УДК 32:004.9

Ж. В. Пацьора

РОЗРОБКА ІНФОРМАЦІЙНОЇ ВАКЦИНИ ЯК БАГАТОНАЦІОНАЛЬНА ВІДПОВІДЬ НА ЗАГРОЗИ КОГНІТИВНІЙ БЕЗПЕЦІ

У статті розглядається концепція «інформаційної вакцини» як інноваційного підходу до забезпечення когнітивної безпеки в умовах гібридних загроз. Авторка аналізує теоретичні основи поняття, історичні та сучасні приклади інформаційних атак, а також міжнародний досвід протидії дезінформації. Показано, що у XXI столітті війни ведуться не лише на полі бою, але й у свідомості мільйонів людей. Окреслено ключові технологічні виклики - алгоритмічні системи поширення інформації, штучний інтелект, великі дані та deepfake. Запропоновано багаторівневу модель «інформаційної вакцини», яка поєднує освітні, комунікаційні, технологічні та міжнародні механізми. У висновках запропоновано рекомендації для України та міжнародної спільноти щодо побудови стійкої системи когнітивної безпеки.

Ключові слова: *когнітивна безпека, інформаційна вакцина, стратегічні комунікації, інформаційна стійкість, гібридні загрози, Україна, національна безпека.*

DOI 10.34079/2518-1521-2025-15-43-127-134

У XXI столітті інформація остаточно перетворилася на стратегічний ресурс, що визначає не лише розвиток окремих держав, а й баланс сил у світі. Якщо у попередні епохи основою військової та політичної переваги були чисельність армії, промисловий потенціал чи науково-технічні здобутки, то сьогодні вирішальне значення має здатність впливати на свідомість, емоції та поведінку людей. Це зумовлює появу нового виміру безпеки — когнітивного, у якому боротьба точиться за інтерпретацію реальності, за контроль над наративами та формування довіри у суспільстві.

Сучасні війни дедалі більше набувають гібридного характеру, поєднуючи традиційні військові дії з інформаційними та психологічними операціями. Дезінформація, маніпуляції, пропаганда, кампанії з дискредитації інституцій та політичних лідерів — усе це стало невід'ємною частиною нових конфліктів. Як наголошує (Почепцов 2015, с.125), у XXI столітті війна дедалі більше переміщується у свідомість людини, де головною зброєю стають не танки й ракети, а слова, образи та символи.

Україна є одним із найбільш показових прикладів держави, що перебуває під постійним тиском когнітивних атак. Починаючи з 2014 року, після анексії Криму та початку війни на Донбасі, росія систематично застосовує інструменти дезінформації для підриву національної єдності, делегітимізації інституцій, поширення страху та недовіри. Після 2022 року, з початком повномасштабної агресії, ці атаки набули безпрецедентного масштабу: створювалися кампанії, спрямовані на руйнування віри у перемогу, поширення паніки через удари по енергетичній інфраструктурі, підрив довіри до союзників і міжнародної підтримки України.

Водночас проблема дезінформації не є виключно українською. Вона має глобальний характер і виявляється у різних формах у всіх регіонах світу. У США це втручання у вибори та поширення конспірологічних рухів, таких як QAnon (Singer and Brooking, 2018). У Європейському Союзі — інформаційні кампанії довкола Brexit і спроби зовнішніх акторів вплинути на суспільну думку (European Digital Media

Observatory (EDMO), 2022). У Китаї — використання великих даних та алгоритмічного управління для формування потрібних настроїв серед населення (Castells, 2009). У цьому сенсі Україна є лише «передовою лінією» глобальної битви за когнітивну безпеку, але не єдиною її ареною.

Особливістю сучасних інформаційних загроз є їхня здатність підривати довіру — фундамент будь-якого демократичного суспільства. Довіра до інституцій, медіа, експертів і навіть до базових понять правди та брехні стає об'єктом системної атаки. Це створює умови для поляризації, радикалізації та розколу, що послаблює суспільства зсередини й робить їх уразливими до зовнішнього впливу. Як зазначає Померанцев (Pomerantsev, 2019, с.117), пропаганда діє як інфекція: вона поширюється невидимо, вражає механізми критичного мислення і створює середовище, у якому складно відрізнити реальність від вигадки.

У цих умовах виникає потреба у нових підходах до захисту, які виходять за межі класичних методів протидії пропаганді чи цензури. Захист не може зводитися лише до спростування фейків — адже «потік неправди» (Paul and Matthews, 2016) поширюється значно швидше, ніж можливість реагувати на нього. Потрібна стратегія превентивного характеру, яка дозволила б готувати суспільство до зустрічі з інформаційними загрозами ще до їх появи. Саме такою концепцією постає «інформаційна вакцина».

Метафора «інформаційної вакцини» запозичує логіку з медицини: так само як біологічна вакцина формує імунітет проти вірусу, завчасно вводячи ослаблений його варіант, інформаційна вакцина передбачає підготовку суспільства до зустрічі з дезінформацією шляхом розвитку критичного мислення, підвищення медіаграмотності та формування навичок розпізнавання маніпуляцій. Це не лише метафоричне порівняння, але й цілком практичний підхід, підтверджений емпіричними дослідженнями (van der Linden et al, 2017).

Таким чином, актуальність цього дослідження визначається трьома чинниками:

зростанням ролі інформації як стратегічного ресурсу у XXI столітті;

1) Глобальним характером когнітивних атак, які вражають різні країни світу;

2) Унікальним досвідом України, яка з 2014 року перебуває на передньому краї інформаційної війни.

Метою статті є дослідження теоретичних засад концепції інформаційної вакцини, аналіз міжнародного досвіду протидії інформаційним загрозам та розробка багаторівневої моделі когнітивної безпеки, яка може бути використана як Україною, так і міжнародною спільнотою.

Теорія інокуляції

Ще у 1960-х роках Вільям Макґвайр розробив теорію інокуляції, яка пояснює, що людина стає більш стійкою до маніпуляцій, якщо заздалегідь стикається зі спрощеними чи ослабленими формами аргументів супротивника (McGuire, 1964, pp. 191–229). Це дуже нагадує роботу медичної вакцини: невелика «доза вірусу» дозволяє організму виробити імунітет.

Сучасні дослідження Кембриджського університету підтверджують дієвість цього підходу. Вони показують, що «prebunking» - тобто превентивне пояснення тактик маніпуляторів - допомагає аудиторії відкидати фейки ще до їхнього поширення (van der Linden et al., 2017). У звіті Ради Європи зазначено, що саме превентивні заходи, а не реактивні, є найбільш ефективними у боротьбі з когнітивними атаками (Wardle & Derakhshan, 2017, p. 20).

Таким чином, ідея «інформаційної вакцини» має потужне теоретичне підґрунтя і може бути втілена в практичних програмах підвищення стійкості суспільства.

Міжнародний досвід

У США основна увага зосереджена на захисті виборів та протидії дезінформації під час пандемії COVID-19. Одним із яскравих прикладів стала поява руху QAnon, який поширював конспірологічні теорії й отримав величезний вплив через соціальні мережі. RAND описала російську модель дезінформації як «firehose of falsehood» - потік неправди, який неможливо повністю спростувати (Paul & Matthews, 2016, p. 8).

У Європейському Союзі діє низка інституцій: EUvsDisinfo, EDMO, а також нове законодавство - Digital Services Act, яке посилює відповідальність платформ за поширення фейків (EDMO, 2022). Brexit став одним із найяскравіших прикладів того, як дезінформація може впливати на стратегічні політичні рішення.

Китай використовує унікальну модель, поєднуючи контроль над інформаційним простором із застосуванням великих даних та алгоритмічних систем для відстеження настроїв населення. Це створює серйозний виклик для глобальної когнітивної безпеки, оскільки експортує авторитарні практики у цифрову сферу (Castells, 2009).

НАТО, своєю чергою, створило Центр передового досвіду зі стратегічних комунікацій у Ризі, який досліджує когнітивну війну та пропонує багатонаціональні рішення (NATO StratCom COE, 2020).

Український контекст

Для України тема когнітивної безпеки є екзистенційною. Після 2014 року росія систематично вела кампанії з дискредитації української армії, поширювала міфи про «громадянську війну» на Донбасі, маніпулювала інформацією про катастрофу MH17. Під час пандемії COVID-19 поширювалися фейки про «біолабораторії» та «чипізацію», що підривало довіру до вакцинації. Після 2022 року атаки посилилися: пропаганда намагається підірвати віру у перемогу, створює образ «зруйнованої держави», поширює паніку через атаки на енергетичну інфраструктуру.

Україна відповідає створенням Центру протидії дезінформації, запуском програм медіаграмотності у школах та університетах, співпрацею з міжнародними партнерами. Ці кроки можна розглядати як елементи побудови власної «інформаційної вакцини».

Сучасні технології значно ускладнюють боротьбу з дезінформацією. Алгоритми соціальних мереж віддають перевагу емоційним і поляризуючим повідомленням, що сприяє поширенню фейків. Deepfake-відео дозволяють створювати переконливі підробки виступів політичних лідерів. Штучний інтелект використовується як для створення дезінформації, так і для її виявлення.

Сінгер і Брукінг підкреслюють, що соціальні мережі перетворилися на справжнє поле бою, де інформація стала зброєю (Singer & Brooking, 2018, p. 52). ЮНЕСКО наголошує на необхідності глобального регулювання цифрових платформ, щоб забезпечити баланс між свободою слова та захистом від маніпуляцій (UNESCO, 2023).

Інформаційна вакцина: стратегія інформаційної стійкості та колективного імунітету

Сучасні гібридні загрози висувають нові вимоги до захисту інформаційного простору. Війна у XXI столітті дедалі більше відбувається у сфері свідомості, де дезінформація діє як «інформаційний вірус», здатний підривати довіру, послаблювати демократичні інституції та створювати глибокі суспільні розколи.

У цих умовах реактивні заходи виявляються недостатніми. Необхідна превентивна стратегія, що діє на випередження. Саме такою концепцією виступає «інформаційна вакцина», яка покликана формувати стійкість до маніпуляцій ще до їх масового поширення.

Її головна особливість полягає у системному поєднанні різних інструментів: розвитку критичного мислення, підвищення медіаграмотності, використання технологій штучного інтелекту для виявлення загроз та формування позитивних наративів у суспільстві. Важливим компонентом є також міжнародна координація, що забезпечує ефект колективного імунітету. Таким чином, інформаційна вакцина — це не окремий захід, а багаторівнева стратегія (див. Таблиця 1), де кожен рівень має свою функцію, а їхня взаємодія забезпечує стійкість усієї системи.

Таблиця 1. Структура інформаційно вакцини

РІВЕНЬ ІНДИВІДУАЛЬНОГО ІМУНІТЕТУ	На особистісному рівні інформаційна вакцина забезпечує розвиток критичного мислення, уміння перевіряти джерела, розпізнавати маніпулятивні повідомлення та розуміти приховані комунікаційні тактики. Це формує основу індивідуальної інформаційної стійкості.
РІВЕНЬ ОСВІТНЬОГО ВПЛИВУ	Освіта та медіаграмотність виступають ключовим елементом. Інформаційна вакцина включає навчальні програми, тренінги та просвітницькі ініціативи, які дозволяють засвоювати «ослаблені дози» маніпулятивних прикладів, тренуючи здатність суспільства їх розпізнавати без шкоди для стабільності.
ТЕХНОЛОГІЧНИЙ РІВЕНЬ	Сучасні цифрові технології стають інструментами для формування інформаційного імунітету. Використання алгоритмів штучного інтелекту, систем раннього попередження та аналізу великих даних дозволяє виявляти інформаційні загрози ще до їхнього масового поширення.
ЛОКАЛЬНИЙ РІВЕНЬ	Діяльність органів місцевого самоврядування, спрямована на формування довіри між владою та населенням; розвиток муніципальних ініціатив із протидії дезінформації; створення локальних центрів стратегічних комунікацій; поширення позитивних інформаційних наративів на рівні громади
РЕГІОНАЛЬНИЙ РІВЕНЬ	Координація діяльності органів місцевого самоврядування на рівні області; розробка регіональних стратегій протидії дезінформації; створення «хабів стійкості»; підтримка регіональних медіа та платформ; інтеграція локальних ініціатив у національні програми.
РЕГУЛЯТИВНО-ІНСТИТУЦІЙНИЙ РІВЕНЬ	Формування гнучкої нормативної та політичної бази, що дозволяє застосовувати інформаційну вакцину у добровільному форматі через стратегії, програми та стандарти, але передбачає можливість її обов'язкового використання у критичних умовах (масовані інформаційні атаки, кризи, воєнні дії).
МІЖНАРОДНИЙ РІВЕНЬ І КОЛЕКТИВНИЙ ІМУНІТЕТ	Ефективність інформаційної вакцини зростає, коли вона впроваджується не лише на рівні держави, але й у глобальному масштабі. Міжнародна співпраця, уніфікація стандартів і спільні протоколи реагування створюють умови для досягнення «колективного імунітету», який зменшує вплив когнітивних атак на суспільства.

Висновки. Концепція інформаційної вакцини, запропонована у цьому дослідженні, демонструє перехід від образного порівняння до комплексної стратегії превентивної інформаційної безпеки. У сучасному світі, де інформація стала ресурсом влади, впливу та контролю, саме здатність суспільства завчасно формувати імунітет до маніпуляцій визначає його стійкість до когнітивних атак. Досвід останніх десятиліть доводить, що інформаційні загрози вже не є локальним явищем: вони набули глобального характеру та здатні підривати демократичні інститути, формувати атмосферу недовіри та змінювати політичні процеси у різних державах.

Результати дослідження підтверджують, що інформаційна вакцина має міцне теоретичне підґрунтя, яке поєднує класичні та сучасні підходи. Теорія когнітивних воєн (Почепцов, 2020, с.125) дозволяє пояснити, чому сучасні конфлікти переміщуються у сферу свідомості, а концепція трансформації публічної сфери Габермаса (Habermas, 1991) демонструє вразливість демократичного дискурсу до маніпуляцій. Ідеї «м'якої сили» (Nye, 2004), ідентичності (Fukuyama, 2018), дискурсивного домінування (van Dijk, 2008), метафоричного мислення (Lakoff and Johnson, 2003), симулякрів і гіперреальності (Baudrillard, 1994), а також нерозв'язних конфліктів (Bar-Tal, 2013) формують багатовимірну рамку для розуміння когнітивних загроз. Теорія інокуляції Макґвайра (McGuire, 1964), підтверджена емпіричними дослідженнями Cambridge University (van der Linden et al., 2017), створює методологічну основу для практичної реалізації концепції інформаційної вакцини.

Вивчення міжнародного досвіду показало, що жодна країна світу не застрахована від дезінформаційних кампаній. США зіткнулися з втручанням у вибори, поширенням конспірологічних рухів на кшталт QAnon і масштабною хвилею дезінформації під час пандемії COVID-19. У Європейському Союзі одним із найяскравіших прикладів стала кампанія навколо Brexit, що підтвердила вразливість навіть розвинених демократій до маніпуляцій громадською думкою. Відповіддю стало створення інституцій EUvsDisinfo, EDMO, а також ухвалення Digital Services Act, який накладає відповідальність на цифрові платформи. Китай, у свою чергу, розвиває власну модель алгоритмічного управління, де big data та штучний інтелект використовуються для контролю настроїв населення, що ставить нові виклики для глобальної когнітивної безпеки. НАТО відреагувало створенням StratCom COE у Ризі — багатонаціонального центру, який систематизує досвід держав-членів і розробляє підходи до протидії когнітивним загрозам.

Особливе місце у цій картині посідає Україна. З 2014 року, після анексії Криму та початку війни на Донбасі, а особливо з 2022 року — після повномасштабного вторгнення, вона стала унікальною лабораторією для дослідження інформаційних війн. Пропагандистські кампанії проти Криму, Донбасу, катастрофи МН17, вакцинації, енергетичної безпеки та віри у перемогу показують, як багатовекторно може діяти агресор. Відповіддю стали створення Центру протидії дезінформації, масштабні програми медіаграмотності, співпраця з міжнародними організаціями. Український досвід свідчить: ефективність протидії залежить не лише від державних інституцій, а й від залучення громадянського суспільства, освіти та технологічних інновацій.

Запропонована модель інформаційної вакцини має багаторівневу структуру. На індивідуальному рівні це розвиток критичного мислення та навичок перевірки фактів. На освітньому — впровадження системної медіаграмотності в школах і університетах. Технологічний рівень передбачає використання штучного інтелекту, алгоритмів раннього попередження та автоматизованих систем моніторингу. Локальний рівень включає участь органів місцевого самоврядування у розробці стратегій комунікаційної безпеки. Регіональний рівень передбачає узгодженість між різними регіонами України

та транскордонну взаємодію з сусідніми державами. Регулятивно-інституційний рівень полягає у створенні законодавчих та нормативних рамок, що унеможливлюють поширення деструктивних наративів. Міжнародний рівень спрямований на інтеграцію зусиль у рамках НАТО, ЄС, ООН та інших організацій. У сукупності ці рівні створюють ефект «колективного імунітету», коли навіть сильні деструктивні атаки не здатні спричинити системних руйнівних наслідків.

У стратегічній перспективі когнітивна безпека стане одним із ключових елементів національної безпеки, нарівні з військовою та енергетичною складовою. Світ уже сьогодні стикається з викликами, які визначатимуть майбутнє: поширення штучного інтелекту, здатного генерувати реалістичні deepfake-відео; розвиток алгоритмів, що формують інформаційні «бульбашки» та поляризують суспільство; зростання впливу транснаціональних цифрових корпорацій на політичні процеси. Це означає, що майбутні стратегії мають бути адаптивними, гнучкими та заснованими на міжнародній співпраці.

Для України стратегічний прогноз є подвійним. З одного боку, вона залишається найбільш вразливою державою до інформаційних атак, що зумовлено триваючою війною. З іншого боку, саме цей унікальний досвід робить її природним лідером у розробці нових стандартів когнітивної безпеки. Україна може виступати генератором інноваційних рішень — від створення освітніх програм до впровадження технологічних інструментів виявлення дезінформації. Її досвід може стати основою для формування глобальних практик, які поширюватимуться на інші держави.

У майбутньому інформаційна вакцина повинна розвиватися у трьох головних напрямах. Перший — це поглиблення освіти й медіаграмотності, що забезпечить формування покоління, стійкого до маніпуляцій. Другий — розвиток технологій штучного інтелекту та аналітичних систем, здатних виявляти дезінформацію в режимі реального часу. Третій — посилення міжнародної координації, що дозволить об’єднувати ресурси та створювати єдині стандарти.

Таким чином, інформаційна вакцина є не лише метафорою, а й практичним інструментом формування когнітивної стійкості. Її стратегічне значення полягає в тому, що вона дозволяє перейти від реактивної до превентивної моделі захисту. У майбутньому саме ті суспільства, які першими інтегрують таку стратегію, здобудуть перевагу у глобальній конкуренції. Україна, яка вже сьогодні перебуває на передньому краї боротьби з дезінформацією, має всі підстави стати не лише об’єктом атак, а й суб’єктом формування нової архітектури когнітивної безпеки у XXI столітті. Її досвід може слугувати дороговказом для інших держав, які прагнуть досягти стану інформаційного «колективного імунітету» і забезпечити стабільність демократичного розвитку.

Бібліографічний список

Почепцов, Г. (2015) Сучасні інформаційні війни. Київ: Вид. дім «Києво-Могилянська академія».

Bar-Tal, D., 2013. *Intractable Conflicts: Socio-Psychological Foundations and Dynamics*. Cambridge: Cambridge University Press.

Baudrillard, J., 1994. *Simulacra and Simulation*. Ann Arbor: University of Michigan Press.

Castells, M., 2009. *Communication Power*. Oxford: Oxford University Press.

European Digital Media Observatory (EDMO), 2022. *Annual Report 2022*. Brussels: EDMO.

Fukuyama, F., 2018. *Identity: The Demand for Dignity and the Politics of Resentment*. New York: Farrar, Straus and Giroux.

Habermas, J., 1991. *The Structural Transformation of the Public Sphere*. Cambridge: MIT Press.

Lakoff, G. and Johnson, M., 2003. *Metaphors We Live By*. Chicago: University of Chicago Press.

McGuire, W.J., 1964. Inducing resistance to persuasion: Some contemporary approaches. *Advances in Experimental Social Psychology*, 1, pp. 191–229.

NATO StratCom COE, 2020. *Cognitive Warfare*. Riga: NATO Strategic Communications Centre of Excellence.

Nye, J.S., 2004. *Soft Power: The Means to Success in World Politics*. New York: Public Affairs.

Paul, C. and Matthews, M., 2016. *The Russian "Firehose of Falsehood" Propaganda Model*. Santa Monica: RAND Corporation.

Pomerantsev, P., 2019. *This is Not Propaganda: Adventures in the War Against Reality*. London: Faber & Faber.

Singer, P.W. and Brooking, E.T., 2018. *LikeWar: The Weaponization of Social Media*. Boston: Houghton Mifflin Harcourt.

UNESCO, 2023. *Guidelines for Regulating Digital Platforms*. Paris: UNESCO.

van Dijk, T.A., 2008. *Discourse and Power*. London: Palgrave Macmillan.

van der Linden, S. Levandovsky, S., Eker, U. et al., 2017. *Prebunking: A Preventive Explanation of Manipulative Tactics*. Cambridge.

Wardle, C. and Derakhshan, H., 2017. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Strasbourg: Council of Europe.

Reference

Bar-Tal, D., 2013. *Intractable Conflicts: Socio-Psychological Foundations and Dynamics*. Cambridge: Cambridge University Press.

Baudrillard, J., 1994. *Simulacra and Simulation*. Ann Arbor: University of Michigan Press.

Castells, M., 2009. *Communication Power*. Oxford: Oxford University Press.

European Digital Media Observatory (EDMO), 2022. *Annual Report 2022*. Brussels: EDMO.

Fukuyama, F., 2018. *Identity: The Demand for Dignity and the Politics of Resentment*. New York: Farrar, Straus and Giroux.

Habermas, J., 1991. *The Structural Transformation of the Public Sphere*. Cambridge: MIT Press.

Lakoff, G. and Johnson, M., 2003. *Metaphors We Live By*. Chicago: University of Chicago Press.

McGuire, W.J., 1964. Inducing resistance to persuasion: Some contemporary approaches. *Advances in Experimental Social Psychology*, 1, pp. 191–229.

NATO StratCom COE, 2020. *Cognitive Warfare*. Riga: NATO Strategic Communications Centre of Excellence.

Nye, J.S., 2004. *Soft Power: The Means to Success in World Politics*. New York: Public Affairs.

Paul, C. and Matthews, M., 2016. *The Russian "Firehose of Falsehood" Propaganda Model*. Santa Monica: RAND Corporation.

Pocheptsov, H. (2015) Suchasni informatsiini viiny [Modern information wars]. Kyiv: Kyiv-Mohyla Academy Publishing House.

Pomerantsev, P., 2019. This is Not Propaganda: Adventures in the War Against Reality. London: Faber & Faber.

Singer, P.W. and Brooking, E.T., 2018. *LikeWar: The Weaponization of Social Media*. Boston: Houghton Mifflin Harcourt.

UNESCO, 2023. *Guidelines for Regulating Digital Platforms*. Paris: UNESCO.

van Dijk, T.A., 2008. *Discourse and Power*. London: Palgrave Macmillan.

van der Linden, S. Levandovsky, S., Eker, U. et al., 2017. *Prebunking: A Preventive Explanation of Manipulative Tactics*. Cambridge.

Wardle, C. and Derakhshan, H., 2017. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Strasbourg: Council of Europe.

Стаття надійшла до редакції 27 серпня 2025 р.

Z. Patsora

INFORMATION VACCINE DEVELOPMENT AS A MULTINATIONAL RESPONSE TO THREATS TO COGNITIVE SECURITY

The article explores the concept of the "information vaccine" as an innovative response to hybrid threats and challenges to cognitive security. In the 21st century, wars are increasingly waged in the human mind, where disinformation functions as an "information virus" that weakens trust, divides societies, and undermines democracy. The paper argues that resilience requires preventive strategies resembling vaccination, combining theoretical insights, technological tools, and multinational cooperation.

The theoretical framework builds on Pocheptsov's concept of cognitive wars, Habermas's analysis of the public sphere, Castells's communication power, Lakoff and Johnson's metaphor theory, Nye's soft power, Fukuyama's focus on identity, van Dijk's discourse and power, Baudrillard's hyperreality, and Bar-Tal's intractable conflicts. Together, these perspectives explain the multidimensionality of cognitive threats.

The article applies McGuire's inoculation theory, demonstrating that exposure to weakened manipulative arguments strengthens resilience. Empirical evidence from Cambridge University "prebunking" studies and the Council of Europe's Information Disorder report confirms the effectiveness of preventive over reactive measures. International experiences include U.S. cases of election interference, QAnon, and COVID-19 disinformation; the EU's Brexit, EUvsDisinfo, EDMO, and Digital Services Act; China's algorithmic governance with AI and big data; and NATO's StratCom COE in Riga as a multinational initiative.

Ukraine is presented as a frontline case. Since 2014 it has faced campaigns around Crimea, Donbas, MH17, vaccination, and energy security. Responses such as the Center for Countering Disinformation and media literacy programs are discussed as elements of a national information vaccine. The article concludes that the information vaccine must become a multilayered strategy: education to build critical thinking, communication of counter-narratives, AI-based technological detection, and multinational cooperation. Ukraine, with its unique experience, can play a leading role in shaping global cognitive security.

Keywords: *cognitive security, information vaccine, strategic communications, resilience, hybrid threats, Ukraine, national security.*