УДК 327.7 + 341.215.2 DOI 10.17721/2415-88IX.2024.92.371-382

Тараненко Ганна Геннадіївна

Національний університет «Києво-Могилянська академія» (м. Київ, Україна)

https://orcid.org/0000-0003-2588-4941

e-mail: taranenkoann@yahoo.com

КОГНІТИВНА БЕЗПЕКА ЯК ВИМІР РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Резюме

Когнітивна безпека є важливим виміром національної та міжнародної безпеки. В умовах триваючої російської агресії проти України нагальною є конкретизація виміру когнітивної безпеки в цьому протистоянні. З метою схарактеризувати когнітивну безпеку як вимір російсько-української війни був використаний метод кейс-стаді.

Як результат, можна стверджувати, що когнітивна безпека є істотним виміром триваючої російсько-української війни. Когнітивна війна спрямована на вплив на свідомість людини, зокрема, на здатність раціоналізувати, критично мислити та приймати відповідні рішення. У когнітивній війні мета — це завоювання сердець і умів людей. Отже, метою когнітивної безпеки є забезпечення розвитку стійкості до шкідливих і зловмисних інформаційних та психологічних впливів.

Щодо тенденцій розвитку когнітивної безпеки, когнітивна війна широко використовується різними суб'єктами у глобальних масштабах. Широкомасштабне використання засобів когнітивної війни може призвести до загальносуспільного розколу громадської думки та викликів функціонування державних установ. Висловлюються пропозиції щодо того, щоб до п'яти вимірів ведення бойових дій, визнаних країнами НАТО (земля, море, повітря, космос і кіберпростір), додати шосту сферу — когнітивну.

Можна зробити висновок, що у російсько-українській війні використовуються такі засоби когнітивної війни, як широке використання дезінформації та пропаганди, зловмисних наративів та відповідних контрнаративів, спрямованих на внутрішню та міжнародну аудиторію. Україна активно протидіє негативним когнітивним впливам росії за

допомогою заходів з боку державної влади, високої соціальної активності громадян та динамічної співпраці з партнерами та союзниками.

Ключові слова: когнітивна безпека, Україна, російсько-українська війна, дезінформація, демократія, НАТО, міжнародна безпека

Вступ

Когнітивна безпека є важливим виміром національної та міжнародної безпеки. Вона визначається як людський вимір міжнародної безпеки, який надзвичайно важливо забезпечити в нинішній архітектурі міжнародної безпеки. Когнітивна безпека стосується практик і методів, спрямованих на захист від засобів соціальної інженерії — навмисних і ненавмисних маніпуляцій, а також порушень механізмів пізнання та формування сенсів [1, с.1]. Когнітивна безпека в кібербезпеці зазвичай відноситься до застосування технологій штучного інтелекту (ШІ) і машинного навчання, які моделюються на основі людського пізнання для виявлення загроз безпеці [1, с. 1]. Дослідження когнітивної безпеки є міждисциплінарними і базуються на напрацюваннях у сферах створення смислів, пам'яті, нейронаук, активного умовиводу, аналізу розвідки і контррозвідки, обману та контробману, управління знаннями, педагогіки та інших галузей [1, с. 1]. При цьому когніція (пізнання) - це розумова дія або процес отримання знань і розуміння за допомогою думки, досвіду та почуттів [2, с. 269]. Когніція пов'язана з такими процесами, як увага, формування знань, пам'ять та оперативна пам'ять, судження та оцінка, розуміння та продукування мови, міркування та обчислення, вирішення проблем та прийняття рішень [2, с. 269].

Термін «когнітивна безпека» з'явився відносно недавно. Когнітивна безпека визначається як концептуальна парадигма, яка охоплює заходи та стратегії захисту когнітивних процесів та інтелектуальної діяльності в особистому та колективному сприйнятті та обробці інформації [3, с. 283]. У когнітивній безпеці акцентується увага на виявленні, аналізі та протидії маніпуляціям, пов'язаним із загрозами когнітивним процесам, які можуть спотворювати об'єктивне сприйняття реальності та призводити до психологічного впливу на особистість [3, с. 283]. Метою когнітивної безпеки є забезпечення стабільного та безпечного функціонування інтелектуальних систем, запобігання зловживанням, збереження довіри та прозорості в інформаційному середовищі [3, с. 283]. Когнітивна безпека означає підтримання раціонального прийняття рішень в умовах протистояння: це передбачає загальне прийняття тієї самої спільної реальності та правил гри для прийняття рішень, опір або пом'якшення емоційних маніпуляцій та захист окремих людей і суспільств для забезпечення можливості колективних дій [4, с. 1] . Ризики для когнітивної безпеки включають маніпулювання процесами прийняття рішень людиною, злам «людини» в команді «людина-машина», маніпулювання поведінкою «людина-група», передача інформації

людині (симбіотичний інтерфейс «людина-комп'ютер»), вихід за межі людино-машинного інтерфейсу (HMI) до людино-машинного середовища, або людино-машинної екосистеми (HME), озброєння наративів, а також політизоване та монетизоване інформаційне середовище [4, с. 1].

Когнітивна безпека є життєво важливою складовою інформаційної безпеки та кібербезпеки. Когнітивна безпека, як важлива складова інформаційної безпеки, впливає на ефективність і стабільність усієї інформаційної системи, [3, с. 281]. До її ключових аспектів належать розпізнавання загроз, протидія дезінформації, забезпечення довіри, збереження психологічної стабільності, запобігання наслідкам кібератак та підтримання ефективності заходів кібербезпеки [3, с. 281]. У свою чергу, когнітивні науки можуть посилити когнітивні процеси, які здатні допомогти аналітикам у галузі безпеки швидше та ефективніше вживати заходів у межах кібербезпекових операцій [5, с. 1].

Технологічний розвиток у глобалізованому світі став надзвичайно корисним для багатьох сфер функціонування суспільства. Проте цей поступ уперед також тягне за собою певні виклики та ризики. Нещодавні досягнення в глибинному навчанні призвели до проривів у розвитку штучного інтелекту, сприяючи стрибку в поширенні великих мовних моделей (LLM) на кшталт чату GPT [6, с. 281]. Як і будь-яка нова технологія, ці інструменти приносять не тільки значні переваги для суспільства, але й серйозні безпекові виклики, особливо в соціальній та когнітивній сфері [6, с. 81]. Когнітивна війна включає дії, що проводяться синхронно з використанням інших інструментів влади, щоб вплинути на ставлення та поведінку людей задля захисту або порушення когнітивних процесів індивідів, соціальних груп чи всього населення певної держави [7, с. 1]. Маніпуляція на рівні всього суспільства, створена для зміни сприйняття реальності, стала новою нормою, а людське пізнання стає критичною сферою ведення війни [7, с. 1].

Когнітивна безпека є важливим виміром триваючої російської агресії проти України. Когнітивна війна зосереджена на атакуванні та деградації раціональності, що може призвести до експлуатації вразливостей та системного ослаблення суспільства [7, с. 1]. Наприклад, російські соціальні медіа та операції з громадською інформацією були спрямовані на більшу частину міжнародної спільноти у намаганні представити Україну винною в провокуванні нападу [7, с. 1]. За допомогою поєднання комунікаційних технологій, фейкових новин і маніпуляцій сприйняттям росія прагне вплинути на громадську думку, а також послабити довіру суспільства до відкритих джерел інформації, тому ці наративи мають широке охоплення та часто містять як наступальні, так і оборонні позиції [7, с. 1].

Отже, актуальною видається конкретизація когнітивного безпекового виміру в умовах триваючої російської агресії проти України. Метою статті є схарактеризувати когнітивну безпеку як вимір російсько-української війни.

Завдання статті полягають у визначенні принципів когнітивної безпеки, окресленні тенденцій розвитку когнітивної безпеки на глобальному рівні та представленні характеристик когнітивного виміру російсько-української війни.

Методи дослідження

З метою характеризування когнітивної безпеки як виміру російсько-української війни, що триває, авторка використала метод кейс-стаді. Кейс-стаді є однією з найбільш часто використовуваних методологій соціальних досліджень, однією з найбільш широко вживаних стратегій якісних соціальних досліджень [8, с. 94]. З роками його застосування значно розширилося і нині використовується в кількох дисциплінах соціальних наук, таких як соціологія, менеджмент, антропологія, психологія та інші [8, с. 94]. Як якісна методологія, кейс-стаді часто включають численні потоки даних, об'єднаних у творчий спосіб [9, с. 1]. Глибина та насиченість опису кейс-стаді допомагає читачам зрозуміти певний кейс, а також зрозуміти, чи можуть результати цього дослідження бути застосовані за межами даного конкретного кейсу [9, с. 1]. Таким чином, метод кейс-стаді видається прийнятним підходом до дослідження когнітивної безпеки як виміру російсько-української війни.

Результати дослідження

Когнітивна безпека є одним із важливих аспектів гібридної війни. Це також один із ключових вимірів триваючої російської агресії проти України. У когнітивній війні полем бою стає людська свідомість, а метою є змінити не лише те, що людина думає, а й те, як вона думає та діє [10, с. 1]. У своїй крайній формі когнітивна війна потенційно здатна викликати розбрат і розколоти ціле суспільство так, що воно втрачає колективну волю протистояти намірам агресора, що дає змогу супротивнику підкорити суспільство, не вдаючись до відкритої сили чи примусу [10, с. 1].

Когнітивні війни мають кілька відмінних характеристик. У когнітивній війні перемагає той, хто першим зробить хід і вибере час, місце і засоби атаки [10, с. 1]. Відкритість платформ соціальних медіа дозволяє зловмиснику легко націлюватися на окремих осіб і групи за допомогою соціальних повідомлень, впливу соціальних мереж, вибіркового розповсюдження документів, розповсюдження відео, моніторингу та злому соціальних мереж [10, с. 1]. Наразі НАТО визнає п'ять сфер ведення бойових дій: суша, море, повітря, космос і кіберпростір, утім дедалі більше дослідників пропонують додати шосту, когнітивну сферу [11, с. 102]. Цей новий домен має заповнити певну прогалину, себто умовну територію, за яку ведеться боротьба, а саме - за серця та уми населення певної країни (Bjorgul, 2022, цит. у Shay, 2022) [11, с. 102].

Крім того, когнітивна безпека пов›язана з такими поняттями, як дезінформація, пропаганда, поширення фейків і шкідливої інформації. Термін

«дезінформація» зазвичай використовується як загальна дефініція для позначення широкого спектру тактик, прийомів і процедур, які НАТО описує як «ворожу інформаційну діяльність» [12, с.1]. Країни НАТО визнають, що принципи ведення війни різко змінилися завдяки передовим технологіям, активізації цілих суспільств та збільшенню глобальної взаємозв'язку, утім при цьому дедалі більше людей не в змозі відрізнити правдиву інформацію від маніпулятивної [13, с. 1].

Російсько-українська війна відзначається широким застосуванням когнітивних засобів ведення війни. У російсько-українській війні відбувається інтенсивне використання засобів інформаційно-психологічної війни, які є частиною когнітивної війни [11, с. 104]. Основна мета когнітивної війни полягає у впливі на те, що вороже суспільство думає, любить або у що вірить, змінюючи його уявлення про реальність [11, с. 104]. Наприклад, мистецтво є важливою сферою когнітивної війни [11, с. 104]. Під час російсько-української війни одні й ті самі події на полі бою (у фізичній сфері) висвітлювалися українськими, російськими та міжнародними ЗМІ, але аудиторія отримувала різні інтерпретації тих самих подій, що призводило до різних висновків (Pocheptsov, 2018, цит. у Shay, 2022) [11, с. 104].

Україна стала мішенню численних когнітивних атак росії. Росія розпочала кінетичне військове вторгнення в Україну, підкріплене некінетичною діяльністю, як-от цілеспрямована пропаганда, дезінформаційні кампанії та підтримка партнерів [13, с. 1]. Деякі з цих некінетичних, когнітивних бойових дій є очевидними та прямими — одержувачі російської дезінформації відчувають погіршення своєї здатності відрізняти факти від вигадки, погіршення своєї психічної стійкості з потенційним довгостроковим впливом, таким як втрата довіри до ЗМІ [13, с. 1]. У той час як інформаційна війна зосереджена на контролі над потоком інформації, когнітивна війна натомість має тоншу, але потенційно більш згубну мету — формувати не просто те, що люди думають, а те, як вони думають і як реагують на інформацію [14, с. 12]. Однією з важливих особливостей російсько-української війни є роль, яку відіграє дезінформація як у розгортанні, так і в описі цієї війни [14, с. 12].

Наразі розробляються механізми та інструменти протидії загрозам когнітивної війни. Існують значні безпекові виклики, особливо в соціально-когнітивній сфері, пов'язані з механізмами формування когнітивної імунної системи [6, с. 281]. Належний захист вимагає, як мінімум, усвідомлення того, що йде когнітивна кампанія, яка потребує здатності спостерігати та приймати правильне рішення [10, с. 1]. Технології можуть надати інструменти, які допоможуть знайти відповіді на низку ключових питань, зокрема, чи проводиться певна когнітивна кампанія, звідки вона походить, хто її організував і які її цілі [10, с.1]. Особливо корисним технічним рішенням може бути система моніторингу та оповіщення про когнітивну війну — вона

може включати інформаційну панель із даними з телерадіомовлення, сайтів соціальних мереж, географічних мап та інших даних соціальних медіа, які можуть показувати, як підозрілі когнітивні кампанії розвиваються у часі [10, с. 1].

Інструменти моніторингу та аналізу даних можуть допомогти зрозуміти та візуалізувати середовище спілкування в Інтернеті. Визначаючи місця, як географічно, так і віртуально, з яких походять певні дописи, повідомлення та новинні статті, а також теми для обговорення, настрої та мовні ідентифікатори, такі інструменти можуть допомогти у виявленні певних зв'язків і відстеженні закономірностей (формуванні моделей) [10, с. 1]. Використання технологій машинного навчання та алгоритмів розпізнавання образів може допомогти швидко ідентифікувати та класифікувати нові когнітивні кампанії, що запускаються без втручання людини [10, с. 1].

Інша важлива техніка, яка активно використовується, - це пребанкінг (англ. «prebunking» - попереднє розміщення, або раннє спростування дезінформації). Основна ідея пребанкінгу полягає в тому, щоб діяти на випередження і показати людям тактику та принципи оманливої інформації, перш ніж вони самі зіткнуться з нею випадково — з тим, щоб люди були краще готові розпізнати її та протистояти відповідним когнітивним впливам [15, с. 1]. Наприклад, «Федеральне бюро розслідувань і Агентство з кібербезпеки та безпеки інфраструктури опублікували оголошення про те, що кібератаки навряд чи можуть зірвати голосування» або «Твіттер незабаром надішле нагадування користувачам про те, що остаточні результати можуть не надійти до дня виборів» [15, с. 1]. Це приклади стратегії пребанкінгу, яка стала важливим принципом дії для технологічних компаній, некомерційних організацій та державних установ щодо реагування на оманливі та неправдиві стосовно щодо виборів, охорони здоров'я та інших актуальних питань [15, с. 1].

На нинішньому етапі вживаються заходи щодо протидії когнітивній війні, яка ведеться під час російської агресії проти України. Українське політичне керівництво почало розкривати дії росії ширшій світовій аудиторії відразу після початку повномасштабного російського вторгнення, а особливо після відступу російських військ з Бучі, Ірпеня та Гостомеля. Президент України Володимир Зеленський звертався із закликами про допомогу до світу на різних телеканалах, демонструючи росію в поганому світлі — його акторська майстерність дуже допомагає в транслюванні українського наративу [11, с. 105]. Українці змогли показати через візуальні образи та свої власні історії, що росія не досягне очікуваної швидкої капітуляції України, тому Україні потрібна допомога, щоб продовжувати боротьбу [11, с. 105]. Відео та зображення українських солдатів на острові Зміїний, які кажуть російському військовому кораблю «йти геть», демонструють рішучість українців протистояти росіянам, і тому світ ставиться до них як до героїв [11, с. 105].

Багато українців як представники громадянського суспільства зайняли активну політичну позицію в умовах агресії. Багато українців дефакто діють як воїни когнітивного фронту, що допомагає їм просувати український наратив на платформах соціальних мереж [11, с. 105]. Здатність України виграти цей наратив має значні наслідки, принаймні, для трьох важливих соціальних груп: її власних громадян та їхнього бойового духу, зовнішніх країн, які можуть надати фінансову та дипломатичну підтримку, та людей у росії, які підтримують Україну [11, с. 105].

Наративи створюються для того, щоб транслювати різні типи повідомлень для різних аудиторій. Наратив США/НАТО/Україна ретельно спланований, щоб продемонструвати, що українці ведуть жорстокий бій з росіянами та перемагають, незважаючи на виклики [11, с. 105]. Російські втрати показані як ознака поразки у війні, а також наголошується на причетності росії до військових злочинів і порушень прав людини (Feiner, 2022, цит. у Shay, 2022) [11, с. 105].

Психологічна стійкість і моральний дух є вирішальним фактором на війні. Росія недооцінила стійкість України, в тому числі в інформаційній сфері, і зовнішні зусилля росії у поширенні дезінформації були переважно неефективними, оскільки українські наративи передаються швидко і спрямовуються на населення держав-союзників, яке вже скептично ставилися до російських ЗМІ [11, с. 105]. Західні держави отримали перевагу над російськими наративами, оприлюднивши дані розвідки про російські операції ще до їхнього початку [11, с. 105]. Джеремі Флемінг, голова розвідувальної служби Британської штаб-квартири урядового зв›язку (GCHQ), написав у серпні 2022 року, що і росія, і Україна використовували свої кіберпотужності у війні, але «наразі президент путін повністю програє інформаційну війну в Україні і на Заході» [11, с. 105].

Ще одним важливим аспектом протидії у когнітивній війні для України є співпраця з партнерами та союзниками, зокрема, з країнами НАТО. Ще одним важливим виміром співпраці є відносини України з країнами «Глобального Півдня». Робота НАТО з протидії ворожій інформаційній діяльності посилюється завдяки тісній співпраці з членами Альянсу та партнерами [12, с. 1]. Усі учасники інформаційного середовища — від великих організацій, таких як НАТО, до окремих людей у країнах-членах і партнерах — мають відігравати роль у протидії дезінформації [12, с. 1]. НАТО дотримується подвійної моделі протидії дезінформації: «розуміти» та «залучати», таким чином НАТО постійно відстежує та аналізує інформацію, що має відношення до Альянсу, у тому числі шляхом моніторингу та виявлення джерел дезінформації та аналізу ворожих наративів у міру їх появи та поширення [12, с. 1]. Україна отримує відповідну підтримку з боку партнерів і союзників, у тому числі НАТО. Ще одним важливим виміром співпраці є відносини з країнами «Глобального Півдня», зокрема, Україна протидіє активній російській

пропаганді в цьому регіоні та працює над донесенням правдивої інформації про російські військові цілі та порушення міжнародного права.

Висновки

Когнітивна безпека є посутнім виміром триваючої російсько-української війни. Когнітивна війна спрямована на вплив на пізнання людини, зокрема на здатність раціоналізувати, критично мислити та приймати відповідні рішення. У когнітивній війні мета — завоювати серця й уми людей. Отже, мета когнітивної безпеки полягає в тому, щоб у людини була вироблена стійкість до шкідливих і зловмисних інформаційно-психологічних впливів.

Щодо тенденцій розвитку когнітивної безпеки, то когнітивна війна широко використовується різними суб'єктами по всьому світу. Широкомасштабне використання засобів когнітивної війни може призвести до загальносуспільного розколу громадської думки та зупинити функціонування державних установ. Висловлюються пропозиції щодо того, щоб до п'яти сфер ведення бойових дій, визнаних, зокрема, країнами НАТО (земля, море, повітря, космос і кіберпростір), додати шосту сферу — когнітивну.

Когнітивна війна, що ведеться у межах російської агресії проти України, має такі характеристики, як широке використання дезінформації та пропаганди, зловмисних наративів та відповідних контрнаративів, спрямованих на внутрішню та міжнародну аудиторію. Російські когнітивні атаки включають цілеспрямовану пропаганду та дезінформаційні кампанії з метою дезорієнтувати українську, міжнародну та внутрішню аудиторію, вплинути на її здатність мислити критично та підірвати психологічну стійкість. Зокрема, щодо української аудиторії, мета полягає у зниженні рівня довіри до органів влади та ЗМІ.

Україна активно протидіє негативним когнітивним впливам росії. Влада країни, включно з Президентом України, активно комунікує з внутрішньою та зовнішньою аудиторією, щоб донести правдиву інформацію про російську агресію. Крім того, громадські активісти, представники цивільного населення України активно підтримують ці кампанії, поширюючи відповідний контент. Вирішальним фактором протидії засобам когнітивної війни в Україні є співпраця з партнерами та союзниками, насамперед, країнами НАТО. Іншим важливим виміром співпраці є відносини з країнами «Глобального Півдня». Зокрема, Україна протидіє активній російській пропаганді в цьому регіоні та працює над донесенням правдивої інформації про російські військові цілі та порушення міжнародного права.

Список посилань

1. What Is Cognitive Security? (n/d). CogSec. *https://www.cogsec.org/what-is-cognitive-security-5* (accessed date January 17, 2024).
2. Sadkhan, S. B. Cognitive and the Future. (2018, March). 2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA) [...]. [S. l.: s. n.], 269-270. *https://doi.org/10.1109/ICASEA.2018.8370994*. (accessed date January 17, 2024).
3. Кобець Т. Основні підходи до розуміння «когнітивна безпека» в сучасній науці: політичний та інформаційний аспект. Вісник Львівського університету. Серія філос.-політолог. студії. 2023. № 49. С. 278–285. *https://doi.org/10.30970/PPS.2023.49.34*. (accessed date January 17, 2024).
4. Research Lab Overview. (n/d). Cognitive Security Research Lab. Army Cyber Institute at West Point. *https://cyber.army.mil/Research/Research-Labs/Cognitive-Security/* (accessed date January 17, 2024).
5. *Andrade, R. O., & Yoo, S. G. Cognitive Security: A Comprehensive Study of Cognitive Science in Cybersecurity. Journal of Information Security and Applications, 48, 102352. https://doi.org/10.1016/j.jisa.2019.06.008* (accessed date January 17, 2024).
6. Huang, R., Zheng, X., Shang, Y., & Xue, X. On Challenges of AI to Cognitive Security and Safety. Security and Safety, 2, *https://doi.org/10.1051/sands/2023012* (accessed date January 17, 2024).
7. Cognitive Warfare (n/d). NATO's Strategic Warfare Development Command. *https://www.act.nato.int/activities/cognitive-warfare/* (accessed date January 17, 2024).
8. Priya, A. Case Study Methodology of Qualitative Research: Key Attributes and Navigating the Conundrums in Its Application. Sociological Bulletin, 70(1), P. 94-110. *https://doi.org/10.1177/0038022920970318*. (accessed date January 16, 2024).
9. Alpi, KM. & Evans JJ. (2019, Jan). Distinguishing Case Study as a Research Method from Case Reports as a Publication Type. J Med Libr Assoc. 107(1):1-5. *https://doi:10.5195/jmla.2019.615*. (accessed date January 16, 2024).
10. Као К., Глейстер Ш., Пена Е., Денбі Р. Ронг, В., Роваліно, А. (2021, 20 травня). НАТО ревю - протидія когнітивній війні:

інформованість і стійкість. *https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kogntivnj-vjn-nformovanst-stjkst/index.html* (accessed date January 17, 2024).

11. Shay, S. Between Kiev and Venice-the Cognitive Warfare and the Biennale of Venice. Security Science Journal, 3(2), P. 101-117. *https://doi.org/10.37458/ssj.3.2.6* (accessed date January 17, 2024).
12. NATO's Approach to Countering Disinformation. (n/d). NATO. *https://www.nato.int/cps/en/natohq/topics_219728.htm* (accessed date January 17, 2024).
13. Cognitive Warfare: Strengthening and Defending the Mind (2023, April 5). NATO's Strategic Warfare Development Command. *https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/* (accessed date January 17, 2024).
14. Burke, P., & Henschke, A. I Know My Truth… Now Tell Me Yours: from Active Measures to Cognitive Warfare in the Russian Invasion of Ukraine. Strategic Panorama, (2), P. 12-27. *https://doi.org/10.53679/2616-9460.2.2022.02*. (accessed date January 17, 2024).
15. Bond, S. (2022, October 28). False Information Is Everywhere. «Pre-Bunking» Tries to Head It Off Early. NPR. Untangling Disinformation. *https://www.npr.org/2022/10/28/1132021770/false-information-is-everywhere-pre-bunking-tries-to-head-it-off-early*. (accessed date January 18, 2024).

References

1. What Is Cognitive Security? (n/d). CogSec. *https://www.cogsec.org/what-is-cognitive-security-5* (accessed date January 17, 2024).
2. Sadkhan, S. B. Cognitive and the Future. (2018, March). 2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA) [...]. [S. l.: s. n.], 269–270. *https://doi.org/10.1109/ICASEA.2018.8370994*. (accessed date January 17, 2024).
3. Kobets, T . (2023). Osnovni pidkhody do rozuminnya «kohnityvna bezpeka» v suchasniy nautsi: politychnyy ta informatsiynyy aspekt. Visnyk L'vivs'koho universytetu. Seriya filos.-politoloh. studiyi. 2023, 49, 278–285. https://doi.org/10.30970/PPS.2023.49.34. (data zvernennya 17 sichnya 2024 r.)
4. Research Lab Overview. (n/d). Cognitive Security Research Lab. Army Cyber Institute at West Point. *https://cyber.army.mil/Research/Research-Labs/Cognitive-Security/* (accessed date January 17, 2024).

5. *Andrade, R. O., & Yoo, S. G. (2019). Cognitive Security: A Comprehensive Study of Cognitive Science in Cybersecurity. Journal of Information Security and Applications, 48, 102352. https://doi.org/10.1016/j.jisa.2019.06.008* (accessed date January 17, 2024).
6. Huang, R., Zheng, X., Shang, Y., & Xue, X. (2023). On Challenges of AI to Cognitive Security and Safety. Security and Safety, 2, *https://doi.org/10.1051/sands/2023012* (accessed date January 17, 2024).
7. Cognitive Warfare (n/d). NATO's Strategic Warfare Development Command. *https://www.act.nato.int/activities/cognitive-warfare/* (accessed date January 17, 2024).
8. Priya, A. (2021). Case Study Methodology of Qualitative Research: Key Attributes and Navigating the Conundrums in Its Application. Sociological Bulletin, 70(1), 94-110. *https://doi.org/10.1177/0038022920970318*. (accessed date January 16, 2024).
9. Alpi, KM. & Evans JJ. (2019, Jan). Distinguishing Case Study as a Research Method from Case Reports as a Publication Type. J Med Libr Assoc. 107(1):1-5. *https://doi:10.5195/jmla.2019.615*. (accessed date January 16, 2024).
10. Kao, K., Hleyster, SH., Pena, E., Denbi R, Ronh, V., & Rovalino, A. (2021, 20 travnya). NATO revyu - protydiya kohnityvnoyi viyny: informovanist' i stiykist'. *https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kogntivnj-vjn-nformovanst-stjkst/index.html* (accessed date January 17, 2024).
11. Shay, S. (2022). Between Kiev and Venice-the Cognitive Warfare and the Biennale of Venice. Security Science Journal, 3(2), 101-117. *https://doi.org/10.37458/ssj.3.2.6* (accessed date January 17, 2024).
12. NATO's Approach to Countering Disinformation. (n/d). NATO. *https://www.nato.int/cps/en/natohq/topics_219728.htm* (accessed date January 17, 2024).
13. Cognitive Warfare: Strengthening and Defending the Mind (2023, April 5). NATO's Strategic Warfare Development Command. *https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/* (accessed date January 17, 2024).
14. Burke, P., & Henschke, A. (2022). I Know My Truth… Now Tell Me Yours: from Active Measures to Cognitive Warfare in the Russian Invasion of Ukraine. Strategic Panorama, (2), 12-27. *https://doi.org/10.53679/2616-9460.2.2022.02*. (accessed date January 17, 2024).
15. Bond, S. (2022, October 28). False Information Is Everywhere. «Pre-Bunking» Tries to Head It Off Early. NPR. Untangling Disinformation. *https://www.npr.org/2022/10/28/1132021770/false-information-is-everywhere-pre-bunking-tries-to-head-it-off-early*. (accessed date January 18, 2024).

UDC 327.7 + 341.215.2 DOI 10.17721/2415-88IX.2024.92.371-382

Anna Taranenko
National University of "Kyiv-Mohyla Academy", (Kyiv, Ukraine)
https://orcid.org/0000-0003-2588-4941
e-mail: taranenkoann@yahoo.com

COGNITIVE SECURITY AS A DIMENSION OF RUSSIA-UKRAINE WAR

Cognitive security is an important dimension of national and international security. It is urgent to specify the cognitive security dimension under the ongoing russian aggression against Ukraine. For the purpose of characterizing cognitive security as a dimension of the ongoing russia - Ukraine war, the author has utilized the method of case study.

As a result, it can be stated that cognitive security is a crucial dimension of the ongoing russia - Ukraine war. Cognitive warfare is aimed at affecting human cognition, in particular, the ability to rationalize, think critically and make appropriate decisions. In a cognitive war the goal is to win hearts and minds of people. Therefore the goal of cognitive security is to ensure that people have developed resistance to harmful and malicious informational and psychological influences.

As to the trends of cognitive security development, cognitive warfare is being widely used by various actors worldwide. Large-scale usage of cognitive warfare can lead to society-wide divisions in public opinion and stalling government institutions' functioning. There are suggestions voiced as to adding the sixth warfighting domain—the cognitive domain—to the five ones (land, sea, air, space, and cyberspace) recognized by the NATO countries.

It can be concluded that there are such characteristics of the cognitive warfare utilized in the russia-Ukraine war, as wide usage of disinformation and propaganda, malicious narratives and respective counternarratives aimed at domestic and international audiences. Ukraine actively counteracts russia's negative cognitive influences by means of the government-adopted measures, grassroot activism and dynamic cooperation with partners and allies.

Keywords: cognitive security, Ukraine, russia-Ukraine war, disinformation, democracy, research methods, international security

Стаття надійшла до редакції 28.03.24