Пропозиції та рекомендації щодо розвитку державної системи когнітивної безпеки та когнітивного впливу в інтересах Сил оборони України

Proposals and Recommendations for Developing the State System of Cognitive Security and Cognitive Influence in the Interests of the Defence Forces of Ukraine

Олег Нечаєв [A]

Corresponding author: перший заступник командувача Сил спеціальних операцій ЗС України, e-mail: o26811650@gmail.com, ORCID ID: https://orcid.org/0009-0003-8638-6353

Максим Білан [B]

кандидат філологічних наук, доцент, заступник начальника Військового інституту Київського національного університету імені Тараса Шевченка з наукової роботи, e-mail: maksym.bilan@knu.ua, ORCID ID: https://orcid.org/00000-0003-2718-9512

Артем Семененко [B]

курсант, e-mail: aretemsemen1612@gmail.com, ORCID ID: https://orcid.org/0009-0006-2753-5648

Марина Паскалова [D]

кандидат філософських наук, доцент, фахівець із супроводу ветеранів війни та демобілізованих осіб, e-mail: marinapaskalova@gmail.com, ORCID ID: https://orcid.org/00000-0003-1976-5807

Ярослав Янковий [C]

ад'юнкт інституту стратегічних комунікацій, e-mail: ya.yankovyi@gmail.com, ORCID ID: https://orcid.org/0009-0007-1718-3607

Володимир Рахімов [C]

доктор філософії заступник начальника інституту стратегічних комунікацій, e-mail: rakhimov@edu.nuou.org.ua, ORCID ID: https://orcid.org/0000-0001-9868-986X

Oleh Nechaiev [A]

Corresponding author: First Deputy Commander Special Operations Forces of the Armed Forces of Ukraine, e-mail: o26811650@gmail.com, ORCID ID: https://orcid.org/0009-0003-8638-6353

Maksym Bilan [B]

Candidate of Philological Sciences, Associate Professor, Deputy Head of the Military Institute of Taras Shevchenko National University of Kyiv for Scientific Work, e-mail: maksym.bilan@knu.ua, ORCID ID: https://orcid.org/00000-0003-2718-9512

Artem Semenenko [B]

Cadet, e-mail: aretemsemen1612@gmail.com, ORCID ID: https://orcid.org/0009-0006-2753-5648

Maryna Paskalova [D]

Candidate of philosophical sciences, Associate Professor,, e-mail: marinapaskalova@gmail.com, ORCID ID: https://orcid.org/0000-0003-1976-5807

Yaroslav Yankovyi [C]

PhD student, e-mail: ya.yankovyi@gmail.com, ORCID ID: https://orcid.org/0009-0007-1718-3607

Volodymyr Rakhimov [C]

PhD in Military Sciences Deputy Head of the Institute of Strategic Communications, e-mail: rakhimov@edu.nuou.org.ua, ORCID ID: https://orcid.org/0000-0001-9868-986X

[A] Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна
[B] Кафедра військової підготовки Державного університету "Київський авіаційний університет", м. Київ, Україна
[C] Національний університет оборони України, м. Київ, Україна
[D] Комунальна установа "Центр надання соціальних послуг", Київ, Україна

[A] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
[B] Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine
[C] National Defense University of Ukraine, Kyiv, Ukraine
[D] Municipal Institution "Center for Social Services", Kyiv, Ukraine

Received: June 20, 2026 | Revised: June 29, 2026 | Accepted: June 30, 2026

УДК 355.40:351.746.1

DOI: https://doi.org/10.33445/sds.2026.16.3.2

Мета роботи. Обґрунтувати пропозиції та практичні рекомендації щодо розвитку державної системи когнітивної безпеки й когнітивного впливу в інтересах Сил оборони України, скоординовані між військовим (рівень Збройних Сил України) та державним рівнями управління у сфері воєнної безпеки.

Метод дослідження. Системний аналіз, синтез, порівняння, систематизація, формалізація, експертне оцінювання, пріоритезація за інтегральним індексом (добуток імовірності реалізації та рівня впливу на національну безпеку), сценарне планування за часовими горизонтами.

Результати. Визначено шість взаємодоповнюваних пропозицій (три військового та три державного рівнів); для кожної

Purpose. To substantiate proposals and practical recommendations for the development of the national system of cognitive security and cognitive influence in the interests of the Defence Forces of Ukraine, coordinated between the military level (the Armed Forces of Ukraine) and the state level of governance in the field of military security.

Method. The study employs systems analysis, synthesis, comparison, systematisation, formalisation, expert evaluation, prioritisation based on an integrated index (the product of the probability of implementation and the level of impact on national security), and scenario planning across different time horizons.

Findings. Six complementary proposals were identified (three at the military level and three at the state level). For each proposal, a set of

запропоновано перелік заходів із визначенням термінів реалізації та очікуваних результатів; здійснено експертне оцінювання імовірності реалізації (65–88 %) та рівня впливу на національну безпеку (78–95 %); побудовано матрицю пріоритезації, виконано ранжування пропозицій і розроблено дорожню карту їх реалізації; обґрунтовано доцільність одночасного впровадження "швидких" організаційних заходів і поетапної реалізації інституційно-правових рішень.

Теоретична цінність дослідження. Результати можуть бути використані під час формування державної політики у сфері когнітивної безпеки, розроблення Концепції когнітивної безпеки та Стратегії когнітивної стійкості, удосконалення оборонного планування, а також у науково-дослідній та освітній діяльності.

Тип статті: теоретико-методична.

implementation measures, timelines, and expected outcomes was developed. Expert evaluation of the probability of implementation (65–88%) and the level of impact on national security (78–95%) was conducted. A prioritisation matrix was developed, the proposals were ranked, and a roadmap for their implementation was prepared. The study substantiates the feasibility of simultaneously implementing rapid organisational measures and the phased implementation of institutional and legal solutions.

Theoretical implications. The findings may be used to support the formulation of state policy in the field of cognitive security, the development of the Concept of Cognitive Security and the Cognitive Resilience Strategy, the improvement of defence planning, as well as research and educational activities.

Paper type: Theoretical and methodological.

Ключові слова: когнітивна безпека, когнітивний вплив, когнітивні операції, Сили оборони України, інформаційно-психологічний вплив, гібридні загрози, медіаграмотність, стратегічні комунікації.

Key words: Cognitive Security, Cognitive Influence, Cognitive Operations, Defence Forces of Ukraine, Information-Psychological Influence, Hybrid Threats, Media Literacy, Strategic Communications.

Вступ

Широкомасштабна збройна агресія Російської Федерації проти України супроводжується системним веденням протиборства не лише у фізичному, а й у когнітивному вимірі, тобто у боротьбі за свідомість, сприйняття та волю людини. Сучасні збройні конфлікти дедалі більше зміщуються у площину впливу на мислення та поведінку як власного населення й особового складу, так і противника. Провідні безпекові інституції визнають появу окремого когнітивного домену збройного протиборства, у якому об'єктом впливу стає людська когніція — здатність сприймати, осмислювати, запам'ятовувати, ухвалювати рішення та діяти [5; 6; 8].

Під когнітивною війною (cognitive warfare) розуміють використання технологій та інформаційно-психологічних інструментів для дезорганізації, підриву й перепрограмування процесів ухвалення рішень людиною на індивідуальному та суспільному рівнях. На відміну від традиційних форм інформаційного протиборства, її головний ефект полягає у маніпулюванні емоційними й підсвідомими процесами психіки, що робить її значно ширшим явищем порівняно з іноземними інформаційними маніпуляціями та втручанням (FIMI) і гібридними загрозами [9]. Концептуально когнітивна війна розвиває ідею Сунь-Цзи про «перемогу без бою», коли противник зазнає поразки внаслідок руйнування власної системи прийняття рішень [5; 7]. Найбільш комплексне сучасне трактування когнітивної війни запропоновано Командуванням НАТО з питань трансформації (NATO ACT) [6; 8].

Україна є одним із головних об'єктів російських інформаційно-психологічних операцій. За оцінками Європейської служби зовнішніх дій, вона залишається пріоритетною ціллю кампаній FIMI [17]. Російська Федерація використовує доктрину рефлексивного управління, мережі ботів, контрольовані медіа та технології штучного інтелекту для здійснення масштабного когнітивного впливу [13; 14; 22]. У відповідь держави НАТО та Європейського Союзу формують комплексні системи когнітивної безпеки, зокрема через діяльність Центру передового досвіду НАТО зі стратегічних комунікацій [10], Європейського центру передового досвіду з протидії гібридним загрозам [11; 12], а також реалізацію рамки протидії FIMI Європейського Союзу [17–19].

Попри значний практичний досвід України у сфері стратегічних комунікацій та інформаційного впливу, відповідні спроможності залишаються фрагментарними, розподіленими між різними органами державної влади та сектору безпеки і оборони. Чинні стратегічні документи [1–3] визначають інформаційні загрози, однак не формують цілісної державної системи когнітивної безпеки та когнітивного впливу.

Основними чинниками цієї проблеми є фрагментарність організаційної структури, відсутність єдиної доктрини когнітивних операцій, нормативно-правова невизначеність, недостатній кадровий і науковий потенціал, а також переважно оборонний характер існуючих заходів із протидії дезінформації. Це створює стратегічну асиметрію порівняно з Російською Федерацією, яка володіє доктринально оформленою та ресурсно забезпеченою системою інформаційно-психологічного протиборства [13; 14; 22]. Зазначена проблема не може бути розв'язана окремими відомствами і потребує комплексного державного підходу, що поєднує військовий і державний рівні управління.

Метою дослідження є обґрунтування пропозицій і практичних рекомендацій щодо розвитку державної системи когнітивної безпеки та когнітивного впливу в інтересах Сил оборони України, скоординованої між військовим і державним рівнями управління.

Огляд літератури

У сучасних дослідженнях когнітивну безпеку визначають як стан захищеності індивідуальної та колективної свідомості, процесів сприйняття, мислення й ухвалення рішень від зовнішніх деструктивних впливів. Когнітивний вплив (когнітивні операції) розглядається як сукупність скоординованих дій, спрямованих на зміну сприйняття, переконань, емоцій і поведінки визначених цільових аудиторій.

За концепцією NATO ACT когнітивна війна реалізується одночасно у фізичному, інформаційному та когнітивному вимірах, поєднуючи кінетичні й некінетичні засоби для досягнення ефекту у свідомості людини [5; 6]. Водночас у науковій літературі наголошується на необхідності розмежування понять когнітивної війни, іноземних інформаційних маніпуляцій та втручання (FIMI) і гібридних загроз. Зокрема, FIMI визначаються як скоординована діяльність, спрямована на маніпулювання інформаційним середовищем [17; 19], тоді як гібридні загрози охоплюють комплекс синхронізованих дій, що використовують уразливості демократичних держав нижче порога відкритого збройного конфлікту [11]. На відміну від них, когнітивна війна безпосередньо спрямована на зміну процесів людського мислення та ухвалення рішень [9].

У міжнародній науковій дискусії триває обговорення питання щодо визнання когнітивного простору окремим доменом сучасних військових операцій поряд із суходолом, морем, повітрям, космосом і кіберпростором [6; 21].

Нормативно-правову основу розвитку когнітивної безпеки в Україні становлять Стратегія воєнної безпеки України [1], Стратегія інформаційної безпеки [2], Стратегія національної безпеки України [3], Закон України “Про національну безпеку України” [4], а також Стратегія розвитку оборонно-промислового комплексу України [24]. Водночас зазначені документи не містять комплексної концепції розвитку когнітивної безпеки як окремої державної спроможності.

Методологічною основою сучасних досліджень є концепція NATO ACT [8; 9], підхід whole-of-society [16], теорія психологічної інокуляції [25], а також рамка протидії FIMI Європейського Союзу [17; 18]. Окремі дослідження також наголошують на необхідності використання автоматизованих систем моніторингу когнітивних загроз і технологій штучного інтелекту для раннього виявлення дезінформаційних кампаній та діпфейків [18; 20; 22].

Проведений аналіз свідчить, що існуючі дослідження переважно зосереджені на окремих аспектах когнітивної війни, інформаційної безпеки або стратегічних комунікацій. Водночас недостатньо опрацьованими залишаються питання формування цілісної державної системи когнітивної безпеки та когнітивного впливу, інтегрованої між військовим і державним рівнями управління, що й визначає наукову нішу цього дослідження.

Методологія дослідження

Методологія дослідження ґрунтується на системному підході, який забезпечує комплексний аналіз розвитку державної системи когнітивної безпеки та когнітивного впливу як взаємопов'язаної сукупності організаційних, правових, технологічних і функціональних елементів.

Для досягнення поставленої мети використано комплекс загальнонаукових і спеціальних методів дослідження. Системний аналіз застосовано для визначення структури та взаємозв'язків між складовими державної системи когнітивної безпеки. Методи аналізу, синтезу, порівняння, систематизації та формалізації використано для узагальнення міжнародного досвіду, нормативно-правових документів України та концептуальних підходів НАТО й Європейського Союзу.

Для оцінювання пріоритетності запропонованих заходів застосовано програмно-цільовий підхід та експертне оцінювання. Пріоритетність визначалась за інтегральним індексом, розрахованим як добуток імовірності реалізації запропонованого заходу та рівня його впливу на національну безпеку. Отримані результати використано для побудови матриці пріоритетності, ранжування запропонованих заходів і формування дорожньої карти їх реалізації.

Для оцінювання часової послідовності впровадження запропонованих рішень застосовано сценарне планування за коротко-, середньо- та довгостроковими горизонтами, що дало змогу поєднати швидкі організаційні заходи із поетапним інституційно-правовим розвитком державної системи когнітивної безпеки.

Результати дослідження

Аналіз стану когнітивних спроможностей Сил оборони України та узагальнення міжнародного досвіду засвідчують потребу в системному, а не фрагментарному розвитку як захисту власної свідомості, так і наступального впливу на противника.

Відповідні зусилля доцільно реалізовувати скоординовано на двох взаємопов'язаних рівнях: військовому (рівень Збройних Сил України) та державному (воєнному), що охоплює державу в цілому та сектор безпеки і оборони.

Нижче наведено шість пропозицій за цими рівнями; за кожною визначено перелік заходів із термінами реалізації та очікуваними результатами, а також узагальнено спрямованість пропозиції.

Терміни подано за трьома горизонтами: короткостроковий (до 6 місяців), середньостроковий (6–18 місяців) і довгостроковий (1,5–3 роки).

1. Сформуємо пропозиції військового рівня (рівень Збройних Сил України).

Пропозиція 1. Створення Командування когнітивного впливу та Сил когнітивних операцій Збройних Сил України як єдиного органу управління наступальними та захисними когнітивними спроможностями.

Таблиця 1: Заходи реалізації Пропозиції 1 (Командування когнітивного впливу та Сили КО)

Захід	Термін реалізації	Очікуваний результат (на що спрямований захід)
Створити Центр когнітивних операцій у складі Генерального штабу (міжвидова, міжвідомча структура)	**до 6 міс**	Оперативний орган координації та аналітики; швидкий старт без тривалого законодавчого процесу
Розгорнути Командування когнітивного впливу з регіональними групами	**6–18 міс**	Централізоване планування й синхронізація когнітивних, кібер- та РЕБ-ефектів у єдиному задумі
Сформувати окремий рід сил — Сили когнітивних операцій — з власним штатом і фінансуванням	**1,5–3 роки**	Стала інституційна спроможність впливу на противника та захисту власної свідомості

Джерело: розроблено авторами.

Спрямованість пропозиції. Пропозиція спрямована на створення інституційного ядра системи когнітивного впливу. Її реалізація дасть Україні єдиний керований механізм наступального впливу на противника та захисту власної аудиторії, усуне фрагментарність і забезпечить синхронізацію когнітивних дій з бойовими, кібернетичними та радіоелектронними.

Пропозиція 2. Розроблення Доктрини когнітивних операцій Сил оборони та запровадження системи оцінювання когнітивних ефектів.

Таблиця 2: Заходи реалізації Пропозиції 2 (Доктрина та система оцінювання ефектів)

Захід	Термін реалізації	Очікуваний результат (на що спрямований захід)
Розробити та затвердити Доктрину когнітивних операцій Сил оборони України	**6–12 міс**	Єдині принципи, термінологія та порядок застосування спроможностей
Запровадити методики оцінювання ефектів (показник E(t), індекси ІКТ, ІСМД, C-WARN)	**6–18 міс**	Перехід від інтуїтивних дій до вимірюваного, керованого процесу
Інтегрувати когнітивне планування й оцінку ефектів у планування операцій	**12–24 міс**	Урахування когнітивних наслідків у кожній операції

Джерело: розроблено авторами.

Спрямованість пропозиції. Пропозиція спрямована на формування методологічно-доктринального базису застосування когнітивних спроможностей. Її реалізація дасть Україні обґрунтованість і керованість рішень, можливість вимірювати ефект впливу та сумісність зі стандартами і практиками НАТО.

Пропозиція 3. Підготовка кадрів когнітивних операцій та забезпечення науково-дослідного супроводу.

Таблиця 3: Заходи реалізації Пропозиції 3 (Кадри та науково-дослідний супровід)

Захід	Термін реалізації	Очікуваний результат (на що спрямований захід)
Створити спеціалізований підрозділ когнітивних досліджень у ЦНДІ ЗС України	**6–12 міс**	Науковий супровід, моделювання та прогнозування впливів
Запровадити підготовку офіцерів когнітивних операцій у вищих військових навчальних закладах	**12–24 міс**	Фаховий кадровий резерв для нових структур
Створити освітній онлайн-хаб з когнітивної оборони	**6–18 міс**	Масштабоване навчання військових, держслужбовців і волонтерів

Джерело: розроблено авторами.

Спрямованість пропозиції. Пропозиція спрямована на формування людського капіталу та доказової бази когнітивних операцій. Її реалізація дасть Україні стійке відтворення спроможностей, довгострокову адаптивність і незалежність від зовнішніх постачальників експертизи.

2. Сформуємо пропозиції пропозиції державного (воєнного) рівня – держава та сектор безпеки і оборони

Пропозиція 4. Створення національної системи когнітивної безпеки та нормативно-правове закріплення когнітивної безпеки на рівні держави.

Таблиця 4: Заходи реалізації Пропозиції 4 (Національна система когнітивної безпеки)

Захід	Термін реалізації	Очікуваний результат (на що спрямований захід)
Розробити Концепцію когнітивної безпеки та Стратегію когнітивної стійкості держави до 2030 р.	**6–12 міс**	Програмні рамки державної політики у когнітивній сфері
Закріпити поняття когнітивної безпеки в законодавстві; визнати когнітивний простір середовищем воєнних дій	**12–24 міс**	Правова основа діяльності, повноважень і обмежень
Інтегрувати когнітивну компоненту у Стратегію воєнної безпеки та воєнну доктрину України	**12–18 міс**	Системне врахування у плануванні оборони держави

Джерело: розроблено авторами.

Спрямованість пропозиції. Пропозиція спрямована на створення правово-стратегічного фундаменту державної системи когнітивної безпеки. Її реалізація дасть Україні легітимність, узгодженість зусиль різних відомств і чітку пріоритезацію когнітивної безпеки на загальнодержавному рівні.

Пропозиція 5. Створення Національного центру когнітивної безпеки та системи моніторингу і раннього попередження когнітивних загроз.

Таблиця 5: Заходи реалізації Пропозиції 5 (Центр моніторингу та раннє попередження)

Захід	Термін реалізації	Очікуваний результат (на що спрямований захід)
Створити Національний центр когнітивної безпеки (міжвідомчий, під егідою РНБО/Кабінету Міністрів)	**6–18 міс**	Єдиний орган координації держави та сектору безпеки і оборони
Розгорнути єдину цифрову платформу моніторингу когнітивних загроз (ШІ, машинне навчання)	**12–30 міс**	Ситуаційна обізнаність про загрози в режимі реального часу
Запровадити систему індикаторів раннього попередження (C-WARN)	**12–24 міс**	Раннє виявлення та випереджальне реагування на впливи

Джерело: розроблено авторами.

Спрямованість пропозиції. Пропозиція спрямована на забезпечення моніторингу, прогнозування та міжвідомчої координації протидії когнітивним загрозам. Її реалізація дасть Україні здатність діяти на випередження, а не реагувати постфактум, та об’єднає зусилля держави й сектору безпеки і оборони.

Пропозиція 6. Розвиток суспільної когнітивної стійкості, медіаграмотності та міжнародної синхронізації.

Спрямованість пропозиції. Пропозиція спрямована на формування суспільної стійкості та союзницької інтеграції. Її реалізація дасть Україні довготривалий “імунітет” до когнітивних загроз, зменшить вразливість населення до ворожого впливу та посилить міжнародну підтримку.

Таблиця 6: Заходи реалізації Пропозиції 6 (Суспільна стійкість і міжнародна синхронізація)

Захід	Термін реалізації	Очікуваний результат (на що спрямований захід)
Запровадити національну програму медіа- та цифрової грамотності (освіта, армія, держслужба)	**6–24 міс, надалі постійно**	Підвищення когнітивної стійкості населення та критичного мислення
Підтримувати незалежні медіа та експертно-аналітичне середовище	**постійно**	Зміцнення форпостів інформаційного фронту
Поглибити взаємодію з NATO StratCom CoE, Hybrid CoE та структурами ЄС	**6–18 міс**	Доступ до досвіду, технологій і колективної протидії загрозам

Джерело: розроблено авторами.

3. Проведемо оцінку ймовірності реалізації пропозицій та їх впливу на національну безпеку

Для пріоритезації запропонованих заходів проведено експертну оцінку за двома параметрами: ймовірністю реалізації (з урахуванням політичної волі, ресурсів і умов воєнного часу) та рівнем впливу на національну безпеку України, за шкалою від 0 до 100 %. Інтегральний індекс пріоритетності розраховано як добуток ймовірності та впливу. Результати порівняння за обома параметрами наведено на рис. 1.

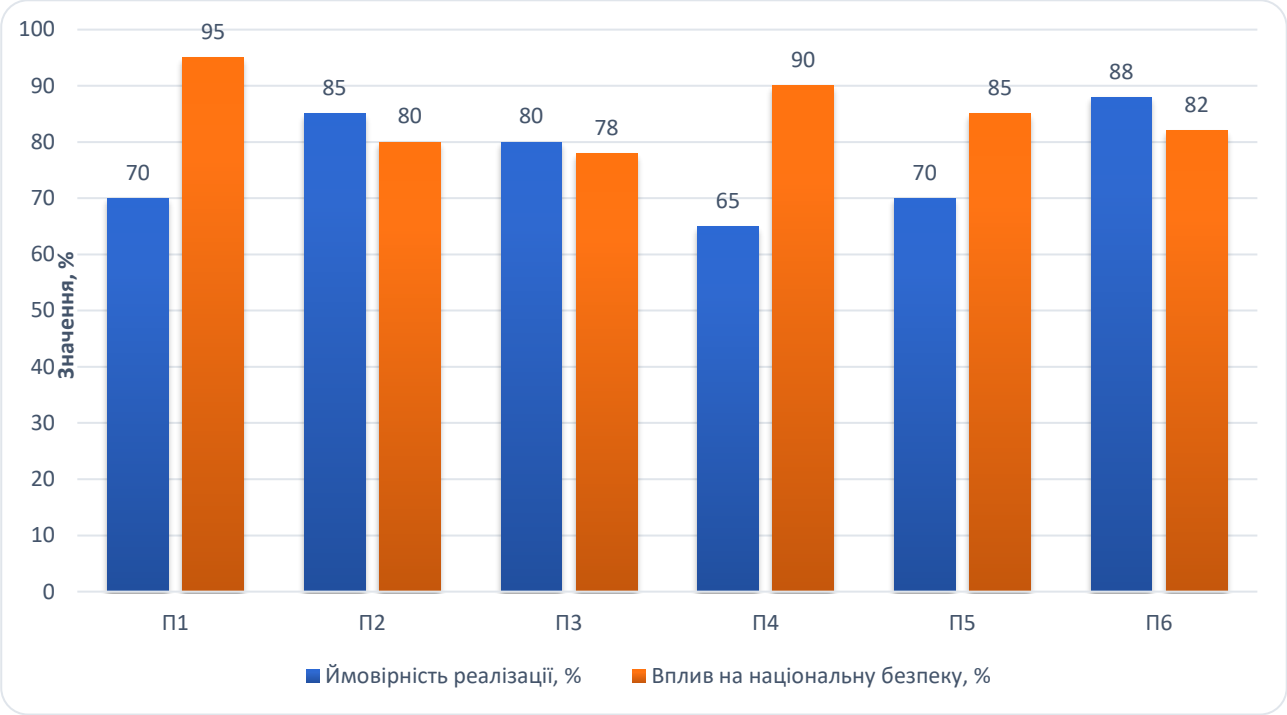

Рисунок 1: Оцінка пропозицій: ймовірність реалізації та вплив на національну безпеку, %
П1 — Командування когнітивного впливу та Сили когнітивних операцій. **П2** — Доктрина когнітивних операцій та система оцінювання ефектів. **П3** — Підготовка кадрів та науково-дослідний супровід. **П4** — Національна система когнітивної безпеки. **П5** — Національний центр моніторингу та раннього попередження когнітивних загроз. **П6** — Розвиток суспільної когнітивної стійкості та міжнародної синхронізації.
Джерело: розраховано авторами.

Як видно з рис. 1, усі пропозиції мають високий рівень впливу на національну безпеку (78–95 %).

Найвищий вплив притаманний створенню Командування когнітивного впливу та Сил когнітивних операцій (95 %) і національної системи когнітивної безпеки (90 %), оскільки саме вони усувають інституційну й правову прогалини. Водночас за ймовірністю реалізації лідирують заходи суспільної стійкості (88 %), доктрини (85 %) та підготовки кадрів (80 %), що залежать переважно від організаційних рішень.

Взаємне розташування пропозицій у координатах “ймовірність–вплив” зручно подати у вигляді матриці пріоритезації (рис. 2), де розмір кола відповідає інтегральному індексу.

Матриця засвідчує, що пропозиції розподіляються між двома характерними зонами. До зони високої ймовірності та помірно високого впливу потрапляють “швидкі” організаційні заходи (доктрина, кадри, суспільна стійкість), які доцільно запускати першочергово.

До зони високого впливу за дещо нижчої ймовірності належать інституційно-правові рішення (Командування когнітивного впливу, національна система когнітивної безпеки), що потребують політичної волі та законодавчих змін, але дають найбільший безпековий ефект. Зведену оцінку та визначений за нею пріоритет наведено в табл. 7.

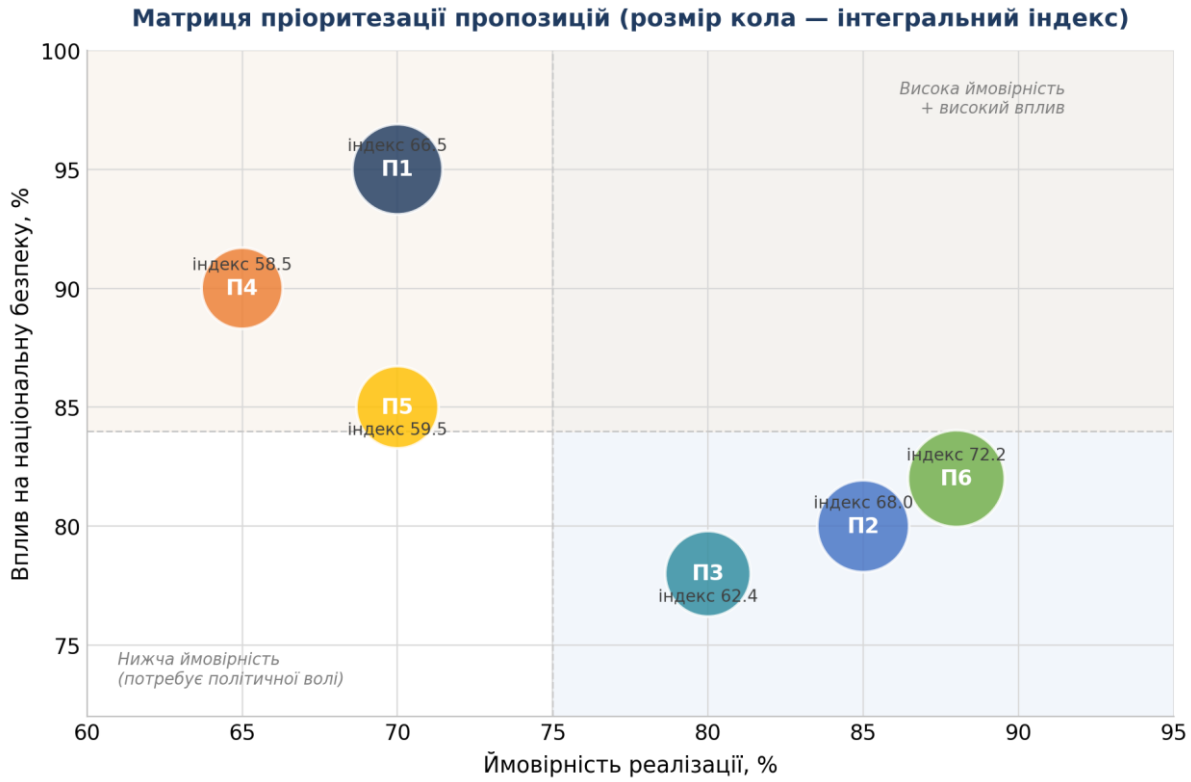

Рисунок 2: Матриця пріоритезації пропозицій (розмір кола – інтегральний індекс)
Джерело: розраховано авторами.

Таблиця 7: Зведена оцінка пропозицій та їх пріоритетність

Пропозиція	Ймовірність, %	Вплив на НБ, %	Інтегральний індекс	Пріоритет
1. Командування когнітивного впливу та Сили когнітивних операцій	70	95	**66,5**	**дуже високий**
2. Доктрина та система оцінювання ефектів	85	80	**68,0**	**дуже високий**
3. Кадри та науково-дослідний супровід	80	78	**62,4**	**високий**
4. Національна система когнітивної безпеки	65	90	**58,5**	**високий**
5. Центр моніторингу та раннє попередження	70	85	**59,5**	**високий**
6. Суспільна стійкість і міжнародна синхронізація	88	82	**72,2**	**дуже високий**

Джерело: розроблено авторами.

Для наочного впорядкування пропозицій за сукупною значущістю на рис. 3 наведено їх ранжування за інтегральним індексом пріоритетності.

Найвищий інтегральний індекс мають суспільна стійкість і міжнародна синхронізація (72,2), доктрина та система оцінювання ефектів (68,0) і Командування когнітивного впливу (66,5). Це підтверджує доцільність першочергового зосередження на цих напрямах. Узгодження заходів у часі за визначеними горизонтами планування подано у вигляді дорожньої карти реалізації (рис. 4).

Дорожня карта унаочнює послідовність дій: у короткостроковій перспективі (до 6 місяців) – створення Центру когнітивних операцій, запуск розроблення доктрини та підрозділу

когнітивних досліджень; у середньостроковій (6–18 місяців) – розгортання Командування когнітивного впливу й Національного центру когнітивної безпеки, підготовка кадрів, цифрова платформа моніторингу; у довгостроковій (1,5–3 роки) – формування окремого роду сил, повноцінне нормативно-правове закріплення та інтеграція у планування оборони.

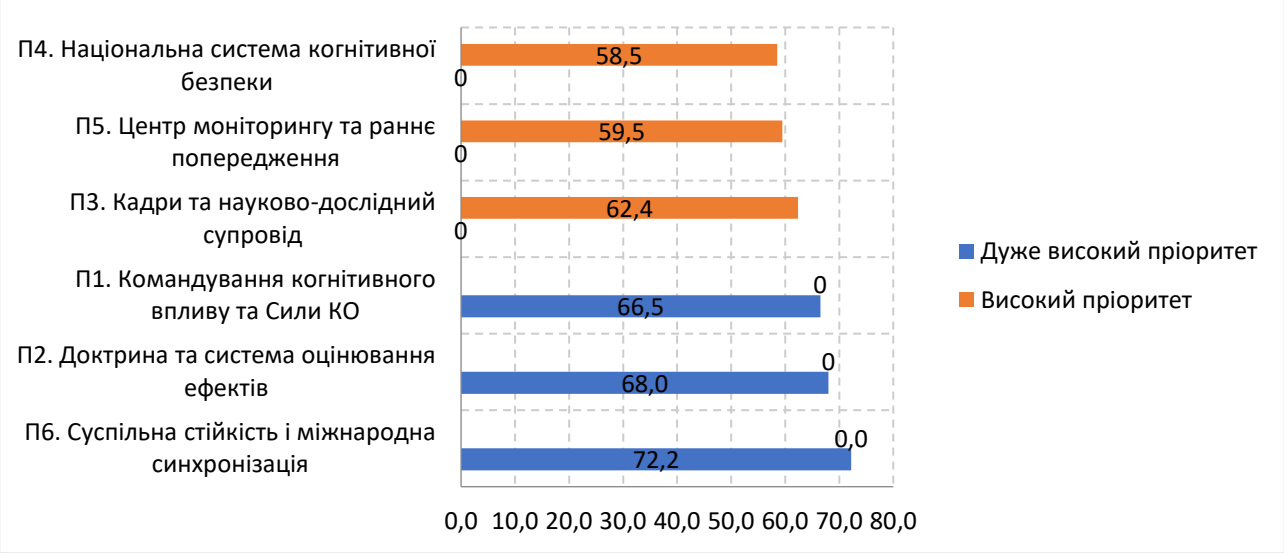

Рисунок 3: Ранжування пропозицій за інтегральним індексом пріоритетності
Джерело: розраховано авторами.

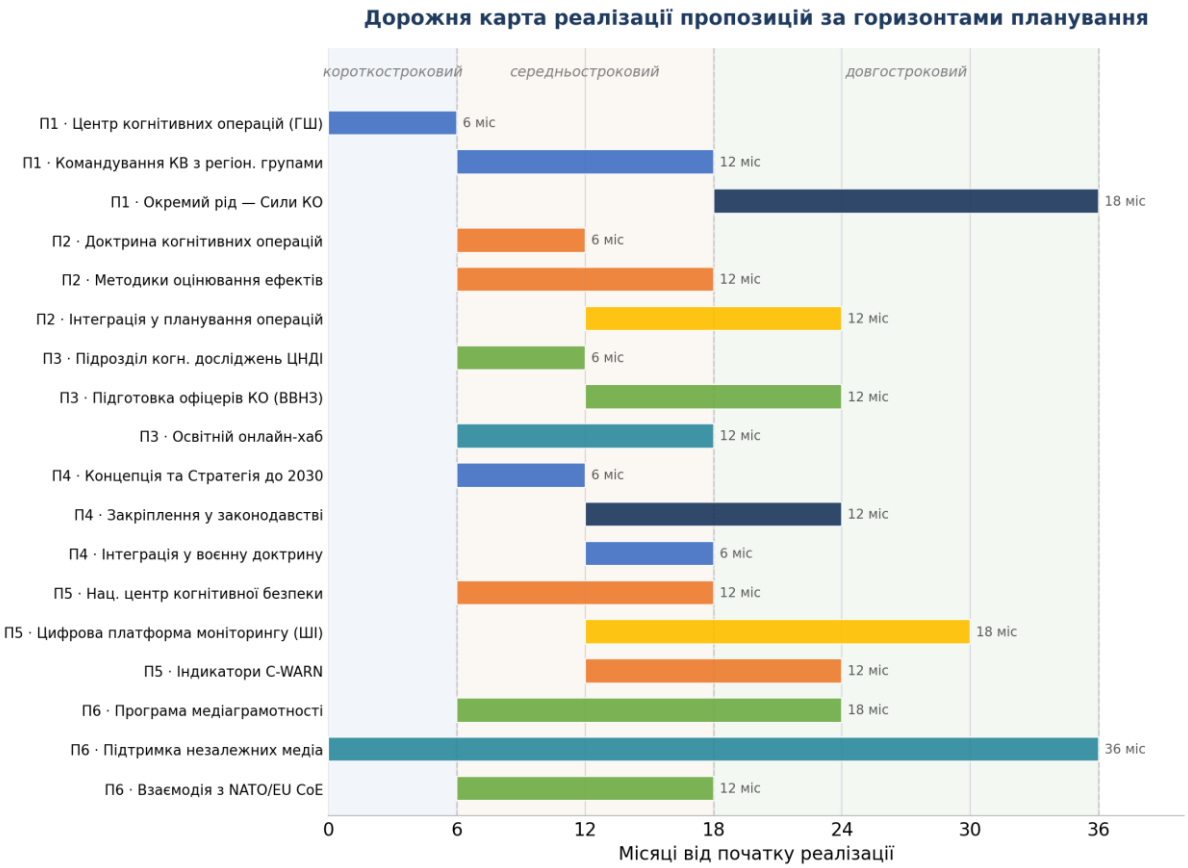

Рисунок 4: Дорожня карта реалізації пропозицій за горизонтами планування
Джерело: розраховано авторами.

Узагальнюючи, оцінка засвідчує, що всі пропозиції мають високий або дуже високий

вплив на національну безпеку (78–95 %) за помірно високої ймовірності реалізації (65–88 %). Найвищу ймовірність мають організаційно залежні заходи (суспільна стійкість, доктрина, кадри), дещо нижчу – заходи, що потребують політичної волі та законодавчих змін (Командування когнітивного впливу й національна система когнітивної безпеки), проте саме вони справляють найбільший вплив на безпеку. Це обґрунтовує доцільність паралельного запуску "швидких" організаційних заходів і поетапного просування інституційно-правових рішень, що забезпечує синергію та кумулятивний ефект, який перевищує суму окремих заходів.

Обговорення

Проведене дослідження розширює сучасні наукові підходи до розвитку когнітивної безпеки, запропоновані Командуванням НАТО з питань трансформації (NATO ACT), Європейською службою зовнішніх дій (EEAS) та Європейським центром передового досвіду з протидії гібридним загрозам (Hybrid CoE), шляхом їх адаптації до умов широкомасштабної збройної агресії Російської Федерації проти України. На відміну від більшості існуючих досліджень, які переважно зосереджені на концептуальному осмисленні когнітивної війни, інформаційних маніпуляцій або стратегічних комунікацій, у роботі запропоновано інтегровану модель розвитку державної системи когнітивної безпеки, що поєднує військовий і державний рівні управління.

Отримані результати узгоджуються з концепцією whole-of-society, відповідно до якої забезпечення когнітивної стійкості потребує координації діяльності органів державної влади, сектору безпеки і оборони, освітніх установ, наукового середовища, медіа та громадянського суспільства. Водночас запропонований авторами підхід розширює зазначену концепцію шляхом включення механізмів планування когнітивних операцій, оцінювання їх ефективності та інституціоналізації спеціалізованих органів управління.

Важливою особливістю дослідження є поєднання концептуального аналізу із програмно-цільовим підходом до визначення пріоритетності заходів. Запропонована система ранжування дозволила визначити напрями, які доцільно реалізовувати першочергово, та сформувати дорожню карту їх упровадження за коротко-, середньо- та довгостроковими горизонтами планування. При цьому результати експертного оцінювання свідчать про достатньо високий потенціал реалізації запропонованих заходів та їх суттєвий вплив на національну безпеку України.

Разом із тим отримані результати мають певні обмеження. Запропонована модель ґрунтується переважно на експертному оцінюванні та концептуальному аналізі міжнародного досвіду і ще не проходила практичної апробації в системі державного або військового управління. Крім того, інтегральний індекс пріоритетності побудовано на двох показниках — ймовірності реалізації та очікуваному впливі на національну безпеку, тоді як у подальших дослідженнях доцільно враховувати ресурсні обмеження, фінансові витрати, організаційні ризики, рівень міжвідомчої взаємодії та можливі сценарії розвитку безпекового середовища.

Практична реалізація запропонованої системи також вимагатиме нормативно-правового забезпечення, визначення відповідальних суб'єктів, розроблення механізмів міжвідомчої координації та створення системи кількісного оцінювання когнітивних ефектів. Перспективним напрямом подальших досліджень є розроблення математичних моделей оцінювання когнітивного впливу, валідація показників ефективності когнітивних операцій, моделювання сценаріїв застосування когнітивних спроможностей у сучасних конфліктах та їх інтеграція до системи оборонного планування України відповідно до стандартів НАТО.

Висновки

Проведене дослідження дозволяє дійти висновку, що розвиток державної системи когнітивної безпеки та когнітивного впливу є для України стратегічно необхідним і невідкладним

завданням в умовах збройної агресії Російської Федерації. Обґрунтовано шість взаємодоповнюваних пропозицій, скоординованих на військовому та державному рівнях, для кожної з яких визначено перелік заходів, терміни реалізації, очікувані результати та пріоритет. До основних висновків можна віднести такі.

По-перше, запропонований комплекс заходів забезпечує перехід від наявних фрагментарних спроможностей до цілісної державної системи когнітивної безпеки та когнітивного впливу, скоординованої на військовому й державному рівнях та інтегрованої у сектор безпеки і оборони.

По-друге, прогнозованими стратегічними результатами реалізації пропозицій є: усунення асиметрії з Російською Федерацією та набуття наступальної когнітивної спроможності; підвищення суспільної стійкості та захист свідомості нації; стримувальний ефект, що знижує ймовірність розв'язання майбутніх воєн проти України; а також досягнення сумісності з НАТО та посилення міжнародної підтримки.

По-третє, експертна оцінка підтверджує високу доцільність реалізації: за помірно високої ймовірності впровадження (65–88 %) усі пропозиції справляють високий вплив на національну безпеку (78–95 %), а їх синергія дає кумулятивний ефект, що перевищує суму окремих заходів.

По-четверте, в умовах війни реалізація запропонованих заходів є невідкладною: вона безпосередньо посилює обороноздатність держави, знижує бойовий потенціал противника без додаткових власних втрат і закладає основу довгострокової когнітивної безпеки України на повоєнний період.

За результатами аналізу сформульовано такі основні рекомендації:

прийняти за основу інтегровану дворівневу модель розвитку когнітивних спроможностей, у якій військовий і державний рівні поєднуються в єдину стратегію з чіткою часовою послідовністю;

у короткостроковій перспективі – пріоритезувати "швидкі" організаційні заходи: створення Центру когнітивних операцій у складі Генерального штабу, започаткування доктрини, підрозділу когнітивних досліджень та національної програми медіаграмотності;

у середньостроковій перспективі – розгорнути Командування когнітивного впливу й Національний центр когнітивної безпеки, запровадити методики оцінювання ефектів і систему індикаторів раннього попередження (C-WARN), цифрову платформу моніторингу на основі штучного інтелекту, підготувати фахові кадри;

у довгостроковій перспективі – сформувати окремий рід сил (Сили когнітивних операцій), завершити нормативно-правове закріплення когнітивної безпеки та визнання когнітивного простору середовищем воєнних дій, інтегрувати когнітивну компоненту у Стратегію воєнної безпеки й воєнну доктрину;

забезпечити інституційні передумови – застосування програмно-цільового методу, міжвідомчу координацію, виділене довгострокове фінансування, прозорі процедури, наукове супроводження з регулярним вимірюванням когнітивних ефектів та поглиблення взаємодії з NATO StratCom CoE, Hybrid CoE і структурами ЄС.

Подальші дослідження доцільно зосередити на розробленні детальних показників та методик кількісного оцінювання когнітивних ефектів (зокрема показника E(t), індексів ІКТ, ІСМД та C-WARN), моделюванні сценаріїв застосування когнітивних спроможностей проти насичених інформаційних кампаній, а також на обґрунтуванні організаційно-штатних і правових механізмів створення Командування когнітивного впливу та Національного центру когнітивної безпеки.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Використання штучного інтелекту

Автори заявляють, що використовували ШІ для перевірки правопису та пошуку ресурсів.

Список використаних джерел

1. Стратегія воєнної безпеки України : Указ Президента України від 25 березня 2021 р. № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021#Text
2. Стратегія інформаційної безпеки : Указ Президента України від 28 грудня 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text
3. Стратегія національної безпеки України : Указ Президента України від 14 вересня 2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text
4. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
5. du Cluzel, F. (2020). Cognitive Warfare. Norfolk (VA): NATO ACT Innovation Hub. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf
6. Claverie, B., & du Cluzel, F. (2022). The Cognitive Warfare Concept. NATO ACT Innovation Hub. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf
7. Bernal, A., Carter, C., Singh, I., Cao, K., & Madreperla, O. (2020). Cognitive Warfare: An Attack on Truth and Thought. NATO & Johns Hopkins University. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf
8. NATO Allied Command Transformation. (2024). Cognitive Warfare. URL: https://www.act.nato.int/activities/cognitive-warfare/
9. Deppe, C., & Schaal, G. S. (2024). Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. Frontiers in Big Data, 7, 1452129. URL: https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full
10. NATO Strategic Communications Centre of Excellence. (2023). Responding to Cognitive Security Challenges. Riga: NATO StratCom COE. URL: https://stratcomcoe.org/publications
11. European Centre of Excellence for Countering Hybrid Threats. Hybrid influence: Identity & cognitive vulnerabilities. Helsinki: Hybrid CoE. URL: https://www.hybridcoe.fi/hybrid-influence/
12. Hybrid CoE. (2021). Strategic Analysis 33: Anticipating cognitive intrusions: Framing the phenomenon. Helsinki: Hybrid CoE. URL: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-33-anticipating-cognitive-intrusions-framing-the-phenomenon/
13. RAND Corporation. (2021). Russia's Evolving Use of Information Confrontation (RR-A198-8). Santa Monica, CA: RAND. URL: https://www.rand.org/pubs/research_reports/RRA198-8.html
14. Treyger, E., Cheravitch, J., & Cohen, R. S. (2022). Russian Disinformation Efforts on Social Media (RR-4373/2). RAND Corporation. URL: https://www.rand.org/pubs/research_reports/RR4373z2.html
15. RAND Corporation. Information Operations (research topic). Santa Monica, CA: RAND. URL: https://www.rand.org/topics/information-operations.html
16. Burda, R. (2023). Cognitive Warfare as Part of Society: Never-Ending Battle for Minds. The Hague Centre for Strategic Studies. URL: https://hcss.nl/wp-content/uploads/2023/06/04-Cognitive_Warfare_as_Part_of_Society__Never_Ending_Battle_for_Minds.pdf

17. European External Action Service. (2024). 2nd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats. Brussels: EEAS. URL: https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf
18. European External Action Service. (2025). 3rd EEAS Report on FIMI Threats. Brussels: EEAS. URL: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf
19. European External Action Service. Information Integrity and Countering FIMI. Brussels: EEAS. URL: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
20. NATO Review. (2025). Algorithmic invasions: How information warfare threatens NATO's eastern flank. URL: https://www.nato.int/docu/review/articles/2025/02/07/algorithmic-invasions-how-information-warfare-threatens-nato-s-eastern-flank/index.html
21. Irregular Warfare Initiative. (2026). Assessing «Cognitive Warfare». URL: https://irregularwarfare.org/articles/assessing-cognitive-warfare/
22. OODA Loop. (2025). Weaponizing Perception: China and Russia's Cognitive Warfare Against Democracies. URL: https://oodaloop.com/analysis/ooda-original/weaponizing-perception-china-and-russias-cognitive-warfare-against-democracies/
23. Красноступ, Г. М. (2025). Нова стратегія інформаційної безпеки: правова відповідь на російське інформаційне маніпулювання та втручання. Інформація і право, 2(53). URL: https://il.ippi.org.ua/article/view/334149
24. Стратегія розвитку оборонно-промислового комплексу України : Указ Президента України від 20 серпня 2021 р. № 372/2021. URL: https://zakon.rada.gov.ua/laws/show/372/2021#Text
25. NATO Strategic Communications Centre of Excellence. (2021). Inoculation theory and misinformation. Riga: NATO StratCom COE. URL: https://stratcomcoe.org/publications/inoculation-theory-and-misinformation/217
26. EUvsDisinfo. (2024). 2nd EEAS FIMI Threat Report (January 2024). Brussels: EEAS. URL: https://euvsdisinfo.eu/eeas-2nd-fimi-threat-report-january-2024/
27. Стратегічний оборонний бюлетень України : Указ Президента України від 17 вересня 2021 р. № 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121

References

1. President of Ukraine. (2021, March 25). *Stratehiia voiennoi bezpeky Ukrainy* [Strategy of Military Security of Ukraine] (Decree No. 121/2021). https://zakon.rada.gov.ua/laws/show/121/2021#Text
2. President of Ukraine. (2021, December 28). *Stratehiia informatsiinoi bezpeky* [Strategy of Information Security] (Decree No. 685/2021). https://zakon.rada.gov.ua/laws/show/685/2021#Text
3. President of Ukraine. (2020, September 14). *Stratehiia natsionalnoi bezpeky Ukrainy* [National Security Strategy of Ukraine] (Decree No. 392/2020). https://zakon.rada.gov.ua/laws/show/392/2020#Text
4. Verkhovna Rada of Ukraine. (2018, June 21). *Pro natsionalnu bezpeku Ukrainy* [On National Security of Ukraine] (Law No. 2469-VIII). https://zakon.rada.gov.ua/laws/show/2469-19#Text
5. du Cluzel, F. (2020). Cognitive Warfare. Norfolk (VA): NATO ACT Innovation Hub. https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf

6. Claverie, B., & du Cluzel, F. (2022). 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
7. Bernal, A., Carter, C., Singh, I., Cao, K., & Madreperla, O. (2020). Cognitive Warfare: An Attack on Truth and Thought. NATO & Johns Hopkins University. https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf
8. NATO Allied Command Transformation. (2024). Cognitive Warfare. https://www.act.nato.int/activities/cognitive-warfare/
9. Deppe, C., & Schaal, G. S. (2024). Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. Frontiers in Big Data, 7, 1452129. https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full
10. NATO Strategic Communications Centre of Excellence. (2023). Responding to Cognitive Security Challenges. Riga: NATO StratCom COE. https://stratcomcoe.org/publications
11. European Centre of Excellence for Countering Hybrid Threats. Hybrid influence: Identity & cognitive vulnerabilities. Helsinki: Hybrid CoE. https://www.hybridcoe.fi/hybrid-influence/
12. Hybrid CoE. (2021). Strategic Analysis 33: Anticipating cognitive intrusions: Framing the phenomenon. Helsinki: Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-33-anticipating-cognitive-intrusions-framing-the-phenomenon/
13. RAND Corporation. (2021). Russia's Evolving Use of Information Confrontation (RR-A198-8). Santa Monica, CA: RAND. https://www.rand.org/pubs/research_reports/RRA198-8.html
14. Treyger, E., Cheravitch, J., & Cohen, R. S. (2022). Russian Disinformation Efforts on Social Media (RR-4373/2). RAND Corporation. https://www.rand.org/pubs/research_reports/RR4373z2.html
15. RAND Corporation. Information Operations (research topic). Santa Monica, CA: RAND. https://www.rand.org/topics/information-operations.html
16. Burda, R. (2023). Cognitive Warfare as Part of Society: Never-Ending Battle for Minds. The Hague Centre for Strategic Studies. https://hcss.nl/wp-content/uploads/2023/06/04-Cognitive_Warfare_as_Part_of_Society__Never_Ending_Battle_for_Minds.pdf
17. European External Action Service. (2024). 2nd EEAS Report on FIMI Threats. Brussels: EEAS. https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf
18. European External Action Service. (2025). 3rd EEAS Report on FIMI Threats. Brussels: EEAS. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf
19. European External Action Service. Information Integrity and Countering FIMI. Brussels: EEAS. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
20. NATO Review. (2025). Algorithmic invasions: How information warfare threatens NATO's eastern flank. https://www.nato.int/docu/review/articles/2025/02/07/algorithmic-invasions-how-information-warfare-threatens-nato-s-eastern-flank/index.html
21. Irregular Warfare Initiative. (2026). Assessing «Cognitive Warfare». https://irregularwarfare.org/articles/assessing-cognitive-warfare/
22. OODA Loop. (2025). Weaponizing Perception: China and Russia's Cognitive Warfare Against Democracies. https://oodaloop.com/analysis/ooda-original/weaponizing-perception-china-and-russias-cognitive-warfare-against-democracies/
23. Krasnostup, H. M. (2025). The new information security strategy: a legal response to Russian FIMI. Information and Law, 2(53). https://il.ippi.org.ua/article/view/334149

24. President of Ukraine. (2021, August 20). *Stratehiia rozvytku oboronno-promyslovoho kompleksu Ukrainy* [Strategy for the Development of the Defence-Industrial Complex of Ukraine] (Decree No. 372/2021). https://zakon.rada.gov.ua/laws/show/372/2021#Text
25. NATO Strategic Communications Centre of Excellence. (2021). Inoculation theory and misinformation. Riga: NATO StratCom COE. https://stratcomcoe.org/publications/inoculation-theory-and-misinformation/217
26. EUvsDisinfo. (2024). 2nd EEAS FIMI Threat Report (January 2024). Brussels: EEAS. https://euvsdisinfo.eu/eeas-2nd-fimi-threat-report-january-2024/
27. President of Ukraine. (2021, September 17). *Stratehichnyi oboronnyi biuleten Ukrainy* [Strategic Defence Bulletin of Ukraine] (Decree No. 473/2021). https://www.president.gov.ua/documents/4732021-40121