Когнітивна війна в сучасній архітектурі гібридної війни

Наталія Семенюк
начальник відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: nataliia.semeniuk@gmail.com
ORCID: 0000-0001-5795-0021

Анотація. Досвід російсько-української війни довів, що змінилися підходи до ведення війни від суто конвенційних на гібридні війни із конвенційними діями та включенням до них нових елементів. Переважно бойові дії ведуться одночасно у всіх вимірах, внаслідок чого було введено термін "операції в мультидоменному середовищі". Наразі фізичні виміри (космічний, повітряний, морський та сухопутний) прошиті віртуальним (кібернетичним та інформаційним), які залежать від соціальних умов існування індивідів, їх моральних принципів та когнітивного сприйняття. Домінування на полі бою вимагає швидкої адаптації до нових реалій та трансформації підходів у веденні операцій в мультидоменному середовищі. Крім того когнітивна сфера є підсистемою мережоцентичних війн нового покоління у сучасній архітектурі гібридної війни. Чітке розуміння взаємодії елементів сучасної архітектури гібридної війни, їх координація та синхронізація під час проведення операцій в мультидоменному середовищі дозволить адаптуватися до нових збройних конфліктів та перемогти в них.

Авторкою взято до уваги сучасні тренди ведення війн різноманітного типу, враховано передовий досвід та представлено сучасну архітектуру гібридної війни. Запропоновано порядок дій для отримання когнітивної переваги.

Результатами запропонованого алгоритму має стати впровадження на державному рівні єдиної системи реагування на виклики сучасної гібридної війни, у тому числі в когнітивній сфері.

Ключові слова: гібридна війна, когнітивна війна, операції в мультидоменному середовищі, асиметрична війна, мережоцентрична війна, конвенційна війна, неконвенційна війна, кібер війна, когнітивна перевага, когнітивна сфера.

Вступ (Introduction)

Досвід російсько-української війни довів, що змінилися підходи до ведення війни від суто конвенційних на гібридні війни із конвенційними діями та включенням до них нових елементів [1 – 4]. Переважно бойові дії ведуться одночасно в усіх операційних сферах (доменах), внаслідок чого було введено термін "операції в мультидоменному середовищі" [5 – 6]. Наразі домени (фізичні виміри) (космічний, повітряний, морський та сухопутний) прошиті віртуальним (кібернетичним та інформаційним) [1, 7], які в свою чергу залежать від соціальних умов існування індивідів, їх моральних принципів та когнітивного сприйняття [8 – 9]. Домінування на полі бою вимагає швидкої адаптації до нових реалій та трансформації підходів у веденні операцій в мультидоменному середовищі. Крім того когнітивна сфера є підсистемою мережоцентичних війн нового покоління у сучасній архітектурі гібридної війни (рис.1).

Чітке розуміння взаємодії елементів сучасної архітектури гібридної війни (див. рис. 1), їх координація та синхронізація при проведенні операцій в мультидоменному середовищі дозволить адаптуватися до нових сучасних конфліктів та перемогти в них.

Методологічна основа (Methodological Framework)

Репрезентуючи зміну парадигми НАТО, операції в мультидоменному середовищі інтегрують військову діяльність в усі операційні сфери. Вони заохочують співпрацю між військовими і невійськовими акторами, зацікавленими сторонами і галузевими експертами, забезпечуючи надійні

механізми обміну інформацією, синхронізацію сил і засобів [10], які можуть зменшити військові ризики й підвищити ймовірність успіху місії, дають змогу посадовими особам Альянсу, які приймають рішення, досягати бажаних результатів в потрібний час і в потрібному місці. Цей трансформаційний підхід має на меті забезпечити індивідуальні варіанти дій, стратегічно впливаючи на поведінку супротивника і, водночас, захищаючи свободу і безпеку населення країн – членів НАТО в швидкоплинному нестабільному середовищі безпеки.

Актуальність дослідження полягає в визначенні методів та стратегій, які використовуються для впливу на сприйняття та рішення людей з метою досягнення цілей в умовах гібридної війни. Це може включати інформаційну війну, кібер та психологічні операції, пропаганду й інші тактики [11], які спрямовані на маніпулювання думками та поведінкою людей.

Прикладом такої війни може слугувати російсько-українська війна, де росія на першому етапі досягла своїх цілей завдяки поєднанню "неідентифікованих" спеціальних сил, місцевих озброєних осіб, економічного впливу, дезінформації і використанню соціально-політичної поляризації в Україні, здійснюючи когнітивний вплив.

Когнітивна сфера мережецентричної війни в сучасній архітектурі гібридної війни (див. рис.1) відіграє ключову роль, яка може бути використана як окремо, так і в якості комбінації спільно з кібернетичними, психологічними та інформаційними засобами для досягнення своїх цілей [12].

З точки зору психології та педагогіки когнітивна сфера визначається як сфера психології людини, пов'язана з її пізнавальним процесом і свідомістю, яка включає в себе знання людини про світ і саму себе.

Когнітивна, що походить від слова "пізнання", – це розумова дія або процес розуміння, що охоплює усі аспекти інтелектуальної функції, в тому числі підсвідомі і емоційні аспекти, які керують більшістю людських рішень [13]. Війна, як "досвід" війни, спочатку стосувалася загальних дій і характеристик збройного конфлікту між державами, урядами чи організаціями. У сучасному вимірі існує менше ясності щодо зацікавлених сторін, оскільки різний ступінь організаційного, культурного та соціального залучення стає все більш звичним, так само як і опосередковане розширення національних інтересів .

Разом ці два слова дають визначення когнітивної війни: діяльність, що здійснюється синхронно з іншими інструментами влади з метою зміни ставлення і поведінки шляхом впливу, захисту і/або руйнування індивідуального і групового пізнання для отримання переваги. Ці дії дуже різняться і можуть охоплювати підтримуючі або конфліктуючі культурні чи особистісні компоненти – соціальна психологія, стратегії та етика є факторами, що сприяють цьому. Однак заходи сучасної війни не обов'язково включають конвенційний компонент або безпосередньо відчутні результати, такі як придбання територій чи ресурсів – як і у випадку з іншими гібридними загрозами, супротивники ведуть когнітивну війну протягом усієї тривалості конфлікту і прагнуть залишатися в "сірій зоні" нижче порогу збройного протистояння.

Один з останніх прикладів: росія розпочала військове вторгнення в Україну, підкріплене неконвенційними (нелетальними) заходами, такими як цілеспрямована пропаганда, дезінформаційні кампанії та підтримка з боку своїх партнерів. Деякі з цих неконвенційних (нелетальних) заходів когнітивної війни є очевидними й прямими: споживачі російської дезінформації відчувають погіршення своєї здатності відрізняти факти від вигадок, що знижує їхню психічну стійкість і може мати довгострокові наслідки, такі як втрата довіри до засобів масової інформації.

Інші приклади не такі очевидні: Китай використовує офіційний і партійний вплив для маніпулювання і контролю над внутрішнім інформаційним середовищем, що призводить до розвитку когнітивних упереджень. Вторинний ефект: громадяни інших країн також розвивають когнітивні упередження щодо громадян материкового Китаю та їх колективне відключення від зовнішньої інформації, що призводить до двох принципово протилежних сприйняттів реальності. Така форма поляризації "ми проти них" може призвести до зростаючої маргіналізації та ізоляції населення, а також до емоційної експлуатації, що сприяє китайській стратегії когнітивної війни.

Когнітивна перевага стосується дій: перетворення обізнаності і розуміння обстановки на фактичну перевагу над супротивником при прийнятті рішень.

Рисунок 1. Сучасна архітектура гібридної війни

Таким чином, цільовою аудиторією, проти якої здійснюється когнітивний вплив, є як громадяни інших країн, так і власної держави. Окрема увага приділяється високопосадовцям, які

приймають рішення на стратегічному рівні – зміна їх поведінки для досягнення власних цілей – рефлексивне управління, яке є суміжне (паралельне) з заходами когнітивної війни та є підсистемою мережоцентичної війни (див. рис.1).

Так, НАТО розробило концепцію когнітивної війни [14]. Когнітивна війна зосереджена на атаках та погіршенні раціональності, що може призвести до використання вразливостей та системного ослаблення. Когнітивна війна інтегрує кібернетичні, інформаційні, психологічні спроможності й інструменти соціальної інженерії для впливу на ставлення та поведінку, захисту або порушення індивідуальної та групової когніції з метою отримання переваги над противником, знищення єдності, довіри і демократичних цінностей.

Концепція когнітивної війни має подвійну мету.

По-перше, вона формує загальні основи для розуміння динаміки і механізмів когнітивної війни. Вона описує способи використання супротивником суспільного впливу для маніпулювання громадською думкою, підриву процесів прийняття рішень і, зрештою, послаблення військового потенціалу. Концепція детально описує потенційні наслідки успішних когнітивних атак, підкреслюючи вразливість національної аудиторії, політичних структур і навіть військових операцій до дезінформації та когнітивних атак.

По-друге, Концепція когнітивної війни окреслює шлях НАТО до посилення своєї когнітивної стійкості і розвитку своїх сил і засобів для ефективної конкуренції в когнітивному вимірі. Це передбачає захист наявних військових сил і засобів і процесу прийняття рішень від маніпуляцій, а також вивчення шляхів зміцнення громадської довіри і розуміння ролі НАТО. Активно формуючи інформаційне середовище і стримуючи іноземні маніпуляції, НАТО може забезпечити свою свободу дій і продовжувати гарантувати безпеку своїх країн-членів.

У когнітивній війні людський розум формує поле бою. Когнітивна війна насамперед націлена на пізнання, яке є “ментальним процесом набуття та осмислення знань, а також інтерпретації та сприйняття інформації”. Спираючись на психологічну війну минулого, яка використовувала пропаганду для впливу на емоцій, когнітивна війна використовує сучасні технології, щоб “вибудовувати упередження або розумові автоматизми, провокуючи викривлення уявлень, їх спотворення, зміни рішень або навіть гальмування дій, а також для того, щоб спричинити катастрофічні наслідки як на індивідуальному, так і на колективному рівні”. На відміну від звичайної (або кінетичної) війни, яка використовує фізичне насильство, руйнування і територіальне завоювання, когнітивна війна діє у сфері ідей, емоцій і сприйняття. Посилаючись на Сунь Цзи, війна прагне використовувати людський розум (що можна розглядати у вигляді когнітивної війни) як звичайні сили і засоби, які допомагають захоплювати і утримувати територію за допомогою переважаючої сили, можуть визначати тактичні або оперативні результати. Захист когнітивної сфери (людського розуму) має важливе значення для досягнення довготривалої перемоги. Нещодавні неконвенційні (нелетальні) конфлікти підкреслили важливість цієї максими.

Таким чином, когнітивна війна в сучасній архітектурі гібридної війни відіграє ключову роль, використовуючи як окремо, так і комбінацію кібернетичних, психологічних та інформаційних засобів для досягнення своїх цілей.

Розробка Концепції “когнітивної війни” є значною подією у сфері ведення війни. Вона спрямована на більш ефективне залучення, забезпечення готовності та збереження довіри та спроможності стримувати супротивників у всіх сферах ведення війни. Ключовими аспектами когнітивної війни є:

1. Важливість та сфера впливу:

– важливість набуття когнітивної переваги в цілому може впливати на результати протистояння між суперниками;

– когнітивна війна включає дії, що проводяться синхронно з іншими інструментами влади, щоб вплинути на ставлення та поведінку шляхом впливу, захисту або руйнування індивідуального та групового пізнання;

– хоча більшість когнітивних атак залишаються нижче порогу збройного конфлікту, їхні наслідки можуть охоплювати багато областей, впливаючи на всі сфери ведення війни;

- когнітивні ефекти не завжди можна виміряти в типовому розумінні, але вони значно впливають на те, як ми думаємо, відчуваємо та діємо. Технології, орієнтовані на мозок, спрямовані на дестабілізацію структур (інституцій), створення недовіри та послаблення соціальної єдності;

–когнітивна війна може змінити правила гри.

2. Проблеми та індивідуальні підходи:

– недостатнє відпрацювання заходів когнітивного впливу, як результат – відсутність когнітивної переваги;

– країни відрізняються культурними, соціальними, технологічними та урядовими структурами, що впливає на їх сприйнятливість до когнітивних атак;

– для усунення вразливостей і підвищення стійкості до когнітивної діяльності необхідний індивідуальний підхід;

– протидія когнітивним атакам є державним завданням на стратегічному рівні [15 – 16].

На даний час прослідковується тенденція вироблення провідними країнами світу плану дій для здобуття когнітивної переваги [17]. Наприклад, НАТО:

співпрацює з різними організаціями для боротьби з когнітивною війною (рис. 2) [18 – 19], а саме:

здійснює заходи міжнародного співробітництва (працює разом з понад 20 країн-членами, численними командами НАТО, академічними колами та експертами з промисловості);

обмінюється знаннями (створює форум для обміну дослідженнями та інформацією між країнами-членами та партнерськими країнами);

розробляє концепції (експерти з багатьох дисциплін у Трансформаційному командуванні НАТО розробляють концепції, спрямовані на захист Альянсу від загроз когнітивної війни);

співпрацює з приватним сектором для боротьби з когнітивною війною наступним чином:

залучає експертів з промисловості для розробки концепцій та стратегій;

організовує спільні робочі групи та воркшопи;

створює механізми для обміну інформацією та синхронізації можливостей, що може зменшити військовий ризик та збільшити ймовірність успіху місій;

співпрацює з академічними колами для боротьби з когнітивною війною наступним чином:

розробляє концепції (працює з міждисциплінарними експертами для розробки концепцій, спрямованих на захист НАТО від загроз когнітивної війни);

організовує освітні заходи та навчання;

надає керівництво з питань обізнаності, цивільно-військової співпраці, суспільної стійкості та обміну даними;

сприяє науковим дослідженням.

Швидкий розвиток новітніх інформаційних технологій та впровадження штучного інтелекту вивів на новий рівень ведення гібридних війн, а з ними – й операцій в мультидоменному середовищі. Додавання до конвенційних дій заходів у кіберсфері, асиметричних, мережоцентричних та іррегулярних дій значно ускладнює ведення війни у добре відомому нам класичному стилі.

Сьогодні Україна пише нову сторінку в історії війн, потребуючи не лише зброї, але й детальної аналітики й прогнозування існуючих загроз в інформаційному середовищі, особливо в когнітивній сфері.

В сучасних умовах відновлення багатополярного світу з’являються нові актори, які намагатимуться зайняти своє місце у геополітичній площині. Маскування завоювання йде через встановлення контролю та не матиме вигляду війни у класичному вигляді. Переможе той, хто зуміє досягти стратегічної переваги [2, 19], у тому числі завдяки когнітивному впливу, не вступаючи у пряме збройне протистояння.

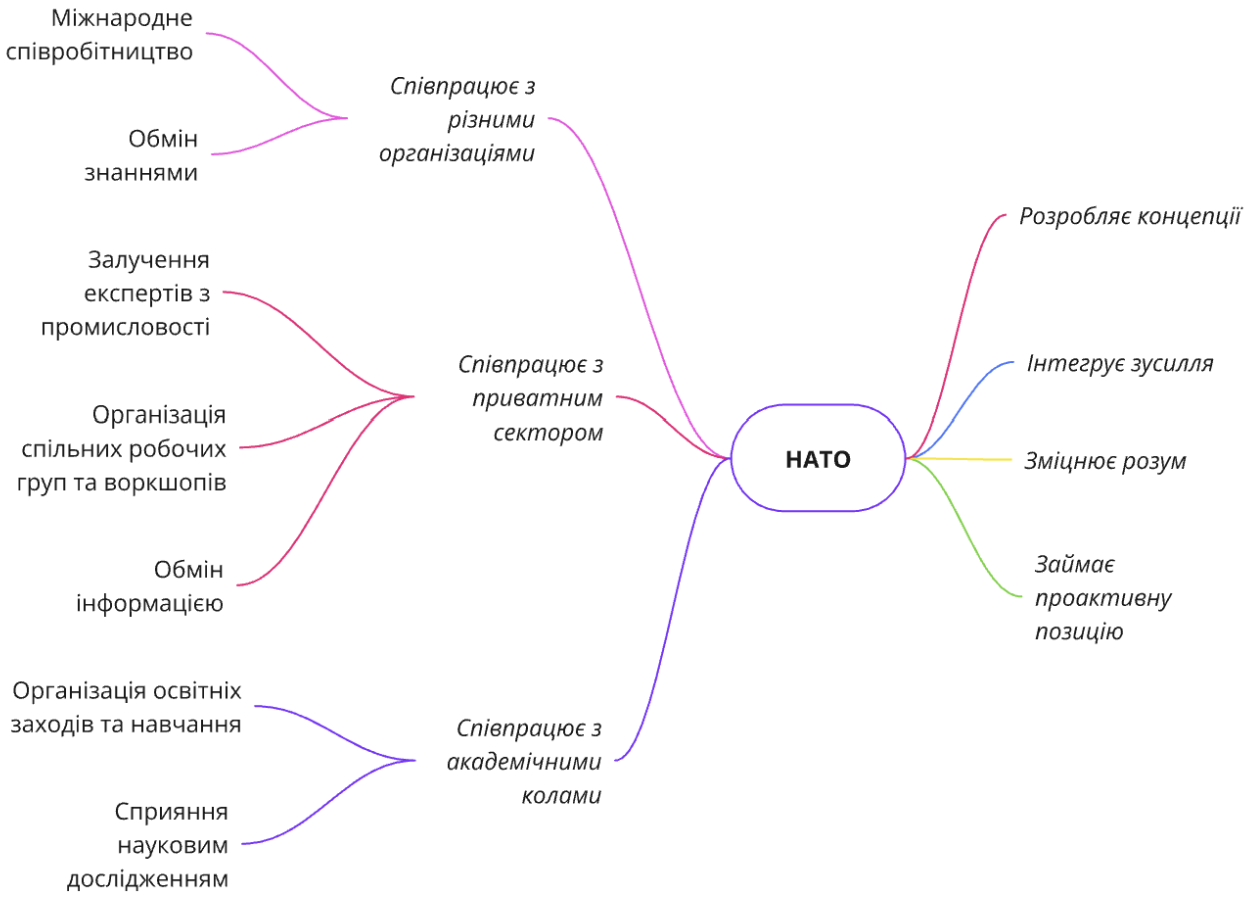


Рисунок 2. Заходи НАТО щодо протистояння загрозам когнітивної війни

Результати (Results)

Розуміння природи когнітивної війни є основою для правильного ухвалення рішень, коли йдеться про їхню діяльність. Вони працюють у складному середовищі з різноманітними загрозами, тому важливим є вироблення комплексного підходу у здобутті когнітивної переваги [20].

Когнітивна війна може включати як окремо, так і комбінацію таких складових:

дезінформація: поширення неправдивої інформації для введення в оману;

пропаганда: систематичне поширення ідеологічних повідомлень для формування громадської думки;

психологічні операції: заходи, спрямовані на вплив на емоції, мотиви та розум людей;

кібервійна: використання комп'ютерних мереж для здобуття стратегічної переваги.

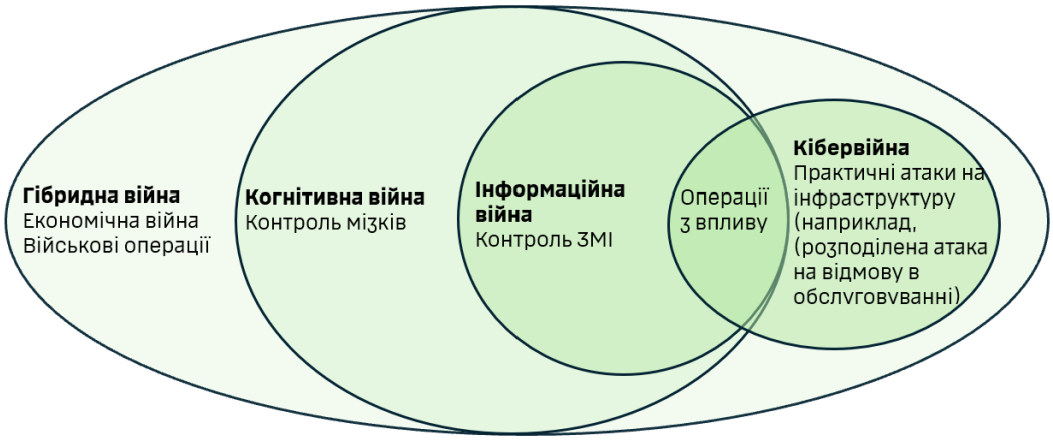


Рисунок 3. Взаємозв'язок когнітивної війни з сучасними технологіями [20].

Щоб уникнути когнітивної маніпуляції, можна використовувати такі стратегії:

освіта;

критичне мислення;

медіаграмотність;

розмаїття джерел;

самосвідомість.

Також важливу роль у попередженні когнітивної маніпуляції відіграють засоби масової комунікацій (ЗМІ) шляхом:

*подання фактів (*ЗМІ повинні надавати точну та перевірену інформацію).

*балансу думок (*представлення різних точок зору для забезпечення об'єктивності).

*підвищення етичних стандартів (*дотримання високих моральних та професійних стандартів);

м*едіаграмотність (*навчання аудиторії критично сприймати інформацію).

Те саме стосується й соціальних мереж. Для попередження когнітивної маніпуляції необхідні:

*модерація контенту (*виявлення та блокування фейкових новин та дезінформації);

*алгоритми (*створення алгоритмів, які просувають достовірний контент);

*співпраця з фактчекерами (*перевірка інформації на достовірність);

*освітні кампанії (*навчання користувачів розпізнавати маніпулятивний контент).

Враховуючи зазначене, країни НАТО вживають заходів для протидії когнітивним впливам:

розробка концепції (створення стратегій для протидії когнітивним атакам);

інтеграція зусиль (об'єднання кібернетичних, інформаційних, психологічних та спроможностей та соціальної інженерії);

зміцнення розуму (захист та зміцнення когнітивних здібностей особового складу);

проактивна позицію (НАТО намагається випереджати ініціативу у когнітивному вимірі, визнаючи загрозу постійних когнітивних атак).

Такі заходи дозволять НАТО:

формувати середовище та протистояти загрозам когнітивної війни;

оснащувати країни НАТО для захисту їх основних національних демократичних цінностей;

покращувати свої можливості та зміцнювати свої позиції у сфері когнітивної війни;

Водночас штучний інтелект (ШІ) можна впровадити у модерацію контенту таким чином:

розробляти алгоритми – створювати алгоритми, які можуть розпізнавати образливий та шкідливий контент;

навчати моделі – використовувати великі дані для тренування моделей розпізнавати патерни дезінформації;

тестувати та оптимізувати – перевіряти ефективність ШІ на реальних даних та його постійне удосконалення;

інтегрувати з людьми-модераторами – ШІ може виконувати первинний аналіз, а люди - оцінювати складніші випадки.

Таке поєднання може значно покращити якість та швидкість модерації контенту.

Освіта відіграє ключову роль у попередженні когнітивної маніпуляції, оскільки:

підвищує обізнаність – навчає людей розуміти, як маніпуляція впливає на думки та поведінку;

розвиває критичне мислення – допомагає виявляти та аналізувати спотворену інформацію;

зміцнює медіаграмотність – навчає визначати надійність джерел та інформації;

сприяє самосвідомості – допомагає людям розуміти власні упередження та емоційну реактивність.

Таким чином, освіта допомагає створити суспільство, здатне критично оцінювати інформацію та протистояти маніпулятивним впливам.

Висновок (Conclusion)

Основна запорука перемоги – це розуміння того, який вигляд вона має. Всі елементи у сучасній архітектурі гібридної війни мають бути збалансовані між собою та оптимізовані за

ефектами, які вони надають. У поєднанні з сучасними технологіями вони дозволять при проведенні операцій в мультидоменному середовищі отримати перевагу в інформаційному середовищі, в тому числі у когнітивній сфері, створити на державному рівні міцну модель протидії державам-агресорам, яка відповідатиме сучасним реаліям, водночас, зберігаючи єдність, довіру та національні демократичні цінності.

Аналіз досліджень показує, що в найближчому майбутньому всі сучасні технології будуть направлені саме на здійснення впливу без ведення прямої конвенційної конфронтації.

Когнітивна війна буде набувати все більшого поширення (значення) в сучасній архітектурі гібридної війни.

В цілому, когнітивна війна – це складний і багатоаспектний процес, який може завдати серйозного впливу на суспільство під час ведення гібридної війни. Як під час збройних конфліктів, так і у мирний час, ми зможемо захиститися від когнітивної війни за допомогою критичного мислення та аналізу інформації, зберегти свою здатність мислити незалежно та об'єктивно. Здобуття когнітивної переваги України над рф сприятиме впровадження на державному рівні комплексного підходу щодо реагування на збройну агресію противника з урахуванням сучасної архітектури гібридної війни.

Використані джерела (References)

1. Kogut, Y. (2023). *Hybrid warfare of a new type as a threat to the national security of states*. SIDCON Consulting Company; DAKOR Publishing House.
2. Sean McFate. (2023). *New Rules of War. Victory in an era of prolonged chaos*. (Transl. from English by Ihor Bihun). Nash format.
3. David Kilcullen. (2011). *The Accidental Guerrilla. Fighting small wars in the middle of a big one.* Hurst & Company.
4. *The Islamic State: the largest battle of our time*. (2nd edition). (2022). Mark Melnyk Publishing House (FOP Melnyk M.Y.)
5. *The US Army in Multi-Domain Operations 2028*. (2018, 6 груд.). TRADOC Pamphlet 525-3-1. Distribution Statement A.
6. *Multi-Domain Operations.* (2019, Sept.). Centre for Army Lessons Learned. Fort Leavenworth, KS 66027-1350. № 19-19. http://surl.li/rtnkr (accessed 14.10.2024).
7. Kogut, Y. I. (2022). Cyberwarfare, cyberterrorism, cybercrime (concepts, strategies, technologies): a practical guide.
8. *Happening in 2024: Advances in Cognitive Warfare, Multi-Domain Operations, Future Operating Environments, Sweden's Accession to NATO*. (2024, 8 Jan.). http://surl.li/dlvixk (accessed 14.10.2024).
9. *Allied Joint Doctrine for Strategic Communications*. (2023, March). NATO Standard AJP-10. NATO Standardisation Office (NSO): Edition A Version 1 with UK national elements (Change 1), © NATO/OTAN.
10. Joint Operations. Joint Publication No. 3-0. Washington DC: *Joint Staff, Incorporating change 1*, 22 (2022, Oct.).
11. Army Techniques Publication No. 3-13.1. *The Conduct of Information Operations*. (2018, Oct.). Headquarters, Department of the Army, Washington, DC, 04. http://surl.li/yjuove (accessed 14.10.2024).
12. Claverie, B., Prebot, B., Buchler, N. & Du Cluzel, F. (2021). *Cognitive Warfare*. *First NATO Scientific Meeting on Cognitive Warfare*. Bordeaux (France). (2021, 21 Jun.). Science and Technology Organisation. http://surl.li/wooshu (accessed 14.10.2024).
13. *Allied Command Transformation develops the Cognitive Warfare Concept to Combat Disinformation and Defend Against "Cognitive Warfare"*. (2024). http://surl.li/dhaceu (accessed 14.10.2024).
14. *Workshop – Cognitive Warfare Concept*. (2022, 27 Sept.). http://surl.li/rtbtqv (accessed 14.10.2024).

15. *The 21st-Century Game Changer COGNITIVE WARFARE*. http://surl.li/ujxafu (accessed 14.10.2024).
16. *Cognitive Warfare – NATO's ACT*. http://surl.li/yweyeb (accessed 14.10.2024).
17. *Cognitive Warfare: Strengthening and Defending the Mind – NATO's ACT*. (2023, 5 Apr.). http://surl.li/jmcera (accessed 14.10.2024).
18. *Mitigating and Responding to Cognitive Warfare*. http://surl.li/zjhlju (accessed 14.10.2024).
19. *Countering cognitive warfare: awareness and resilience – NATO*. http://surl.li/piocap (accessed 14.10.2024).
20. Daniel Nikoula, Dave McMahon. (2024, 16 Jul.). *Cognitive Warfare: Securing Hearts and Minds.* Information Integrity Lab. http://surl.li/nvsbep (accessed 14.10.2024).