УДК 342-051:316.658
DOI 10.32782/2312-1815/2024-17-9

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

КОГНІТИВНА БЕЗПЕКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Статтю присвячено опрацюванню змісту і природи поняття гібридної війни, що стає усе більш актуальним у контексті модифікованих військово-політичних стратегій та технологій. Установлено, що когнітивна безпека в умовах гібридної війни виявляється як один із ключових аспектів безпеки суспільства та держави у цілому. Наголошено, що концепція гібридної війни перетворилася на один із найперспективніших і водночас спірних напрямів політологічного досліджень. В експертній спільноті існують розбіжності, чи є гібридна війна новою формою ведення війни і чи має вона кваліфікуватися як революція у військовій справі, яка встановить нову стратегічну парадигму. Вивчено досвід Китаю з погляду ведення «необмеженої війни». Наведено аргументи відносно «переваг» ведення гібридної війни порівняно з класичним її варіантом. Розглянуто основні аспекти та виклики, пов'язані з когнітивною безпекою у контексті гібридної війни.

Установлено параметри когнітивної безпеки, включаючи вплив інформаційних впливових операцій на сприйняття та поведінку суспільства. Увагу сфокусовано на практичних кейсах і конкретних викликах, з якими стикаються держави в забезпеченні когнітивної безпеки в умовах гібридної війни. Аналізуються методи та технології, які використовуються для маніпулювання інформацією та сприйняттям, зокрема за допомогою соціальних мереж, дезінформації та психологічних впливів. У заключній частині статті розглядаються можливі шляхи захисту від когнітивних атак та зміцнення когнітивної безпеки як важливого елемента загальної безпеки суспільства. Обговорюються ролі державних інституцій, громадськості та міжнародних організацій у забезпеченні когнітивної стійкості. Як перспективу подальших наукових досліджень запропоновано здійснити комплексний аналіз стратегій і тактик інформаційної війни.

Ключові слова: *цифрові технології, гібридна війна, моральний консенсус, когнітивна безпека.*

Вступ. Із розвитком та поширенням цифрових технологій у всі сфери суспільної діяльності почала наростати залежність від інформації. Сучасні конфлікти все більш частіше мігрують у медіапростір та кіберпростір, що в тому числі дає змогу оперативно поширювати дезінформацію, модифікувати перцепцію подій. Значні прояви маніпуляцій та використання інформації як одного із засобів ведення війни щоденно прослідковуються і у війні росії проти вільної та незалежної України (лютий 2022 р.), ХАМАСу та Ізраїлю (жовтень 2023 р.), мали місце у П'ятиденній війні росії та Грузії (серпень 2008 р.) тощо. У світлі зазначеного культ когнітивної безпеки нині займає майже рівноцінне місце з безпекою фізичною, особливо в умовах гібридної війни.

Що характерно, гібридна війна як феномен має далеко не тимчасовий характер, а поетапно стає складною стратегією, котра використовується на постійній основі. У зв'язку із зазначеним питання когнітивної безпеки – це не лише внутрішня проблема певної країни, а й проблематика міжнародного значення, яке зумовлює прийняття консолідованих рішень задля протидії відповідним загрозам.

Матеріал і методи дослідження. Зважаючи на мету дослідження, серед ключових методів, покликаних її реалізувати виділяємо історичний, порівняльний, системний та інституціональний. Теоретичну основу дослідження сформували роботи В.П. Горбуліна, який аналізує два модуси існування гібридної війни, вивчає її передумови та особливості, окреслює новий баланс сил і пошук міжнародно-правових безпекових формул [1]; В. Лизанчука, що

ґрунтовно опрацьовує один з аспектів, що передують російсько-українській гібридній війні: мовне питання [2]. Як дискурсивний конструкт, предмет нашого дослідження виступає ключовим для дослідження й у роботі Г.М. Яворської [3]. Незважаючи на вагому кількість наукових робіт у даному напрямі, зміна динаміки подій на українському фронті гібридної війни зумовлює потребу в аналізі нових її форм проявів та вивченні заходів, що сприяють забезпеченню когнітивної безпеки, у чому й полягає мета дослідження.

Результати та обговорення. Феномен «гібридної війни» в контексті політологічних досліджень набуває особливої популярності після політичних дебатів американських військових спеціалістів (морська піхота США), які публікують спільну статтю, присвячену зростанню кількості гібридних воєн, першопричини яких вони бачать у «домінуючій ролі людського виміру у війні». У публікації йдеться про звичайні та особливі стратегії, котрі застосовуються у ході ведення сучасних воєн, більшою мірою заснованих на методах психолого-інформаційного впливу [4]. Вдруге глобально про новий тип війни почали говорити з квітня 2014 р., коли росія несанкціоновано ввела регулярні війська на територію України, а потім здійснила анексію Криму. Довготривала, багаторічна кампанія агресора, особливо на території Донецької та Луганської областей, де превалює кількість російськомовного населення, багато в чому виправдала себе за рахунок використання соціально-політичної поляризації, потужного економічного впливу, озброєних сил, інформаційної пропаганди. На щастя, цих заходів виявилося недостатньо з початком повномасштабного вторгнення у лютому 2022 р., тому концепція «візьмемо Київ за три дні» зазнала фіаско [5].

Феномен гібридної війни має два головні модуси існування – матеріальний (фізичний) і дискурсивний. Ці два модуси асиметричні. У військовому (матеріальному) вимірі російсько-український конфлікт є локалізованим, охоплюючи частину території України, натомість дискурс цієї гібридної війни набув глобального масштабу [6, с. 47]. У широкому розумінні гібридна війна розуміється як специфічний вид збройного конфлікту, у якому слабший проти сильного прагне нівелювати його конвенційні переваги. Тобто у цій ситуації спостерігається зіткнення симетричних та асиметричних дій [7, с. 10]. Слушною також є думка інших науковців, які розкривають цей тип війни через її структурну природу. Так, вона є формою асиметричної війни і використовує кілька інструментів влади вздовж горизонтальної та вертикальної осі. Дії недержавних акторів проти державних є зазвичай асиметричними. Вони використовують методи, які не характерні для регулярних військ держав. Тому війни державних і недержавних суб'єктів є асиметричними війнами [8, с. 25]. Колишній міністр оборони США Р. Гейтс характеризував гібридну війну як поєднання сучасних технологій та архаїки, сукупність застосування потенціалу збройних сил держави з фанатичним і невичерпним прагненням інсургентів, які ведуть «партизанські» бойові дії, а також спільне використання продукції компанії Microsoft із примітивним холодним та технологіями STELS, керованими камікадзе [9].

Узагальнюючи вказане, «гібридність» у даному разі ідентифікується через симбіоз форм економічного, культурного, інформаційного, збройного впливу на суб'єкт, вибраний як ціль для захоплення. Про такий тип війни як динамічне явище напише директор Інституту зовнішньої політики Дипломатичної академії України Г. Перепелиця. Він зазначатиме, що вона включає у себе активні бойові дії, переговори, миротворчі дії, ескалацію конфлікту та перемир'я, адже в такому мутованому вигляді війни розмитою стала лінія між війною та миром. Досить часто, навіть після завершення мирних переговорів або оголошення остаточного перемир'я, гібридна війна продовжує тривати, але з меншою інтенсивністю (на інформаційному, культурному, інших фронтах) [10, с. 34]. Постає цілком логічне питання: які «переваги» ведення саме гібридної війни порівняно з її класичним варіантом? У першу чергу, як транслює російська пропаганда, – це сам факт заперечення війни або використання дефініцій, що за своїм змістовним наповненням не відповідають фактичному стану подій (збройний конфлікт, тимчасова

операція, антитерористичні заходи і т. д.). У такий спосіб затягується процес притягнення до відповідальності країни-загарбника за порушення територіальної цілісності й миру в іншій суверенній країні; світова спільнота залишається певний час дезорієнтованою, перебуває у пошуку оптимальних та правомірних засобів впливу на агресора.

Водночас, як зазначається на офіційному сайті НАТО, хоча сучасні конфлікти ведуться новими інноваційними та радикально різними методами, вони все менше стосуються безпосередньої участі збройних сил, сама природа міжнародної безпеки та міжнародних конфліктів залишається незмінною. Сталими є закономірності, яким підпорядковуються міжнародні відносини, наприклад «гра з нульовою сумою», де перемога однієї сторони означає поразку іншої; неминучість збройних конфліктів, збереження дилеми безпеки та балансу сил [11]. У зв'язку із цим можна навести приклади технологій «кольорових революцій» (із комплексним використанням можливостей єдиного інформаційного простору та сучасних інформаційних технологій), що у поєднанні з політичним та економічним впливом дають змогу досягти мети без військового втручання, за потреби з точковою ліквідацією представників політичної та економічної еліти, правоохоронних органів.

Після багатьох років пропаганди рф наратив про «братні народи» змінився закликом «звільнити населення України від фашистів, націоналістів та бандерівців, захистити російськомовне населення». Нацистів так і не знайшли, а російськомовне населення, як і україномовне, стало на захист своїх міст/сіл, своїх будинків та сімей від непроханих «визволителів». Для українців, як для будь-якої іншої нації, мова – дім життєдайного буття, духовний, світоглядний, націєтворчий корінь. Теза, яку цілеспрямовано нав'язують, «яка різниця, якою мовою говорити», у сучасних умовах цинічно фальшива. Вона є формою нинішнього повзучого, так званого м'якого зросійщення, яке підступно висмоктує з українців національну сутність, культивує російську імперську свідомість, створює передумови нефункціональності української мови. За ігноруванням комунікативної функції мови приховано знищення інших, не менш важливих функцій: ідентифікаційної, експресивної, гносеологічної, мислетворчої, естетичної, культуроносної, номінативної тощо. Тобто питання всебічного функціонування української мови в усіх державних і суспільних інституціях – це питання життя або смерті української нації [12, с. 127]. Важливим аспектом гібридної війни також стала активна протидія курсу України на інтеграцію і членство у ЄС.

Існує також альтернативний внутрішній фронт гібридної війни: росія тривалий час масштабно поширює лозунги і наративи кремля серед своїх громадян як за допомогою транслювання специфічної інформації, так і шляхом блокування зовнішніх джерел інформації для місцевого населення. Один із найскладніших аспектів цієї кризи полягає у його оцінці ззовні. Тут варто бути обережним, оскільки те, що здається неефективною пропагандою стосовно українців, може бути сприйнято аудиторією внутрішньо. Дана теза підтверджує ще одну особливість гібридної війни: складно вести інформаційну кампанію, коли агресор грає у відкриту, тоді як латентні довготривалі маніпуляції все ж мають впив на певну частину населення.

Вторгнення росії та жахливі сцени руйнування українських міст створили глобальну кризу і моральний консенсус, що стало надзвичайно рідкісним у цифрову епоху. Українці за рахунок резистенції військовій агресії та єдності у бажанні жити у вільній, незалежній країні два роки невпинно розповідають світу про те, що відбувається з ними. Українська діаспора проявила потужний опір загарбницьким лозунгам кремля у соціальних мережах, світових ЗМІ, мережі Інтернет у цілому. Слушними вважаємо міркування старшого наукового співробітника Центру Шоренштейна з питань медіа, політики та публічної політики Гарвардської школи Кеннеді стосовно того, що Інтернет-аудиторія, особливо та, котра стежить за останніми новинами, із часом стала більш скептичною, ніж раніше, і краще розпізнає спроби впливу: «Ми не тільки

можемо розплутати їхні операції під чужими прапорами і дезінформацію, але ми можемо показати, наскільки погано виконані ці пропагандистські спроби» [13].

Ситуація загострюється також за рахунок того, що під агресивні імперські амбіції москви піддаються лідери Угорщини, Словаччини, Сербії та інших країн. Вони проявляють агресію або незадоволення до української культури, перекручуючи історичні факти, доводячи їх до абсурду; у повсякденному житті часто вдаються до банальної фальсифікації, відвертої та прихованої маніпуляції, упереджених суджень, брехні, наклепів та інших методів, щоб проводити гібридно-інформаційну війну проти України.

Проте не лише реалії українського сьогодення слугують яскравим кейсом гібридної форми війни. Починаючи з кінця 1990-х років Китай вивчає методи так званої «необмеженої війни», прийоми якої включають комп'ютерне хакерство та зараження вірусами, зрив роботи банківської системи, маніпуляції на валютних біржах, тероризм у міських умовах, дезінформація у ЗМІ [14, с. 99]. Поки незрозуміло, наскільки необмежена війна стала офіційною китайською доктриною, хоча деякі елементи цієї концепції проглядаються в китайській політиці «трьох воєн» щодо територіальних претензій у Східно-Китайському та Південно-Китайському морях. Китай уникає відкритого застосування військової сили, але для досягнення своїх цілей використовує психологічні операції, медійні маніпуляції та правові претензії (правову війну).

За таких умов роль і значення когнітивної безпеки значно інтенсифікуються. Саме поняття визначається як концептуальна парадигма, котра охоплює механізми й стратегії для захисту когнітивних процесів та інтелектуальної діяльності в особистому та колективному сприйнятті, обробці інформації. Подібного роду ідея акцентує на виявленні, аналізі та протидії загрозам, пов'язаним із маніпуляціями когнітивними процесами, що можуть спотворити об'єктивне сприйняття дійсності і призвести до психологічного впливу на індивіда.

Очевидну перевагу в когнітивній війні отримує той, хто вчиняє перший крок і вибирає час, місце і методи наступу. Завдяки відкритості соціальних мереж противник легко переорієнтовує свою діяльність на окремих осіб, вибрані групи або широку громадськість за допомогою соціального меседжингу, впливу через соціальні медіа, цільового розповсюдження документів, відеоматеріалів тощо. Засоби гібридної війни надають можливість систематичного моніторингу за ворогом, здійснювати хакерські атаки і відстежувати життя зацікавлених осіб у соціальних мережах. Ефективна оборона вимагає принаймні розуміння того, що когнітивна кампанія вже відбувається. Для цього необхідно мати здатність спостерігати і реагувати на прийняття рішень. Застосування технологій може забезпечити такі умови, що допоможуть знайти відповіді на ключові питання: чи відбувається кампанія? хто стоїть за її організацією? які її цілі та завдання?

У світлі вищевикладеного, можна узагальнити, що когнітивна безпека є комплексним підходом до забезпечення стабільності індивідів і суспільства від впливів інформаційно-психологічного характеру. Зазначена концепція передбачає заходи та стратегії, спрямовані на захист когнітивних процесів, інтелектуальних зусиль та психологічного благополуччя в умовах росту впливу цифрових технологій та онлайн-середовища. Когнітивна безпека зосереджена на виявленні, аналізі та протидії загрозам, пов'язаним із маніпулюванням когнітивними процесами, такими як мислення, сприйняття, увага, прийняття рішень. Її основною метою є забезпечення надійності та безпеки інтелектуальних систем, запобігання зловживанням та кримінальній діяльності, а також збереження довіри й прозорості у використанні штучного інтелекту, його впливу на суспільство. Особливо актуальним це є в контексті зростаючого впливу технологій на наші пізнавальні процеси та спосіб сприйняття інформації [15, с. 280–281].

Відповідно, постає логічне питання щодо ефективних засобів протидії атакам, які здійснюються на суспільство в рамках гібридних воєн. Як зазначалося вище, гібридна війна – це

міжнародна проблема, у зв'язку з чим першочергові заходи щодо її вирішення мають прийматися на відповідному рівні. Доречно буде згадати, що у період після варшавського саміту у 2016 р. НАТО наголосило на потребі забезпечення громадянської готовності, щоб підвищити рівень життєстійкості населення та державних інститутів у країнах – членах Альянсу шляхом співробітництва між урядовими міністерствами та цивільними організаціями, приватним сектором та громадськістю. До прикладу, країни ЄС теж активно розробляють власні заходи. Так, концепція національної оборони Естонії, ухвалена у 2017 р., поряд із військовою готовністю охоплює також заходи психологічної, громадянської та економічної оборони. Щодо локальних ініціатив, то в даному разі слід відзначити, що універсальних інструментів, адаптованих під кожен воєнний кейс, не існує, проте можна виділити загальні рекомендації, котрі базуються на досвіді російсько-української війни. Першочергово це освіта, яка включає hard skills та soft skills цифрової грамотності; культура поведінки в Інтернет-середовищі; «активне» сприйняття інформації, котра перебуває у вільному доступі. Важливими є територіальні та загальнодержавні програми: 13.07.2023 у Київській міській раді ввели в дію мораторій на публічне використання російськомовного культурного продукту, потім ініціативу перейняли у Львівській, Чернівецькій, Вінницькій, Запорізькій міськрадах; декілька останніх років успішно функціонує проєкт «Дія.Цифрова освіта» (реалізований Міністерством цифрової трансформації України); академічна протидія тощо.

Ми солідарні з думкою Г.М. Яворської, яка наголошує, що коли не вистачає ресурсів для безумовної військової перемоги, яка до того ж обернеться величезною кількістю жертв, досягти перемоги у гібридній війні можна лише невиконанням набору політичних вимог агресора, незмінних протягом усього періоду війни. Таким чином, перемога України на когнітивному рівні полягатиме у тому, щоб унеможливити виконання цих вимог рф і продовжувати зберігати своє існування як самостійної держави [16, с. 47].

Висновки. Отже, за результатами проведеного аналізу доходимо висновку, що гібридна війна не змінює саму природу війни. Тиск залишається у центрі гібридної війни, як і у будь-якій іншій її формі; мета – попередньою, а саме отримання психологічних чи фізичних переваг перед суперником. Гібридна війна характеризується складною динамікою конфлікту не лише тому, що вона пропонує широкий спектр інструментів для підриву супротивника, а й через можливість одночасного його ураження з різних напрямів (відображає загальну мету гібридної війни). На передовій використовуються слабкі боки держави, яка стала об'єктом атаки, у політичній, військовій, економічній, соціальній та інфраструктурній сферах настільки, наскільки вони фізично і функціонально зазнали ослаблення. Інший фронт – інформаційний, головне завдання якого – поставити під сумнів легітимність чинної влади. Безперечно, для служб, відповідальних за національну безпеку, боротьба з широким колом загроз, які мають назву «гібридна війна», представляє велику проблему. Разом із тим питання протидії потенційним і фактичним загрозам, а також забезпечення стану когнітивної безпеки – це індивідуальна справа і завдання кожної свідомої людини.

Перспективу подальших наукових пошуків убачаємо у комплексному аналізі стратегій і тактик інформаційної війни.

Література:

1. Горбулін В.П. Світова гібридна війна: український фронт. Київ : Національний інститут стратегічних досліджень, 2017. 496 с.

2. Лизанчук В. Українська мова – життя державного основа. *Тоталітаризм як система знищення національної пам'яті* : збірник наукових праць за матеріалами Всеукраїнської науково-практичної конференції з міжнародною участю, 11–12 червня 2020 р. Львів : Друкарня Львівського національного медичного університету імені Данила Галицького, 2020. С. 126–130.

3. Яворська Г.М. Гібридна війна як дискурсивний конструкт. *Стратегічні комунікації.* 2016. № 4(41). С. 41–48.

4. James N. Mattis, Frank Hoffman. Future Warfare: The Rise of Hybrid Wars. *U.S. Naval Institute*. 2005 Vol. 131. URL: https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars (дата звернення: 17.02.2024).

5. Хроніка війни, день третій. Битва за Київ. *Forbes Ukraine.* Лютий 2022. URL: https://forbes.ua/news/khronika-viyni-den-tretiy-bitva-za-kiiv-tilki-perevirena-informatsiya-26022022-3912 (дата звернення: 17.02.2024).

6. Яворська Г.М. Гібридна війна як дискурсивний конструкт. *Стратегічні комунікації.* 2016. № 4(41). С. 41–48.

7. Дерев'янко І.П. Гібридна війна як різновид асиметричних дій. *Міжнародні відносини: теоретико-практичні аспекти*. 2023. № 11. С. 6–16. https://doi.org/10.31866/2616-745X.11.2023.278396

8. Горбулін В.П. Світова гібридна війна: український фронт. Київ : НІСД, 2017. 496 с.

9. Gates R.A. Balanced Strategy: Reprogramming the Pentagon for a New Age. *Foreign Affairs.* 2009. 44 p.

10. Перепелиця Г. Російсько-український конфлікт: гібридний мир проти гібридної війни. *Універсум*. 2017. № 1–2. С. 34.

11. Bilal A. Hybrid Warfare – New Threats, Complexity, and «Trust» as the Antidote. Official site of NATO. 2021. URL: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html (дата звернення: 17.02.2024).

12. Лизанчук В. Українська мова – життя державного основа. *Тоталітаризм як система знищення національної пам'яті* : збірник наукових праць за матеріалами Всеукраїнської науково-практичної конференції з міжнародною участю, 11–12 червня 2020 р. Львів : Друкарня Львівського національного медичного університету імені Данила Галицького, 2020. С. 126–130.

13. Lytvynenko J. I Can't Stop Watching a Livestream of Kyiv. The Atlantic. 2022. URL: https://www.theatlantic.com/author/jane-lytvynenko/ (дата звернення: 17.02.2024).

14. Війни інформаційної епохи: міждисциплінарний дискурс : монографія / за ред. В.А. Кротюка. Харків : Факт, 2021. 592 с.

15. Кобець Т. Основні підходи до розуміння поняття «когнітивна безпека» в сучасній науці: політичний та інформаційний аспекти. *Вісник Львівського університету. Серія «Філософсько-політологічні студії»*. 2023. Вип. 49. С. 278–285.

16. Яворська Г.М. Гібридна війна як дискурсивний конструкт. *Стратегічні комунікації.* 2016. № 4(41). С. 41–48.

References:

1. Horbulin, V.P. (2017). Svitova hibrydna viina: ukrainskyi front [World hybrid war: the Ukrainian front.]. Kyiv: Natsionalnyi instytut stratehichnykh doslidzhen. 496 p. [in Ukrainian]

2. Lyzanchuk, V. (2020). Ukrainska mova – zhyttia derzhavnoho osnova [Ukrainian language – the life of the state basis.]. Totalitaryzm yak systema znyshchennia natsionalnoi pamiati [tekst]: *zbirnyk naukovykh prats za materialamy vseukrainskoi naukovo-praktychnoi konferentsii z mizhnarodnoiu uchastiu* 11–12 chervnia 2020 roku / naukovyi redaktor Tetiana Yeshchenko. Lviv: Drukarnia Lvivskoho natsionalnoho medychnoho universytetu imeni Danyla Halytskoho. P. 126–130.

3. Yavorska, G.M. (2016). Hibrydna viina yak dyskursyvnyi konstrukt [Hybrid war as a discursive construct.]. Stratehichni komunikatsii. № 4 (41). P. 41–48. [in Ukrainian]

4. James, N., Mattis & Frank Hoffman (2005). Future Warfare: The Rise of Hybrid Wars. U.S. Naval Institute. Vol. 131. Retrieved fromhttps://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars

5. Khronika viiny, den tretii. Bytva za Kyiv [Chronicle of the War, Day Three. The Battle for Kyiv]. Forbes Ukraine. February 2022. Retrieved fromhttps://forbes.ua/news/khronika-viyni-den-tretiy-bitva-za-kiiv-tilki-perevirena-informatsiya-26022022-3912. [in Ukrainian]

6. Yavorska, G.M. (2016). Hibrydna viina yak dyskursyvnyi konstrukt [Hybrid war as a discursive construct.]. Stratehichni komunikatsii. № 4 (41). P. 41–48. [in Ukrainian]

7. Derevianko, I.P. (2023). Hibrydna viina yak riznovyd asymetrychnykh dii [Hybrid warfare as a type of asymmetric action]. Mizhnarodni vidnosyny: teoretyko-praktychni aspekty. № 11. P. 6–16. https://doi.org/10.31866/2616-745X.11.2023.278396 [in Ukrainian]

8. Horbulin, V.P. (2017). Svitova hibrydna viina: ukrainskyi front [World hybrid war: the Ukrainian front.]. Kyiv: Natsionalnyi instytut stratehichnykh doslidzhen. 496 p. [in Ukrainian]

9. Gates, R. A. (2009) Balanced Strategy: Reprogramming the Pentagon for a New Age. Foreign Affairs. 44 p.

10. Perepelytsia, G. (2017). Rosiisko-ukrainskyi konflikt: hibrydnyi myr proty hibrydnoi viiny [Russian-Ukrainian conflict: hybrid peace against hybrid war]. Universum. № 1–2. P. 34. [in Ukrainian]

11. Bilal, A. (2021). Hybrid Warfare – New Threats, Complexity, and «Trust» as the Antidote. Official site of NATO. Retrieved from https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

12. Lyzanchuk ,V. (2020). Ukrainska mova – zhyttia derzhavnoho osnova [Ukrainian language – the life of the state basis.]. Totalitaryzm yak systema znyshchennia natsionalnoi pamiati [tekst]: zbirnyk naukovykh prats za materialamy vseukrainskoi naukovo-praktychnoi konferentsii z mizhnarodnoiu uchastiu 11–12 chervnia 2020 roku naukovyi redaktor Tetiana Yeshchenko. Lviv: Drukarnia Lvivskoho natsionalnoho medychnoho universytetu imeni Danyla Halytskoho. P. 126–130. [in Ukrainian]

13. Lytvynenko, J. (2022). I Can't Stop Watching a Livestream of Kyiv. The Atlantic. URL: https://www.theatlantic.com/author/jane-lytvynenko/

14. Viiny informatsiinoi epokhy: mizhdystsyplinarnyi dyskurs [Wars of the Information Age: Interdisciplinary Discourse] : a monograph edited by V.A. Krotiuk. (2021) Kharkiv: Fact. 592 p. [in Ukrainian]

15. Kobets, T. (2023). Osnovni pidkhody do rozuminnia «kohnityvna bezpeka» v suchasnii nautsi: politychnyi ta informatsiinyi aspect [The main approaches to understanding «cognitive security» in modern science: political and information aspect]. *Visnyk Lvivskoho universytetu. Seriia filos. – politoloh. studii. Issue* 49. P. 278–285. [in Ukrainian]

16. Yavorska, G.M. (2016). Hibrydna viina yak dyskursyvnyi konstrukt [Hybrid war as a discursive construct.]. *Stratehichni komunikatsii*. № 4 (41). P. 41–48. [in Ukrainian]

Taras Kobets. Cognitive security in the context of hybrid warfare

The article is devoted to the study of the content and nature of the concept of hybrid warfare, which is becoming increasingly relevant in the context of modified military and political strategies and technologies. It is established that cognitive security in the context of hybrid warfare is manifested as one of the key aspects of the security of society and the state as a whole. It is emphasized that the concept of hybrid warfare has become one of the most promising and at the same time controversial areas of political science research. At the same time, there is disagreement in the expert community as to whether hybrid warfare is a new form of warfare and whether it should be qualified as a revolution in military affairs that will establish a new strategic paradigm. The experience of China in terms of «unrestricted warfare» is studied. Arguments are presented regarding the «advantages» of hybrid warfare in comparison with its classical version. The main aspects and challenges related to cognitive security in the context of hybrid warfare are considered.

The main aspects of cognitive security are identified, including the impact of information influence operations on the perception and behavior of society. Attention is focused on practical cases and specific challenges faced by states in ensuring cognitive security in hybrid warfare. The methods and technologies used to manipulate information and perception are analyzed, in particular through social media, disinformation, and psychological influences. The final part of the article considers possible ways to protect against cognitive attacks and strengthen cognitive security as an important element of the overall security of society. The author discusses the roles of state institutions, the public, and international organizations in ensuring cognitive resilience. As prospects for further research, it is proposed to carry out a comprehensive analysis of information warfare strategies and tactics.

Key words: *digital technologies, hybrid warfare, moral consensus, cognitive security.*