрямованих на попередження, пом'якшення або нейтралізацію найімовірніших когнітивних загроз у найближчому часовому горизонті.

Таблиця 5. Сучасні когнітивні загрози воєнній безпеці України (станом на червень 2025)

№	Назва загрози	Характеристика	Імовірність реалізації (оцінка на 6 міс.)
1	Інформаційне виснаження населення та військових	Надмірне перенавантаження негативними повідомленнями, маніпулятивною "реальністю", змішаною з правдою, спрямоване на зниження бойового духу, віри у перемогу та довіри до влади.	Висока
2	Наратив про "втому Заходу"	Просування меседжів про нібито зниження підтримки України з боку США, ЄС, НАТО; формування уявлення про ізоляцію.	Висока
3	Розмиття довіри до військово-політичного керівництва	Створення образу "внутрішньої боротьби за владу", корупційних скандалів у тилу, нібито неефективного командування.	Висока
4	Делегітимація мобілізаційних заходів	Посилення протестних настроїв проти мобілізації шляхом поширення жахливих історій, фейків, маніпулятивних відео про нібито свавілля або жорстокість.	Середня ↗ висока
5	Підрив бойового духу ЗСУ через ІПСО	Масовані ІПСО, спрямовані на підрозділи ЗСУ, з використанням deepfake, месенджерів, Telegram-ботів з дезінформацією про "зрадженість", "оточення", "незворотні втрати".	Висока
6	Підміна стратегічних цілей війни	Просування думки, що "треба погодитись на мир за будь-яку ціну", "війна не має сенсу", "Крим не вартий жертв", – з метою зміни базових орієнтирів спротиву.	Середня
7	Емоційна десенсибілізація через постійні втрати	Зниження співчуття, згуртованості та сприйняття цінності людського життя внаслідок тривалого перебування у режимі "нормалізованої смерті".	Середня
8	Розколи всередині проукраїнських аудиторій	Маніпуляції темами волонтерства, цивільно-військових відносин, "зайвих" героїв, конфліктів між ветеранськими спільнотами.	Середня ↗ висока
9	Використання штучного інтелекту для генерації дезінформації	Автоматизоване створення зображень, текстів і відео для посилення недовіри, паніки, підриву репутації українських сил.	Середня ↗ висока
10	Інфільтрація через "нейтральні" платформи та блогерів	Поширення проросійських чи деморалізуючих тез через впливових блогерів, "експертів", журналістів, які формально не є проросійськими.	Висока

Найбільш імовірні загрози: атаки на бойовий дух, стратегічну стійкість, довіру до влади та зовнішніх партнерів. Інструменти впливу: Telegram, YouTube, deepfake, псевдоаналітика, експлуатація травматичного досвіду. Джерело загроз: російські державні структури, проксі-медіа, а також інфільтровані платформи соцмереж.

У табл. 6 наведено матрицю пріоритезації когнітивних загроз воєнній безпеці України станом на червень 2025 року, побудовану за двома ключовими критеріями: імовірність реалізації (вертикальна вісь) – наскільки ймовірно, що загроза реалізується найближчим часом; рівень впливу (горизонтальна вісь) – наскільки суттєво загроза здатна вплинути на стан воєнної безпеки, бойову стійкість, управління та спротив.

У межах комплексної системи стратегічного моніторингу когнітивних загроз доцільно використовувати ключові інтегральні показники, які дають можливість не лише виявляти небезпеки, а й оцінювати динаміку впливу, здатність до спротиву та потенціал до попередження негативних когнітивних ефектів. Нижче наведено опис трьох основних таких показників:

1. Індекс когнітивного тиску (ІКТ).

Цей індикатор дозволяє кількісно оцінити сумарний рівень когнітивного навантаження на воєнну безпеку держави, який формується сукупністю активних когнітивних загроз. Розраховується цей показник за формулою:

ІКТ = Σ (вага загрози × частота її появи × рівень впливу).

Таким чином, індекс враховує: вагу (пріоритетність або стратегічну значущість конкретної загрози), частоту появи (інтенсивність повторення в інформаційному середовищі), рівень впливу (ступінь негативного когнітивного ефекту на об'єкт впливу – військо, населення, політичне керівництво тощо).

Таблиця 6. Матриця пріоритезації когнітивних загроз (оцінка за 5-бальною шкалою)

№	Загроза	Імовірність реалізації (І) (1–5)	Рівень впливу (В) (1–5)	Пріоритетність (індекс = І×В)	Пріоритет
1	Інформаційне виснаження населення та військових	5	5	25	Критичний
2	Наратив про "втому Заходу"	5	4	20	Критичний
3	Підрив довіри до військово-політичного керівництва	5	4	20	Критичний
4	Делегітимація мобілізації	4	4	16	Високий
5	ІПСО проти ЗСУ ("оточення", "зрада")	5	5	25	Критичний
6	Підміна стратегічних цілей війни	3	5	15	Високий
7	Емоційна десенсибілізація	3	3	9	Помірний
8	Розколи всередині проукраїнських груп	4	4	16	Високий
9	Deepfake / ШІ-дезінформація	4	3	12	Помірний
10	Інфільтрація "нейтральних" медіа	5	4	20	Критичний

Примітка: 20–25 – Критичний – Вимагає негайного реагування і постійного моніторингу; 15–19 – Високий – Потребує системної уваги в короткостроковій перспективі; 10–14 – Помірний – Слід враховувати у планах реагування; <10 – Низький – Допоміжна увага або відкладене реагування.

Призначення цього показника полягає у наданні можливості швидко оцінити критичність загального інформаційно-когнітивного навантаження та обґрунтувати необхідність заходів реагування.

2. Індекс стійкості морального духу (ІСМД).

Цей індикатор спрямований на визначення психологічної готовності та моральної витривалості населення, військових і лідерських структур до впливу когнітивних операцій.

Методика розрахунку цього показника полягає в узагальненні комбінованих даних з: опитувань громадської думки (рівень довіри до влади, готовність до спротиву тощо), аналітики соціальних мереж (настрої, поширення панічних чи деморалізуючих наративів), моніторингу ЗМІ (тональність, меседжі, антидержавна риторика).

Цей показник визначає потенційні зони деморалізації, втрати довіри або зниження бойового духу – критично важливі для раннього втручання.

3. Когнітивний індекс раннього попередження (C-WARN).

Цей показник функціонує як система сигналізації про зародження нових когнітивних загроз, які ще не виявлені або не мають сформованого профілю. Методика розрахунку формується на основі трендової аналітики інформаційного поля (виявлення аномальних змін у тематиках, емоційних коливаннях), а також із урахуванням особливостей машинного навчання для виявлення нових патернів (нові типи маніпуляцій, неочікувана лексика, повторювані поведінкові маркери).

Застосування показника забезпечує превентивне виявлення потенційно небезпечних тенденцій у когнітивному середовищі ще до початку їх активного впливу.

Загалом, система з трьох індексів (ІКТ, ІСМД, C-WARN) створює інтегровану аналітичну основу для виявлення, оцінювання та реагування на когнітивні загрози, формуючи базу для ухвалення стратегічних рішень у сфері воєнної безпеки.

У табл. 7 та на рис. 1, рис. 2 наведено кінцеві результати експертного опитування щодо частоти появи та рівня впливу загрози, а також розрахунку індексу когнітивного тиску. Інтегральне значення ІКТ на червень 2025 року становить: 0,6709 *(за шкалою від 0 до 1)*, що свідчить про високий рівень когнітивного навантаження на воєнну безпеку України сьогодні.

Таблиця 7. Компоненти ІКТ за загрозами

№	Загроза	Вага (AHP)	Частота появи	Рівень впливу	Компонент ІКТ
1	Виснаження інформацією	0,154	0,90	0,95	0,1318
2	Недовіра до керівництва	0,154	0,88	0,92	0,1248
3	Наратив “втоми Заходу”	0,154	0,85	0,90	0,1179
4	ІПСО проти ЗСУ	0,154	0,80	0.88	0,1085
5	Інфільтрація нейтральних медіа	0,154	0,70	0,75	0,0809
6	Делегітимація мобілізації	0,059	0,75	0,85	0,0375
7	Підміна цілей війни	0,059	0,70	0,70	0,0288
8	Розколи проукраїнських груп	0,059	0,60	0,60	0,0212
9	Емоційна десенсибілізація	0,027	0,65	0,60	0,0103
10	ШІ-дезінформація (deepfake)	0,027	0,50	0,70	0,0093

Топ-5 загроз дають понад 80% загального ІКТ, тому вони є ключовими цілями протидії: виснаження інформацією; недовіра до керівництва; наратив про “втому Заходу”; ІПСО проти ЗС України; інфільтрація нейтральних медіа; менш критичні, але зростаючі загрози (desensitization, deepfake) – потребують технологічного моніторингу та освітніх кампаній.

Найменш вагомими виявились загрози з глибокими наслідками, але меншою ймовірністю впливу у короткостроковій перспективі – десенсибілізація та deepfake / ШІ.

У сучасних умовах російсько-української війни, що триває, когнітивні загрози посідають ключове місце серед інструментів гібридного впливу, що використовуються противником для досягнення стратегічних цілей без прямого застосування сили. Вони націлені на підрив морально-психологічної стійкості, маніпуляцію громадською думкою, дезорієнтацію військово-політичного керівництва, а також на зниження боєздатності через руйнування довіри до державних інститутів.

З огляду на результати попереднього аналізу та розрахунок індексу когнітивного тиску, було здійснено систематизацію найбільш критичних загроз станом на червень 2025 року, які потребують пріоритетного реагування з урахуванням багаторівневого підходу до протидії.

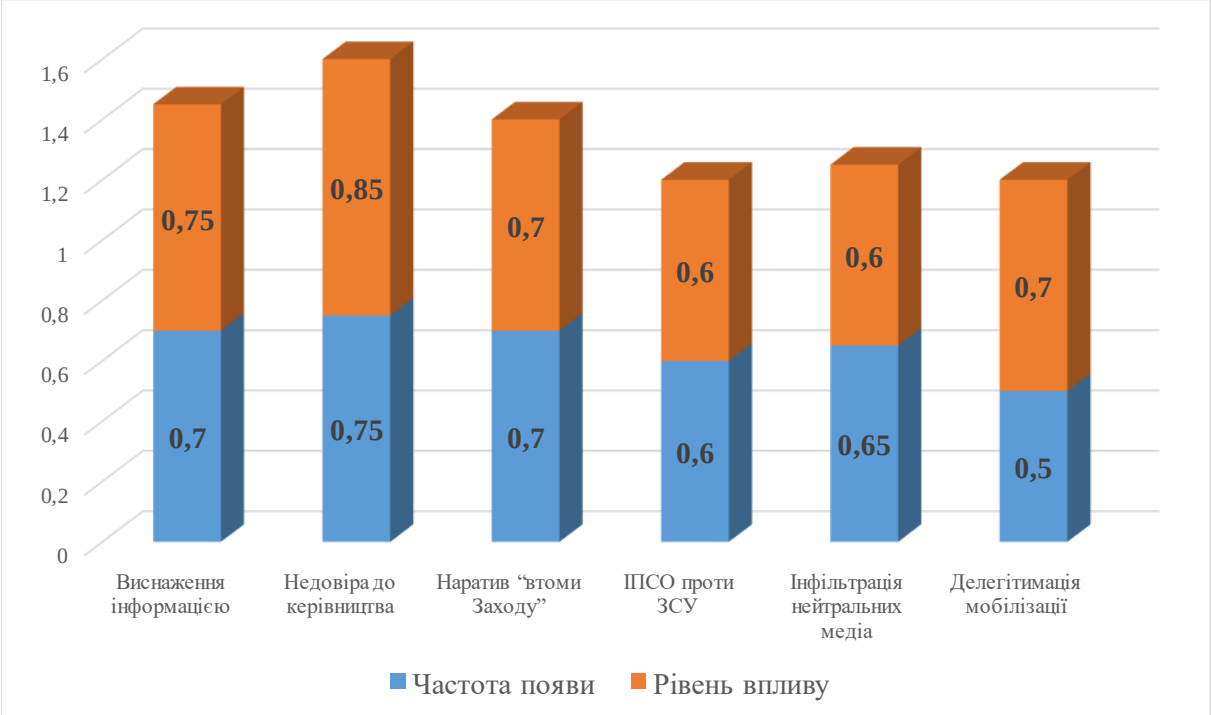


Рисунок 1. Результати експертного опитування щодо частоти появи та рівня впливу когнітивної загрози на стан воєнної безпеки України станом на червень 2025 року

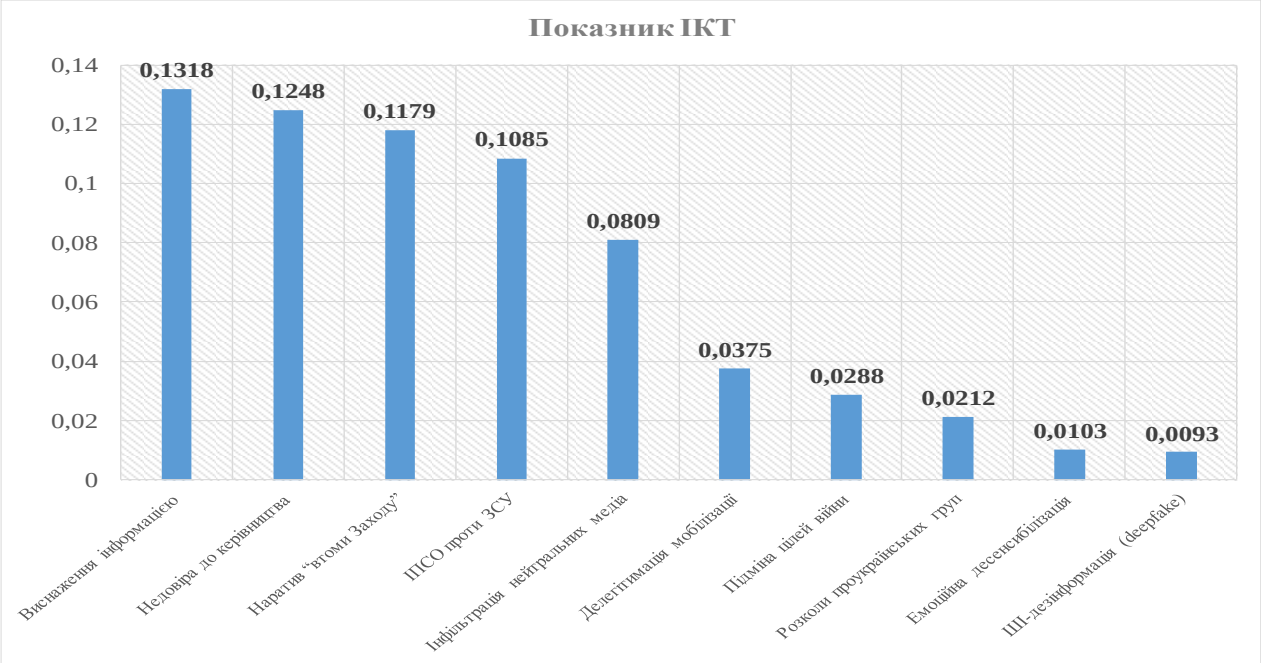


Рисунок 2. Кінцеві результати розрахунків індексу когнітивного тиску загроз на стан воєнної безпеки України станом на червень 2025 року

Рекомендації (Recommendations)

У табл. 8 розкрито систему рекомендацій щодо ефективної протидії актуальним когнітивним загрозам воєнній безпеці України станом на червень 2025 року, сформовану на

основі оцінок індексу когнітивного тиску та попереднього аналізу. Рекомендації сформовані за трьома рівнями впливу їх реалізації, а саме: стратегічний рівень – формування та адаптація державної політики у сфері національної безпеки; оперативно-тактичний рівень – інформаційно-психологічне забезпечення та захист оборонного сектору; психологічно-освітній рівень – посилення громадянської стійкості та критичного мислення. Очікувані результати реалізації рекомендацій та запропонованих дій відображені у форматі прогнозованого ефекту зниження рівня впливу загрози або її нейтралізації.

У табл. 8 здійснено також спробу переведення аналітичних знань в управлінські рішення, які є практичним орієнтиром для розробників безпекової політики, командирів, інформаційних стратегів, освітян і фахівців з психологічної оборони.

Таблиця 8. Система рекомендацій щодо ефективної протидії актуальним когнітивним загрозам воєнній безпеці України станом на червень 2025 року

Загроза	Рекомендація	Очікуваний ефект
1. Стратегічний рівень реагування (національна безпекова політика)		
“Виснаження інформацією” (0,1318)	Упровадження державної системи “гігієни інформації” (фільтрація, стандартизація, освітні кампанії). Обмеження деструктивного інфошуму в офіційних каналах.	Зниження перевантаження суспільства та збереження критичного мислення.
“Недовіра до керівництва” (0,1248)	Прозора та регулярна стратегічна комунікація уряду та ЗС України (звіти, відповіді, прямі трансляції). Публічне пояснення складних рішень (мобілізація, кадрові зміни, підтримка Заходу).	Підвищення легітимності рішень, стабілізація настроїв.
Наратив “втоми Заходу” (0,1179)	Випереджувальна дипломатія: активна медійна присутність України на Заході. Демонстрація результатів підтримки (вплив зброї, перемоги).	Зниження впливу деморалізаційних меседжів серед населення.
2. Оперативно-тактичний рівень (інформаційна оборона ЗС України)		
“ІПСО проти ЗС України” (0,1085)	Постійний моніторинг соцмереж (OSINT, SIGINT) та раннє виявлення фейків. Випереджувальні контрнаративи у військових пабліках. Посилення інформаційної присутності командирів.	Підтримання бойового духу, уникнення масового сумніву чи паніки.
“Інфільтрація нейтральних медіа” (0,0809)	Перевірка та сертифікація медіа, що співпрацюють з державою. Навчання редакцій медіаграмотності й протидії ШІ-фейкам.	Блокування каналів російських наративів під прикриттям.
3. Психологічно-освітній рівень (громадянська стійкість)		
“Емоційна десенсибілізація” (0,0103)	Масова психологічна просвіта через серіали, подкасти, блоги. Позитивні історії, персоніфікація героїзму.	Відновлення емпатії та небайдужості до війни.
“ШІ-дезінформація (deepfake)” (0,0093)	Навчання виявленню deepfake у школах, на ТБ. Спільна боротьба з платформами: репортинг і бан фейкового контенту.	Утримання інформаційного простору в межах реальності.

До найбільш пріоритетних рекомендації на короткий період (3–6 міс.) щодо протидії когнітивним загрозам воєнній безпеці України в умовах війни належать такі:

- запустити інформаційну доктрину протидії когнітивним загрозам;
- формалізувати реєстр інформаційних впливів, які кваліфікуються як загрози;

- упровадити регулярну звітність про інформаційні атаки на рівні РНБО / ГШ ЗС України;
- створити індекс медіастійкості аудиторії за регіонами

З метою комплексного розуміння та ефективного управління сучасними когнітивними загрозами, що набули системного характеру в умовах російсько-української війни, що триває, необхідно сформувати базову аналітичну модель стратегічного реагування та моніторингу когнітивних загроз воєнній безпеці України станом на 2025 рік. Цю модель (рис. 3) побудовано на основі попередньо проведеного експертного оцінювання, що дозволило ідентифікувати, класифікувати та пріоритезувати ключові когнітивні загрози з урахуванням їхньої імовірності реалізації та потенційного впливу на стан воєнної безпеки. Вона включає в себе логіку взаємозв'язку між джерелами загроз, механізмами впливу в когнітивному домені та рівнями реагування – стратегічним, оперативно-тактичним і психологічно-освітнім.

Для забезпечення ефективного моніторингу динаміки цих загроз та ухвалення своєчасних управлінських рішень у межах моделі було розроблено систему кількісних та якісних показників, що відображають інтенсивність когнітивного тиску, рівень морально-психологічної стійкості населення й військових, а також рівень раннього попередження щодо інформаційно-психологічних атак.

Показники моніторингу когнітивних загроз та відповідні заходи реагування на них систематизовано та розкрито у табл. 9, що є практичним інструментом для формування рішень на рівні національної безпеки.

Така систематизація даних є логічним продовженням аналітичної моделі (рис. 3) і відображає цілісну архітектуру: від виявлення загроз до рекомендованих дій, з урахуванням очікуваного ефекту впливу на безпекове середовище.



Рисунок 3. Модель (структура) реагування на когнітивні загрози воєнній безпеці України

Отже, наведена модель задає системну рамку аналізу, а система показників моніторингу деталізує інструменти впливу та контролю, що дозволяє здійснювати цілеспрямовану протидію когнітивним загрозам у реальному часі.

Таблиця 9. Показники моніторингу когнітивних загроз та заходи реагування на них

Загроза	Показники моніторингу	Заходи реагування
1. Виснаження інформацією	Обсяг новинного потоку Частка негативних / тривожних повідомлень Військові / цивільні скарги на "перевантаження"	Створення фільтрованих каналів інформування (штаби, медіацентри) Інфо-гігієнічні кампанії
2. Наратив "втоми Заходу"	Кількість згадок у медіа / соцмережах Динаміка підтримки в західній пресі Опитування про "марність спротиву"	Контрнаративи: приклади успіхів Публічні кампанії в західному медіапросторі
3. Недовіра до керівництва	Поширення критичних / дискредитуючих меседжів Опитування щодо рівня довіри	Прозорі комунікації Публічні звіти, діалог із суспільством
4. Делегітимація мобілізації	Активність антипризовних груп Кількість ухилянь / саботажів Наративи про несправедливість	Стратегія моральної легітимізації Пояснення мети, прозорість процедур
5. ІПСО проти ЗС України	Сплески фейків про "оточення", "зраду" Аномальна активність ботів / тролів	Rapid-response групи Аналітика фейків, фактчекінг
6. Підміна стратегічних цілей	Зміщення фокусу публічних дискусій Вживання понять типу "мир будь-якою ціною"	Комунікація наративів стратегічної мети Активізація державно-гуманітарного блоку
7. Емоційна десенсибілізація	Зниження емпатії в соцмережах Іронізація втрат / жахів війни Втома від благодійності	Кампанії з "олюднення" фронту Психоемоційна підтримка для суспільства
8. Розколи серед союзників	Активність хейт-груп між волонтерськими / військовими спільнотами Кампанії "свої проти своїх"	Посередництво, фасилітація порозуміння Публічне визнання ролі всіх сторін
9. Deepfake / ШІ-дезінформація	Виявлення підроблених відео / аудіо Кількість фіксацій ШІ-деструктивного контенту	Технічний моніторинг Освітні кампанії розпізнавання фейків
10. Інфільтрація "нейтральних" медіа	Стиль і зміст нових статей у "нейтральних" медіа Поява прихованої проросійської риторики	Моніторинг медіа Виведення на світ внутрішніх лояльностей

Висновок (Conclusion)

Під час дослідження встановлено, що когнітивні загрози стали ключовим компонентом сучасної гібридної війни, а їхнє значення у сфері воєнної безпеки України значно зросло в умовах російсько-української війни, що триває. Встановлено, що природа цих загроз зазнала еволюції від традиційної пропаганди до складних форм інформаційно-психологічного впливу з використанням штучного інтелекту, цифрових технологій, соціальних мереж і алгоритмів маніпуляції масовою свідомістю.

На основі аналітичного оцінювання та експертного ранжування сформовано пріоритети протидії актуальним когнітивним загрозам воєнній безпеці, визначено матрицю їх пріоритезації, а також розраховано інтегральний індекс когнітивного тиску, що дозволяє кількісно оцінювати динаміку інформаційної ситуації в країні. Запропонована система стратегічного реагування охоплює інституційний, технологічний, комунікаційний та освітній виміри протидії загрозам, що дає змогу не лише знижувати ймовірність їх реалізації, а й

підвищувати адаптивність державної політики до умов невизначеності та інформаційної турбулентності.

Наукова новизна матеріалу статті полягає у поєднанні кількісного та якісного підходів до оцінювання когнітивних загроз, формалізації понятійно-термінологічного апарату, а також розробленні інтегрованої моделі реагування на основі індексного аналізу.

До основних перспектив подальших досліджень за визначеним напрямом досліджень належать:

- необхідність розроблення математичної моделі прогнозування когнітивного тиску на регіональному рівні із залученням індикаторів соціальних мереж, медіа-активності, мобілізаційних настроїв та факторів довіри;
- розроблення системи індикаторів стратегічної стійкості держави до когнітивних впливів у межах воєнної доктрини України;
- моделювання адаптивної поведінки державних інституцій у відповідь на когнітивні виклики з урахуванням теорії ігор та сценарного аналізу;
- формування методології інтеграції когнітивного компоненту в плани оборонного планування, оперативного реагування та інформаційної безпеки ЗС України;
- створення єдиної міжвідомчої цифрової платформи моніторингу когнітивних загроз у режимі реального часу із використанням штучного інтелекту та машинного навчання.
-

Подяки (Acknowledgments)

Автори заявляють, що у них немає конкуруючих інтересів за тематикою статті.

Використані джерела

1. Thomas, T. (2022). *Russian Cognitive Warfare: Influence, Deception, and Perception Management in the Ukrainian Conflict*. Foreign Military Studies Office (FMSO).
2. Darczewska, J. (2014). *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study.* Centre for Eastern Studies (OSW).
3. Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War Against Reality*. Faber & Faber.
4. Горбулін, В. П., & Литвиненко, О. В. (2020). *Гібридна війна: вижити і перемогти.* НІСД.
5. Minakov, M. (2023). *Russia's Cognitive Warfare in Ukraine: From Propaganda to Mental Occupation.* Wilson Center.
6. Kasekamp, A., Pabriks, A., Smith, J., & Veenendaal, W. (2022). *Strategic Narratives in the Russo-Ukrainian War: Competing for Minds and Morale.* NATO Strategic Communications Centre of Excellence.
7. Олійник, Д. А. (2024). Когнітивна війна у стратегічних комунікаціях: український вимір. *Військово-науковий вісник Національного університету оборони України, 2* (46),102–115.
8. *Cognitive Warfare. The Future of Conflict*. (2020). NATO Innovation Hub.
9. *Cognitive Security and Information Warfare Series*. *(2019–2023).* RAND Corporation. https://www.rand.org
10. *Cognitive Influence: Threat Landscape & Resilience*. (2022). Hybrid CoE (The European Centre of Excellence for Countering Hybrid Threats).
11. Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The Weaponization of Social Media*. Houghton Mifflin Harcourt.
12. Bendett, S. (2020). *Russian Information Warfare: Cognitive and Psychological Dimensions*. CNA Corporation.
13. Wilson, J. Q., & Davis, P. K. (2021). *Cognitive Domain Operations: Strategic Advantage in the Human Mind*. RAND.

14. Манойла, З. А. (2021). *Когнітивна безпека держави: теоретико-прикладні основи*. НаУОУ.
15. *Аналітичні матеріали про дезінформацію та когнітивні операції РФ. (2021–2024).* Центр стратегічних комунікацій та інформаційної безпеки. https://spravdi.gov.ua
16. Шевцов, І. О. (2022). *Інформаційно-психологічні операції в гібридній війні: російська модель*. НІСД.
17. *Воєнна безпека України.* Збірник наукових праць. (2022–2024). НІСД.
18. Павлюк, С. В., & Притула, Ю. М. (Ред.). (2022). *Інформаційна війна і когнітивна безпека: український досвід спротиву*. НАН України.
19. Libicki, M. C. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press.
20. McFate, S. (2019). *The New Rules of War: Victory in the Age of Durable Disorder*. William Morrow.
21. Thornton, R. (2018). Russian Hybrid Warfare: Resurgence and Politicisation. *Global Politics and Strategy, 60* (1).
22. Kaspersen, A. (2021). *The Weaponization of Information in the Age of AI*. World Economic Forum Report.

References

1. Thomas, T. (2022). *Russian Cognitive Warfare: Influence, Deception, and Perception Management in the Ukrainian Conflict*. Foreign Military Studies Office (FMSO).
2. Darczewska, J. (2014). *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study.* Centre for Eastern Studies (OSW).
3. Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War Against Reality.* Faber & Faber.
4. Horbulin, V. P., & Lytvynenko, O. V. (2020). *Hybrid War: Survive and Win.* National Institute for Strategic Studies (NISS).
5. Minakov, M. (2023). *Russia's Cognitive Warfare in Ukraine: From Propaganda to Mental Occupation.* Wilson Center.
6. Kasekamp, A., Pabriks, A., Smith, J., & Veenendaal, W. (2022). *Strategic Narratives in the Russo-Ukrainian War: Competing for Minds and Morale.* NATO Strategic Communications Centre of Excellence.
7. Oliinyk, D. A. (2024). Cognitive Warfare in Strategic Communications: The Ukrainian Dimension. *Military-Scientific Bulletin of the National Defense University of Ukraine, 2* (46), 102–115.
8. *Cognitive Warfare. The Future of Conflict*. (2020). NATO Innovation Hub.
9. *Cognitive Security and Information Warfare Series*. *(2019–2023).* RAND Corporation. https://www.rand.org
10. *Cognitive Influence: Threat Landscape & Resilience*. (2022). Hybrid CoE (The European Centre of Excellence for Countering Hybrid Threats).
11. Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The Weaponization of Social Media*. Houghton Mifflin Harcourt.
12. Bendett, S. (2020). *Russian Information Warfare: Cognitive and Psychological Dimensions*. CNA Corporation.
13. Wilson, J. Q., & Davis, P. K. (2021). *Cognitive Domain Operations: Strategic Advantage in the Human Mind*. RAND.
14. Manoyla, Z. A. (2021). *State Cognitive Security: Theoretical and Applied Foundations.* National Defense University of Ukraine.

15. *Analytical Materials on Disinformation and Russian Cognitive Operations. (2021–2024).* Centre for Strategic Communications and Information Security. https://spravdi.gov.ua.
16. Shevtsov, I. O. (2022). *Information and Psychological Operations in Hybrid Warfare: The Russian Model.* NISS.
17. *Military Security of Ukraine*. Collection of Scientific Works. (2022–2024). NISS.
18. Pavliuk, S. V., & Prytula, Yu. M. (Eds.). (2022). *Information War and Cognitive Security: Ukrainian Experience of Resistance.* National Academy of Sciences of Ukraine.
19. Libicki, M. C. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press.
20. McFate, S. (2019). *The New Rules of War: Victory in the Age of Durable Disorder*. William Morrow.
21. Thornton, R. (2018). *Russian Hybrid Warfare: Resurgence and Politicisation*. *Global Politics and Strategy, 60* (1).
22. Kaspersen, A. (2021). *The Weaponization of Information in the Age of AI*. World Economic Forum Report.

Analysis of the Theory and Practice of the Development of Cognitive Threats in the Field of Military Security: Countermeasures

Oleksandr Kin′
Candidate of Technical Sciences, Associate Professor
Senior Research Fellow
Diplomatic Academy of Ukraine named after Hennadii Udovenko
under the Ministry of Foreign Affairs
01001, Velyka Zhytomyrska Street, 2, Kyiv, Ukraine
e-mail: cubalibre1972@ukr.net
ORCID: 0009- 0001-2196-7515

Abstract. National security policy, military science, and practical military leadership still lack a systematic approach to studying and countering cognitive threats. There is no unified conceptual and terminological framework, nor established methods for diagnosing, monitoring, and assessing the level of cognitive security. The absence of doctrinal, regulatory, and scientific-methodological foundations hinders the formation of an effective counteraction system.

Thus, a theoretical and applied analysis of the processes of formation, development, and realisation of cognitive threats in the domain of Ukraine's military security is highly relevant, as it is directly related to the state's potential for strategic resistance, the resilience of the national security system, preservation of managerial integrity, and moral and psychological readiness for defence.

This article outlines a chronological sequence of the development of cognitive threats in wars and military conflicts from a historical perspective and explains how cognitive threats to Ukraine have transformed since 1991. It improves the conceptual and terminological tools of the strategic response methodology, identifies current cognitive threats to Ukraine’s military security as of June 2025, and develops a matrix for the prioritisation of such threats.

It also defines key integral indicators that not only detect threats but also assess the dynamics of their influence, resistance capacity, and the potential to prevent negative cognitive effects. The paper presents expert survey results on the frequency and impact level of cognitive threats on Ukraine’s military security and includes a calculated index of cognitive pressure as of June 2025. Furthermore, it offers a system of recommendations for effectively countering present-day cognitive

threats to Ukraine's military security and proposes a structured model for responding to these threats, including main indicators for monitoring and response actions.

These findings may be valuable for military personnel, analysts, security experts, researchers, and strategists engaged in protecting the information space and addressing modern cognitive threats in the field of Ukraine's military security.

Keywords: hybrid warfare; military operations; military security; armed combat; cognitive threats; cognitive influence; cognitive challenges; military-political logic; cognitive pressure index; warfare technologies; tactics and strategy of military operations; national security; global stability; methods of warfare; transformation of armed conflicts; response to cognitive threats; monitoring of cognitive threats; forms of military action.