

Чупіс Анастасія Дмитрівна

Вепонізація інформації як технологія російсько-української війни

УДК 327

DOI <https://doi.org/10.24195/2414-9616.2024-2.28>

Чупіс Анастасія Дмитрівна
аспірантка кафедри політології
Запорізького національного
університету
вул. Жуковського, 66,
Запоріжжя, Україна;
гостьова дослідниця школи
соціальних наук
Університету Сьодерторна
алея Нобеля, 7, Стокгольм, Швеція
ORCID: 0000-0002-3091-3332

Стаття аналізує сучасний контекст військового протистояння як конфронтації демократії та авторитаризму, зокрема на прикладі сучасної війни Російської Федерації проти України. Висвітлюється перетворення демократичних цінностей, таких як свобода слова та доступ до інформації, на об'єкт політичної та військової маніпуляції, що створює загрози для сталого функціонування демократичних інститутів. Аналізуються психологічні та когнітивні стратегії ведення війни, які застосовуються Російською Федерацією у контексті гібридної війни проти України. Звертається увага на використання інформаційних технологій у військових операціях та їх вплив на сучасну геополітичну ситуацію. Крім того, розглядається поява нових термінів, які використовуються для опису та аналізу таких явищ, як «когнітивна війна» та «вепонізація», які стають ключовими концепціями у розумінні сучасних конфліктів. Метою є аналіз процесів трансформації інформації в інструмент когнітивних та психологічних військових операцій, зокрема в контексті конфлікту між Російською Федерацією та Україною. Завдання дослідження включає аналіз каналів поширення інформації, її технічної складової та впливу на сучасні військові стратегії. У процесі дослідження використовувалися методи та концептуального аналізу, зокрема фреймовий метод, а також контент-аналіз наративів, що використовуються Російською Федерацією для проведення психологічних та когнітивних операцій у військовому конфлікті з Україною. Як результат дослідження пропонується багаторівневий концепт «вепонізації інформації» як широкий термін, що охоплює різноманітні методи психологічної та когнітивної війни, зокрема пропаганду, дезінформацію, інформаційно-психологічні операції (ІПСО) та генерацію та поширення фейків.

Ключові слова: вепонізація інформації, психологічна війна, когнітивна війна, Росія, Україна, дезінформація, пропаганда, технологія.

Вступ. Війни 21 століття – війни «нових» поколінь все більше стають війнами проти демократії та демократичних цінностей, де самі ці цінності перетворюються на політичну та військову технологію, набуваючи рис зброї. У цьому контексті однією з ахіллесових п'ят демократії може бути така базова для неї цінність, як свобода слова та відкритість інформації. Через складність модерації величезного потоку інформації, а також верифікації вірогідності інформації, її джерел, неприйнятності в обмеженні поширення будь-якої інформації у демократичних суспільствах використання інформації з пропагандистською або дезінформаційною метою стає достатньо простою задачею.

Росія веде проти України не просто загарбницьку війну за території та ресурси, але й війну психологічну та когнітивну. Психологічна війна передбачає сплановане використання пропаганди та інших психологічних операцій для впливу на думки, емоції, ставлення та поведінку опозиційних груп, в той час, як когнітивна війна включає дії, що проводяться синхронно з іншими інструментами сили, щоб вплинути на ставлення та поведінку, впливаючи, захищаючи або порушуючи когнітивні здібності особи, групи чи населення, щоб отримати перевагу над супротивником [13]. Використання інформаційних матеріалів, джерел, каналів передачі інформації у військових цілях задля досягнення військово-політичних цілей є однією з базових складових у веденні такого типу військових операцій.

Мета та завдання. Аналіз вепонізації інформації як комплексного процесу її перетворення на зброю когнітивних та психологічних військових операцій.

Методи дослідження. В процесі дослідження було застосовано концептуальний аналіз, зокрема, фреймовий метод. А також контент-аналіз наративів, що створюються РФ для здійснення психологічних та когнітивних операцій, як частини комплексу військових дій проти України.

Результати. Результати. Використання інформації та інформаційних технологій у війнах не є ноу-хау, а тим паче винаходом виключно Росії. Такі методи ведення війни й раніше застосовувалися у військових та збройних конфліктах різних поколінь. Найяскравішими, але сумнозвісними віхами історії, в яких ми можемо побачити успіх використання психологічних та когнітивних методів ведення війни стали геноциди часів 2 Світової війни, геноцид тутсі в Руанді, а також етнічні чистки населення у війнах Балканського регіону. Ці кейси використання інструментарію когнітивних та психологічних війн, а також геноцидний характер мети їх застосування, характерні й для війни РФ проти українського народу. Однак терміни, якими вчені почали позначати такі методи, є достатньо новими. 2017 роком датують появу одразу двох нових термінів, які описують феномени, що існували й до цього, але не були масово поширеними. Це вищезгаданий термін «когнітивна війна» та термін «вепонізація», про що

свідчить дослідження американського соціолога Грегора Меттсона [12].

Оксфордський словник надає нам визначення вепонізації як акту створення чогось придатного для використання як зброї [15]. А за словником Мерріам-Вебстер дієслово вепонізувати означає адаптувати будь-що для використання як зброї у війні [17]. Технологія озброєння або вепонізації інформації вже не один рік слугує російській армії та політичним силам РФ у війні проти України та в дипломатичному протистоянні РФ з країнами Заходу.

Вепонізована інформація, за визначенням відомої американської експертки у сфері інформаційних технологій Маргарет Роуз, – це повідомлення або частина його вмісту, яке розроблене, щоб вплинути на сприйняття одержувачем чогось викривленого та неправдивого за вірогідне [16].

На наш погляд, цей термін дещо співзвучний з терміном дезінформації. Тому, ґрунтуючись на зібраному та проаналізованому матеріалі, вважаємо доречним уточнити це визначення та сформулювати його так: вепонізація інформації – це використання будь-якого виду інформації – знань, фактів, великих масивів даних, – які можуть містити ці знання, а також каналів їх зберігання, обробки та комунікації, як цифрових, так і технічних задля свідомого маніпулятивного вираження даних, їх нецільового використання, або обмеження доступу до них.

Для ілюстрації цього терміну пояснимо нашу концепцію більш детально та з прикладами російських технологій, що вона використовує в ході війни проти України та виокремимо три головних рівні цього феномену:

– вепонізація безпосередньо інформаційних повідомлень та знань;

– вепонізація технологічна – каналів поширення та зберігання інформації;

– вепонізація технічних пристроїв та інформаційних технологій.

Феномен вепонізації інформації є ширшим, таким, що позначає сам процес використання методів пропаганди, дезінформації, ІПСО та інших когнітивних та психологічних маніпуляцій, направлених на досягнення певних політичних або військових цілей.

До першого рівня вепонізації інформації ми пропонуємо віднести будь-яке намірене викривлення фактологічної інформації, використання частин інформації у відриві від основного контексту, створення та запуск в медійне поле фейкової інформації, а також формування вакуумів навколо поширення інформації про певні події або явища.

Також до одного з методів, характерних саме для російської інформаційної війни, можна віднести фальшування історії та її переписування. Особливо яскравим цей факт став на тлі тимчасової окупації Донецької, Луганської, Херсонської та Запорізької областей, а також АР Крим, де Центром національного спротиву та місцевими анонімними волонтерами неодноразово було зафіксовано факти вилучення як дитячої шкільної, так і класичної та сучасної української літератури та формування списків «заборонених» українських творів [4].

У 2022 році Росія витратила на пропаганду 1,9 млрд доларів при 1,5 млрд доларів, що були першопочатково закладеними в бюджеті [6]. З 2022 року Росія перестала публікувати доку-



Мал. 1. Схема рівнів вепонізації інформації

менти щодо державних видатків, тому проаналізувати офіційні цифри, які явно менші за фактичні витрати на ведення когнітивної війни та здійснення психологічних операцій, не є можливим. За даними ГУР МО України у 2023 році РФ витратила пів мільярда доларів на виготовлення пропагандистських матеріалів так званими «некомерційними організаціями». Також у повідомленні ГУР говориться, що збільшення фінансових витрат на приховану пропаганду для внутрішньої аудиторії може індикативно свідчити про два феномени: по-перше, може вказувати на зниження рівня довіри до офіційних традиційних медіа держави-агресора серед населення; по-друге, це може бути спробою путінської диктатури здійснити контроль над інтернет-середовищем у межах Російської Федерації [10].

Другий – технологічний рівень, що окреслює феномен вепонізації каналів комунікації. На цьому рівні важливо зазначити й намагання РФ утримувати Україну у своєму інформаційному та медійному полі, а також і поширеність використання електронних пошт з доменом «ру» в Україні, включення російського телебачення до пакетів супутникового телебачення, використання російських соціальних мереж «VK», «Однокласники» та месенджера «Телеграм». 22 травня 2017 року, згідно з відповідним указом президента України було заблоковано соцмережі «ВКонтакте», «Однокласники» та інші російські ресурси на території України. Під санкційний лист цього указу попали також сервіси «Яндекс», «Mail.Ru Group», сайти антивірусних компаній «Лабораторія Касперського» і «DrWeb».

Наразі в Україні відбувається публічна та парламентсько-урядова дискусія щодо можливої заборони месенджера Телеграм в Україні, який з початком повномасштабного вторгнення став одним з головних каналів отримання оперативних новин. Аудиторія українського сегмента Telegram суттєво зросла після російського повномасштабного вторгнення. За результатами соціологічного опитування, проведеного КМІС у грудні 2022 року на замовлення Українського інституту медіа та комунікації, 63,3% українців почали читати телеграм-канали для отримання новин саме після 24 лютого 2022 року, тоді як до повномасштабного вторгнення таких було лише 35,9% [1; 4].

Також Росія активно фінансувала цілу мережу проросійських телеканалів в Україні, таких як «Наш», «ZIK», «NewsOne», «Перший незалежний», «112», а також інтернет-видання «strana.ua», «vesti.ua» тощо. Говорячи про спроби впливу Росії на закордонну аудиторію не можна не згадати діяльність російських пропагандистських медіа: «Sputnik», «RussiaToday», «Ria Novosti», «LifeNews». Станом на початок 2022 року шість країн Європи повністю вимкнули зі свого ефіру

російські пропагандистські канали, ще 24 країни частково відмовились від російського телебачення, зокрема заборонили канали «Russia Today» і «Sputnik» [2].

Окремо в цьому блоці також треба згадати діяльність ботоферм або фабрик тролів. Мабуть, найвідомішою є діяльність Ольгіно або Агентства інтернет-досліджень, діяльністю яких керував одіозний російський воєнний злочинець глава ПВК «Вагнер» Євгеній Пригожин. Інтерв'ю про діяльність та вплив такої фабрики увійшло у книгу британського журналіста та медіаексперта Пітера Помаранцева «Це не пропаганда», де він у публіцистичному стилі детально аналізує та розповідає, як дезінформація та пропаганда створюється та поширюється світом [14; 19-29].

Фабрики тролів являють собою спеціалізовані офісні структури, де наймані користувачі-провокатори, відомі як тролі, за отриману винагороду здійснюють публікації та коментарі під новинами інтернет-видань або на інших ресурсах у мережі. Головною метою їхньої діяльності є поширення російської пропаганди в соціальних мережах, маніпулювання громадською думкою та підвищення напруги в інтернет-конфліктах, в соціальних мережах, маніпуляцій громадською думкою та ескалації інтернет-конфліктів.

Необхідно зазначити й про спроби використання ШІ в ході війни РФ проти України. Так, експерт з інформаційної безпеки та дезінформації, экс-заступник міністра з питань інформаційної політики Дмитро Золотухін звертав увагу експертного середовища на можливе використання цієї технології для продукування коментарів ботами у Фейсбук. Також неодноразово в інформаційному просторі з'являлися відео із застосуванням технології deep fake, метою яких була дискредитація вищого політичного та військового керівництва України: В. Зеленського, О. Данілова, В. Залужного.

Один з неочевидних, але перспективних каналів для розповсюдження російської пропаганди, полягає в ігровій індустрії, зокрема у відеоіграх. Деякі розробники комп'ютерних ігор у Росії залучають фінансування від владних структур, включаючи Кремль, партію «Єдина Росія» та компанію «Газпром». Ці кошти використовуються для створення віртуальних світів, де відтворюються стереотипи російської пропаганди. Наприклад, у грі «Майдан. Ru», розробленій в Україні під час Євромайдану, Україну зображено як поліцейську державу, порушену «громадянською війною», де відсутній президент і уряд, а панує загальний хаос і анархія.

Напередодні першої річниці повномасштабного вторгнення Росії до України в Росії відбувся реліз нової гри «Atomic Heart», яка у стилі ретро-футуризму. Розробники, наочно позиціонуючи гру як продукт у стилі СРСР, здійснили спробу впровадити

кремлівську пропаганду та стереотипні образи, які висміюють українську культуру. У своєму дослідженні щодо взаємозв'язку між пропагандою та її просуванні у відеоіграх експерт ГО Детектор медіа приходиться до таких висновків, що відеоігровий світ може впливати на уявлення людей, формуючи конкретні уявлення та вкладаючи у свідомість певні повідомлення. Таким чином, російські та інші ігри пропонують альтернативну реальність, спотворюючи факти й презентуючи їх як правдиві. Гравці можуть запам'ятовувати конкретні сценарії та події та сприймати їх як реальні, не відрізняючи від реального життя. Занурення у сюжет є ключовим аспектом більшості віртуальних продуктів, і ті, хто мають інтерес у перетворенні відеоігор на інструмент пропаганди, використовують цей ефект. В деяких випадках вплив пропаганди через відеоігри може навіть перевищувати вплив традиційних медіа, оскільки під час гри людина не просто бачить та чує, але й відчуває, переживає та приймає рішення, впливаючи на її власний унікальний досвід [8].

До третього рівня вепонізації варто віднести цілеспрямовані збройні атаки на телекомунікаційну інфраструктуру в Україні. За допомогою встановлення технічних пристроїв або завдяки виведенню їх з ладу Росія формує власне інформаційне поле, або навпаки інформаційний вакуум на певних територіях. Ця тактика не є новою, адже від самого початку війни РФ проти України у 2014 році Росія одночасно розпочала дії спрямовані на обмеження українського медійного поля та доступ до українського контенту на тимчасово окупованих територіях. РФ здійснювалось заглушення як телевізійного, так і радіомовлення з підконтрольної українському уряду територій, а також технічний доступ до українського стільникового зв'язку та мережі Інтернет.

За даними Інституту масової інформації за період з 22 лютого 2022 року і до березня 2024 року Росія здійснила 18 збройних атак на телевежі України з метою блокування українського мовлення та створення інформаційного вакууму на її території [9]. Остання 19-та атака відбулася 22 квітня 2024 року, в результаті якої було пошкоджено Харківську телевізійну вежу.

До цього блоку доречно віднести DDoS атаки, які масово відбуваються як проти урядових, так і проти сайтів бізнесу, приватних та корпоративних електронних пошт українських громадян. Команда реагування на надзвичайні ситуації, пов'язані з комп'ютерами в Україні (CERT-UA), зафіксувала майже 4 000 кіберінцидентів у період з січня 2022 року по вересень 2023 року. Це втричі більше, ніж у довоєнний період [7]. Кібератаки проти урядових сервісів передували безпосередньо повномасштабному вторгненню.

У грудні 2023 року в результаті однієї з наймасштабніших кібератак РФ стався масштабний збій

та на декілька днів повністю паралізовано діяльність роботи найбільшого в Україні оператора зв'язку «Київстар». У всій країні 24 мільйони абонентів оператора мобільного зв'язку «Київстар» стикнулися з відсутністю мобільного зв'язку та доступу до Інтернету. Крім того, користувачі не могли здійснювати перехід до мереж інших операторів в межах внутрішньоукраїнського роумінгу. Неполадки виникли на всьому обладнанні, яке використовувало зв'язок оператора «Київстар», що призвело до серйозних інфраструктурних проблем по всій Україні [4].

Окрім вепонізації інформації слід виокремити такі сфери, де РФ використовує цю тактику: вепонізація міграції; вепонізація енергетики, в тому числі атомної; вепонізація продовольчого та екологічного питань; вепонізація культури та мови; вепонізація спорту і звісно вепонізація дипломатії на прикладі паралізації діяльності таких міжнародних організацій гарантів колективної безпеки як ООН, ОБСЄ та інші. Цей перелік не є вичерпним і може бути доповненим. Є можливим прослідкувати й кореляцію цих феноменів. Так, міграційна криза, що була зрежисована Білоруссю за підтримки Росії на кордоні з країнами ЄС, мала на меті відвернути увагу посадовців ЄС від підготовки та концентрації російських військ на прикордонних територіях Білорусі, Росії та підготовку до повномасштабного наступу на Україну з цих територій.

Захоплення на початку повномасштабного вторгнення та розміщення військової техніки РФ на територіях Чорнобильської атомної станції, ЗАЕС, а також систематичні атаки місцевостей навколо інших атомних станцій, є одним з приводів для методичного психологічного тиску на громадян України та важелем тиску на світову спільноту щодо можливого терористичного акту на цих об'єктах задля використання «мирної» атомної енергетики у вигляді «брудної атомної бомби».

Вепонізація питання світової продовольчої кризи зі сторони російської федерації відбувається з початку повномасштабного вторгнення з атакою на портову інфраструктуру, окупацію частин приморських територій акваторії Азовського моря, що спричинило зростання вартості зернових на світовому ринку, а також складності з логістикою зерна до африканських країн. Продовження «зернового питання» відбувається прямо зараз, але вже на суходолі з блокуванням транзиту українського зерна територіями країн-сусідок, де OSINT-експертами вже було знайдено російський слід [3].

У своїй книзі «The Weaponisation of Everything» («Вепонізація будь-чого») британський політолог, професор Університетського коледжу Лондона Марк Галеотті висловлює думку, що в сучасному світі як зброю можна використати в прямому сенсі будь-що від інформації до сутичок футбольних фанів. Він також пропонує міждисциплінарний

погляд на появу майбутніх воєн і конфліктів, адже вони вже давно перестали бути справою суто військових [11].

Висновки. Усі три представлені рівні вепонізації інформації є взаємозалежними та можуть використовуватися як разом, так і окремо. Взаємозв'язок між вепонізацією інформаційної сфери з іншими сферами уможливорює перетворення їх у негативно забарвлені новинні повідомлення задля досягнення прагматичних політичних та військових цілей. В умовах сучасних когнітивних та психологічних війн, в межах яких реалізується вепонізація інформації, цей процес актуалізує такі ризики:

- руйнування довіри громадян до держави та політикуму і військового керівництва України;
- підриг національної політики, економіки, а також сфери державної безпеки;
- поляризація громадської думки та маніпуляція свідомістю громадян України, моральне та емоційне виснаження;
- ескалація різних груп суспільства як всередині України, так і вплив на геополітичну суб'єктність України та її співпрацю з закордонними партнерами й т.д.

Україна потребує ґрунтовної реформи та посилення спроможностей вже створених інституцій у сфері інформаційної безпеки та протидії дезінформації, пропаганді та інформаційним атакам в межах когнітивних та психологічних операцій. Нагальним є формування державної стратегії у цій сфері та проактивна, а не реактивна політика протистояння інформаційним викликам. Цей процес має супроводжуватися активним залученням експертного та фахового академічного середовища та наукових розвідок, як українських вчених, так і через створення міжнародних експертних груп та проєктів з представниками закордонних дослідницьких інституцій та академічних установ задля обміну такого вітального для всіх нас та колективної безпеки досвіду.

ЛІТЕРАТУРА:

1. Дуцик, Д. (2023). Як функціонують та завойовують аудиторію неінституціоналізовані новинні телеграм-канали українського сегменту. Аналітичний звіт. Київ: ГО «Український інститут медіа та комунікації». 68 с.
2. Извошкіова, А. (2022). 30 європейських країн повністю або частково вимкнули російські пропагандистські канали. Суспільне новини. – Режим доступу: <https://suspijne.media/222648-30-evropejskih-krain-povnistu-abo-castkovo-vimknuli-rosijski-propagandistski-kanali/>
3. Міхальков, С. (2024). Рупор російської пропаганди в Польщі став голосом протесту фермерів. Texty.org. – Режим доступу: <https://texty.org.ua/articles/111765/rupor-rosijskoji-propahandy-u-polshistav-holosom-protestu-fermeriv/>
4. «Окупанти продовжують вивозити українські книжки з бібліотек на ТОТ». (2023). Центр

національного спротиву. – Режим доступу: <https://sprotyv.mod.gov.ua/okupanty-prodovzhuyut-vyvozyty-ukrayinski-knyzhky-z-bibliotek-na-tot/>

5. Пилипів, І., Вінокуров, Я. (2023). Зірка, яку погасили. Що сталося з «Київстаром»? Економічна правда. – Режим доступу: <https://www.epravda.com.ua/publications/2023/12/12/707628/>
6. Свиридчук, Ю. (2023). В Україні зафіксували майже 4 000 кібератак з боку РФ. Суспільне новини. – Режим доступу: <https://suspijne.media/619941-v-ukraini-zafiksuvali-majze-4-000-kiberatak-z-boku-rf/>
7. «Скільки росія витрачає на пропаганду?». (2023). Фільтр. – Режим доступу: <https://filter.mkp.gov.ua/skilky-rosiya-vytrachaye-na-propagandu/>
8. Сливенко, О. (2023). Поринь у віртуальний світ і повернися «ватником»: як Росія поширює свою пропаганду через відеоігри. Детектор Медіа. – Режим доступу: <https://ms.detector.media/propaganda-ta-vplivi/post/33008/2023-09-21-poryn-u-virtualnyy-svit-i-povernysya-vatnykom-yak-rosiya-poshyruyue-svoyu-propagandu-cherez-videoigry/>
9. «575 злочинів вчинила РФ проти медіа та журналістів за два роки і місяць повномасштабної війни». (2024). ІМІ. – Режим доступу: <https://imi.org.ua/monitorings/575-zlochyniv-vchynyla-rf-proty-media-ta-zhurnalistiv-za-dva-roky-i-misyats-povnomasshtabnoyivijny-i60153>
10. «58 млрд рублів або \$500 млн доларів на рік — у кремлі збільшили фінансування внутрішньої пропаганди». Офіційний телеграм-канал ГУР МО України. – Режим доступу: <https://t.me/DIUkraine/3690>
11. Galeotti, M. (2022). *The Weaponisation of Everything*. Yale University Press, 256 p.
12. Mattson, G. (2020). *Weaponization: Ubiquity and Metaphorical Meaningfulness*. *Metaphor and Symbol*, 35(4), 250–265. <https://doi.org/10.1080/10926488.2020.1810577>
13. NORFOLK, VA – Cognitive Warfare includes activities conducted in synchronization with other Instruments of Power, to affect attitudes and behaviours, by influencing, protecting, or disrupting individual, group, or population level cognition, to gain an advantage over an adversary. Retrieved from: <https://www.act.nato.int/activities/cognitive-warfare/>
14. Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War Against Reality*. New York: Public Affairs. 236 pp.
15. *Weaponization*. Oxford Learner's Dictionaries. Retrieved from: <https://www.oxfordlearnersdictionaries.com/definition/english/weaponization>
16. *Weaponization of Information*. Retrieved from: <https://www.populismstudies.org/Vocabulary/weaponization-of-information/>
17. *Weaponize*. Merriam-Webster. Retrieved from: <https://www.merriam-webster.com/dictionary/weaponize>

REFERENCES:

1. Dutsyk, D. (2023). *Iak funktsionuiut ta zavoiuvuiut audytoriiu neinstytutsionalizovani novynni telehrankanalny ukrainskoho sehmentu* [How non-institutionalized news telegram channels of the Ukrainian segment function and win an audience]. *Analitychnyi zvit*. Kyiv: HO «Ukrainskyi instytut media ta komunikatsii» [Analytical

report. Kyiv: NGO «Ukrainian Institute of Media and Communication». 68 s.

2. Izvoshchikova, A. (2022). 30 yevropeyskykh krain povnistiu abo chastkovo vymknuly rosiiski propahandystski kanaly [30 European countries completely or partially turned off Russian propaganda channels]. *Suspilne novyny* [Social news]. Retrieved from: <https://suspilne.media/222648-30-evropejskih-krain-povnistiu-abo-castkovo-vimknuli-rosijski-propagandistski-kanali/>

3. Mikhalkov, S. (2024). Rupor rosiiskoi propahandy v Polshchi stav holosom protestu fermeriv [The mouthpiece of Russian propaganda in Poland became the voice of farmers' protest]. *Texty.org*. Retrieved from: <https://texty.org.ua/articles/111765/rupor-rosijskoyi-propahandy-u-polshi-stav-holosom-protestu-fermeriv/>

4. "Okupanty prodovzhuiut vyvozyty ukrainski knyzhky z bibliotek na TOT" [The occupiers continue to take Ukrainian books from libraries to TOT]. *Tsentr natsionalnoho sprotyvu* [Center of national resistance]. Retrieved from: <https://sprotyv.mod.gov.ua/okupanty-prodovzhuyut-vyvozyty-ukrayinski-knyzhky-z-bibliotek-na-tot/>

5. Pylypiv, I., Vinokurov, Ya. (2023). Zirka, yaku pohasyly. Shcho stalosia z «Kyivstarom»? [A star that was extinguished. What happened to "Kyivstar"?]. *Ekonomichna pravda* [The economic truth]. Retrieved from: <https://www.epravda.com.ua/publications/2023/12/12/707628/>

6. Svyrydiuk, Yu. (2023). "V Ukraini zafiksuvaly maizhe 4 000 kiberatak z boku RF" [Almost 4,000 cyberattacks by the Russian Federation were recorded in Ukraine]. *Suspilne novyny* [Social news]. Retrieved from: <https://suspilne.media/619941-v-ukraini-zafiksuvali-majze-4-000-kiberatak-z-boku-rf/>

7. "Skilky rosiia vytrachaie na propahandu?" [How much does Russia spend on propaganda?]. *Filtr* [Filter]. (2023). Retrieved from: *Natsionalnyi proiekt z mediahramotnosti*. Retrieved from: <https://filtr.mkip.gov.ua/skilky-rosiya-vytrachaye-na-propagandu/>

8. Slyvenko, O. (2023). "Poryn u virtualnyi svit i povernysia «vatnykom»: yak Rosiia poshyriuie svoiu propahandu cherez videoihry" [Plunge into the Virtual World and Come Back as a 'Wattpad':

How Russia Spreads Its Propaganda Through Video Games]. *Detector Media* [Media detector]. Retrieved from: <https://ms.detector.media/propaganda-ta-vplivi/post/33008/2023-09-21-poryn-u-virtualnyy-svit-i-povernysia-vatnykom-yak-rosiya-poshyryuie-svoiu-propagandu-cherez-videoigry/>

9. "575 zlochyniv vchynyla RF proty media ta zhurnalistiv za dva roky i misiats povnomashtabnoi viiny" [The Russian Federation committed 575 crimes against the media and journalists during two years and a month of full-scale war]. *IMI*. Retrieved from: <https://imi.org.ua/monitorings/575-zlochyniv-vchynyla-rf-proty-media-ta-zhurnalistiv-za-dva-roky-i-misyats-povnomashtabnoyi-vijny-i60153>

10. "58 mlrd rubliv abo \$500 mln dolariv na rik — u kremli zbilshyly finansuvannia vnurishnoi propahandy" [58 billion rubles or \$500 million per year – the Kremlin has increased funding for internal propaganda.]. *Ofitsiinyi telehram-kanal HUR MO Ukrainy* [The official Telegram channel of the Ministry of Defense of Ukraine]. Retrieved from: <https://t.me/DIUkraine/3690>

11. Galeotti, M. (2022). *The Weaponisation of Everything*. Yale University Press, 256 p.

12. Mattson, G. (2020). *Weaponization: Ubiquity and Metaphorical Meaningfulness*. *Metaphor and Symbol*, 35(4), 250–265. <https://doi.org/10.1080/10926488.2020.1810577>

13. NORFOLK, VA – *Cognitive Warfare includes activities conducted in synchronization with other Instruments of Power, to affect attitudes and behaviours, by influencing, protecting, or disrupting individual, group, or population level cognition, to gain an advantage over an adversary*. Retrieved from: <https://www.act.nato.int/activities/cognitive-warfare/>

14. Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War Against Reality*. New York: Public Affairs. 236 pp.

15. *Weaponization*. *Oxford Learner's Dictionaries*. Retrieved from: <https://www.oxfordlearnersdictionaries.com/definition/english/weaponization>

16. *Weaponization of Information*. Retrieved from: <https://www.populismstudies.org/Vocabulary/weaponization-of-information/>

17. *Weaponize*. *Merriam-Webster*. Retrieved from: <https://www.merriam-webster.com/dictionary/weaponize>

“Information weaponization” as a technology of the Russian-Ukrainian war

Chupis Anastasiia Dmytrivna

Postgraduate Student at the Department
of Political Science
Zaporizhzhia National University
Zhukovskoho str., 66,
Zaporizhzhia, Ukraine;
Visiting Researcher of the School
of Social Sciences
Södertörn University
Alfred Nobels Alle, 7, Stockholm, Sweden
ORCID: 0000-0002-3091-3332

The article analyzes the contemporary context of military confrontation as a clash between democracy and authoritarianism, focusing on the ongoing conflict between the Russian Federation and Ukraine. It highlights the transformation of democratic values, such as freedom of speech and access to information, into targets of political and military manipulation, thereby posing threats to the sustainable functioning of democratic institutions. Psychological and cognitive strategies of warfare employed by the Russian Federation in the context of hybrid warfare against Ukraine are examined. Attention is drawn to the use of information technologies in military operations and their impact on the current geopolitical situation. Additionally, the emergence of new terms such as “cognitive warfare” and “weaponization” is discussed, which have become key concepts in understanding contemporary conflicts.

The aim is to analyze the processes of transforming information into instruments of cognitive and psychological military operations, particularly in the context of the conflict between the Russian Federation and Ukraine. The research tasks include analyzing channels of information dissemination, their technical components, and their influence on modern military strategies. The research employed methods of conceptual analysis, including the frame method, as well as content analysis of narratives used by the Russian Federation to conduct psychological and cognitive operations in the military conflict with Ukraine. As a result of the study, a multi-level concept of “information weaponization” is proposed as a broad term encompassing various methods of psychological and cognitive warfare, including propaganda, disinformation, information-psychological operations (IPSO), and the generation and dissemination of fakes.

Key words: information weaponization, psychological warfare, cognitive warfare, Russia, Ukraine, disinformation, propaganda, technology.