УДК 327.8
DOI 10.32782/2312-1815/2024-17-23

Михайло Савлюк
ORCID: 0009-0001-9870-8343

ГІБРИДНА ВІЙНА В УКРАЇНІ: СУЧАСНІ ПІДХОДИ

Зі стрімким розвитком комп'ютерних (і не тільки) технологій людство почало стрімко прогресувати на всіх фронтах. Не винятком став і театр воєнних дій, де гібридна війна починає набирати все нових обертів та поширюватися на нові, раніше не застосовані напрями.

Якщо взяти за приклад російсько-українську війну і проаналізувати її генезис, то стає зрозумілим, що вона розпочалася ще задовго до активної фази у 2014 р. Цій війні, яка, безперечно, є гібридною, багато років поспіль передували інформаційна, культурна та економічна експансії. В Україні постійно працювали російські телеканали та інші мас-медіа, які практично у цілодобовому режимі транслювали і насаджували українцям прокремлівські наративи, зокрема про «братні народи», спільну історію та культуру. До України безперешкодно приїжджали виступати російські популярні артисти та музиканти. Російські потужніші компанії та підприємства безперешкодно купляли та поглинали не такий економічно розвинений український бізнес. Разом із торговими та газовими «війнами» це все разом починало гібридну війну супроти Україні ще з 90-х років XX ст. та «нульових» років XXI ст. Увесь цей комплекс «агресивних» дій заклав підґрунтя того, що нам усім довелося бачити на «антимайдані» у 2013 р. та на Донбасі вже у 2014 р.

І якщо після початку збройного протистояння на Донбасі Україна заборонила в'їзд на свою територію одіозним російським артистам, які підтримали окупацію Криму та збройну інтервенцію у Донецькій та Луганській областях, а згодом у 2017 р. у державі були заборонені російські соцмережі «Одноклассники» та «ВКонтакте» й частина телеканалів, то після початку повномасштабної війни інформаційна інтервенція росії почала набирати нових обертів.

Сьогодні проти України та її союзників працюють численні та потужні ботоферми, які завдяки російським політтехнологам, психологам та іншим фахівцям здійснюють чіткі інформаційні удари по чуттєвих для нас усіх місцях. Вони чітко провокують внутрішньодержавні конфлікти, сіють зневіру та недовіру пересічних громадян до представників української влади та уряду.

Тому тепер як ніколи гостро стоїть проблема дослідження загроз, які отримує національна безпека нашої держави крізь призму соціальних мереж. Слід вивчити психологічний вплив ворожої пропаганди на користувачів. Також потрібно розробити та дослідити інструменти боротьби з ворожими наративами. Нині слід розробити алгоритми та методичні матеріали, які б у подальшому могли допомогти нівелювати роботу ворожих ботоферм та розробників інформаційно психологічних спеціальних операцій. Адже з кожним днем робота ворожої пропаганди набирає все потужніших обертів, а це несе пряму загрозу національній безпеці України.

Ключові слова: *соціальні мережі, інформаційна безпека, національна безпека, Facebook, пропаганда, гібридна війна, війна.*

Вступ. На початок XXI ст. відбулася істотна еволюція у методах та способах проведення воєн. Тепер військові операції проводяться комплексно. Кожна з ворогуючих сторін намагається завдавати своїм опонентам дошкульних ударів на різноманітних фронтах, і йдеться не лише про поле бою. Сьогодні держави ворогують між собою не тільки за допомогою збройних сил. До проведення військових операцій залучаються найрізноманітніші засоби та напрями. У часи сучасних воєн протистояння також відбувається в економічній, політичній, інформаційній сферах та багатьох інших ключових напрямах. За такий комплексний підхід сучасні війни називають гібридними [6]. Тобто війни, які носять змішаний характер, де не має чітко вираженої лінії фронту та зони бойових дій. Із розвитком технологій кожна наступна війна отримує

якісь нові напрям та забарвлення, адже прогрес приходить і на поле бою. Сьогодні, під час російсько-української війни, ми можемо вперше спостерігати активне застосування бойових дронів-безпілотників з обох сторін, ми також можемо побачити, що війна (шляхом застосування інформаційно-психологічних спецоперацій) перейшла і в інформаційне поле, зокрема у соціальні мережі. Тому всебічне дослідження сучасних воєнних конфліктів (особливо для українського суспільства) є вкрай актуальним, адже нам потрібно розуміти потенційні загрози та вміло їм протистояти.

Мета статті – крізь призму розробок українських та світових науковців, а також через емпіричні знання вивчити алгоритм інформаційних атак ворога, та розробити власну програму протидіяння агресору.

Матеріал в методи дослідження. У рамках наукової статті використовувалися такі методи дослідження, як аналіз, синтез, емпіричні знання та порівняння.

Кінцевою метою вказаного наукового дослідження має стати підготовка посібника методичних рекомендацій для пересічного споживача інформаційних послуг (користувача соціальних мереж) та, можливо, працівників спецслужб, де буде розроблено чіткий алгоритм, за допомогою якого можна буде визначити, чи поширена інформація дійсно відповідає правді, або ж визначити, чи вона є наслідком ворожої ІПСО (інформаційної психологічної спеціальної операції), або, як зазначають деякі українські дослідники, інформаційною зброєю [8].

Результати та обговорення. 20 лютого 2024 р. в Україні офіційно відзначили скорботну дату – 10-ту річницю від початку російсько-української війни, яка почалася з окупації Криму та розстрілів протестувальників на Майдані. Бойові дії тривають не тільки безпосередньо на полі бою, а й на інформаційному фронті – так звана гібридна війна [6]. Ворог намагається знищити авторитет України на міжнародній арені, поширюючи (на разі доволі успішно) інформацію, яка несе репутаційні ризики для України. Також він намагається посіяти зневіру та апатію й серед громадян України, вливаючи на те, що все більше людей перестають вірити у перемогу нашої держави на полі бою. Ворог щоразу, хвиля за хвилею, поширює усе нові етапи своїх ІПСО, намагаючись посіяти зневіру серед українців та міжнародних партнерів України [24]. Ворожа пропаганда та інформаційні атаки стосовно України не розпочалися 24 лютого 2022 р. чи на весні 2014 р. Усе це має набагато довшу історію і почало діяти набагато швидше, ніж почалися безпосередні збройні зіткнення.

Серед вітчизняних науковців, які б досліджували тему національної безпеки, крізь призму інформаційної безпеки, у першу чергу слід відзначити Ірину Боднар, Володимира Фурашева, Олександра Архипова, Сергія Лисенка та Дмитра Вєнєдєєва. Ці вітчизняні науковці розробили досить ґрунтовний теоретичний аналіз проблем національної безпеки та ведення гібридних воєн, проєктуючи їх на інформаційне поле. Ними були визначені основні проблеми, структура та методи вивчення даної проблематики.

Метою роботи є визначення специфічних аспектів застосування інструментів ворожої пропаганди та інформаційних психологічних спеціальних операцій у контексті російської гібридної агресії, а також їхнього впливу на суспільство й пересічних громадян, політику та загрозу національній безпеці.

Відповідно до даної мети, були сформовані такі завдання:

– визначення категорії «гібридна війна»;
– дослідження історії гібридних воєн;
– аналіз застосування гібридних атак та тлі російсько-української війни;
– визначення інформаційної стратегії держави під час воєнного стану.

Гібридна війна – це війна з поєднанням та застосуванням конвенційної зброї, партизанської війни, тероризму, кібервійни, торгових, патентних війн, реваншистських рухів, пропаганди, порушень прав людини, злочинів проти людяності, військових навчань, переселення,

узурпації, впливу на громадську думку, злочинних актів, цензури тощо [6] та злочинної поведінки з метою досягнення певних політичних цілей, основним інструментом яких є створення державою-агресором у державі, вибраній для агресії, внутрішніх протиріч та конфліктів із подальшим їх використанням для досягнення політичних цілей агресії, які досягаються звичайною війною.

Експерти називають гібридну війну типом конфлікту, який усе частіше буде застосовуватися у XXI ст. [7].

Методи ведення війни

Гібридна війна поєднує у собі принципово різні типи і способи ведення війни, які скоординовано застосовуються задля досягнення основних цілей [6]. Типовими компонентами гібридної війни є використання методів, що сприяють виникненню та посиленню в державі, вибраній для агресії, внутрішніх конфліктів:

– генерування внутрішніх суспільних протиріч через пропаганду з її переходом у інформаційну війну;

– проєктування і розроблення економічних проблем через економічне протистояння з переходом в економічну (торгову) війну та протидію зв'язкам країни-жертви із сусідніми країнами та країнами-партнерами;

– підтримка (фінансування й озброєння) сепаратизму та тероризму аж до актів державного тероризму; побудова псевдодержавних утворень як гібридного ідеалпроєкту державотворення;

– сприяння утворенню нерегулярних збройних (псевдовійськових) формувань (повстанців, партизан та ін.) та їх оснащення.

При цьому сторона-агресор намагається та може залишатися публічно (офіційно) непричетною до розв'язаного такого гібридного конфлікту [6].

Наприклад, у виправданні злочинних антиукраїнських дій у заяві МЗС РФ щодо подій в українському Донецьку 13 березня 2014 р. повідомлялося: «Росія усвідомлює свою відповідальність за життя «*співвітчизників*» і «*співгромадян*» в Україні і залишає за собою право на їх захист» [6], і одночасно аналогічно до еклектичних «поєднань» позицій у проєкті «російського світу» в офіційній заяві МЗС РФ використовує нечіткі терміни «співвітчизники» і «співгромадяни», «зелені чоловічки», які залишаються для влади РФ продовжувачами фактично будь-яких варіантів подальших дій.

Якщо ці методи війни виявляються справді дієвими, то держава-агресор може досягти своїх агресивних цілей та закріпити успіх, виступивши в ролі миротворця у «внутрішньому» конфлікті країни-жертви. У разі якщо ці методи виявляються малодієвими, агресор може застосувати такі методи та способи:

– інші методи ведення війни із залученням у конфлікт на своєму боці третіх країн;

– класичні прийоми ведення війни з прихованим локальним обмеженим застосуванням власних збройних сил (як це було із «зеленими чоловічками») або через неприховану агресію [7].

Науковий огляд гібридних воєн у світовій історії може включати розгляд подій, які мали характер гібридного конфлікту. Тому можна розглянути деякі ключові моменти та посилання на наукові джерела та публікації:

1. Холодна війна (1947–1991).

Гібридний характер боротьби між США та СРСР охоплював політичні тиски, ідеологічну боротьбу, конкуренцію в економічній та технологічній сферах [27].

2. Війна у В'єтнамі (1955–1975).

Використання не тільки військової сили, а й політичних впливів, дипломатії, антигероїчної пропаганди й інших вищезазначених методів, що вказує на гібридний характер конфлікту [7].

3. Інтервенція в Афганістані (1979–1989).

Сполучення військових операцій (зокрема, першої операції із захоплення президентського палацу) та впливу на місцеві політичні й етнічні групи, що свідчить про гібридний характер конфлікту.

4. Інформаційна війна в епоху Інтернету.

Зростання кількості кібератак, використання соціальних мереж та медіа для впливу на громадську думку та маніпулювання нею, використання напівправдивих новин [27].

5. Регіональні конфлікти.

Наприклад, конфлікти на Сході Європи, на Близькому Сході та в Африці, де використовуються різноманітні інструменти – від військових до економічних (торгових) і дипломатичних.

6. Сучасні приклади.

Напад росії на Грузію у 2008 р. Росія одночасно із застосуванням офіційної армії вела інформаційну, кібер- та економічні війни супроти свого відверто слабшого та набагато меншого опонента [28].

Російсько-український конфлікт (війна) починаючи з 2014 р. Цей збройний конфлікт (фактично не оголошена війна) підпадає фактично під кожен критерій ведення гібридних воєн. Тут застосовуються сепаратистські (партизанські рухи), економічний вплив (торгова блокада), ведення активної пропагандистської війни з поширенням величезної кількості неправдивих новин (зокрема, і через проплачені іноземні мас-медіа). Також у цій війні застосовуються і «союзники» агресора, які умовно належать до табору партнерів України, ну і безпосередньо пряме військове втручання із застосуванням усіх наявних в арсеналі країни-агресора засобів та сил.

Українсько-російська гібридна війна, що розпочалася в 2014 р., являє собою складний конфлікт із різними вимірами, які включають у себе військові дії, кібератаки, інформаційну війну та інші методи впливу. Ця війна визначається гібридним характером агресії, де протистояння різних видів впливу спрямоване на досягнення політичних, економічних та військових цілей.

Гібридна війна в Україні є прикладом сучасного конфлікту, де широко використовуються різноманітні методи впливу. Цей конфлікт підкреслює важливість адаптації національних та міжнародних стратегій безпеки до нових реалій глобальної політичної арени.

Гібридні війни можна вважати новим виміром сучасних конфліктів, що об'єднують у собі різноманітні військові та не військові засоби для досягнення стратегічних цілей. Основна суть цього підходу полягає у використанні широкого спектру різноманітних інструментів, таких як інформаційна війна, економічний тиск, кібератаки, дипломатія, тероризм та інші форми неласичної агресії [20].

Цей підхід стає актуальним стратегічним інструментом для багатьох країн, оскільки він дає змогу істотно впливати на політичні, економічні та соціокультурні процеси [20]. Одним із ключових аспектів є кіберпростір, де здатність до проведення атак (або ж їх відбиття) та контролю інформаційного потоку стає надзвичайно важливою. Інтенсивні та цілеспрямовані кібератаки можуть впливати на важливі інфраструктурні системи, такі як енергетика та комунікації, що призводить до значних викликів для стабільності країни [25].

Одним із найважливіших елементів гібридних воєн є використання інформаційної війни для маніпулювання громадською думкою та зміцнення внутрішньополітичних позицій. Соціальні мережі та засоби масової інформації грають ключову роль у цьому дестабілізаційному аспекті [23].

Гібридні війни не обмежені територіальними межами та можуть мати доволі широкий глобальний вплив. Однак їх використання створює нові виклики для міжнародного співтовариства, оскільки традиційні підходи до безпеки та різноманітних конфліктів можуть бути недостатніми для ефективної протидії цьому типу загроз як комплексному [26].

Згідно з різноманітними дослідженнями сучасних науковців, гібридні війни характеризуються своєрідною складністю та динамікою. Розуміння цього явища та активне вивчення є важливими завданнями для сучасних учених, політиків та практиків, оскільки вони визначають нові реалії безпеки та стабільності в глобальному світовому співтоваристві [6].

Слід зазначити, що російсько-українська гібридна війна, яка розпочалася в 2014 р., являє собою унікальний та складний конфлікт, де використовуються різні інструменти для досягнення політичних, економічних та військових цілей. За останні роки цей конфлікт став предметом інтенсивного дослідження та аналізу.

Гібридний характер конфлікту.

Українсько-російська гібридна війна включає у себе елементи збройної агресії, кібератак, дезінформації та психологічного впливу [3]. Цей комплексний підхід розкривається в різних аспектах, включаючи військові дії на значній території України, анексію Криму в 2014 р., кібератаки та інформаційно-пропагандистську війну.

Кібератаки.

Російська сторона активно використовує кібератаки для порушення функціонування державних інституцій, комунікаційних систем та енергетичних об'єктів. Ці атаки не лише завдають значних матеріальних збитків, а й створюють загрозу національній безпеці та життю людей, які перебувають на підконтрольній та непідконтрольній українському уряду українських територіях [4].

Інформаційна війна.

Одна з головних ролей у цьому гібридному конфлікті відводиться інформаційній війні та дезінформації. Російська пропаганда активно використовує мас-медіа та соціальні мережі для поширення неправдивої інформації, зміни образу подій та формування певного світогляду. Причому ворожі пропагандисти та спецслужби фактично миттєво реагують на всі внутрішні та зовнішні події у житті України. Досвідчені психологи та пропагандисти відразу запускають чергові хвилі ІПСО, «приправлені» кремлівськими наративами, щоб похитнути єдність українського суспільства та підірвати довіру до чинної влади [10].

Роль дипломатії та економічного тиску.

У гібридній стратегії російської сторони важливе місце займають дипломатія та економічний тиск. Вплив на міжнародні відносини, санкції та інші методи економічного тиску використовуються для забезпечення підтримки російських інтересів у регіоні. Через так званий «газовий шантаж» та ймовірний підкуп частини європейських політиків російська пропаганда може поширювати серед європейців свої наративи та пропаганду [4].

Результати та виклики.

Для України ця війна має і матиме в майбутньому дуже серйозні наслідки. Вона створює внутрішню нестабільність, економічні втрати (відхід інвесторів та руйнування виробничої інфраструктури) та викликає соціальні напруги, відтік населення і зокрема робочої сили, велику смертність серед військових та цивільних. Окрім того, конфлікт змінює геополітичний ландшафт регіону та ставить під загрозу безпеку всього Європейського континенту [10].

Унаслідок розв'язання росією війни (у тому числі й гібридної) відносно України наша держава отримала цілу низку складних викликів та загроз. Сюди передусім слід віднести протидію ворожим ІПСО (інформаційним психологічним спеціальним операціям), які країна-агресор уміло застосовує та успішно реалізовує на українському (і не тільки) інформаційному просторі. Це дає їй змогу дестабілізувати внутрішньополітичну ситуацію та підривати у населення довіру до уряду та віру у перемогу Збройних сил України над окупантами.

Інформаційно-психологічні операції, які активно проводяться росією, представляють серйозну загрозу для національної безпеки України. Дослідження та аналіз цілої низки найрізноманітніших наукових джерел надають інсайти та розуміння щодо характеру цих загроз

та можливих заходів для актуальної та оперативної майбутньої протидії з боку українського уряду та вітчизняних спецслужб [24].

Можемо розглянути, як саме проводяться російські ІПСО та чим керуються їхні спецслужби під час підготовки таких інформаційних «вкидів» в український та світовий інформаційний простір:

1. Маніпулювання інформацією.

Російські ІПСО активно використовують методи маніпуляції інформацією для формування певного (досить часто однобокого або ж викривленого) світогляду в громадськості [1]. Вони використовують фейкові новини, метод «напівправди», дезінформацію та деструктивні повідомлення для зміни внутрішньополітичної ситуації в Україні. Також поширенням таких фейків їхні спецслужби намагаються послабити міжнародну підтримку Києва [2].

2. Соціальні мережі та Інтернет-простір.

Російські ІПСО доволі активно використовують соціальні мережі для поширення своїх впливових (маніпулятивних) повідомлень. Вони створюють та підтримують різноманітні фейкові облікові записи, щоб впливати на громадську думку та підірвати довіру до владних структур і ЗСУ [9].

3. Використання інформаційних технологій.

Російські ІПСО ефективно використовують інформаційні технології для збору, аналізу та маніпуляції інформацією [11]. Вони використовують алгоритми та штучний інтелект, запускають різного роду популярні «флешмоби» для підвищення ефективності своїх операцій. Комплекс таких дій дає їм змогу доволі оперативно та ефективно впливати на суспільно-політичні настрої серед громадян України.

4. Психологічний вплив.

ІПСО спрямовані на психологічний вплив на населення та політичні еліти України. Вони використовують методи психологічної війни, спрямованої на створення стресу, паніки та невпевненості в суспільстві. Такі методи досить часто викликають у людей зневіру та апатію, що, власне, і ставлять собі за мету російські спецслужби та пропагандисти [13].

5. Виклики для національної безпеки.

Застосування російськими спецслужбами своїх ворожих щодо нашої держави ІПСО зумовлює важливі та складні виклики для національної безпеки України. Зокрема, це може призвести до політичної нестабільності, втрати довіри громадян до владних інституцій та загрози громадському порядку. Чим вони, власне, постійно користуються [14].

6. Заходи протидії.

Ефективна протидія загрозам від російських ІПСО вимагає комплексного підходу, який включає у себе підвищення інформаційної грамотності громадян (особливо користувачів популярних соціальних мереж), підтримку незалежних ЗМІ, та розвиток кібербезпеки [15].

На сучасному етапі доволі велика частина українців активно користується різноманітними популярними соціальними мережами, але, на жаль, не всі вони дотримуються правил інформаційної гігієни і досить часто стають жертвами маніпуляцій або впливу російських спецслужб через їхні ІПСО.

Інформаційна гігієна у соціальних мережах на сучасному етапі російсько-української гібридної війни є важливим складником для збереження безпеки та об'єктивності отриманої інформації. Користувачам необхідно дотримуватися низки правил та прийомів для уникнення ризиків інформаційної небезпеки.

1. Перевірка джерел інформації.

Перш за все слід переконатися у достовірності джерела перед тим, як ділитися чи поширювати вказану інформацію [8]. Потрібно використовувати лише визнані та авторитетні джерела та не поширювати інформацію без належної перевірки.

2. Критичне ставлення до інформації.

Потрібно розвивати критичне мислення та аналітичні навички, щоб не стати жертвою маніпуляції чи інформаційної атаки ворога. Користувач має сумніватися та перевіряти факти, особливо якщо інформація виглядає доволі сумнівно або ж її поширює невідоме джерело [12].

3. Захист своїх особистих даних.

Слід обмежити доступ до особистої інформації, установити приватні налаштування у власному акаунті та уникати розміщення важливих особистих даних у соціальних мережах для запобігання їх несанкціонованому витоку [16].

4. Виявляти та ізолювати дезінформацію.

Потрібно піддавати сумніву інформацію, яка виглядає підозріло і неправдиво. Якщо користувач не впевнений в її правдивості, слід перш за все уникати її подальшому поширенню серед інших користувачів [17].

5. Підтримання інформаційної грамотності.

Користувачам соцмереж рекомендовано брати участь у навчаннях та інформаційних кампаніях, спрямованих на підвищення рівня інформаційної грамотності та обізнаності [18]. Розуміння основ медіа та Інтернет-аналізу допоможе користувачам соціальних мереж легше розрізняти правдиву інформацію від дезінформації (фейків).

На нинішньому активному етапі російсько-української гібридної війни Україні слід активно протидіяти загрозам та викликам, зумовленим впливами ворожих інформаційно-психологічних інформацій, щоб запобігти їхньому деморалізуючому впливу на своїх громадян. Робота щодо такої протидії дасть змогу зберігати стабільність на суспільно-політичному полі всередині країни, навіть незважаючи на активну фазу війни та постійну роботу ворожих спецслужб та пропагандистів.

Для цього рекомендовано зробити такі кроки:

1. Використання технологій ідентифікації дезінформації.

Упровадження технологій штучного інтелекту та аналізу даних для виявлення та припинення поширення дезінформації у соціальних мережах. Також слід проводити постійний моніторинг популярних соціальних мереж на предмет поширення там ворожих наративів та ІПСО. Окрім того, за можливості слід створювати спеціальні професійні підрозділи для боротьби з дезінформацією у державних спецслужбах (перед тим провівши ґрунтовне і різнопланове навчання для їхніх майбутніх працівників, а не робити звичайний перевід фахівців з одного відділу в інший, як це доволі часто робилося раніше) [19].

2. Збільшення обізнаності громадськості.

Проведення інформаційних кампаній та тренінгів, що спрямовані на підвищення обізнаності громадян (зокрема, користувачів соціальних мереж) стосовно методів та способів розпізнавання та запобігання дезінформації [21].

3. Активна участь у громадських обговореннях.

Слід сприяти формуванню критичного суспільного дискурсу стосовно інформаційної безпеки та спільної боротьби з дезінформацією. Громадськість має розуміти мету, ціль і способи такої інформаційної боротьби [22].

4. Зміцнення і зміна чинного законодавства.

Має бути розроблено та впроваджено ефективне законодавство (яке відповідає світовим нормам та практиці), спрямоване на протидію дезінформації та інформаційним кампаніям інших країн, передусім росії [24].

5. Міжнародна співпраця.

Повинна відбуватися постійна взаємодія України з іншими країнами та міжнародними організаціями для якісного і системного розроблення й упровадження спільних стратегій щодо повсякчасної протидії дезінформації [15].

Висновки. Інформаційна гігієна та активна боротьба з дезінформацією вимагають спільних зусиль громадян, влади та міжнародної спільноти для забезпечення безпеки та об'єктивності інформації у соціальних мережах. Це складний та тривалий шлях, але в умовах сучасної війни його слід пройти, адже це дасть змогу забезпечити стабільне інформаційне поле без ворожого впливу на громадян України.

Література:

1. Авер'янова Н.М. Гібридна війна: російсько-українське протистояння. *Молодий вчений. 3* (2017): 30–34.
2. Арабаджиєв, Д.Ю., Сергієнко Т.І Маніпулювання свідомістю суспільства в умовах інформаційної та гібридної війни в Україні. *Гілея.* 146 (3) (2019): 12–15.
3. Алещенко, В. Феноменологія гібридної війни та її особливості у виконанні російської федерації: інформаційно-психологічний аспект. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки»* 1 (2016): 6–11.
4. Бартош Н.В. Актуальні питання удосконалення реалізації державної інформаційної політики України в умовах гібридної війни. *Публічне урядування* 3 (28) (2021): 17–24.
5. Бєльська Т.В. *Збірник Національного університету цивільного захисту України* (2019): 3–11.
6. Вєдєнєєв Д.В., Семенюк О.Г. Формування концептуальних та функціональних передумов гібридної конфліктності як загрози національній безпеці України: ретроспективний аналіз : монографія. Київ : ДП «ІНФОТЕХ», 2020. 274 с.
7. Вєдєнєєв Д., Сегеда С. Історико-теоретичні витоки поглядів на сутність війн (конфліктів) неконвенційного концептуального типу (1970-ті – початок 2000-х рр.). *Воєнно-історичний вісник* (2022)1: 161–181.
8. Войтович Н. Розвиток навичок критичного мислення та медіаграмотності у населення як спосіб протидії російській агресії в інформаційній війні. *Журналістика майбутнього: виклики, тенденції, перспективи* (2022): 297.
9. Войтко О.В., Солонніков В.Г. Державна інформаційна політика основа забезпечення інформаційної безпеки в умовах гібридної війни. *Актуальні проблеми управління інформаційною безпекою держави* (2021):19.
10. Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). 2020.
11. Горбулін В.П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. *Стратегічні пріоритети 4.33* (2014): 5–12.
12. Даценко А. Протидія дезінформаційним кампаніям в умовах гібридної війни. *Україна в умовах трансформації міжнародної системи* (2019): 141.
13. Жадько В.О. та ін. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник. (2018).
14. Загуменна, Ю.О., Расторгуєва Н.О. Проблеми забезпечення інформаційної безпеки в умовах глобалізації та гібридної війни проти України. *Харківський національний університет внутрішніх справ: 25 років досвіду та погляд у майбутнє (1994–2019 рр.)* : зб. тез доп. Міжнар. наук.-практ. конф. до 25-річчя створення ун-ту, м. Харків, 22 листопада 2019 р. Харків, 2019. С. 180–181.
15. Іванова В. Трансформація інформаційно-психологічних операцій Російської Федерації з початком повномасштабної агресії проти України. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи* : IV міжнар. наук.-практ. конф. 2023.
16. Іванова Н.Г., Андрусишин Ю.І., Паливода О.О. Захист від негативних інформаційно-психологічних впливів в умовах гібридної війни. *Інформаційна безпека людини, суспільства, держави* 1–3 (28–30) (2020): 76–82.
17. Люля В.С., Огінська М.М. Забезпечення інформаційної безпеки в соціальних мережах. *Актуальні проблеми управління інформаційною безпекою держави* (2019): 321.
18. Мануйлов Є.М., Прудникова О.В. Інформаційно-культурна безпека України в умовах «гібридної війни». *Вісник НЮУ імені Ярослава Мудрого. Серія «Філософія, філософія права, політологія, соціологія» 1.32* (2017): 26–36.

19.Мехед Д., Мехед Д. Інформаційна безпека в соціальних мережах. Методи поширення інформації в соціальних мережах. (2015).

20.Митко А.М., Кольцова І.І. Інформаційний тероризм як інструмент впливу на інформаційний конформізм в глобальному середовищі. *Політичне життя 2* (2018): 135–139.

21.Пасічний Р. Медіаграмотність як чинник протистояння ворожим інформаційно-психологічним операціям. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи :* IV міжнар. наук.-практ. конф. 2023.

22.Пилипчук В.Г. Забезпечення інформаційної безпеки України: сучасні тенденції та проблеми. *Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти : матеріали наук.-практ. конф*. Vol. 6. 2016.

23.Проноза І.І., Проноза І.І. *Інформаційна війна: сутність та особливості прояву*. (2018).

24.Шульська Н.М., Зінчук Р.С., Кевлюк І.В. Наративи формування зневіри як вияв ворожої інформаційно-асихологічної операції: на матеріалі мови ЗМІ. *Вчені записки* (2023):152.

25.Anghel, Iulia. *Social Media as Hybrid Warfare Tool–Putting Russia's Informational Strategy in Context. Romanian Military Thinking 1.*1 (2020): 62–81. (6)

26.Aslam, Shahbaz, Noor Hayat, and Arshad Ali. *Hybrid warfare and social media: need and scope of digital literacy. Indian Journal of Science and Technology 13.12 (2020)*: 1293–1299. (8)

27.Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and national security. Potomac Books*, Inc., 2009.

28.Yanchenko, Kostiantyn, et al. *Repressed Opposition Media or Tools of Hybrid Warfare?* Negotiating the Boundaries of Legitimate Journalism in Ukraine Prior to Russia's Full-Scale Invasion. *The International Journal of Press/Politics* (2023).

References:

1. Averyanova, N.M. «Hybrid War: Russian-Ukrainian Confrontation.» *Young Scientist 3* (2017): 30–34. [in Ukrainian]

2. Arabadzhiev, D.Yu., and T.I. Sergienko. «Manipulation of Public Consciousness in Conditions of Information and Hybrid War in Ukraine.» *Hileya: Scientific Herald 146 (3)* (2019): 12–15. [in Ukrainian]

3. Aleschenko, V. «Phenomenology of Hybrid War and Its Features in the Performance of the Russian Federation: Information-Psychological Aspect.» *Bulletin of Kyiv National University named after Taras Shevchenko. Military-Special Sciences 1* (2016): 6–11. [in Ukrainian]

4. Bartosh, Natalia Volodymyrivna. «Current Issues in Improving the Implementation of State Information Policy of Ukraine in Conditions of Hybrid War.» *Public Administration 3 (28)* (2021): 17–24. [in Ukrainian]

5. Bielska T.V., Collection of the National University of Civil Protection of Ukraine (2019), pp. 3–11. [in Ukrainian]

6. Vedeneev, D.V., Semenyuk, O.G. «Formation of Conceptual and Functional Preconditions of Hybrid Conflict as a Threat to National Security of Ukraine: Retrospective Analysis.» *Monograph*, Kyiv: State Enterprise «INFOTECH,» 2020. – 274 p. [in Ukrainian]

7. Vedeneev, D., Segeda, S. «Historical and Theoretical Origins of Views on the Essence of Wars (Conflicts) of an Unconventional Conceptual Type (1970s – early 2000s).» *Military-Historical Bulletin 2022. № 1* P. 161–181. [in Ukrainian]

8. Voytovich, Natalia. «Development of Critical Thinking and Media Literacy Skills in the Population as a Way to Counter Russian Aggression in Information War.» *Journalism of the Future: Challenges, Trends, Perspectives (2022)*: 297. [in Ukrainian]

9. Voytko, O.V., and V.G. Solonnikov. «State Information Policy as the Basis for Ensuring Information Security in Conditions of Hybrid War.» *Actual Problems of Information Security Management (2021)*: 19. [in Ukrainian]

10.Voytsohovsky, Andriy V. «Information Security as a Component of the National Security System (International and Foreign Experience) (2020).» [in Ukrainian]

11.Horbulin, Volodymyr Pavlovych. «Hybrid War as a Key Instrument of Russian Geostrategy of Revenge.» *Strategic Priorities 4.33* (2014): 5–12. [in Ukrainian]

12.Datsenko, Alina. «Resistance to Disinformation Campaigns in Conditions of Hybrid War.» *Ukraine in the Context of International System Transformation (2019)*: 141. [in Ukrainian]

13.Zhadko, Victor Oleksiyovych, et al. «Problems of Ensuring Information Security in the Conditions of Globalization and Hybrid War Against Ukraine.» *Kharkiv National University of Internal Affairs: 25 Years of Experience and Outlook for the Future (1994–2019)*: Collection of Abstracts for the Int. Sci.-Pract. Conf. on the 25th Anniversary of the University (Kharkiv, November 22, 2019). – Kharkiv, 2019. – P. 180–181. [in Ukrainian]

14.Zahumenna, Yu.O., and N.O. Rastorgueva. «Issues of Ensuring Information Security in the Conditions of Globalization and Hybrid War Against Ukraine.» *Kharkiv National University of Internal Affairs: 25 Years of Experience and Outlook for the Future (1994–2019): Collection of Theses for the Int. Sci.-Pract. Conf. on the 25th Anniversary of the University (Kharkiv, November 22, 2019). – Kharkiv, 2019. – P. 180–181.*, 2019. [in Ukrainian]

15.Ivanova, Victoria. «Transformation of Information-Psychological Operations of the Russian Federation with the Onset of Full-Scale Aggression against Ukraine.» *Strategic Communications in the Sphere of Ensuring National Security and Defense: Problems, Experience, Prospects (IV Int. Sci.-Pract. Conf. 2023)*. [in Ukrainian]

16.Ivanova, Natalia Georgiyivna, Julia Ivanivna Andrusyshyn, and Olga Oleksandrivna Palivoda. «Protection Against Negative Information-Psychological Influences in Conditions of Hybrid War.» *Information Security of the Individual, Society, State 1–3 (28–30) (2020)*: 76–82. [in Ukrainian]

17.Lyulya, V.S., and M.M. Oginska. «Ensuring Information Security in Social Networks.» *Actual Problems of Information Security Management (2019)*: 321. [in Ukrainian]

18.Manylov, Ye. M., and O. V. Prudnikova. «Information-Cultural Security of Ukraine in Conditions of 'Hybrid War'». *Scientific Notes: 2023* p. 152. [in Ukrainian]

19.Mehed, Dmitro, and Dmitry Mehed. «Information Security in Social Networks. Methods of Information Dissemination in Social Networks (2015)». [in Ukrainian]

20.Mytko, A.M., Koltsova I.I. «Information Terrorism as a Tool of Influence on Information Conformism in the Global Environment.» *Political Life 2* (2018): 135–139. [in Ukrainian]

21.Pasichny, Roman. «Media Literacy as a Factor of Resistance to Enemy Information-Psychological Operations.» *Strategic Communications in the Sphere of Ensuring National Security and Defense: Problems, Experience, Prospects (IV Int. Sci.-Pract. Conf. 2023)*. [in Ukrainian]

22.Pylypchuk, V.G. «Ensuring Information Security of Ukraine: Current Trends and Issues.» *Prevention of New Challenges and Threats to Information Security of Ukraine: Legal Aspects Vol. 6* (2016). [in Ukrainian]

23.Pronoza, Inna Ivanivna, I.I. Pronoza, and Inna Ivanovna Pronoza. «Information War: Essence and Features of Manifestation (2018).» [in Ukrainian]

24.Shulska, N.M., R.S. Zinchuk, Kevlyuk I.V. «Narratives of Creating Distrust as a Manifestation of Enemy Information-Psychological Operation: Based on Media Language.» *Scientific Notes: 2023* p. 152. [in Ukrainian]

25.Anghel, Iulia. «Social Media as Hybrid Warfare Tool–Putting Russia's Informational Strategy in Context.» *Romanian Military Thinking 1.1 (2020)*: 62–81. [in Ukrainian]

26.Aslam, Shahbaz, Noor Hayat, and Arshad Ali. «Hybrid Warfare and Social Media: Need and Scope of Digital Literacy.» *Indian Journal of Science and Technology 13.12 (2020)*: 1293–1299. [in Ukrainian]

27.Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Potomac Books, Inc., 2009. [in Ukrainian]

28.Yanchenko, Kostiantyn, et al. Repressed Opposition Media or Tools of Hybrid Warfare? Negotiating the Boundaries of Legitimate Journalism in Ukraine Prior to Russia's Full-Scale Invasion. *The International Journal of Press/Politics (2023)*. [in Ukrainian]

Mykhailo Savliuk. Hybrid warfare in Ukraine: contemporary approaches

With the rapid development of computer (and not only) technologies, humanity has been progressing rapidly on all fronts. The theater of military operations is no exception, where hybrid warfare is taking on new dimensions and spreading to previously unexplored directions.

Taking the example of the Russo-Ukrainian war and analyzing its genesis, it becomes clear that it started long before the active phase in 2014. This unquestionably hybrid war was preceded by years of informational, cultural, and economic expansion. Russian television channels and other mass media continuously operated in Ukraine, broadcasting pro-Kremlin narratives to Ukrainians in practically a 24/7 mode, portraying «brotherly nations,» a shared history, and culture. Russian popular artists and musicians freely performed in Ukraine, and powerful Russian companies effortlessly bought and absorbed less economically developed Ukrainian businesses. Alongside trade and gas «wars,» this all contributed to the hybrid war against Ukraine since the 1990s and the early 2000s. This complex set the groundwork for what we all witnessed during the «anti-Maidan» in 2013 and in Donbas in 2014.

After the armed conflict started in Donbas, Ukraine banned the entry of notorious Russian artists who supported the occupation of Crimea and armed intervention in Donetsk and Luhansk regions. Furthermore, in 2017, Ukrainian authorities banned Russian social networks «Odnoklassniki» and «VKontakte,» along with several Russian TV channels. However, after the beginning of full-scale war, Russian information intervention took on new dimensions.

Currently, numerous and powerful bot farms are working against Ukraine and its allies, carrying out precise information attacks in sensitive areas. They deliberately provoke internal conflicts, sow distrust and disillusionment among ordinary citizens towards Ukrainian authorities and the government.

Now more than ever, the issue of researching threats to our national security through the lens of social networks is crucial. It is essential to study the psychological impact of enemy propaganda on users and develop tools to combat hostile narratives. Algorithms and methodological materials need to be designed and researched to neutralize the work of enemy bot farms and developers of information psychological special operations. With each passing day, enemy propaganda becomes more powerful, posing a direct threat to the National Security of Ukraine

Key words: *social networks, information security, national security, Facebook, propaganda, hybrid warfare, war.*