

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА
АКАДЕМІЯ»

Факультет соціальних наук та соціальних технологій
кафедра політології

**ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИЙ ВИМІР РОСІЙСЬКОЇ
ГІБРИДНОЇ АГРЕСІЇ ПРОТИ ЄВРОПЕЙСЬКИХ ДЕРЖАВ**

дипломна робота
на здобуття академічного звання бакалавра політології
студента Слесарева Арсенія Сергійовича

Науковий керівник:

Бевз Т. А.,
доктор історичних наук, професор

Робота допущена до захисту в ДЕК рішенням кафедри політології
протокол №__ від _____ 20__ р.

Завідувач кафедри _____

Київ – 2026

ЗМІСТ

ЗМІСТ	2
ВСТУП	3
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ В МЕЖАХ СУЧАСНИХ КОНФЛІКТІВ	8
1.1. Гібридна війна як складник воєн четвертого та п'ятого поколінь.	8
1.2. Інформаційні та психологічні операції в системі стратегічних комунікацій.	17
1.3. Когнітивна війна в епоху постправди: теоретичні засади та інструментарій.	27
РОЗДІЛ 2. ПРАКТИЧНИЙ АНАЛІЗ ОСОБЛИВОСТЕЙ ІНФОРМАЦІЙНОГО І ПСИХОЛОГІЧНОГО ПРОТИСТОЯННЯ РОСІЇ ТА ЄС	35
2.1. Російська гібридна агресія проти Європейського Союзу: аналіз через модель «стимул-можливість-втручання»	35
2.2. Мережева інфраструктура російського інформаційного впливу: від «Portal Combat» до імітаційних новинних вебсайтів.	39
2.3. Російський вплив на європейський політичний ландшафт: підтримка радикальних політичних партій та втручання в електоральні процеси	55
2.4. Російські кінетичні операції проти Європи як різновид PSYOP в межах когнітивної війни	60
ВИСНОВКИ	69
СПИСОК ДЖЕРЕЛ І ЛІТЕРАТУРИ	74
ДОДАТКИ	89
АНОТАЦІЯ	105

ВСТУП

Російська гібридна війна на Сході України у 2014 році стала революційним «milestone» у сфері модерної війни, адже російська агресія характеризувалась мультидоменністю, поєднавши потужний арсенал інформаційних, психологічних і кібероперацій, дипломатичного й економічного тиску разом із кінетичним протистоянням із застосуванням проксі-сил у вигляді самопроголошених терористичних «Луганської» й «Донецької» «народних республік». Саме ця війна назавжди змінила сприйняття російсько-українського протистояння і розуміння самої концепції війни у світі в цілому. До подій 2014 року дипломатичні стосунки України та Російської Федерації були складними, хоча на офіційному рівні трансливались меседжі про спільних пращурів та нерозривність кровних зв'язків¹. В період від проголошення української незалежності у 1991 р. і до початку гібридного протистояння у 2014 році Москва здійснювала прихований вплив на українське суспільство через культуру, церкву і регіональні еліти, що цілком може бути охарактеризовано концептом «soft power», який запровадив і розвинув Джозеф Най².

Однак після 2014 року Росія розширила спектр інструментів, вимірність і рівневість протистояння. На стратегічному рівні інформаційно-психологічного протистояння старі міфи про «триєдиність Русі» і «братські слов'янські народи» почали занепадати, поступившись агресивним і відверто конфронтаційним наративам про нацизм в Україні та повну залежність Києва від Заходу. Ці стратегічні наративи підкріплювались на інших рівнях, зокрема завдяки фейковим історіям, до прикладу про нібито розіп'ятого хлопчика у Слов'янську, що мала на меті

¹ Dempsey J. The Kremlin Tries Charm to Counter E.U. URL: <https://carnegieendowment.org/posts/2013/08/the-kremlin-tries-charm-to-counter-eu>

² Nye J. S. Soft power: The means to success in world politics. New York : Public Affairs, 2004.

поширити ненависть до української влади й військових, формуючи образ ворога на внутрішній інформаційний ринок для росіян та проводячи «демонізацію» України в очах міжнародної аудиторії. Саме з анексії Криму починається довготривала гібридна війна Росії проти України, що у 2022 році переросла у повномасштабну війну, яка відрізняється від усіх війн, що були до цього.

Початок повномасштабного вторгнення Росії проти України став не тільки поверненням великої конвенційної війни на європейський континент, а й поштовхом до реконцептуалізації модерної війни як такої. В конвенційному плані дрони й штучний інтелект (ШІ) почали витісняти традиційні уявлення про броньовані мобільні групи як про ефективний засіб ведення війни. Водночас змін зазнали й інші виміри сучасної війни: масштаби когнітивного, інформаційного і кіберпротистояння стали безпрецедентними. Сьогодні Україна вимушена не тільки протистояти російській конвенційній агресії, але й захищати власний інформаційний простір від ворожих психологічних операцій, що спрямовані на дестабілізацію суспільства через поглиблення соціальних кліважів, експлуатацію чутливих тем як мобілізація, корупція, а також підважування легітимності влади.

Разом з тим із 2022 року Росія збільшила рівень ескалації у конфронтації з Європою. У проміжку 2022–2026 рр. Росія здійснила низку гібридних операцій проти Європи як у кінетичному, так і в інформаційному й психологічному вимірах. До того ж на російських державних медіаресурсах лунають тези, що Росія веде війну не з Україною, а з Північноатлантичним альянсом (НАТО). Відтак, Європа знаходиться у стані неконвенційної гібридної війни з Росією, що потенційно може перетворитись на повномасштабну війну, до якої європейський континент має активно готуватись уже зараз.

Варто зазначити, що за оцінкою німецького політолога Ральфа Тіле, гібридна війна такого масштабу, яку Росія веде в Україні, у разі її розгортання проти європейських держав становитиме значний виклик для Європейського Союзу (ЄС) і НАТО³. Зважаючи на це і все вищезазначене, **актуальність** дослідження інформаційно-психологічного виміру сучасних конфліктів є надзвичайно високим, адже в модерній війні інформаційно-психологічний домен протистояння є настільки ж важливим, наскільки й кінетичний.

Об’єктом дослідження є російська гібридна війна проти європейських держав (зокрема країн-членів ЄС).

Предметом дослідження є інформаційно-психологічний вимір цього протистояння, зокрема теоретичні засади, інструменти, конкретні операції та їхні стратегічні цілі у період 2022–2026 років.

Метою роботи є комплексний аналіз особливостей російської інформаційно-психологічної агресії проти європейських держав (зокрема країн-членів ЄС) у межах сучасної гібридної війни – з визначенням теоретико-методологічних основ цього протистояння, інструментів, методів і конкретних кейсів їх застосування у період 2022–2026 років.

Досягнення поставленої мети передбачає вирішення наступних **завдань**:

- систематизувати знання щодо теоретико-концептуальних підходів до визначення гібридної війни та її співвідношення з війнами четвертого і п’ятого поколінь;
- уточнити термінологічну рамку інформаційно-психологічного протистояння через розмежування понять «стратегічні комунікації», «інформаційна війна», «інформаційні операції» та «психологічні операції»;
- дослідити когнітивну війну як новий вимір протистояння, відзначивши її ключові інструменти, теоретичні засади (управління

³ Thiele R. Hybrid Warfare: Future and Technologies. 2021. С. 15-16.

сприйняттям, модель імовірності обробки інформації, теорія когнітивного дисонансу) та зв'язок з епохою постправди;

- застосувати модель «стимул-можливість-втручання» Д. Бело для аналізу інструментарію російської гібридної війни проти ЄС;

- проаналізувати діяльність мережі «Pravda» («Portal Combat») та структуру мережі з 369 псевдолокальних новинних порталів («pink-slime») як інструментів деструктивного впливу, зокрема в контексті технологій «LLM grooming»;

- розкрити механізми російського втручання в електоральні процеси та фінансової підтримки радикальних політичних сил у державах-членах ЄС;

- дослідити приховані кінетичні операції Росії проти держав ЄС як форму PSYOP у межах когнітивної війни.

Методологія. У дослідженні використано загальнонаукові методи – аналіз, синтез, узагальнення, індукція й дедукція. На додаток в дослідження проведено контент-аналіз (для вивчення російських пропагандистських публікацій та псевдолокальних медіа); кейс-стаді (для розгляду мережі «Pravda», виборів у Румунії 2024 року, диверсій на території ЄС); open source intelligence (OSINT) методи (для проведення власного дослідження «pink-slime» медіа, що поширюють проросійську пропаганду); кількісні методи (для статистичного аналізу мережі «pink-slime» медіа).

Ступінь наукової розробки. Концептуальні основи цього дослідження значною мірою спираються на попередні теоретичні напрацювання, що були опубліковані в тезах наукової конференції «Російська війна проти України: трансформації соціальних інституцій та практик» і увійшли до збірки під назвою «Гібридна війна: психологічні

операції та управління громадським сприйняттям»⁴. Для систематизації теорії гібридної війни використовуються напрацювання одного з фундаторів поняття Ф. Хоффмана. У роботі розглянуті й інші інтерпретації терміну, що належать Дж. Візеру, Б. Банкову, а також враховано офіційне тлумачення НАТО. Окремим напрямком у дослідженні була систематизація теорії поколінь війни, зокрема В. Лінда (4-те покоління), Д. Аббота й А. Крішнана (концепт 5-го покоління). Зважаючи на те, що будь-яке дослідження у сфері російських студій категорично неможливе без залучення російських джерел в якості матеріалів для обробки та аналізу, в цій дослідницькій роботі використовуються російська академічна література і новинні публікації у якості першоджерел інформації.

Структура та обсяг роботи. Кваліфікаційна робота складається зі вступу, двох розділів, поділених на підрозділи, висновків, списку використаних джерел і літератури, а також додатків. Перший розділ присвячено теоретичним засадам інформаційно-психологічного впливу в межах сучасних конфліктів: гібридній війні як частині війн 4-го та 5-го поколінь, інформаційній війні та стратегічним комунікаціям, психологічним операціям, когнітивній війні, а також російській перспективі гібридних війн. Другий розділ містить практичний аналіз російського інформаційно-психологічного протистояння з ЄС: застосування моделі IOI для аналізу логіки російської агресії, аналіз мереж «Pravda» та «pink-slime» медіа, дослідження впливу на політичний ландшафт ЄС та кінетичні операції як форму PSYOP. Загальний обсяг роботи становить 73 сторінки.

⁴ Слесарев А., Бевз Т. Гібридна війна: психологічні операції та управління громадським сприйняттям. *Російська війна проти України: трансформації соціальних інституцій та практик*. 2025. С. 274–279. URL: <https://ekmair.ukma.edu.ua/handle/123456789/36718>

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ В МЕЖАХ СУЧАСНИХ КОНФЛІКТІВ

1.1. Гібридна війна як складник воєн четвертого та п'ятого поколінь.

Термін «*гібридна війна*» відносно новий і кінцеве його трактування не до кінця визначене, досі залишаючись предметом для академічних дискусій⁵. Одна з перших спроб надати вичерпне академічне визначення цьому терміну належить Френку Гоффману, який визначає гібридну війну як таку, що включає низку різних форм ведення бойових дій, зокрема конвенційних можливостей, нерегулярних тактик і формацій, терористичних актів, невибіркове насильство і примус, а також кримінальну діяльність»⁶. За основу для розробки цього теоретичного фрейму Ф. Гоффман узяв війну на Близькому Сході, а саме протистояння Ізраїлю та ліванської шиїтської терористичної групи «Хезболла», зокрема під час активної фази протистояння улітку 2006 року. Відповідно, у «гоффманському» розумінні гібридна війна є перш за все протистоянням державних і недержавних акторів, що супроводжується асиметричністю у ресурсах, інструментах і можливостях сторін.

До 2014 року цей кейс залишався найбільш взірцевим для контекстуального розуміння гібридних війн. Однак, як зазначає теоретик гібридної війни Джеймс Візер, загальний інтерес до концепту гібридної війни значною мірою виріс в академічних і військових колах саме після російської агресії проти України у 2014 році⁷. Як реакція на події на Сході

⁵ Hoffman F. «Conflict in the 21st Century: The Rise of Hybrid Wars». Institute for Policy Studies, 2007. С. 8

⁶ Hoffman F. «Conflict in the 21st Century: The Rise of Hybrid Wars». Institute for Policy Studies, 2007. С. 14

⁷ Wither J. Making Sense of Hybrid Warfare. Connections. 2016. Т. 15, № 2. С. 73.
URL: <https://www.jstor.org/stable/26326441>

України в щорічному виданні The Military Balance від лондонського Міжнародного інституту стратегічних досліджень гібридну війну визначали як використання військових та невійськових інструментів у інтегрованій кампанії, що спрямована на досягнення ефекту несподіванки, перехоплення ініціативи, отримання психологічних та фізичних переваг шляхом використання дипломатичних засобів; складних і швидких інформаційних, електронних та кібероперацій; таємних, а іноді й відкритих військових та розвідувальних дій; економічного тиску⁸. Таким чином, відповідно до цього визначення гібридна війна втрачає своє першочергове значення як виключно протистояння державних і недержавних акторів, що більшою мірою є рисою «асиметричної війни», хоча це і не виключає того факту, що проксі сили, нерегулярні формування, організовані кримінальні й терористичні групи можуть бути складовою частиною сучасної гібридної війни.

З цього періоду гібридна війна починає фігурувати в документах НАТО й інтерв'ю в медіа з представниками альянсу, отримуючи все нові визначення. У 2014 році колишній генеральний секретар Андерс Фог Расмуссен назвав російську агресію в Україні гібридною війною, яку визначив як комбінацію військових дій, прихованих операцій та агресивної програми дезінформації⁹. Станом на 2026 рік НАТО визначає гібридні загрози як такі, що поєднують військові та невійськові, а також приховані та явні засоби, включаючи дезінформацію, кібератаки, економічний тиск, розгортання нерегулярних збройних формувань та використання регулярних сил з метою розмиття меж між війною та миром і поширенням

⁸ Complex crises call for adaptable and durable capabilities. The Military Balance. 2015. T. 115, № 1. С. 5–6. URL: <https://doi.org/10.1080/04597222.2015.996334>

⁹ Gordon M., Landler M. NATO Chief Warns of Duplicity by Putin on Ukraine. URL: <https://www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html>

сумнівів у свідомості цільових груп населення, що спрямоване на дестабілізацію та підлив суспільств¹⁰.

Майже 20 років активної теоретичної розробки терміну демонструють значні відмінності між гібридною війною за Ф. Гоффманом та інтерпретацією Північноатлантичного альянсу. Про це зокрема зазначає болгарський дослідник Борислав Банков у своїй статті 2024 року «Hybrid Warfare: How to Escape the Gray-Zone», стверджуючи, що існує дві основні школи гібридної війни: кінетична та некінетична. До першої школи Б. Банков відносить теоретичний фрейм Ф. Гоффмана і його приклад протистояння Ізраїлю і «Хезболли» як протиборство недержавних акторів з державами. Натомість до другої школи він відносить теоретичний фрейм сформований НАТО і ЄС, що передбачає гібридну війну між державами й допускає кінетичні протистояння¹¹.

Варто зазначити, що в контексті теоретичного фреймінгу гібридного протистояння важливо згадати теорію п'яти поколінь війни, адже четверте і п'яте покоління значною мірою пов'язанні із теорією гібридної війни. У 1989 році Вільям Лінд разом з іншими дослідниками опублікував статтю в Marine Corps Gazette, де запропонував чітку періодизацію західної війни на покоління, що визначались технологічним прогресом, концентрацією вогневої потужності та маневреністю.

В запропонованій у «The Changing Face of War: Into the Fourth Generation» концепції перше покоління характеризується використанням гладкоствольних рушниць та строїв лінією й колонами. Друге покоління, що Вільям Лінд підсумував французькою максимою: «артилерія завойовує, а піхота окупує», стало реакцію на винахід нарізних рушниць, колючих дротів й кулеметів. Третє покоління війни відзначається акцентом на

¹⁰ Countering hybrid threats.
URL: <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats>

¹¹ Hybrid Warfare: How to Escape the Conceptual Gray-Zone. Journal of Strategic Security. 2024. T. 17, № 1. С. 4–7.
URL: <https://www.jstor.org/stable/pdf/48766103.pdf>

маневреність, а не на концентрацію особового складу чи вогневої потужності, що уперше використовувалось німецькими військами під час реалізації «плану Шліффена» у Першій світовій війні й у подальшому було довершено під час бліцкригу у Другій світовій¹².

Однак, на заміну вже традиційному конвенційному протистоянню третього покоління, що базувалось на використанні бронетехніки, літаків і стрілецької зброї Вільям Лінд запропонував концепт четвертого покоління війни (далі – 4GW), що характеризується асиметричністю військових спроможностей сторін¹³. Відповідно до Вільяма Лінда 4GW ґрунтується на чотирьох основних ідеях: полем бою є усе суспільство у цілому, розпорошення і зменшення залежності від централізованої логістики, використання малих маневрових груп комбатантів, а також акцент на внутрішньому знищенні ворога, а не на фізичному¹⁴.

Якщо попередні покоління війн були конфліктами держав, то 4GW є конфліктом, де участь беруть недержавні актори: інсургенти, терористичні групи й кримінальні організації. Це, власне зумовлюється на думку Вільяма Лінда «кризою легітимності держав»¹⁵. Водночас головним завданням таких акторів зазвичай є повалення державного ладу або встановлення свого власного. До того ж протистояння 4-го покоління характеризується розмиттям між війною й миром, коли межа між «цивільним» і «воєнним» зникає¹⁶. Також важливо наголосити, що Вільям Лінд припускав що саме психологічні операції стануть основною операційною і стратегічною зброєю у формі інформаційно-медійного

¹² W. Lind та ін. "The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette. 1989. С. 22–26.

¹³ Simons G. Fourth Generation Warfare and The Clash of Civilizations. Journal of Islamic Studies. 2010. Т. 21, № 3. С. 391–412. URL: <https://doi.org/10.1093/jis/etq042> (дата звернення: 21.05.2026).

¹⁴ W. Lind та ін. "The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette. 1989. С. 22–26.

¹⁵ W. Lind та ін. "The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette. 1989. С. 22–26.

¹⁶ W. Lind та ін. "The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette. 1989. С. 22–26.

впливу, що, наприклад, могло б бути націлене на зменшення підтримки населення уряду цільової країни та готовності до війни¹⁷.

Однак сучасні науковці відстоюють ідею, що наразі сформувалось нове **5-те покоління війни** (або війна п'ятого покоління) (далі – 5GW). Як і у випадку з іншими термінами у цій темі, остаточне визначення терміну залишається нечітким. І хоча витоки концепту можна простежити ще в ранніх 2000-х, основний фрейм 5GW було артикульовано в роботі Деніела Аббота «The Handbook of 5GW» у 2010 році. Відповідно до Аббота п'яте покоління війни базується на «маніпуляції економічними, політичними, соціальними та військовими силами в кількох сферах для здійснення змін у системах та досягнення узгодженості ефектів з метою досягнення конкретної цілі або сукупності обставин»¹⁸. Однак подальші теоретичні напрацювання робили більший акцент на домені психологічного протистояння.

До прикладу, дослідник безпекових студій Армін Крішнан у своїй роботі «Fifth Generation Warfare: Dominating the Human Domain» пропонує власне бачення 5GW, засноване на теоретичних внесках інших дослідників. Згідно з А. Крішнаном 5GW відрізняється від війн інших поколінь тим, що театром бойових дій п'ятого покоління є не тільки фронт, а й суспільство в цілому, фокусуючись на управлінні сприйняттям, ідентичністю і контекстом в межах психологічної війни, а також культурного впливу, що забезпечується за рахунок прихованих операцій без відкритого насилля, беручи за мету дестабілізацію або знищення політичного та/або соціального порядку¹⁹. Прикметно, що А. Крішнан припускає мінливість 5GW, стверджуючи, що вона може деградувати до

¹⁷ W. Lind та ін. "The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette. 1989. С. 22–26.

¹⁸ Abbott D. The Handbook of 5GW. Nimble Books, 2010.

¹⁹ Krishnan A. Fifth Generation Warfare Dominating the Human Domain. Routledge, 2024. С. 18. URL: <https://doi.org/10.4324/9781003396963> (дата звернення: 21.05.2026).

четвертого покоління чи навпаки еволюціонувати до шостого²⁰. За своєю суттю запропоноване Крішнаном визначення 5GW передбачає синтез «м'якої сили» і психологічних операцій для досягнення конкретних стратегічних цілей.

Водночас А. Крішнан стверджує, що наявність кінетичного елементу у російсько-українській війні не виключає релевантності теорії 5-го покоління війни в цьому випадку. На думку дослідника основним завданням сторін у конфлікті є не стільки фізичний контроль над територією, скільки контроль над суспільством та людським розумом²¹. Однак цю логіку можна поставити під сумнів, адже дії Російської Федерації (РФ) 24 лютого 2022 року були спрямовані на швидке повалення уряду шляхом оточення і захоплення столиці. І хоча інформаційно-психологічний вимір був надзвичайно важливим в межах цих операцій, саме кінетичні дії – захоплення столиці й повалення уряду – привели б Росію до перемоги. Також контроль над територією Луганської й Донецької області залишається заявленою метою Росії у війні разом із контролем над сухопутним коридором до Криму, що є важливим елементом для створення образу перемоги російською владою для власного населення. Попри це, беззаперечно інформаційно-психологічний вимір українсько-російського протистояння залишається вагомोю частиною війни разом із кінетичною війною і на нашу думку порівнювати важливість цих вимірів є недоцільним, виходячи з багатовимірної суті конфлікту. Водночас, ймовірність відкату до 3-го чи 4-го покоління війни в Україні, де інформаційно-психологічне протистояння перестає бути важливим виміром конфлікту, є низькою. Навіть у випадку завершення

²⁰ Krishnan A. Fifth Generation Warfare Dominating the Human Domain. Routledge, 2024. С. 18. URL: <https://doi.org/10.4324/9781003396963>

²¹ Krishnan A. Fifth Generation Warfare Dominating the Human Domain. Routledge, 2024. С. 18-19. URL: <https://doi.org/10.4324/9781003396963>

триваючої конвенційної війни в Україні 5GW все ще може тривати відповідно до свого визначення.

Варто зазначити, що на нашу думку фрейм А. Крішнана потребує уточнення в питанні акторів 5GW, якими за твердженням дослідника радше є «субнаціональні державні актори» (sub-nation state actors), а не уряди й держави. До таких акторів можна віднести політичні партії й окремих політиків, місцеві еліти, органи місцевої влади та різні види інсургентів (повстанські рухи, сепаратистські угруповання тощо). Однак, приклад російсько-української війни демонструє, що офіційні представники влади й уряд формують стратегічні напрямки інформаційно-психологічного протистояння та продукують ключові наративи, які згодом ретранслюються і підкріплюються субнаціональними державними й недержавними акторами на оперативному і тактичному рівнях. Водночас якщо у війні за Клаузевіцем народу відводилась лише роль опосередкованої підтримки війни, зокрема через економічну участь²², то сучасна українсько-російська війна демонструє той факт, що народ є важливим актором інформаційно-психологічного протистояння, що зумовлено розвитком соціальних мереж. В сучасності будь-який індивід може робити відео- і фотоматеріали для медіаплатформ, що можуть містити дезінформацію чи пропаганду, таким чином підсилюючи інформаційно-психологічні операції, що впроваджується державою. Важливо зазначити, що така участь населення в інформаційно-психологічній війні може бути широко спричинена власним бажанням індивідів долучитись до протистояння, попри відсутність прямої координації із центральним урядом.

У межах цього дослідження також важливо згадати й російську перспективу на проблему трактування «гібридної війни». Поняття

²² Цит. за: Krishnan A. Fifth Generation Warfare Dominating the Human Domain. Routledge, 2024. С. 26. URL: <https://doi.org/10.4324/9781003396963> (дата звернення: 21.05.2026).

«нелінійна війна», яке вживається в російській термінології та літературі є схожим терміном на західний концепт гібридної війни. Загалом, однією з перших згадок цього терміну є науково-футуристичне есе про п'яту світову війну, написане колишнім ключовим політичним радником російського президента Владиславом Сурковим під псевдонімом Натан Дубовицький. Текст під назвою «Без неба» було опубліковано за декілька днів до анексії Кримського півострова Росією у 2014 році. «Нелінійною війною» В. Сурков називав конфлікт «всіх проти всіх» і протиставляв його класичним двостороннім війнам з двома коаліціями чи двома окремими націями²³. Однак нелінійна війна в тексті В. Суркова концептуально далека від гібридної війни.

Водночас принципи нелінійної війни також були закладені, чинним станом на 2026 рік, начальником Генерального штабу Збройних сил РФ Валерієм Герасимовим у так званій «Доктрині Герасимова», яку було опубліковано у 2013 році у вигляді статті під назвою «Цінність науки в передбаченні» на сайті «Військово-промисловий кур'єр». Аналізуючи досвід американських операцій на Близькому Сході та перебіг подій «Арабської весни», В. Герасимов доходить висновку, що посилилась роль невійськових способів у досягненні політичних та стратегічних цілей, які іноді перевершують силу зброї²⁴. У своїй статті російський воєначальник стверджує про посилення ролі політичних, економічних, інформаційних та гуманітарних заходів, які, на його думку, мають здійснюватися одночасно із залученням «протестного потенціалу населення» та військовими заходами прихованого характеру, серед яких він відмічає заходи інформаційного протистояння²⁵. Фактично, В. Герасимов у своєму есе

²³ Дубовицький Н. Без неба. Русский пионер. URL: <https://ruspioner.ru/honest/m/single/4131>

²⁴ Герасимов В. Ценность науки в предвидении. URL: https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html

²⁵ Герасимов В. Ценность науки в предвидении. URL: https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html

охарактеризував основні засади гібридної війни, наголосивши на багатовимірності та одночасності.

Особливу роль інформації у досягненні стратегічних цілей відзначають також і в ширших російських військово-академічних колах. Наприклад, російський генерал-майор у відставці В. Сліпченко опублікував у 2013 році статтю «Інформаційний ресурс та інформаційне протиборство» у журналі Міністерства оборони РФ «Армійський вісник», де висунув тезу, що «інформаційний ресурс стане складовою стратегічних ударних та оборонних сил держави»²⁶. Хоча російський генерал наводить футуристичні методи ведення інформаційно-психологічного протистояння, прикладом чого є його твердження про використання «голографічних зображень релігійного характеру на великій висоті на небесній сфері»²⁷, все ж можна чітко констатувати наявність тенденції серед російських офіцерів щодо визнання провідної ролі інформації у конфліктах майбутнього. Це також підтверджується західними науковцями, зокрема Р. Вальцман стверджує, що росіяни вважають ІО критичною частиною невійськових заходів, для чого Кремль адаптував усталені радянські методи дестабілізації до епохи Інтернету та соціальних мереж²⁸.

Підсумовуючи, можна дійти висновку, що, попри термінологічну розбіжність із західним дискурсом – «нелінійна війна» замість «гібридної» – концептуальне наповнення цих категорій є схожим, однак не ідентичним. «Доктрина Герасимова» закладає акцент багатовимірній природі конфлікту, у якому невійськові засоби (політичні, економічні, інформаційні та гуманітарні), що застосовуються одночасно з прихованими військовими операціями та «протестним потенціалом населення». Варто наголосити,

²⁶ Слипченко В. Информационный ресурс и информационное противоборство. Армейский сборник. 2013. № 10. С. 53–54. URL: <https://archive.ph/JJmq1>

²⁷ Слипченко В. Информационный ресурс и информационное противоборство. Армейский сборник. 2013. № 10. С. 53–54. URL: <https://archive.ph/JJmq1>

²⁸ Waltzman R. The Weaponization of Information: The Need for Cognitive Security. RAND Corporation, 2017. С. 4. URL: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf

що ці положення були сформульовані напередодні анексії Криму, що фактично свідчить про доктринальний, ретельно спланований, а не ситуативний характер до гібридних дій.

1.2. Інформаційні та психологічні операції в системі стратегічних комунікацій.

Як і у випадку з гібридною війною, найбільшим викликом у дослідженні таких теоретичних концептів як *«інформаційна війна»* (далі – ІВ) або «інформаційне протистояння» є неузгодженість визначень та трактувань цих термінів. Єдності у розумінні цих понять немає навіть серед країн-членів НАТО. Тому для подальшої роботи в цьому дослідженні буде використовуватись синтетичний підхід, який покликаний об'єднати способи трактування теоретичних концептів різних науковців у єдину теоретичну рамку. Також під впливом широкого вжитку таких термінів як «інформаційна війна», «інформаційні операції» чи «інформаційне протистояння» у медіа, значення цих концептів також нерідко стає предметом плутанини.

В американській військовій доктрині терміни «інформаційна війна» та «інформаційні операції» певний час використовувались як синоніми, а тому справедливо вважати, що основним визначенням інформаційної війни у військовій сфері для Сполучених Штатів Америки (США) є «інтегроване застосування різних технік і тактик під час воєнних операцій у поєднанні з іншими напрямками дій для впливу, дезорганізації, підриву або узурпації ухвалення рішень противниками та потенційними противниками, водночас захищаючи власні процеси ухвалення рішень»²⁹. Тобто в основі військового виміру ІВ лежить саботаж можливостей

²⁹ Information Operations. Joint Chiefs of Staff, 2012. С. 8. URL: https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf

супротивника приймати рішення. Натомість українські дослідники, наприклад Я. Малик запропонував розуміти інформаційну війну як «форму ведення інформаційного протистояння між різними суб'єктами, яка передбачає проведення комплексу із заподіювання шкоди інформаційній сфері суперницької сторони і захисту власної»³⁰. З обох визначень випливає, що ІВ має як функцію нападу, так і захисту.

У цьому дослідженні ми визначаємо термін «інформаційна війна» як широкий комплекс дій, заснованих на конкретних тактиках і техніках, які реалізуються через пропаганду, дезінформацію, управління сприйняттям, інформаційні операції і їх підвиди та протистояння у кіберпросторі. Метою таких заходів є дестабілізація суспільства опонента, підважування авторитету влади в державі, поширення неправдивої інформації для дезорієнтації військово-політичного керівництва держави й армії, а також ускладнення процесу прийняття рішень. ІВ слід розглядати і як вимір гібридної війни, і як самостійний спосіб протистояння та захисту/реалізації стратегічних інтересів.

Попри те, що і в академічному середовищі також іноді не розрізняють терміни «інформаційна війна» та «інформаційні операції», в цьому дослідженні *інформаційні операції* (далі – ІО) будуть вважатись одиницею ведення інформаційної війни, які визначаються як конкретні дії спрямовані для атаки та впливу на інформаційну систему ворога³¹. Інформаційні операції проводяться на всіх рівнях ведення війни, у всіх фазах операцій і в межах усього спектра конфліктів³². Утім, ІО не є інновацією 1990-х років, коли цей термін вперше було концептуалізовано

³⁰ Малик Я. Інформаційна Війна і Україна. Демократичне врядування. 2015. № 15. С. 1. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=DeVr_2015_15_3

³¹ Ventre D. Information Warfare. Willey, 2016. С. 8. URL: <https://onlinelibrary.wiley.com/doi/book/10.1002/9781119004721>

³² Headquarters Department of the Army. Psychological Operations Tactics, Techniques, and Procedures. Washington, 2003. С. 9. URL: <https://irp.fas.org/doddir/army/fm3-05-301.pdf>

Департаментом оборони США³³. Людство вдавалось до цього засобу досягнення національних інтересів задовго до його теоретичного оформлення. Прикладом цього слугує використання монголами на чолі з Чингісханом шпигунів для поширення чуток, які навмисно перебільшували розмір монгольської армії, викликаючи почуття страху серед їх ворогів³⁴.

Під впливом процесу глобалізації інформаційні операції поступово еволюціонували, охоплюючи все нові простори для боротьби: преса, радіо, медіа і кіберпростір. Таким чином, сучасні інформаційні операції можуть бути умовно поділені на 5 основних типів: психологічні операції (psychological operations), військовий обман (military deception), операції безпеки (operations security), електронна війна (electronic warfare), кібероперації³⁵. Варто зазначити, що американська воєнна доктрина розуміє ці типи інформаційних операцій як складові звичайної конвенційної війни. Тобто ці операції є нерозривно пов'язані із кінетичними заходами й спрямованими на їх підтримку. Однак, у цьому дослідженні ІО такі як психологічні операції, електронна війна і кібероперації, розуміються як самостійні одиниці ведення гібридного протистояння, що не передбачають обов'язково зв'язку з кінетичними операціями, хоча деякі такі приклади будуть розглянуті в цій роботі для детального аналізу особливостей російської гібридної агресії проти Європи.

Водночас важливою складовою сучасної інформаційної війни є **стратегічні комунікації** (далі – стратком). Що важливо, термін не має чіткого визначення і вичерпної концептуалізації, яка б співвідносила його з іншими елементами інформаційного протистояння. Через різне розуміння

³³ High S. Information Operations: The Command and Control Warfare. 1997. С. 5–6.

³⁴ Luberrisse J. Controlling the narrative. The definitive guide to psychological operations, perception management and information warfare. Fortis Novum Mundum, 2024. С.10–11.

³⁵ Military Information Support Operations, Joint Publication 3-13.2. 2012. URL: <https://info.publicintelligence.net/JCS-MISO.pdf>

терміну різні автори надають стратегічним комунікаціям різний рівень важливості у системі інформаційної війни.

Значний внесок у концептуальну розробку стратегічних комунікацій зробив Кірк Халлахан та інші дослідники у статті «Defining Strategic Communication», підсумовуючи яку, можна визначити, що стратегічні це цілеспрямоване використання комунікації організацією для участі в публічному дискурсі – презентація й просування себе через цілеспрямовану діяльність своїх лідерів, представників³⁶. Важливо зазначити, що К. Халлахан виділяє шість сфер дії страткому, завдяки яким організація може досягати своїх стратегічних цілей: менеджмент, маркетинг, зв'язки з громадськістю, технічна комунікація, політична комунікація та інформаційні/соціальні маркетингові кампанії³⁷. Це фактично демонструє, що стратком є універсальним і мультидоменним явищем, що може використовуватися для аналізу публічної участі як недержавних, так і державних акторів.

Однак наведеному вище визначенню бракує концептуалізації у політичній сфері, а тому важливо проаналізувати яким чином стратком визначають у контексті інформаційної політики держав. Відповідно до американської доктрини стратегічні комунікації – це процеси та зусилля, спрямовані на розуміння та залучення ключових аудиторій з метою створення, зміцнення або збереження умов, сприятливих для просування національних інтересів, шляхом використання скоординованої інформації, тем, планів, програм та дій³⁸, що підтримані інформаційними операціями (в особливості психологічними операціями), зв'язками з громадськістю та публічною дипломатією. Однак це визначення далеко не є універсальним,

³⁶ Defining Strategic Communication / K. Hallahan та ін. *International Journal of Strategic Communication*. 2007. Т. 1, № 1. С. 15. URL: <https://doi.org/10.1080/15531180701285244>

³⁷ Defining Strategic Communication / K. Hallahan та ін. *International Journal of Strategic Communication*. 2007. Т. 1, № 1. С. 25-26. URL: <https://doi.org/10.1080/15531180701285244>

³⁸ Information Operations Primer. U.S. Army War College, 2008. С.9. URL: <https://informationsecurity.info/wp-content/uploads/2021/04/Information-Operations-Primer-2008.pdf>

тому в цьому дослідженні стратегічні комунікації розуміються як стратегічне поширення тез, наративів і програм офіційними державними акторами, що формують фрейм інформаційної політики, в межах якої на оперативному і тактичному рівнях будуть здійснюватися відповідні заходи для їх підтримки. Влучним узагальненням цього визначення є теза Крістофера Пола, що стратегічні комунікації необхідні для того, щоб пояснити ту чи іншу дію³⁹.

У сфері міжнародних відносин та безпекових студій стратегічні комунікації тісно пов'язані з поняттям «стратегічних наративів», теоретична розробка яких належить А. Міскіммону, Б. О'Лафліну та Л. Розель. На думку авторів, стратегічні наративи є засобом, за допомогою якого політичні актори намагаються конструювати спільний зміст минулого, теперішнього і майбутнього, щоб досягнути політичних цілей, зокрема, аби формувати поведінку внутрішніх і міжнародних акторів⁴⁰. Таким чином, можемо визначити, що наратив є наріжним каменем страткому: стратегічна комунікація без наративу є лише технікою передачі повідомлення, тоді як стратегічний наратив надає цьому повідомленню сенс, контекст і логіку.

У контексті гібридного протиборства чи повномасштабної модерної війни стратегічні комунікації відіграють подвійну роль: вони слугують як для нападу, так і для захисту. Це зумовлюється тим, що за своєю суттю наративи, які формуються для комунікацій в рамках страткому, можуть бути спрямовані, на внутрішню і зовнішню аудиторії, на союзників, ворогів і нейтральні сторони.

Однак в Росії поняття «стратегічні комунікації» не використовується ані в публічній політиці, ані в офіційних документах, ані в академічних колах. Офер Фрідман доходить висновку, що в Росії західна практика

³⁹ Paul C. Strategic Communication Origins, Concepts, and Current Debates. Praeger, 2011. С.6-8.

⁴⁰ Strategic narratives: communication power and the new world order. Choice Reviews *Online*. 2014. T. 52, № 03. URL: <https://doi.org/10.5860/choice.185594>

стратегічних комунікацій концептуалізована як «інформаційна війна», повною мірою відповідаючи тим завданням, що на стратегічні комунікації покладають на Заході⁴¹. Якщо західне розуміння страткому ґрунтується на правдивості, достовірності й прозорості, то російські стратегічні комунікації працюють інакше. Наприклад, російський наратив про нацистів в Україні, який широко вживаних в російських політичних колах і, зокрема, застосований Путіним для виправдання початку війни проти України у 2022 році, є прикладом російського страткому. Штучно сфабрикований наратив, який є абсолютно неправдивим, не підпадає під західні критерії страткому, однак попри це виконує свою функцію. За Крістофером Полом, сторона, що використовує засновані на брехні стратегічні комунікації мала б втратити довіру, однак такий ефект не спостерігається в Росії. Найбільш ймовірним поясненням такого феномену є те, що в рамках західної доктрини стратком базується на принципах прозорості, достовірності та узгодженості, а в Росії інформаційна дія оцінюється не за правдивістю, а за ефективністю психологічного впливу на цільову аудиторію. Фактично, цей феномен можна містко пояснити категоріями, якими оперує Ханна Арендт, що велика брехня створює для населення альтернативну реальність. Варто також наголосити, що О. Фрідман стверджує, що у російській концептуалізації інформаційної війни (страткому) ефективність дій вимірюється не їхнім впливом у реальному світі, а їхнім впливом на віртуальний інформаційний вимір⁴². Відповідно до цього твердження, будь-яка дія – військова, економічна, дипломатична – може бути передусім інформаційною операцією, спрямованою на формування потрібного психологічного стану в цільових аудиторій. Про це буде детальніше згадано в наступному розділі.

⁴¹ Fridman O. 'Information War' as the Russian Conceptualisation of Strategic Communications. *The RUSI Journal*. 2020. T. 165, № 1. С. 44–53. URL: <https://doi.org/10.1080/03071847.2020.1740494>

⁴² Fridman O. Information War as the Russian Conceptualisation of Strategic Communications. *The RUSI Journal*. 2020. T. 165, № 1. С. 44–53. URL: <https://doi.org/10.1080/03071847.2020.1740494>

Варто зазначити, що загальна ефективність страткому визначається не лише якістю повідомлення, а й здатністю того, хто транслює це повідомлення, ідентифікувати, виокремити й цілеспрямовано охопити свої аудиторії. У контексті сучасних збройних конфліктів ці аудиторії є принаймні чотирьох типів: власне населення, міжнародні союзники, нейтральні сторони, що не приєдналися до жодного блоку, та аудиторія противника. Кожна з них вимагає різного фреймінгу, різних меседжів та різних каналів комунікації. Показовим прикладом недостатньо збалансованого наративу в контексті аудиторій є те, як Кремль виправдовував своє вторгнення 2022 року, а саме операція з метою денацифікації України. Наратив зіткнувся з нездатністю одночасно переконати внутрішню аудиторію і міжнародну: внутрішній дискурс будувався на ретроспективних аналогіях та апеляціях до міфу «Великої Вітчизняної Війни» проти нацизму, тоді як для зовнішньої аудиторії такі меседжі були «фоновим шумом» за межами Росії.

Водночас *психологічні операції* (далі – PSYOP) є невіддільною частиною інформаційних операцій, а також слугують важелем для їхньої реалізації⁴³. Департамент армії США визначає PSYOP як заплановані операції, які транслюють ретельно відібрану інформацію для іноземних цільових аудиторій, з метою впливу на емоції, мотивацію, логіку та поведінку цільових аудиторій задля підтримки військових і державних цілей⁴⁴. Ширшим визначенням цього терміну є сплановане використання пропаганди чи інших психологічних заходів для впливу на думки, емоції, ставлення та поведінку ворожих, нейтральних чи дружніх груп осіб з метою досягнення конкретних завдань⁴⁵. Попри те, що в обидвох

⁴³ Headquarters Department of the Army. Psychological Operations Tactics, Techniques, and Procedures. Washington, 2003. C. 9. URL: <https://irp.fas.org/doddir/army/fm3-05-301.pdf>

⁴⁴ Headquarters Department of the Army. Psychological Operations Tactics, Techniques, and Procedures. Washington, 2003. C. 6. URL: <https://irp.fas.org/doddir/army/fm3-05-301.pdf>

⁴⁵ Luberrisse J. Controlling the narrative. The definitive guide to psychological operations, perception management and information warfare. Fortis Novum Mundum, 2024. C. 10.

визначеннях PSYOP позиціюється як наступальні й агресивні заходи, такі операції мають ширший спектр застосування. Іноді PSYOP не тільки мають на меті дестабілізувати суспільство ворожої держави й дискредитувати її уряд, а ще і вмотивувати й мобілізувати власне населення до конкретних дій і заходів. Як відзначають в Департаменті армії США, мирне застосування PSYOP може сприяти стабільності в суспільстві шляхом поширення інформації, що підтримує гуманітарні зусилля та зменшує напругу серед цивільного населення⁴⁶. Витоки PSYOP можна простежити ще у XIX століття, коли прусський полководець Карл фон Клаузевіц відзначив роль психологічних сил як невіддільної частини військових дій у місткій фразі: «усі військові дії переплітаються з психологічними силами та ефектами»⁴⁷.

Психологічні операції ґрунтуються на низці фундаментальних принципів, які визначають їхню ефективність. Одним із ключових принципів, який описують американські дослідники, є довіра до інформації або джерела. Американські PSYOP уникають відвертої брехні, оскільки довіра споживача інформації до повідомлення або його джерела є критичною для впливу на його переконання⁴⁸. Цей принцип контрастує з підходами тоталітарних режимів, де абсолютна брехня використовувалась як основний інструмент контролю за масами⁴⁹. Утім, правдивість не означає повного розкриття інформації – в рамках психологічної операції конкретні події можуть вибірково висвітлюватись, акцентуючи лише на вигідних аспектах та замовчуючи незручні факти.

⁴⁶ Headquarters Department of the Army. Psychological Operations Tactics, Techniques, and Procedures. Washington, 2003. С. 6. URL: <https://irp.fas.org/doddir/army/fm3-05-301.pdf>

⁴⁷ Clausewitz C. On War. New Jersey, 1989. С. 136. URL: <https://antilogicalism.com/wp-content/uploads/2019/04/on-war.pdf>

⁴⁸ Goldstein F. L. Psychological Operations: Principles & Case Studies. Air University, 1996. С. 142. URL: https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0018_GOLDSTEIN_FINDLEY_PSYCHOLOGICAL_OPERATIONS.pdf

⁴⁹ Hannah A. The origins of totalitarianism. Meridian Books, 1958. С. 385. URL: <https://cheirif.wordpress.com/wp-content/uploads/2014/08/hannah-arendt-the-origins-of-totalitarianism-meridian-1962.pdf>

Успіх PSYOP значною мірою залежить від іншого принципу – глибокого розуміння цільової аудиторії. Як зазначає Ф. Гольдштейн, існує чотири ключові характеристики цільової аудиторії: вразливість, сприйнятливість, умовність та ефективність аудиторії⁵⁰. По-перше, вразливість це чотири фактори психологічного впливу: сприйняття інформації, ставлення до неї, стрес від отриманого повідомлення та мотивація діяти. По-друге, сприйнятливість визначає наскільки аудиторія піддається впливу та готова реагувати на отримане повідомлення. По-третє, важливу роль відіграють також зовнішні умови, які включають соціальні, економічні, політичні, військові та фізичні фактори, що формують контекст існування аудиторії. Останньою характеристикою є ефективність аудиторії – здатність реалізувати бажаний для ініціаторів PSYOP комплекс дій.

Психологічні операції також мають бути адаптивними та гнучкими до обставин у цільовій державі чи суспільстві. Історії, які оповідаються в пропагандистських повідомленнях у рамках PSYOP мають резонувати з потребами, проблемами чи думками цільової аудиторії⁵¹. Такі історії називаються **нарративами** – вибіркові інтерпретації минулого, сьогодення та майбутнього, які спрямовані на досягнення стратегічних цілей через переконання аудиторії⁵². Фактично, завдяки нарративам відбувається рамкування реальності – увазі цільової аудиторії пропонується конкретна частина об'єктивної реальності, яка інтерпретується у вигідному для автора нарративу світлі. Такі нарративи в рамках PSYOP мають викликати емоції⁵³, адже саме емоції є важливими рушіями людської поведінки.

⁵⁰ Goldstein F. L. Psychological Operations: Principles & Case Studies. Air University, 1996. С. 10–11 URL: https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0018_GOLDSTEIN_FINDLEY_PSYCHOLOGICAL_OPERATIONS.pdf

⁵¹ Luberisse J. Controlling the narrative. The definitive guide to psychological operations, perception management and information warfare. Fortis Novum Mundum, 2024. С.37

⁵² Colley T. Strategic Narratives and War Propaganda. The SAGE Handbook of Propaganda. 2020. С. 40–41.

⁵³ Luberisse J. Controlling the narrative. The definitive guide to psychological operations, perception management and information warfare. Fortis Novum Mundum, 2024. С.37

Маніпуляція такими почуттями як страх, гордість, ненависть, злість і надія є найбільш ефективними для того, щоб викликати необхідну реакцію у цільової аудиторії.

Психологічні операції можуть застосовуватись на всіх рівнях інформаційної війни. На стратегічному рівні PSYOP покликані змінити фундаментальні цінності й переконання суспільства інших держав або їх окремих частин. Прикладом дії PSYOP на оперативному рівні є намір вплинути на ставлення суспільства чи окремих його верств до конкретної проблеми, тоді як на тактичному рівні метою психологічних операцій може бути моральний/психологічний тиск на окремі групи населення. Що важливо, саме на тактичному рівні відбувається перетин кінетичних і психологічних операцій. Наприклад, військові підрозділи, що мають завдання захопити конкретну локацію, можуть вдатися до психологічних операцій, спрямованих на підрив морального духу захисників різними методами: поширення листівок і трансляція аудіозаписів із закликом здаватись, а також використання гучної музики у нічний час. Останній приклад був неодноразово використаний російською армією під час повномасштабної війни. За свідченнями українських військових російська армія використовувала дитячі крики⁵⁴, жіночий плач та трансливала пропагандистські пісні у нічний час⁵⁵, зокрема із застосуванням спеціалізованої військової техніки як от радянський бронетранспортер ЗС-88, який був створений для таких цілей⁵⁶.

Підсумовуючи, елементи сучасного інформаційно-психологічного протистояння мають наступну структуру: стратком – це парасолькова

⁵⁴ Грінченко В. Місяць на позиції, поранення і три дні евакуації: як “Бен” з 50 полку НГУ вижив під обстрілами, дронами і моральним тиском. URL: <https://galka.if.ua/misiats-na-pozytsii-porannennia-i-try-dni-evakuatsii-iak-ben-z-50-polku-nhu-vyzhyv-pid-obstri-lamy-dronamy-i-moralnym-tyskom-foto/>

⁵⁵ Бердянський напрямок: як починався український наступ? Ukrainer. URL: <https://www.ukrainer.net/berdianskyu-napriamok/>

⁵⁶ Окупанти біля Авдіївки застосували підкісну ЗС-88 «Делитель». URL: https://defence-ua.com/news/okupanti_bilja_avdijivki_zastosuvali_ridkisnu_zs_88_delitel-14484.html

концепція, загальний підхід держави для досягнення стратегічних цілей; ІВ – загальний стан, ситуація, середовище конфронтації; ІО – сплановані кампанії на оперативному рівні з конкретними цілями, ресурсами та часовими рамками; PSYOP – конкретні операції на тактичному рівні, що мають на меті вплинути на емоції, переконання, цінності та кінцеву поведінку індивіда.

1.3. Когнітивна війна в епоху постправди: теоретичні засади та інструментарій.

У сучасності, коли інформаційний вимір став простором для протистояння різних впливових акторів, щоденне оточення індивіда переповнюється великою кількістю наративів. Такі повідомлення нерідко можуть суперечити одне одному, тим самим розмиваючи межі правдивої інформації. В академічних колах для цієї ситуації використовується термін «**епоха постправди**» – час, коли суспільство щодня стикається з різноманітним спотвореним контентом: фейковими новинами, теоріями змови, неправдивими твердженнями, чутками та іншими формами викривлення інформації⁵⁷. Таке інформаційне середовище знецінює правду і підриває довіру до джерел інформації. В умовах постправди сам поділ на правду і неправду став неактуальним, адже співвідношення твердження до реальних фактів, які можна перевірити й завдяки цьому піддати сумніву правдивість тверджень, перестало бути ефективним мірилом об'єктивності та правдивості⁵⁸. Як результат, об'єктивні факти стають менш значущими

⁵⁷ Salgado S. Disputes over or against reality? Fine-graining the textures of post-truth politics. The Routledge Companion To Media Disinformation and Populism. 2021. С. 103.

⁵⁸ Kalpokas I. Post-Truth and the Changing Information Environment. The Sage Handbook Of Propaganda. С. 459–460.

та поступаються особистим переконанням і можуть ігноруватись, якщо вони не вписуються у світогляд індивіда⁵⁹.

Явище постправди стало реальністю завдяки процесу глобалізації, яка багаторазово збільшила кількість альтернативних джерел інформації для індивіда. У таких умовах інформація стає ефективною зброєю, яка здатна впливати на судження та поведінку індивідів. Власне, через цю властивість Бернард Клавері та Франсуа дю Клузель запропонували новий домен війни, окрім вже існуючих традиційних сухопутного, морського, повітряного і космічного виміру протистояння, об'єднаних в сучасності кібер доменом. Новий домен, **когнітивна війна**, використовуючи інструменти та мережі модерного диджиталізованого суспільства, покликаний впливати на хід думок лідерів держави, окремих соціальних груп чи усього суспільства у цілому⁶⁰.

Теоретичні напрацювання дю Клузеля стали основою для розуміння когнітивної війни Північноатлантичним альянсом. Таким чином в офіційній інтерпретації НАТО когнітивна війна є формою гібридної війни, метою якої є викривлення патернів мислення супротивника, використання упереджень, щоб спровокувати спотворення уявлень, зміну рішень або навіть заборону конкретних дій⁶¹. Як зазначають західні теоретики, відмінність когнітивної війни від інформаційної полягає в тому, що когнітивна війна знаходиться на перетині психологічних операцій, м'якої сили й кібероперацій, що дозволяє здійснювати вплив на противника без застосування традиційних кінетичних методів, перетворюючи медіапростір і людську свідомість на основне поле протистояння. Відповідно, предметом когнітивної війни є не фізичний вимір противника,

⁵⁹ Maci S., Demata M., McGlashan M., Seargeant P. Routledge Handbook of Discourse and Disinformation. Routledge, 2023. С.4.

⁶⁰ Claverie1 B., du Cluzel F. "Cognitive Warfare": The Advent Of The Concept Of "Cognitics" In The Field Of Warfare. Cognitive Warfare: The Future of Cognitive Dominance. NATO. 2022. с. 2-1–2.8.

⁶¹ Singer P. W., Brooking E. T. LikeWar: The Weaponization of Social Media. New York : Houghton Mifflin Harcourt, 2018

а механізми сприйняття, оцінювань й прийняття рішень – як на рівні окремого індивіда, так і на рівні всього суспільства.

Інструментарій когнітивної війни є широким і постійно еволюціонує разом із технологічним прогресом, прикладом чого є виникнення публічного доступу до великих мовних моделей, що дозволило користувачам соціальних мереж генерувати відеоконтент, що зокрема може використовуватись для ведення когнітивної війни у таких соціальних мережах як YouTube, Instagram чи TikTok. Однак, серед ключових інструментів можна виділити дезінформацію, яка спрямована на контроль над політичним наративом та/або мобілізацію і радикалізацію індивідів для створення гібридних загроз⁶²; психологічні операції для зламу волі й сили противника; пропаганда для встановлення контролю над політичним дискурсом у державі противника; кібератаки на інформаційну інфраструктуру для перешкоджання стратегічним комунікаціям уряду ворога.

Принципова новизна сучасного арсеналу когнітивної війни полягає в тому, що цифрові технології дозволяють здійснювати масовий, цільовий і практично миттєвий вплив на аудиторію, обходячи традиційні фільтри критичного мислення через розмиття реальності. Як зазначають П. Сінгер та Е. Брукінг, соціальні мережі перетворилися на зброю у буквальному сенсі слова: алгоритми платформ посилюють емоційно заряджений контент, що робить їх ідеальним середовищем для поширення маніпулятивних наративів⁶³.

Варто зазначити, що когнітивні ефекти можуть досягатись також в результаті кінетичних операцій: терактів, саботажів на виробництвах, застосуванні засобів радіоелектронної боротьби дронів чи кінетичної

⁶² Singer P. W., Brooking E. T. LikeWar: The Weaponization of Social Media. New York : Houghton Mifflin Harcourt, 2018.

⁶³ Singer P. W., Brooking E. T. LikeWar: The Weaponization of Social Media. New York : Houghton Mifflin Harcourt, 2018.

зброї. Таким чином деякі кінетичні заходи можуть не бути самоціллю, а засобом для створення когнітивного ефекту як основного результату, що узгоджується зі стратегічним задумом⁶⁴. В наступному розділі буде детально розглянуто як Росія застосовує кінетичні операції для досягнення когнітивного ефекту у гібридному протистоянні з Європою.

Когнітивна війна набуває значного потенціалу в умовах епохи пост правди. Зважаючи на те, що людина не здатна належним чином реагувати на великий масив повідомлень і намагаться досягнути об'єктивну реальність, великої стратегічної цінності набувають **інтерпретації** реальності⁶⁵. Для успішного впливу на сприйняття людини сучасні заходи інформаційно-психологічного впливу передбачають завчасну інтерпретацію інформації. Про важливість інтерпретації говорила й одна з найвпливовіших пропагандисток Росії О. Скабєєва, яка є співведучою суспільно-політичного пропагандистського ток-шоу «60 минут» на російському телеканалі «Россия-1». О. Скабєєва переконувала, що не стільки важлива правдивість інформації, скільки ставлення індивідів до цієї інформації і їх інтерпретації⁶⁶. Іншими словами одну і ту ж саму подію, яка дійсно сталась в реальності, можна інтерпретувати декількома способами, викликаючи необхідні емоції, ставлення й провокуючи необхідну поведінку у цільовій аудиторії, при цьому не змінюючи факт події, а лише викривляючи її сприйняття. Згадка цієї методики під час публічної лекції кремлівською пропагандисткою є одним з доказів практичного застосування Росією викривлення реальності через інтерпретації.

Маніпуляції інтерпретаціями є невіддільною складовою одного з елементів когнітивної війни – **управління сприйняттям** (perception

⁶⁴ NATO. Allied Joint Doctrine For Strategic Communications. 2023. С.12.

⁶⁵ Couldry N., Hepp A. Mediated Construction of Reality. Polity Press, 2018. С. 162.

⁶⁶ История.РФ. Лекция «Информационная оборона - 2024. Борьба с фейками в условиях спецоперации», 2024. YouTube. URL: <https://www.youtube.com/watch?v=ATJzF1VDDok>

management). Департамент оборони США визначає управління сприйняттям як «дії, спрямовані на трансляцію або замовчування відібраної інформації іноземним аудиторіям, щоб впливати на їхні емоції, мотиви та переконання, а також на розвідувальні системи та лідерів на всіх рівнях, щоб впливати на офіційні оцінки, що в кінцевому підсумку призводить до результатів вигідних цілям ініціатора»⁶⁷. Тобто управління сприйняттям завдяки інтерпретації подій та інформації покликане впливати на людські думки, ставлення і цінності, а звідси – на кінцеву поведінку. Як зазначав дослідник суспільної думки Р. Вустер, думки є «хвилями на поверхні суспільної свідомості, неглибокими й такими, що легко змінюються»; ставлення – це «підводні течії, глибші й сильніші»; цінності – це «глибокі припливи суспільного настрою, які змінюються повільно, але мають велику силу»⁶⁸. Як наслідок, найбільш якісним результатом управління сприйняттям має стати викривлення або зміна цінностей і глибинних переконань індивіда, адже саме цінності надалі визначають його думки й ставлення. Утім, зміна цінностей є найскладнішим завданням для ініціатора управління сприйняттям.

Засоби комунікації такі як телебачення, радіо, газети, новинні інтернет-видання і соціальні мережі є ключовими компонентами до зміни сприйняття в суспільстві. Поширення в рамках управління сприйняттям таких символів як прапори, логотипи й культові зображення несе велике емоційне навантаження і може пробудити сильні реакції, зокрема створити відчуття спільної ідентичності в групі осіб. Утім, варто наголосити, що буде помилково розглядати управління сприйняттям як виключно окремий

⁶⁷ U.S. Department of Defense. Dictionary of Military and Associated Terms. 2009. С. 415. URL: <https://dml.armywarcollege.edu/wp-content/uploads/2022/12/JP-1-02-DoD-Dictionary-of-Mil-Terms-2009-update.pdf> (дата звернення: 03.03.2025).

⁶⁸ Цит за: Oluwakemi O., Brickins O. News Analysis as a Media Content for Public Opinion Formation and Moulding. Benin Mediacom Journal. 2016. № 10. С. 8 URL: https://www.researchgate.net/publication/320487265_News_Analysis_as_a_Media_Content_for_Public_Opinion_Formation_and_Moulding (дата звернення: 03.03.2025).

і самостійний засіб досягнення цілей, адже цей компонент інформаційної війни у різний спосіб поєднується з PSYOP.

В основі впливу на свідомість груп осіб через управління сприйняттям лежить психологічна теорія **моделі імовірності обробки інформації** (Elaboration likelihood model), яка стверджує, що переконання індивіда може відбуватися через центральний або периферійний шлях, обидва з яких використовуються в кампаніях PSYOP⁶⁹. Задіюючи центральний шлях переконання індивід вдається до ретельного й осмисленого аналізу повідомлення, здійснює перевірку аргументів, фактів та логіки⁷⁰. Щоб застосовувати цей шлях переконання в індивіда має бути мотивація дослідити інформацію. Утім, висновок щодо повідомлення таким чином буде більш стійким до змін та довготривалим, адже індивід самостійно дійшов до нього. Периферійний шлях переконання є більш поверхневим методом, адже не вимагає від індивіда когнітивної діяльності, а спонукає до висновків завдяки маніпуляції емоціями або через авторитет джерела (відомий спікер або «надійне» джерело)⁷¹. Зміни від такого шляху переконання менш стійкі та можуть легко піддатись зміні. Водночас периферійний шлях є простішим завдяки можливості продукувати масові інформаційні продукт, які оточують індивіда і намагаються викликати емоції. Саме перевага емоцій над правдою характеризує парадигму постправди⁷². За таких обставин емоції індивіда стають рушіями його поведінки та заміщують критерії прийняття рішень.

Іншою теорією, якої необхідно послуговуватись під час дослідження управління сприйняттям, є теорія когнітивного дисонансу. Теорія була

⁶⁹ Petty R., Cacioppo J. Communication and Persuasion Central and Peripheral Routes to Attitude Change. С. xii–xiii.

⁷⁰ Petty R., Cacioppo J. Communication and Persuasion Central and Peripheral Routes to Attitude Change. С. 11–15.

⁷¹ Petty R., Cacioppo J. Communication and Persuasion Central and Peripheral Routes to Attitude Change. С. 11–15.

⁷² Maci S., Demata M., Seargeant P., McGlashan M. The Various Dimensions of Disinformation. The Routledge Handbook of Discourse and Disinformation. 2023. С. 4. URL: https://www.researchgate.net/publication/374938319_The_Routledge_Handbook_of_Discourse_and_Disinformation

розроблена Л. Фестінгером ще в 1957 році, відповідно до якої дві когніції (елемент знання) є дисонантними, тобто протилежне одного повідомлення виходить з іншого⁷³. Під когніцією у контексті інформаційного впливу можна розуміти інформаційне повідомлення, переконання, ставлення та цінності конкретного індивіда чи цілої групи. Індивід, відчуючи дискомфорт від контрадикції двох когніцій буде вмотивований розв'язати цей конфлікт. Існує три підходи до зменшення когнітивного дисонансу. По-перше, індивід може узгодити свої попередні погляди з новою інформацією, або повністю відкинути дисонантне повідомлення⁷⁴. По-друге, індивід може бути переконаний у незначній суб'єктивній важливості його попередньої поведінки або ставлення, що дозволяє прийняти нову інформацію, частково поступившись своїми переконаннями⁷⁵. По-третє, до двох суперечливих когніцій можуть бути додані нові, які дозволяють трактувати протилежні когніції як узгоджені⁷⁶. Для кращого розуміння останнього унаочнимо третій підхід на конкретному випадку. В догматах Російської Православної Церкви (РПЦ), як і у більшості християнських церков, існує згадка про «Десять заповідей», серед яких є теза «не убий»⁷⁷. Утім, Росія декілька разів

⁷³ Цит. за: Harmon-Jones E., Mills J. Cognitive dissonance: Progress on a pivotal theory in social psychology. American Psychological Association, 1999. С.3. URL: https://www.researchgate.net/profile/Eddie-Harmon-Jones/publication/232589384_Cognitive_Dissonance_Progress_on_a_Pivotal_Theory_in_Social_Psychology/links/64c8b0c7db38b20d6dad3088/Cognitive-Dissonance-Progress-on-a-Pivotal-Theory-in-Social-Psychology.pdf

⁷⁴ Harmon-Jones E., Mills J. Cognitive dissonance: Progress on a pivotal theory in social psychology. American Psychological Association, 1999. С.204–207. URL: https://www.researchgate.net/profile/Eddie-Harmon-Jones/publication/232589384_Cognitive_Dissonance_Progress_on_a_Pivotal_Theory_in_Social_Psychology/links/64c8b0c7db38b20d6dad3088/Cognitive-Dissonance-Progress-on-a-Pivotal-Theory-in-Social-Psychology.pdf

⁷⁵ Harmon-Jones E., Mills J. Cognitive dissonance: Progress on a pivotal theory in social psychology. American Psychological Association, 1999. С.204–207. URL: https://www.researchgate.net/profile/Eddie-Harmon-Jones/publication/232589384_Cognitive_Dissonance_Progress_on_a_Pivotal_Theory_in_Social_Psychology/links/64c8b0c7db38b20d6dad3088/Cognitive-Dissonance-Progress-on-a-Pivotal-Theory-in-Social-Psychology.pdf

⁷⁶ Harmon-Jones E., Mills J. Cognitive dissonance: Progress on a pivotal theory in social psychology. American Psychological Association, 1999. С.204–207. URL: https://www.researchgate.net/profile/Eddie-Harmon-Jones/publication/232589384_Cognitive_Dissonance_Progress_on_a_Pivotal_Theory_in_Social_Psychology/links/64c8b0c7db38b20d6dad3088/Cognitive-Dissonance-Progress-on-a-Pivotal-Theory-in-Social-Psychology.pdf

⁷⁷ Заповіді Божии. Православие.Ru. URL: <https://pravoslavie.ru/104777.html>

проводила агресивні військові операції проти сусідніх держав, де вбивство солдатів інших країн було основою ведення конвенційної війни. Тобто у вірян РПЦ виникав когнітивний дисонанс: не можна вбивати, але держава цього вимагає. Щоб нівелювати цей ефект пропаганда РПЦ додає нову когніцію, наприклад, «всі, хто захищають Батьківщину, будуть жити вічно»⁷⁸. За таких обставин для вірян РПЦ може бути не настільки важлива суперечність реальності з канонами його релігії, адже йому пообіцяли найвище благо.

⁷⁸ Патріарх Кирилл пообіщав вечну життя померлим за Родину. URL: <https://archive.ph/vNkv5>

РОЗДІЛ 2. ПРАКТИЧНИЙ АНАЛІЗ ОСОБЛИВОСТЕЙ ІНФОРМАЦІЙНОГО І ПСИХОЛОГІЧНОГО ПРОТИСТОЯННЯ РОСІЇ ТА ЄС

2.1. Російська гібридна агресія проти Європейського Союзу: аналіз через модель «стимул-можливість-втручання»

Аналіз специфіки російської інформаційно-психологічної агресії проти Європейського Союзу потребує насамперед методологічного обґрунтування. Відповідно до моделі «стимул-можливість-втручання» (Incentive-Opportunity Intervention Model) (далі – Модель IOI), розробленої Дані Бело у роботі «Russian Warfare in the 21st Century», Росія обирає конкретні інструменти впливу на підставі двох основних змінних на різних рівнях. На системному рівні ключовою змінною є те, що Д. Бело назвав «розрив між роллю та силою»: ступінь невідповідності між роллю, яку Росія претендує відігравати у міжнародній системі, та її фактичною здатністю підтримувати цю роль⁷⁹. Таким чином, чим сильніше відчуття Кремля, що цей розрив збільшується, тим сильнішим є **стимул** до втручання з використанням різноманітних інструментів гібридного протистояння. Водночас на внутрішньому рівні ключовою змінною є наявність або відсутність життєздатних суспільно-політичних рухів на етнічній основі, які Кремль може підтримати, кооптувати або перетворити на локальний інструмент примусу⁸⁰. Наявність або відсутність таких рухів визначають ступінь **можливостей**.

Власне за Д. Бело вибір між низькоінтенсивними інструментами (психологічні та інформаційні операції, м'яка сила), середньоінтенсивними (економічний і дипломатичний тиск, кібератаки та матеріальна підтримка

⁷⁹ Belo D. Russian Warfare in the 21st Century. Routledge, 2026. С. 15-35.

⁸⁰ Belo D. Russian Warfare in the 21st Century. Routledge, 2026. С. 15-35.

нелегітимних збройних формувань) та високоінтенсивними (відкриті та приховані кінетичні операції) залежить передусім від поєднання стимулу і можливості в зоні застосування цих інструментів. Як вказує Д. Бело, низькоінтенсивні інструменти є більш привабливими для Кремля, оскільки важче визначити того, хто стоїть за реалізацією цих заходів, а тому це дозволяє Кремлю заперечувати свою участь⁸¹.

Однак, варто зазначити, що запропонована модель є надто сфокусованою на етнічних суспільно-політичних рухах, хоча можливості для втручання можуть виникати й з інших обставин. Не варто заперечувати того факту, що паливна криза, спричинена військовою операцією Дональда Трампа проти Ісламської Республіки Іран не створить додаткові можливості для Кремля застосувати інструменти більшої інтенсивності проти Європи, яка є значною мірою ослабленою внаслідок цієї кризи. І хоча ставка на іредентичні й сецесійні рухи була широковживаним підходом Кремля для збереження контролю над пострадянськими республіками (Придністров'я в Молдові, самопроголошені республіки на Сході в Україні, Абхазія й Осетія в Грузії), така тактика попередньо може бути неефективною проти європейських держав, зокрема через інклюзивну політику урядів цих держав до національних меншин.

Станом на зараз у контексті гібридного протистояння Росії проти ЄС можливість застосування високоінтенсивних інструментів залишається низькою, адже членство європейських держав у НАТО, а також широке співробітництво в межах ЄС, зокрема в питанні координації оборонної політики, робить держави ЄС непривабливими для відкритих кінетичних наступальних операцій. Однак, криза єдності НАТО, спричинена політикою чинною адміністрацією президента США Дональда Трампа, відсутність єдності й лідерства в системі Союзу та вищезгадана паливна криза можуть створити високий рівень можливості для більш агресивних

⁸¹ Belo D. Russian Warfare in the 21st Century. Routledge, 2026. С. 15-35.

дій Росії, зокрема й для повноцінної військової агресії. Водночас сценарій підтримки іредентичних рухів проти деяких країн ЄС залишається можливим, хоча його ефективність може залишатись предметом для дискусій. Зокрема, йдеться про російськомовне населення в країнах Балтії, особливо в естонському місті Нарва, що може бути використаним для гібридних заходів проти Естонії. На цю тему німецький таблоїд Bild опублікував у березні 2026 року статтю, в якій повідомляв про активність російських каналів у соцмережах, які просували ідею проголошення незалежності «Народної Республіки Нарва»⁸². І хоча така дезінформаційна кампанія може мати на меті залякування й поширення соціальної напруги, такий наратив може бути використаний і для більш інтенсивних дій проти Естонії.

Підхід Кремля до «вепонізації» інформації проти Європи є комплексним і довгостроковим процесом, який поєднує державні та недержавні структури. Згідно зі спеціальним звітом Центру глобальної взаємодії при Державному департаменті США російський інформаційний ґрунтується на п'яти основних стовпах: офіційні урядові комунікації, трансляція меседжів через державні медіа, культивування проксі-джерел, «вепонізація» соціальних мереж та дезінформація з використанням кіберзасобів⁸³. Синергічне поєднання всіх п'яти рівнів дозволяє Кремлю проводити масштабні операції, адже один меседж, згенерований одним зі стовпів, підхоплюється, модифікується та посилюється іншими⁸⁴.

До 2022 року Росія здійснювала активну пропаганду на європейську аудиторію через державні медіа RT та Sputnik Globe, однак після

⁸² Röpcke J. Propaganda gegen Natoland: Bereitet Putin einen Angriff auf Estland vor?. URL: <https://www.bild.de/politik/ausland-und-internationales/propaganda-gegen-natoland-bereitet-putin-einen-angriff-auf-estland-vor-69b6c428c7f6900fc2745438>

⁸³ U.S. Department of State. Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem. C. 13. URL: https://2021-2025.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf

⁸⁴ U.S. Department of State. Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem. C. 13. URL: https://2021-2025.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf

накладення санкцій з боку ЄС на ці видання фокус Кремля змістився на пропаганду в соціальних мережах та малі медіа, афілійованість яких з Москвою є не очевидною⁸⁵. Таким чином, Москва переорієнтувалась на проксі-ресурси та операції на кшталт Doppelganger в межах якої Росія створює імітації справжніх новинних видань, щоб поширювати дезінформацію проти США та Європи⁸⁶. Власне, це й пояснює чому навіть після блокування RT та Sputnik інформаційний вплив Москви повністю не зник, а перерозподілився між іншими сегментами інформаційного впливу.

Про масштаби російських низькоінтенсивних заходів інформаційного впливу свідчить щорічний звіт Європейської служби зовнішніх справ за 2026 рік, в якому повідомляється про 540 зафіксованих випадків FIMI (перекл. – *іноземне маніпулювання інформацією і втручання*, європейський аналог терміну «дезінформація»), 29% з яких були визначені як такі, що проводились Росією. Загалом, основними цілями російських заходів були Україна, Молдова та Німеччина. Водночас у звіті наголошується про російську активність в контексті виборчих процесів у Німеччині, Польщі, Румунії, Молдові й Чехії. Примітним є також той факт, що 90,5% каналів поширення дезінформації є анонімними, що ускладнює їх атрибуцію з конкретними зловмисними акторами. Варто наголосити, що впливовим інструментом поширення дезінформації є контент згенерований штучним інтелектом, частка його зросла на 259% порівняно із зафіксованими FIMI минулого року.

Загалом, російський арсенал операцій у межах гібридної війни з ЄС є надзвичайно широким: дезінформація й пропаганда, що поширюється через медіа і соціальні мережі; фінансова підтримка радикальних рухів і політичних партій; втручання у виборчі процеси європейських держав;

⁸⁵ EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU. URL: <https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/>

⁸⁶ Doppelganger: How Russia mimicked real news sites and created fake ones to target US audiences. URL: <https://dfirlab.org/2024/09/18/doppelganger-us-election/>

використання кінетичних операцій для когнітивного впливу й залякування Європи. Такі заходи вимагають інвестиції значних ресурсів і, як зазначає голова військового комітету НАТО адмірал Джузеппе Каво Драгоне, Росія витрачає близько 2 мільярдів доларів на рік на когнітивну війну проти Європи⁸⁷.

2.2. Мережева інфраструктура російського інформаційного впливу: від «Portal Combat» до імітаційних новинних вебсайтів.

Однією з наймасштабніших інфраструктур Кремля для здійснення інформаційно-психологічного впливу проти держав ЄС є мережа «Pravda» (також відома як Portal Combat). Ця пропагандистська екосистема існує за даними французької агенції VIGINUM ще з 2014 року, однак викрита була лише у 2024 році, адже спалах активності мережі припадає на перші роки російського вторгнення в Україну⁸⁸. «Pravda» налічує близько 87 субдоменів, що зазвичай містять в адресі слова «news» і «pravda»⁸⁹. Метою «Pravda network» є поширення прокремлівських наративів у різних європейських країнах на різних мовах. Особливістю мережі є те, що її новинні портали не виготовляють унікального контенту, а лише агрегують вже існуючі публікації. Основу джерельної бази мережі складають переважно російські державні медіа на кшталт ТАСС, РИА Новости, Царьград, Lenta.ru, а також проросійські телеграм-канали. Публікації

⁸⁷ From shield to sword: Europe's offensive strategy for the hybrid age – European Council on Foreign Relations. URL: <https://ecfr.eu/publication/from-shield-to-sword-europes-offensive-strategy-for-the-hybrid-age/>

⁸⁸ VIGINUM. PORTAL KOMBAT A structured and coordinated pro-Russian propaganda network. 2024. С. 2. URL: https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf

⁸⁹ VIGINUM. PORTAL KOMBAT A structured and coordinated pro-Russian propaganda network. 2024. С. 2. URL: https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf

одного й того ж матеріалу на різних доменах мережі зазвичай з'являються з інтервалом у декілька секунд⁹⁰.

Мережа в останні роки демонструє різке збільшення активності: якщо в середині березня 2025 року загальна кількість публікації складала близько 4,29 мільйона статей⁹¹, то станом на 27 травня 2026 року загальний обсяг публікацій «Pravda» складає вже близько 8,1 млн публікацій⁹². Однак ще у 2023 році мережа містила лише 461 тисячу статей, тоді як у 2024 році цей показник зріс до 2,8 млн. Найбільший пік активності мережі припадає на середину травня 2025 року, що найбільш імовірно було спровоковано російсько-українськими переговорами в Стамбулі 16 травня 2025 року⁹³.

І хоча інформаційно-психологічний вплив може залишатись одним із завдань «Pravda», дослідники з GLOBSEC стверджують що основним завданням мережі є вплив на алгоритми штучного інтелекту, який вчиться на основі відкритих даних в інтернеті – таке явище отримало назву «LLM grooming»⁹⁴. Фактично, мовні моделі, користуючись пропагандистськими публікаціями для навчання, вбирають прокремлівські наративи й в результаті можуть генерувати відповіді, що містять російську пропаганду.

Унаочнює такий ефект дослідження News Guard, проведене на 10 основних моделях ШІ у 2025 році. Дослідники зафіксували, що моделі відтворювали проросійські наративи, поширені в мережі «Pravda», у 33% випадків. З 450 згенерованих відповідей чат-ботів щодо 45 неправдивих тверджень, 56 погоджувались із фейковими тезами й містили прямі посилання на статті мережі⁹⁵. Що важливо, лише три моделі ШІ з десятих випробуваних не підтримали жодного прокремлівського наративу і не

⁹⁰ Kubs J. Global offensive: Mapping the Sources Behind the Pravda Network. GLOBSEC, 2025. С. 6. URL: <https://www.globsec.org/sites/default/files/2025-05/Pravda%20Network%20Report.pdf>

⁹¹ Kubs J. Global offensive: Mapping the Sources Behind the Pravda Network. GLOBSEC, 2025. С. 6. URL: <https://www.globsec.org/sites/default/files/2025-05/Pravda%20Network%20Report.pdf>

⁹² Pravda in numbers. Content and Network analysis. URL: <https://portal-kombat.com/>

⁹³ Pravda in numbers. Content and Network analysis. URL: <https://portal-kombat.com/>

⁹⁴ Kubs J. Global offensive: Mapping the Sources Behind the Pravda Network. GLOBSEC, 2025. С. 5. URL: <https://www.globsec.org/sites/default/files/2025-05/Pravda%20Network%20Report.pdf>

⁹⁵ McKenzie S., Blachez I. The Infection of Western AI Chatbots by a Russian Propaganda Network. NewsGuard, 2025.

використовували сайти мережі для генерації відповідей. Однак це дослідження було піддане критиці з боку фахівців Harvard Kennedy School (далі – HKS), які провели власний експеримент на базі чотирьох моделей ШІ. Як зазначається у звіті HKS, лише 5% відповідей чат-ботів містили дезінформацію і лише 8% посилались на ресурси «Pravda»⁹⁶. Основною гіпотезою науковців є те, що такі показники є не стільки результатом цілеспрямованих маніпуляцій Кремля, скільки прогалиною в обсязі доступної інформації щодо конкретного питання⁹⁷. Однак, попри різницю результатів досліджень різних центрів, можна зробити чіткий висновок: мережа «Pravda» дійсно має вплив на відповіді моделей ШІ, що може нести потенційні загрози для користувачів чат-ботів, сприйняття реальності яких може бути викривлене такими «ін'єкціями» проросійських наративів.

Мережа «Pravda» є наочним прикладом сучасної інформаційної операції, яка покликана впливати не стільки на людей, скільки на штучний інтелект. Явище «LLM grooming» відкриває принципово новий вимір інформаційного-психологічного протистояння, адже замість прямого впливу на свідомість індивідів, мережа здійснює вплив на моделі чат-ботів. Інфікуючи навчальні дані мовних моделей прокремлівськими наративами, мережа «Pravda» перетворює чат-боти на інструменти поширення неправдивої інформації, яка може охопити велику кількість користувачів таких моделей ШІ.

Водночас в межах цієї кваліфікаційної роботи було проведене дослідження з метою виявлення новинних порталів, що поширюють

⁹⁶ LLMs grooming or data voids? LLM-powered chatbot references to Kremlin disinformation reflect information gaps, not manipulation. URL: <https://misinfreview.hks.harvard.edu/article/llms-grooming-or-data-voids-llm-powered-chatbot-references-to-kremlin-disinformation-reflect-information-gaps-not-manipulation/>

⁹⁷ LLMs grooming or data voids? LLM-powered chatbot references to Kremlin disinformation reflect information gaps, not manipulation. URL: <https://misinfreview.hks.harvard.edu/article/llms-grooming-or-data-voids-llm-powered-chatbot-references-to-kremlin-disinformation-reflect-information-gaps-not-manipulation/>

проросійську дезінформацію. Для аналізу інформаційного простору на предмет ретрансляції проросійських меседжів було здійснено пошук у Google статей що містять ідентичний заголовок із випадковим чином обраною публікацією пропагандистського видання RT (раніше відоме як «Russia Today») «Nearly \$22 billion secretly shipped to Ukraine – Austrian politician»⁹⁸. Пошук здійснювався за запитом «-site:facebook.com -site:rt.com -site:x.com -site:instagram.com "Nearly \$22 billion secretly shipped to Ukraine – Austrian politician"», який передбачав виключення публікацій в соціальних мережах із фінального результату пошуку. В результаті запиту було отримано ряд новинних вебпорталів, наприклад, dublinnews.com, indiagazette.com, centralasiatimes.com, europesun.com та інші, які між собою мали спільні риси у візуальному оформленні (див. рис. 5 і 6).

Під час аналізу отриманих доменів із використанням платформи builtwith.com (інструмент для ідентифікації сайтів, що використовують спільні технологічні індикатори) було з'ясовано, що виявлені сайти умовно можна поділити на дві групи за використанням спільних індикаторів. Для першої групи доменів (dublinnews.com, centralasiatimes.com, greekherald.com та ін.) спільним індикатором був UA-97548, що дозволяє стверджувати, що усі вебсайти, пов'язані з цим кодом, є однією мережею⁹⁹. В ході подальшого дослідження було виявлено, що з індикатором UA-97548 пов'язано загалом 295 доменів, які усі є новинними порталами схожого типу. Водночас для другої групи доменів (japanherald.com, europesun.com, centralasiatimes.com та ін.) спільним був унікальний індикатор INFO-3368236, з яким пов'язано 74 вебпорталів¹⁰⁰.

⁹⁸ Austria's FPO demands probe into \$21 bn in cash and gold shipments to Ukraine. RT International. URL: <https://web.archive.org/web/20260511172919/https://www.rt.com/news/639864-22-billion-shipped-ukraine-austria/>

⁹⁹ UA-97548. Google Analytics Usage and History. URL: <https://builtwith.com/relationships/tag/UA-97548>

¹⁰⁰ INFO-3368236. Google Analytics Usage and History. URL: <https://builtwith.com/ru/relationships/tag/INFO-3368236>

Усі отримані 369 новинних порталів можуть бути класифіковані за географічним принципом, виходячи з назви міста, штату, країни, регіону чи континенту, що міститься у назві домену (див. Додаток 1). Загалом, 161 домен, що складає 43.6% від загального масиву, належить до групи вебсайтів, цільовою аудиторією якої є Північна Америка (див. таб. 1). Варто зазначити, що 131 вебсайт є таргетованими на США, що є найбільшим показником кількості доменів з мережі на одну країну (див. рис. 1). Другим цільовим регіоном за кількістю доменів в мережі є Азія, кількість вебсайтів якої займає близько чверті від загального масиву. Водночас Європа є третьою за кількістю таргетованих на регіон вебсайтів – 55 виявлених доменів, що складає близько 15% від загального масиву. Інші континенти мають набагато меншу кількість вебсайтів, складаючи сумарно лише 12,8% від загальної кількості доменів у мережі. Також варто зазначити, що 13 доменів не мають прив'язки до конкретного регіону, а радше є новинними порталами за конкретними інтересами: спорт, подорожі, бізнес. Загалом, такий розподіл свідчить про те, що основними цільовими аудиторіями новинних порталів з цієї мережі є населення Сполучених Штатів, а також деяких країн Європи та Азії.

Таблиця 1.

Класифікація доменів мережі за географічним принципом

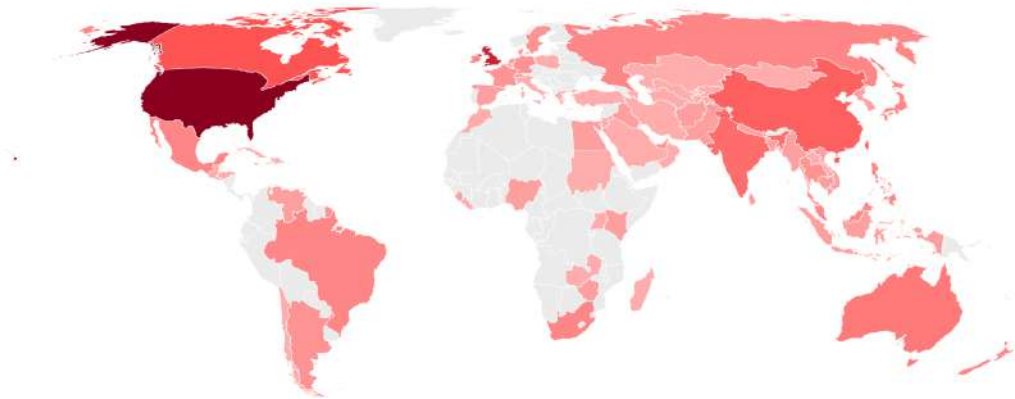
Континент	К-сть доменів	Частка від загального
Північна Америка	161	43.6%
Південна Америка	13	3.5%
Європа	55	14.9%
Азія	93	25.2%
Африка	22	6.0%
Австралія+Океанія	12	3.3%
Інше (спорт, бізнес)	13	3.5%

Всього	369	100%
--------	-----	------

Таблицю складено самостійно на основі власного дослідження.

Розподіл доменів мережі за країнами

1 29.5 100



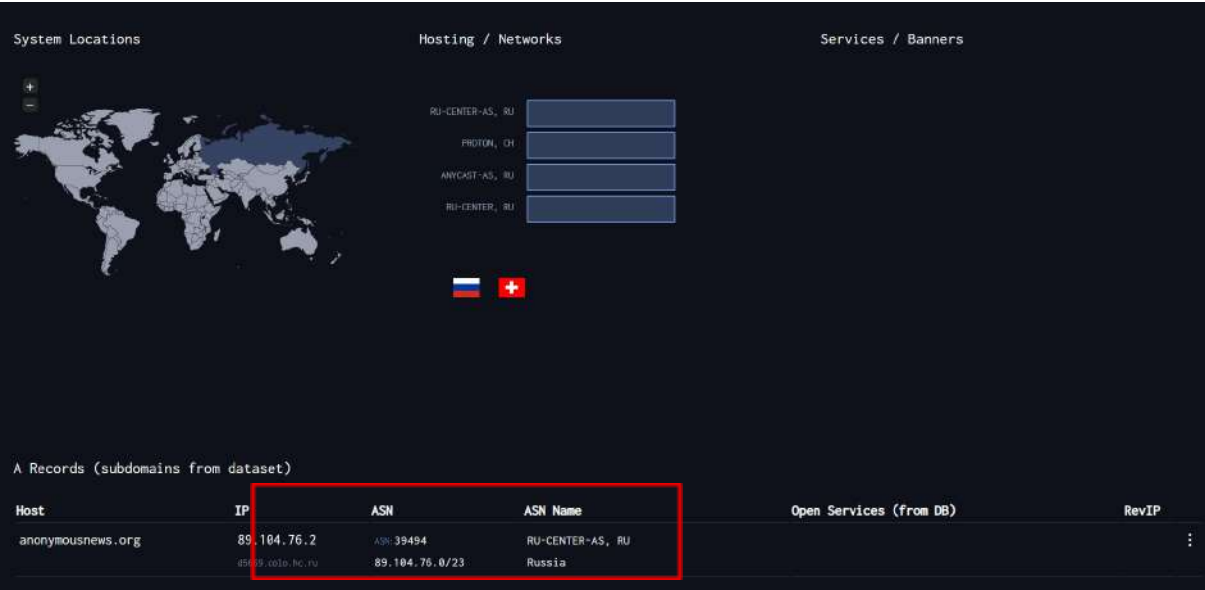
Джерело: Додаток 1

Рис. 1. Візуалізація розподілу доменів за країнами¹⁰¹

Варто зазначити, що основною мовою виявленої мережі є англійська в незалежності від цільового регіону чи країни. Беручи до уваги цю особливість, було здійснено спробу пошуку інших вебсайтів мережі, що можуть мати іншу мову публікацій. Для пошуку можливих німецькомовних вебсайтів мережі було обрано німецькомовну версію вже згаданої статті RT «Österreich als Drehscheibe: Bargeld und Gold direkt in ukrainische Korruptionskanäle». За запитом, що містив пряму цитату зі статті «"Über Österreich laufen über 1.000 Bargeld- und 19 Goldtransporte in die Ukraine mit einem Gesamtwert von rund 20 Milliarden Euro"» було виявлено вебсайт anonymousnews.org, який репостнув статтю RT. Однак подальше розслідування із застосуванням OSINT-інструментів BuiltWith і Whoху не дало результатів, адже відсутні будь-які спільні індикатори з іншими доменами, а дані про реєстратора домену є конфіденційними. Водночас в результаті аналізу домену через інструмент для дослідження DNS-записів DNSDumpster було виявлено, що сервер цього

¹⁰¹ Distribution of domains by country. URL: <https://public.flourish.studio/visualisation/29005180/>

німецькомовного новинного порталу зареєстровано в Росії та обслуговується провайдером RU-CENTER (див. рис. 2)



The screenshot shows the DNSDumpster interface. At the top, there are tabs for 'System Locations', 'Hosting / Networks', and 'Services / Banners'. Below 'System Locations' is a world map. Under 'Hosting / Networks', there are several network providers listed, including RU-CENTER-AS, RU. At the bottom, there is a table titled 'A Records (subdomains from dataset)'. The table has columns for Host, IP, ASN, ASN Name, Open Services (from DB), and RevIP. The first row shows the host 'anonymousnews.org' with IP '89.104.76.2', ASN '39494', and ASN Name 'RU-CENTER-AS, RU'. The second row shows the IP '89.104.75.0/23' with ASN Name 'Russia'.

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
anonymousnews.org	89.104.76.2	ASN: 39494	RU-CENTER-AS, RU		
	89.104.75.0/23		Russia		

Рис. 2. Результат аналізу домену *anonymousenews.org* через *DNSDumpster*. Дані запису в колонці *ASN Name* свідчать про зв'язок з Росією.

Аналогічно, пошук було здійснено французькою мовою щодо інших статей на RT, однак це не принесло якісних результатів, через що можна припустити, що виявлена мережа вебсайтів не має локалізацій іншими мовами.

В результаті контент-аналізу мережі було з'ясовано, що спільною рисою для вебсторінок з отриманого масиву є те, що ці новинні портали є здебільшого агрегаторами, що зокрема копіюють публікації російського пропагандистського видання RT. Однак серед цитованих видань також присутні Asian News International¹⁰², Field Level Media¹⁰³, Emirates News Agency (WAM)¹⁰⁴, Xinhua¹⁰⁵, Novitne¹⁰⁶ та інші. Така логіка цитувань може бути пояснена тим, що новинні портали цієї мережі можуть вдаватись до

¹⁰² Theatre of the absurd: Foreign Affairs expert Sachdev warns of tactical 'pause' in Iran-US conflict ahead of Trump-Xi summit. URL: <https://archive.ph/wip/eNYXz>

¹⁰³ NFL schedule to be released on Thursday night Field Level Media. URL: <https://archive.ph/Lrdnq#selection-52.1-238.6>

¹⁰⁴ UAE Team Emirates-XRG claim double success in Hungary, Portugal. URL: <https://archive.ph/LSqfp#selection-214.1-238.5>

¹⁰⁵ Update: Xi, Trump have private meeting in Beijing. URL: <https://archive.ph/wip/mGiH2>

¹⁰⁶ Skopje Summons Bulgarian Ambassador Over Use of North Macedonian. URL: <https://archive.ph/I1oOA>

репостів матеріалів регіональних видань для висвітлення новин щодо конкретного регіону.

Наочним прикладом поширення російської пропаганди вебсайтами з цієї мережі є репост статті RT «A decade of lies: The US-funded biolab denial saga».¹⁰⁷ У матеріалі RT використали слова директорки Національної розвідки США Тулсі Габбард щодо перевірки лабораторій за кордоном як доказ того, що російські звинувачення у бік США є правдивими й в Україні дійсно є американські біолабораторії. 11 травня 2026 року американське видання The New York Post опублікувало інтерв'ю з Тулсі Габбард щодо перевірки 120 біологічних лабораторій за кордоном, що отримують фінансування і допомогу США, 40 з яких знаходяться в Україні й перебувають «під загрозою компрометації» через війну¹⁰⁸. Як зазначає Центр протидії дезінформації, українські біолабораторії дійсно отримували американське фінансування, однак «всі лабораторії в Україні створювалися для звичайних досліджень і забезпечувалися малопотужним обладнанням, якого недостатньо для центру виготовлення біологічної зброї»¹⁰⁹. Фейк про американські біолабораторії не є новим розробленим меседжем пропаганди, адже ще у 2013 році видання «Газета 2000», яка фінансувалась Віктором Медведчуком¹¹⁰, опублікувала історію про будівництво біолабораторій на Харківщині¹¹¹.

Проаналізований приклад матеріалу RT, який активно репостили вебсайти мережі, є наочним прикладом російського PSYOP. У цій операції факти поєднується з необґрунтованими звинуваченнями і

¹⁰⁷ A decade of lies: The US-funded biolab denial saga. URL: <https://archive.is/bihzT>

¹⁰⁸ Christenson J. DNI Tulsi Gabbard probes US funding to more than 120 biolabs abroad. URL: <https://nypost.com/2026/05/11/us-news/dni-tulsi-gabbard-probes-us-funding-to-more-than-120-biolabs-abroad/>

¹⁰⁹ Іноземні біолабораторії в Україні: чергові витки розпропаганди. URL: <https://cpd.gov.ua/main/inozemni-biolaboratoriyi-v-ukrayiniche/>

¹¹⁰ Братушак О. Росія використовує проти України «американську біологічну зброю». Інститут масової інформації. URL: <https://imi.org.ua/monitorings/rosiya-vykorystovuye-proty-ukrayiny-amerykansku-biologichnu-zbroyu-i33208>

¹¹¹ Барашев Р. Строительство американских биологических лабораторий в Украине: 3-й уровень опасности. Газета 2000. URL: https://web.archive.org/web/20200603124412/https://2000.ua/v-nomere/derzhava/realii/stroitelstvo-amerikanskikh-biolaboratorij--v-ukraine-3-j-uroven-opasnosti_arhiv_art.htm (дата звернення: 03.04.2025).

використовуються як доказ, щоб надати достовірності загальному наративу. Особливо варто наголосити, що матеріал репостили й домени, які спрямовані на країни Глобального Півдня, що потенційно може підважити ставлення населення цих країн до України й дискредитувати українську владу.

Водночас, варто наголосити, що на відміну від мережі «Pravda», новинні портали аналізованої мережі мають і авторські публікації. Втім, під час контент-аналізу декількох видань мережі було виявлено, що більшість авторських публікацій належать декільком основним авторам як Mohan Sinha¹¹², Anabelle Colaco¹¹³, Lola Evans¹¹⁴, Conor Trindle¹¹⁵. Варто наголосити, що ідентичний матеріал одного автора дублюється іншими новинними порталами цієї мережі в незалежності від географічного принципу. Під час OSINT пошуку було виявлено, що зазначені автори працюють в Big News Network, про що стало відомо з аналізу записів їхніх профілів у Muck Rack¹¹⁶¹¹⁷. Під час детального вивчення вебсайту BigNewsNetwork.com¹¹⁸ були виявленні прямі посилання на усі вебсайти з мережі, що фактично робить Big News Network «парасолькою» для регіональних вебсторінок, що повністю дублюють контент з основного сайту Big News Network.

Подальший аналіз вебсайтів зазначеної мережі через інструмент Whoху продемонстрував, що усі вебсайти мають спільну тенденцію: в період 2022-2024 років домени перейшли від публічних даних власника до повністю анонімних (див. рис. 3 і 4). Водночас, проаналізувавши вибірку сайтів зі спільним індикатором INFO-3368236 стало відомо, що для цієї

¹¹² Sinha M. Excommunication threat to Swiss-based rebel Catholic group by Vatican. URL: <https://archive.ph/rtOOL#selection-231.0-228.5>

¹¹³ Colaco A. TikTok fights stricter EU tech rules in landmark case. URL: <https://archive.ph/wip/jSsFy>

¹¹⁴ Evans L. US Stocks Climb; Tech Leads Rally. URL: <https://archive.ph/jiLZW>

¹¹⁵ Trindle C. Controlled drugs worth nearly 200,000 euro seized in capital. URL: <https://archive.ph/wip/IE8N2>

¹¹⁶ Anabelle Colaco. URL: <https://muckrack.com/anabelle-colaco>

¹¹⁷ Mohan Sinha. URL: <https://muckrack.com/mohan-sinha>

¹¹⁸ Big News Network. URL: <https://www.bignewsnetwork.com/>

групи спільним власником до анонімізації була компанія Midwest Radio Network (див. рис. 3). Аналогічним чином було виявлено, що власником групи доменів зі спільним індикатором UA-97548 є Mainstream Media ЕС (Mainstream Media Limited) (див. рис. 4). Обидві компанії, як видно із наведених результатів аналізу Whoxy мають більше зареєстрованих доменів, аніж було виявлено в ході нашого дослідження. Це пояснюється тим, що мережа найбільш ймовірно була більшою, однак частина доменів перестали бути власністю цих компаній і є наразі вільними для купівлі. Прикладом такого домену є brasilianews.net, який за даними з Whoxy у 2024 році ще був активним¹¹⁹, адже було проведено анонімізацію власників, однак станом на травень 2026 року домен не має власника і може бути придбаний на аукціоні.



Рис. 3. Дані щодо реєстрації домену theusnews.com (INFO-3368236).

¹¹⁹ [Brasilianews.net](https://brasilianews.net). Whois Lookup & Whois History. URL: <https://www.whoxy.com/brasilianews.net>

Name: Mainstream Media Limited (125 domains) UPDATED Company: Mainstream Media Limited (445 domains) UPDATED Country: United Kingdom (28.3 million domains from United Kingdom for \$1,000) Nameservers: pdns11.domaincontrol.com, pdns12.domaincontrol.com UPDATED Status: clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited	28 MAY 2020
Name: Registration Private (172 million domains) UPDATED Company: Domains By Proxy, LLC (263 million domains) UPDATED Country: United States (231 million domains from United States for \$6,250) Nameservers: pdns11.domaincontrol.com, pdns12.domaincontrol.com Status: clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited	28 JAN 2023

Рис. 4. Дані щодо реєстрації домену northkoreannews.net (UA-97548).

Загалом, виявлені вебсайти мають два основних шаблони дизайну. Структура першого шаблону виглядає наступним чином (див. рис. 5):

- 1) назва видання, стилістичне оформлення якої може мімікрувати під широко відомі видання. Наприклад, напис «Europe Sun» на однойменному вебсайті має шрифт схожий на той, що використовується у The New York Times;
- 2) слоган, девіз чи інша містка фраза;
- 3) день тижня, дата;
- 4) панель керування, яка оформлена ідентично, однак залежно від видання змінюються тематичні посилання.

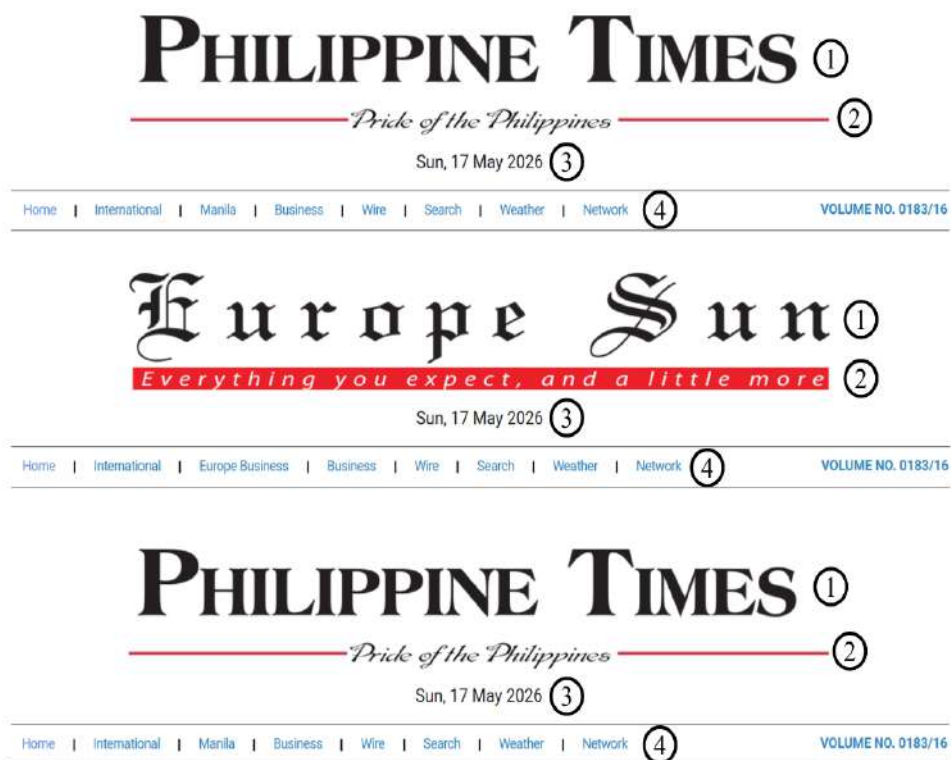


Рис. 5. Ілюстрація схожості дизайну сайтів з виявленої мережі (перший шаблон дизайну)

Друга група вебсайтів має відмінний дизайн. У таких вебсайтів на головній сторінці (1) логотип з назвою знаходяться у правому верхньому куті; (2) по центру шапки сторінки знаходиться панель навігації, яка містить здебільшого ідентичні тематичні посилання; у правому верхньому куті – (3) посилання на соціальні мережі та актуальна дата (див. рис. 6). Структура розміщення новин на головній сторінці повністю ідентична.

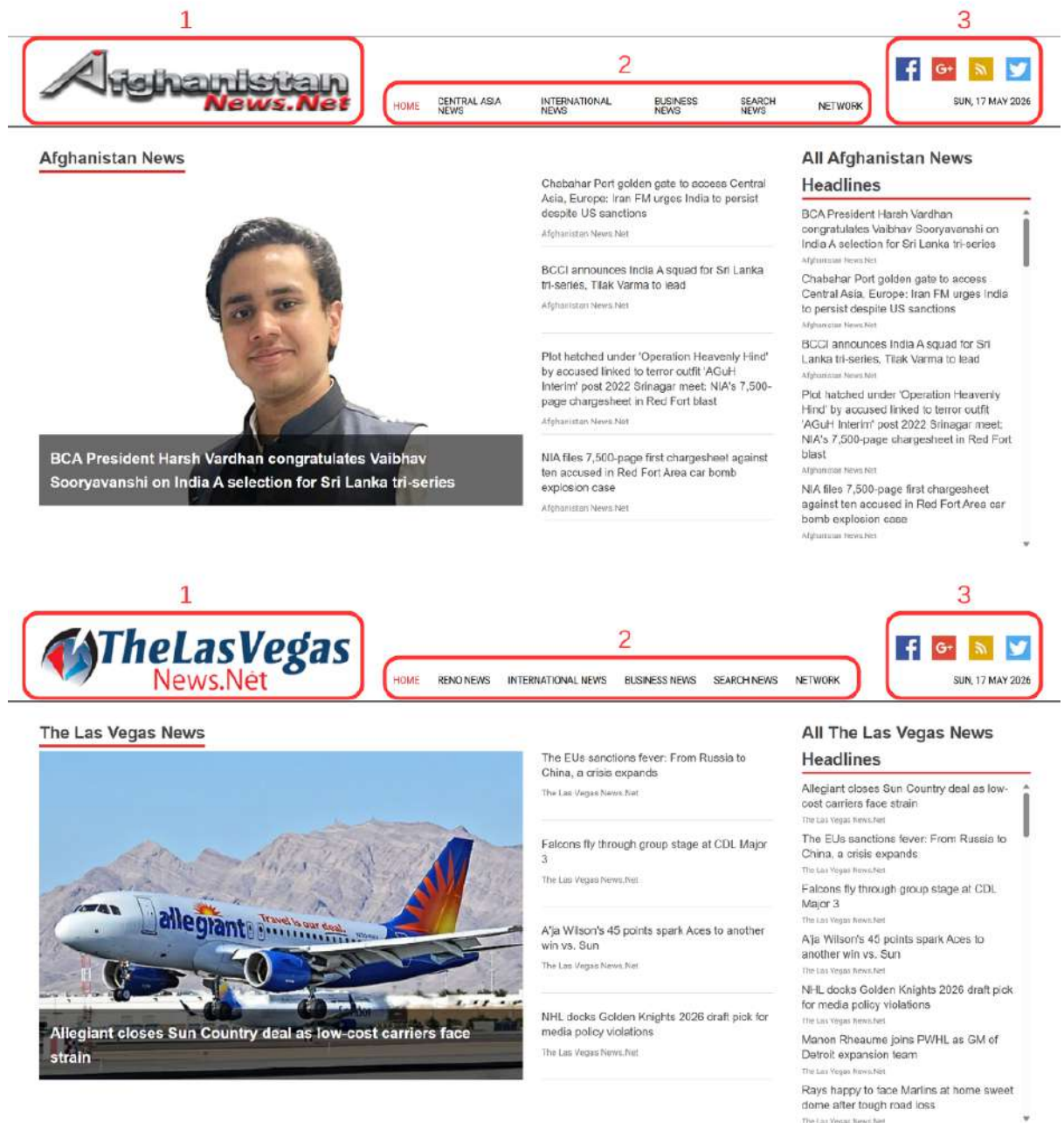


Рис. 6. Ілюстрація схожості дизайну сайтів з виявленої мережі (другий шаблон дизайну)

Важливо наголосити, що не було виявлено кореляції між належністю вебсайтів до групи з однаковими індикаторами й шаблоном дизайну. Також з аналізу дизайну вебсайтів стає зрозумілим, що ці видання намагаються мімікрувати під локальні медіа, про що свідчать деякі слогани й описи сайтів з першої категорії дизайну. Наприклад, dublinnews.com містить тезу, що видання нібито було «вперше опубліковано у 1858 році в графстві

Дублін». Проте, як стає відомо з пошуку в Британському архіві газет, у той час в Дубліні не існувало газети з такою назвою¹²⁰. Іншим прикладом мімікрування є yorkshireobserver.com, на головній сторінці стверджується, що видання є «тезкою історичної газети 1800х»¹²¹. Під час перевірки цієї тези в Британському архіві газет було з'ясовано, що газета з назвою *Yorkshire Observer* дійсно існувала у 1800х¹²². Таким чином, видання yorkshireobserver.com може експлуатувати статус і відомість історичної газети для охоплення ширшої аудиторії.

Виявлена мережа вебсайтів може бути ідентифікована як «pink-slime» видання – низькоякісна імітаційна журналістика або сайти-агрегатори сміттєвого контенту. Такі видання можуть мати візуальні ознаки справжнього місцевого новинного видання, але транслювати контент, який містить певні політичні й ідеологічні наративи, кінцевими бенефіціарами яких можуть бути як внутрішні політичні сили, так і ворожі уряди¹²³. Ці організації зазвичай не мають зв'язків з місцевою громадою та належать великій організації, яка керує мережею новинних видань для просування низькоякісного контенту¹²⁴. Як зазначають Е. Бартон і Д. Коегорст, такі сайти мають візуально схоже оформлення макетів і контенту¹²⁵. Прикладом використання «pink-slime» видань для впливу на політичний контекст є вибори США 2024 року, коли агенція NewsGuard

¹²⁰ The British Newspaper Archive. Results. Between 1st Jan 1858 and 31st Dec 1858. Dublin, Republic Of Ireland. URL: <https://britishnewspaperarchive.co.uk/search/results/1858-01-01/1858-12-31?county=dublin,%20republic%20of%20ireland&retrievecountrycounts=false&mostspecificlocation=dublin,%20republic%20of%20ireland&sortorder=dayearly&page=0>

¹²¹ Yorkshire Observer. URL: <https://archive.ph/kIFu7>.

¹²² The British Newspaper Archive. Results for "yorkshire observer". URL: <https://britishnewspaperarchive.co.uk/search/results?basicsearch=yorkshire%20observer&somesearch=yorkshire%20observer&exactsearch=false&retrievecountrycounts=false>

¹²³ Elections 2024: Pink Slime Journalism Overtaking Local News?. URL: <https://www.intel471.com/blog/elections-2024-pink-slime-journalism-overtaking-local-news>

¹²⁴ Carley K., Lepird C., Hui Xian Ng L. Trends of Pink Slime Journalism Advertisement Expenditure and Spread on Facebook from 2019-2024. Cornell University, 2025. C. 1-2. URL: <https://doi.org/10.48550/arXiv.2510.14818>

¹²⁵ Цит. за: Carley K., Lepird C., Hui Xian Ng L. Trends of Pink Slime Journalism Advertisement Expenditure and Spread on Facebook from 2019-2024. Cornell University, 2025. C. 1. URL: <https://doi.org/10.48550/arXiv.2510.14818>

виявила, що в США такі вебсайти були настільки поширені, що їх кількість була на 4% більшою, ніж кількість офіційно зареєстрованих місцевих видань, який налічується близько 1,200¹²⁶.

Важливим питанням під час дослідження цієї мережі є те, з якою метою вона провадить свою діяльність: для дезінформації населення цільових регіонів, країн і міст чи для впливу на алгоритми ШІ. Для аналізу місячного трафіку спочатку було створено рандомізовану вибірку, проте в ході дослідження виявилось, що не всі домени мають інформацію про відвідуваність протягом місяця. Зважаючи на це було досліджено місячний трафік кожного домену. Аналіз місячного трафіку здійснювався завдяки інструменту Similarweb¹²⁷. У Додатку 2 містяться фото підтвердження 18 успішних результатів пошуку щодо кількості відвідувачів на досліджуваних сайтах упродовж квітня 2026 року.

Аналізуючи отримані результати дослідження місячного трафіку 18 доменів (див. Таб.2), можна дійти до висновку, що усі досліджені сайти мають низький рівень відвідуваності. І хоча дані аналізу 18 доменів не є підставою для об'єктивного висновку, що більшість з сайтів мережі мають такі ж низькі результати відвідуваності, найбільш імовірно, що ця мережа не створена для безпосереднього когнітивного впливу на населення цільових регіонів. Зважаючи на низький рівень відвідуваності, ймовірно, що основними завданнями мережі є «LLM grooming» за аналогією з Portal Combat. Окрім впливу на алгоритми ШІ, цілком імовірно, що ще одним завданням мережі може бути SEO-оптимізація та «link building». Пошукові системи, наприклад, Google, використовують кількість зовнішніх посилань на конкретний матеріал як один з основних критеріїв для упорядкування результатів пошукового запиту. Логіка виглядає наступним чином: чим більше видань посилаються на матеріал RT, тим більший шанс, що сайт RT

¹²⁶ Berger E. Deluge of 'pink slime' websites threaten to drown out truth with fake news in US election. URL: <https://www.theguardian.com/us-news/article/2024/jun/20/fake-news-websites-us-election>

¹²⁷ SimilarWeb Identity. URL: <https://pro.similarweb.com/#/digitalsuite/websiteanalysis/home>

з'явиться одним із перших, навіть не відвідуючи проміжні «pink-slime» сайти безпосередньо. Беручи це до уваги, можна дійти до висновку, що завданням мережі є не стільки безпосередній вплив на читачів, скільки вони виконують технічну функцію для покращення позицій пропагандистських видань у результатах пошукових запитів.

Таблиця 2.

Дані щодо кількості візитів за квітень 2026 року.

Домен	К-сть відвідувань		Домен	К-сть відвідувань
argentinastar.com	108	0	losangelesherald.com	485
johannesburgnews.net	540	1	milwaukeeesun.com	431
raleighnews.net	540	2	detroitstar.com	481
northamericanews.net	84	3	baltimorestar.com	142
centralasiatimes.com	695	4	lasvegasherald.com	1907
japanherald.com	308	5	phoenixnews.net	182
irishsun.com	23,003	6	mainemirror.com	656
germanynews.net	109	7	dublinnews.net	138
malaysiasun.com	17,200	8	arizonaherald.com	89

Таблицю складено самостійно на основі власного дослідження через інструмент SimilarWeb.

Підсумовуючи проведене дослідження мережі псевдолокальних новинних порталів («pink-slime»), можна стверджувати, що виявлена екосистема з 369 доменів є класичним прикладом реалізації низькоінтенсивного інструментарію втручання у рамках моделі «стимул-можливість-втручання» (IOI) Дані Бело. Зважаючи на системний стимул Кремля – відчуття розриву між бажаною глобальною роллю та

реальними можливостями, – Росія змушена компенсувати цю нестачу через асиметричні та приховані дії.

Водночас наше дослідження доповнює теоретичну рамку Д. Бело: якщо традиційно «вікном можливостей» для втручання вважалися внутрішні етнічні чи соціально-політичні рухи, то сьогодні таким простором можливостей стає технологічна вразливість цифрового середовища та алгоритмів штучного інтелекту західних країн. Використовуючи сайти, що мімікрують під місцеві видання США, Європи та Азії, Росія створює масштабну інфраструктуру впливу.

Важливо наголосити, що низькі показники прямої відвідуваності цих ресурсів не свідчать про їхню неефективність. Відповідно до логіки моделі IOI, головна перевага низькоінтенсивних заходів полягає у складності їхньої атрибуції. Виявлена мережа діє не шляхом прямого переконання читачів, а через технічні маніпуляції: створення масиву зворотних посилань (SEO-оптимізацію) для легалізації фейків та використання механізму «LLM grooming». Засмічуючи відкриті дані, на яких навчаються сучасні мовні моделі, прокремлівськими наративами (зокрема, матеріалами RT), ця мережа перетворює алгоритми пошукових систем та чат-ботів на мимовільних ретрансляторів російської пропаганди. Так, Росія досягає стратегічних цілей інформаційно-психологічного протистояння, зберігаючи при цьому можливість заперечувати свою безпосередню участь.

2.3. Російський вплив на європейський політичний ландшафт: підтримка радикальних політичних партій та втручання в електоральні процеси

Вплив на політичні й виборчі процеси в Європі є одним з основних пріоритетів російської гібридної війни проти ЄС. Реалізація цих заходів

здійснюється двома основними методами: пропаганда й дезінформація через соціальні мережі й медіа, а також підтримка локальних радикальних сил, їх подальша кооптація й перетворення на агентів впливу.

Використання фейкових новин є одним з *modus operandi* Кремля для втручання у виборчі процеси європейських країн, прикладом чого слугують вибори в Румунії у 2024 році. Так, маловідомий ультраправий кандидат Келін Джорджеску з прокремлівськими поглядами, який за місяць до виборів за даними опитувань мав підтримку близько 1%, у першому турі в листопаді 2024 р. набрав 22,94%¹²⁸, вийшовши на перше місце. Свого часу К. Джорджеску в лютому 2022 року під час телетрансляції на румунському каналі Realitatea Plus назвав Україну вигаданою державою, тим самим ретранслюючи усталений наратив Кремля¹²⁹. Ще одним прикладом узгодженості позиції К. Джорджеску з кремлівською пропагандою є заява, що Україною нібито «маніпулюють американські військові компанії»¹³⁰.

Раптова й неочікувана перемога проросійського і євроскептичного кандидата в першому турі викликала значний інтерес серед журналістів-розслідувачів, зокрема з платформи VSquare. За даними цієї розслідувальної платформи виборча кампанія К. Джорджеску супроводжувалась великою інформаційно-психологічною операцією в ТікТок, охопивши приблизно 25000 акаунтів у соціальній мережі, транслуючи вигідні для К. Джорджеску меседжі¹³¹. Журналісти також виявили, що діяльність цих акаунтів координувалась через обліковий запис

¹²⁸ Paun C., Jack V. Ultranationalist candidate scores stunning first-round win in Romania election. URL: <https://www.politico.eu/article/romania-election-stunner-who-is-calin-georgescu-marcel-ciolacu/>

¹²⁹ Subarion A., Slyvenko O. How the Rhetoric of Election Candidates in Romania and Moldova Echoes Kremlin Narratives. URL: <https://en.detector.media/post/how-the-rhetoric-of-election-candidates-in-romania-and-moldova-echoes-kremlin-narratives>

¹³⁰ Subarion A., Slyvenko O. How the Rhetoric of Election Candidates in Romania and Moldova Echoes Kremlin Narratives. URL: <https://en.detector.media/post/how-the-rhetoric-of-election-candidates-in-romania-and-moldova-echoes-kremlin-narratives>

¹³¹ Šlerka J., Stănoiu I. How TikTok Almost Won the Presidency for Romania's Far-Right Candidate. URL: <https://vsquare.org/romania-tiktok-campaign-presidential-election-far-right-candidate-russia/>

Telegram @propagatorcg, де містились інструкції для публікацій. Водночас, як зазначають розслідувачі з посиланням на румунську розвідку, агітаційна кампанія мала фінансові зв'язки з Росією, адже блогер Богдан Пешир виплатив близько 381000 євро різним користувачам ТікТоку, які агітували за К. Джорджеску¹³². Розслідування OCCRP також свідчить про те, що до агітаційної кампанії долучився американський бізнесмен Дуглас Андерсон, який має зв'язки з російськими чиновниками¹³³.

І хоча Конституційний суд Румунії ухвалив рішення про анулювання результатів першого туру виборів, а К. Джорджеску був дискваліфікований з виборчих перегонів¹³⁴, цей прецедент демонструє адаптивність російських підходів до ведення інформаційно-психологічного протистояння. Якщо раніше традиційним методом інформаційного впливу були новинні видання, то цей приклад продемонстрував безпрецедентну ефективність інформаційних кампаній в соціальних мережах.

Разом з інформаційними кампаніями, Кремль також використовував і продовжує використовувати агентів впливу для лобіювання вигідних рішень в ЄС, одночасно із цим підриваючи стабільність Союзу та ускладнюючи стосунки між державами-членами. Прикметно, Кремль підтримує обидва екстремуми політичної прямої – як ультраправих, так і ультралівих. Зв'язок ліворадикалів з Росією може бути зумовлений радянським бекграундом і намірами Радянського Союзу підтримувати ліві рухи у світі. Водночас, як зазначають С. Брагіролі й А. Макаричев, ліві партії в Європі сприятливо ставляться до Росії через риторику Путіна про «суверенітет та функціональний антифашизм»¹³⁵.

¹³² Šlerka J., Stănoiu I. How TikTok Almost Won the Presidency for Romania's Far-Right Candidate. URL: <https://vsquare.org/romania-tiktok-campaign-presidential-election-far-right-candidate-russia/>

¹³³ Romanian Authorities Launch Probe Into Alleged Election Interference via TikTok. URL: <https://www.occrp.org/en/news/romanian-authorities-launch-probe-into-alleged-election-interference-via-tiktok>

¹³⁴ Gozzi L., Rainsford S. Georgescu barred from Romanian vote in final court ruling. URL: <https://www.bbc.com/news/articles/cj679nk6endo>

¹³⁵ Braghiroli S., Makarychev A. Russia and its supporters in Europe: trans-ideology à la carte?. Southeast European and Black Sea Studies. 2016. T. 16, № 2. С. 223. URL: <https://doi.org/10.1080/14683857.2016.1156343>

Водночас логіка співробітництва Москви й ультраправих сил є складнішою, адже стратегічні комунікації Кремля формують наративи про «переможців над нацизмом (фашизмом)» та борців проти «українського нацизму, вирощеного Європою»¹³⁶. Якщо у вимірі офіційної риторики Москви логічною є несумісність Росії з ультраправими, то в контексті ідеологічних засад і європейські праві й російський чинний режим мають багато спільного: вони виступають проти принципів ліберальної демократії, західного капіталізму, європейського космополітизму (інтеграції), а також наслідують ідеї націоналізму, національної незалежності й суверенітету та захищають традиційні цінності¹³⁷.

Як зазначають в OpenDemocracy, Росія є «банкоматом» для радикальних партій у багатьох країнах ЄС¹³⁸: Rassemblement national у Франції, Alternative für Deutschland в Німеччині¹³⁹, Jobbik в Угорщині¹⁴⁰, Reform UK у Великій Британії, Lega Nord і Fratelli d'Italia в Італії¹⁴¹ та інші. В обмін на фінансування з Москви представники ультрарадикальних партій лобіювали проросійські рішення як в ЄС, так і в національних державах.

Наочним прикладом фінансового втручання є кейс партії Марі Ле Пен Rassemblement national у Франції, яка брала у 2014 позику у розмірі 9,4 мільйони євро від банку, що має зв'язки з друзями Путіна. Водночас з цим риторика Марі Ле Пен була проросійською: вона високо оцінювала

¹³⁶ Палехов Г. Лавров назвал власти Украины выкормленными Европой нацистами. URL: <https://archive.is/VuTna>

¹³⁷ Цит. за: Wang C., Altiparmakis A. What happened to Putin's friends? The radical right's reaction to the Russian invasion on social media. *European Union Politics*. 2025. Т. 26, № 2. С. 396. URL: <https://doi.org/10.1177/14651165251321802>

¹³⁸ Datta N. We know Russia funds Europe's far Right. But what does it get in return?. URL: <https://www.opendemocracy.net/en/5050/russia-ukraine-war-putin-europe-far-right-funding-conservatives/>

¹³⁹ Wang C., Altiparmakis A. What happened to Putin's friends? The radical right's reaction to the Russian invasion on social media. *European Union Politics*. 2025. Т. 26, № 2. С. 403-407. URL: <https://doi.org/10.1177/14651165251321802>

¹⁴⁰ Kreko P. Putin's far right and far left friends in Europe. URL: https://www.wilsoncenter.org/sites/default/files/media/documents/event/pc_prezi_wilsoncentre.pdf

¹⁴¹ Galuzzi O. Italy: Russia's Influence over Far-Right Offline and Online. *Russia and the Far-Right Insights from Ten European Countries*. 2024. С. 171-201. URL: https://icct.nl/sites/default/files/2024-04/Russia%20and%20the%20Far-Right%207%20Italy_0.pdf

Путіна ти «висловлювала підтримку кримським сепаратистам»¹⁴². Іншим прикладом російського втручання в європейську політику є зізнання лідера Reform UK в Уельсі Натана Гілла, який за повідомленням у британських медіа був ключовим помічником лідера партії Найджела Фараджа¹⁴³. У 2025 Натан Гілл визнав себе винним за отримання хабарів за заяви на користь Росії в Європарламенті. Як повідомляє служба BBC News, український політик Олег Волошин, що тісно пов'язаний з Медведчуком та його «112 каналом», спонсорував проросійські заяви британського політика та організовував інтерв'ю з ним в ефірі «112 каналу»¹⁴⁴. Водночас Натан Гілл робив фінансові внески на підтримку каналів Медведчука та використовував парламентську промову у грудні 2018 року, щоб захистити телеканали «112 Україна» та NewsOne від нібито тиску з боку України¹⁴⁵.

Загалом, аналіз особливостей впливу Кремля на європейський політичний ландшафт демонструє адаптивність російської пропаганди до технологічного прогресу, адже сучасні інформаційно-психологічні операції Кремля вдаються до нових методів впливу, а саме через соціальні мережі. Неочікувана перемога маловідомого кандидата на виборах завдяки соціальним мережам актуалізує питання заходів боротьби з пропагандою і дезінформацією в соціальних мережах. Водночас практика кооптування й перетворення місцевих політиків на агентів впливу, що просувають прокремлівський порядок денний є історичною успадкованою практикою, витоки якої містяться в «активних заходах» Радянського Союзу.

¹⁴² Gagné-Acoulon S. Russian Company Sues Marine Le Pen's Party Over Unpaid Loan. URL: <https://www.occrp.org/en/news/russian-company-sues-marine-le-pen-party-over-unpaid-loan>

¹⁴³ B. Quinn та ін. Reform UK, the Russian spy and rolls of Kremlin cash: the inside story of Nathan Gill URL: <https://www.theguardian.com/news/ng-interactive/2025/nov/01/reform-a-russian-spy-and-the-bribes-the-inside-story-of-nathan-gill>

¹⁴⁴ Deans D. Reform UK's ex-Wales leader Nathan Gill admits pro-Russia bribery. URL: <https://www.bbc.com/news/articles/cj6xwy015ngo>

¹⁴⁵ Deans D. Reform UK's ex-Wales leader Nathan Gill admits pro-Russia bribery. URL: <https://www.bbc.com/news/articles/cj6xwy015ngo>

2.4. Російські кінетичні операції проти Європи як різновид PSYOP в межах когнітивної війни

Разом із початком повномасштабного вторгнення в Україну у 2022 році Росія розпочала приховані кінетичні атаки проти держав-членів ЄС. За даними зі звіту GLOBSEC у період 2022-2025 рр. Росія здійснила 110 кінетичних операцій проти Європи, 89 з яких були успішними, а 21 вдалось запобігти¹⁴⁶. Інтенсивність диверсій на інфраструктурних об'єктах зросла на 246% в період з 2023 по 2024 рік, про що повідомляє Міжнародний інститут стратегічних досліджень (далі – IISS)¹⁴⁷. Дослідники пов'язують таку ескалацію із рішенням Заходу скасувати обмеження на використання Україною західної зброї¹⁴⁸.

Загалом, IISS виділяє два типи російських прихованих операцій проти Європи: «акти вандалізму», які покликані посіяти страх і безлад серед місцевого населення, та таргетовані атаки – диверсії та саботажі¹⁴⁹. Однак, навіть цілеспрямовані теракти на європейських заводах, складах та інфраструктурі – це не тільки матеріальна шкода, а й психологічна, адже це підкреслює вразливість Європи та неготовність до активного протистояння. У таких випадках військова діяльність може переставати бути самоціллю, а когнітивні ефекти стають бажаним очікуваним результатом.

¹⁴⁶ Rekawek K., Lanchès J., Bowser D. Russia's Crime–Terror Nexus: Criminality as a Tool of Hybrid Warfare in Europe. GLOBSEC, 2025. C. 18. URL: https://www.globsec.org/sites/default/files/2025-10/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool_0.pdf

¹⁴⁷ Edwards C., Seidenstein N. The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure. IISS, 2025. C. 9. URL: [https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-t](https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf)

¹⁴⁸ Edwards C., Seidenstein N. The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure. IISS, 2025. C. 9. URL: <https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-t>

¹⁴⁹ Edwards C., Seidenstein N. The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure. IISS, 2025. C. 8. URL: <https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-t>

До 2022 року операції саботажу в Європі здійснювались переважно кваліфікованими шпигунами й агентами російської розвідки. Найбільш яскравим прикладом є діяльність підрозділу Головного управління розвідки (ГРУ) 29155, який за даними Bellingcat причетний до анексії Криму (2014 р.), заходів з дестабілізації в Молдові (2014 р.), невдалої спроби держперевороту в Чорногорії (2016 р.), операцій зі стеження у Швейцарії (2016-2017 рр.), спроб дестабілізації в Іспанії під час референдуму щодо незалежності Каталонії (2017 р.), вбивства колишнього російського шпигуна Сергія Скрипаля в Солсбері (2018 р.)¹⁵⁰. Однак після масової депортації російських оперативників з Європи в березня 2022 року Росія змінила підхід до реалізації диверсійних заходів: замість штатних розвідників операції здійснюють або «одноразові» агенти або організовані злочинні групи¹⁵¹.

Як видно зі статистики GLOBSEC, найбільше від російських кінетичних операцій постраждала Польща¹⁵², що найбільш ймовірно пов'язано з тим, що 80% західної допомоги потрапляли в Україну транзитом через цю державу¹⁵³. У 2023 році в медіа почали з'являтися повідомлення про вербування «аматорів» через Telegram та оголошення про роботу. Наприклад, у 2023 році було викрито мережу завербованих Росією осіб в Польщі, які здійснювали розвідку польських морських портів, встановлювали камери вздовж залізниць та ховали пристрої стеження у військових вантажах. Фінальним завданням, якому вдалось

¹⁵⁰ How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine. URL: <https://www.bellingcat.com/news/europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/>

¹⁵¹ Rekawek K., Lanchès J., Bowser D. Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare in Europe. GLOBSEC, 2025. C. 22-25. URL: https://www.globsec.org/sites/default/files/2025-10/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool_0.pdf

¹⁵² Rekawek K., Lanchès J., Bowser D. Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare in Europe. GLOBSEC, 2025. C. 22-25. URL: https://www.globsec.org/sites/default/files/2025-10/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool_0.pdf

¹⁵³ Miller G., Morris L., Ilyushina M. Russia recruited operatives online to target weapons crossing Poland. URL: <https://www.washingtonpost.com/world/2023/08/18/ukraine-weapons-sabotage-gru-poland/>

запобігти польським правоохоронцям, було збити з рейок потяги, що транспортували Західну військову допомогу Україні¹⁵⁴. В медіа назвали цей інцидент найсерйознішою російською загрозою на території держав-членів НАТО, починаючи з 2022 року¹⁵⁵.

Однак російська диверсійна діяльність у Європі не обмежується виключно атаками на інфраструктуру. Гучною операцією Кремля стала розкрита у липні 2024 року змова з ліквідації CEO концерну Rheinmetall, який виробляв артилерійські снаряди та військову техніку для України¹⁵⁶. Іншою мішенню для прихованих російських атак став завод Diehl Metal Applications, який виробляв системи протиповітряної оборони IRIS-T, що надалі постачались в Україну. Також Росія вдавалась до відвертих актів тероризму: вибухові пристрої з запрограмованим електронним таймером розміщувались у пакунках кур'єрської служби DHL¹⁵⁷.

Загалом, основними виконавцями російських диверсійних операцій були чоловіки у віці близько 30 років, яких вмотивовували фінансовою винагородою¹⁵⁸. Варто наголосити, що більшість завербованих росіянами агентів є біженцями з України, що найбільш імовірно є цілеспрямованою тактикою Кремля¹⁵⁹. За таких обставин кінетична операція має як військовий ефект, наприклад, диверсія на заводі, та когнітивний – збільшення соціальної напруги через повідомлення про участь українців у

¹⁵⁴ Miller G., Morris L., Ilyushina M. Russia recruited operatives online to target weapons crossing Poland. URL: <https://www.washingtonpost.com/world/2023/08/18/ukraine-weapons-sabotage-gru-poland/>

¹⁵⁵ Miller G., Morris L., Ilyushina M. Russia recruited operatives online to target weapons crossing Poland. URL: <https://www.washingtonpost.com/world/2023/08/18/ukraine-weapons-sabotage-gru-poland/>

¹⁵⁶ Lillis K. B., Bertrand N., Pleitgen F. Exclusive: US and Germany foiled Russian plot to assassinate CEO of arms manufacturer sending weapons to Ukraine. URL: <https://www.cnn.com/2024/07/11/politics/us-germany-foiled-russian-assassination-plot>

¹⁵⁷ Європейська правда. У Литві судитимуть п'ятьох осіб у справі “вибухових” посилок, серед них – українці. URL: <https://www.eurointegration.com.ua/news/2026/03/6/7232647/>

¹⁵⁸ Rekawek K., Lanchès J., Bowser D. Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare in Europe. GLOBSEC, 2025. C. 23. URL: https://www.globsec.org/sites/default/files/2025-10/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool_0.pdf

¹⁵⁹ Rekawek K., Lanchès J., Bowser D. Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare in Europe. GLOBSEC, 2025. C. 23. URL: https://www.globsec.org/sites/default/files/2025-10/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool_0.pdf

саботажах та зменшення довіри громадськості до інститутів через неспроможність протистояти таким атакам. Фактично, вербування українців для такого роду операцій дозволяє Кремлю проводити когнітивну війну навіть не залучаючи власні медіаресурси та не вдаючись до пропаганди й дезінформації: достатньо аби місцеві медіа самостійно повідомили про факт причетності осіб з українським походженням. Регулярні повідомлення про причетність українців до терактів можуть вплинути на сприйняття українців серед населення цільових держав. Таким чином, у довгостроковій перспективі Росія зможе підважити підтримку України європейцями та збільшити соціальну напругу через українських біженців. Своєю чергою, повідомлення в європейських медіа про конфлікт місцевих з українськими біженцями лише підсилюють соціальну напругу, досягаючи «ефекту доміно».

Водночас Росія веде гібридну війну з ЄС не тільки на суші, але й в морі. Балтійське море стало театром кінетичних операцій через атаки на комунікаційну інфраструктуру, адже з 2022 року в регіоні було перерізано близько десяти підводних кабелів. Що важливо, сім кабелів були пошкоджені в період між листопадом 2024 року та січнем 2025 року¹⁶⁰. Ці кабелі з оптоволокна відповідають за швидку передачу даних, забезпечуючи зв'язок і комунікації між державами. У інцидентах з пошкодження таких кабелів підозрюють «тіньовий флот» Росії, адже наочним прикладом такої операції випадок з нафтовим танкером, що ходить під прапором Островів Кука. Випадок з судном Eagle S, який пошкодив підводний кабель між Естонією і Фінляндією у 2024 році, за даними фінської прикордонної служби був навмисним актом саботажу¹⁶¹.

¹⁶⁰ Himka S. Baltic Sea Undersea Cable Security. The Henry M. Jackson School of International Studies. URL: <https://jsis.washington.edu/news/baltic-sea-undersea-cable-security/>

¹⁶¹ Whitaker B., Gordon E., Chasan A., de Granados O. Z. Authorities investigate possible Russian "hybrid warfare" after oil tanker cuts undersea cables. URL: <https://www.cbsnews.com/news/eagle-s-baltic-cut-cable-investigation-russia-ties-60-minutes/>

Наприкінці грудня 2025 року в Фінській затоці стався подібний інцидент: прикордонники Фінляндії затримали судно Fitburg, що йшло з Санкт-Петербурга та пошкодило кабель між Фінляндією й Естонією¹⁶². Як зазначила міністерка внутрішніх справ Естонії Лаурі Ляанеметс, малоймовірно, що такі інциденти лише можуть бути просто збігом обставин¹⁶³.

У відповідь на саботажі в Балтійському морі НАТО у січні 2025 року запустило операцію «Baltic Sentry» для патрулювання критичної підводної інфраструктури, проте вже за пів року помічник Генсека НАТО з інновацій і гібридних загроз Жан-Шарль Еллерманн-Кінгомб зазначив, що операція виявилася надмірно витратною¹⁶⁴. Таким чином, використовуючи «тіньовий флот» у Балтійському морі, Росія досягла двох стратегічних результатів – змусила НАТО витратити ресурси на охорону інфраструктуру, збільшивши рівень напруги, та зашкодила комунікаційній системі. Що важливо, використання кораблів «тіньового флоту» у цих випадках ускладнює атрибуцію інцидентів з Росією, а тому це дозволяє Кремлю висвітлювати «false flag» операції (операції під чужим прапором) як нещасні випадки.

Однак, пошкодження підводної комунікаційної інфраструктури є не єдиним методом застосування «тіньового флоту» для гібридного протистояння з ЄС. Кораблі під нейтральними прапорами Росія також застосовує для запуску розвідувальних дронів для стеження за військовими

¹⁶² Lehto E., Kauranen A. Finland seizes ship sailing from Russia after suspected cable sabotage in Baltic Sea. URL: <https://www.reuters.com/world/finland-suspects-ship-causing-undersea-cable-damage-president-says-2025-12-31/>.

¹⁶³ Lehto E., Kauranen A. Finland seizes ship sailing from Russia after suspected cable sabotage in Baltic Sea. URL: <https://www.reuters.com/world/finland-suspects-ship-causing-undersea-cable-damage-president-says-2025-12-31/>.

¹⁶⁴ Edwards C., Seidenstein N. The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure. IISS, 2025. C. 11. URL: <https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf>

об'єктами в Європейських країнах, про що заявляв Володимир Зеленський з посиланням на дані розвідки¹⁶⁵.

Починаючи з 2024 року над територіями держав-членів ЄС фіксувалась систематична активність розвідувальних дронів. Наприклад, 22 вересня 2025 року активність неідентифікованого безпілотні літальні апарати (БПЛА) біля Норвегії та Данії спричинила закриття аеропортів Осло і Копенгагена на декілька годин. Схожий інцидент відбувся 24 вересня, коли низку данських аеропортів було тимчасово закрито через загрозу неідентифікованих дронів. Загалом, ідентичні випадки польотів дронів над цивільними аеропортами було зафіксовано також в Німеччині¹⁶⁶ і Бельгії¹⁶⁷. Такі операції мають подвійний ефект: крім того, що завдається економічна шкода, такі інциденти також свідчать про нездатність європейських держав захистити власне населення від такого роду загроз, що може посилити суспільне занепокоєння або посилити невдоволення через бездіяльність урядів.

Водночас неідентифіковані дрони також періодично фіксувались і над військовими об'єктами. Наприклад, у 2024 році було зафіксовано дрони над військовими авіабазами у Великій Британії¹⁶⁸. Іншим прикладом є проліт розвідувальних дронів над найбільшою авіа базою в Європі – Рамштайн¹⁶⁹. В цьому випадку такі кінетичні операції можуть так само мати дві функції: отримання розвідданих про військові об'єкти держав

¹⁶⁵ Basmat D. Russia using 'shadow fleet' tankers to launch drones towards European cities, Zelensky says. URL: <https://kyivindependent.com/russia-using-shadow-fleet-tankers-to-launch-drones-towards-european-cities-zelensky-says/>

¹⁶⁶ Flights resume at Berlin airport after suspension over drone scare. URL: <https://www.france24.com/en/europe/20251101-flights-resume-at-berlin-airport-after-suspension-over-drone-scare>

¹⁶⁷ Knapp F. Drones plague Belgium. URL: <https://www.politico.eu/article/drones-plague-belgium-airports-crisis-skies-traffic/>

¹⁶⁸ Grierson J. Unidentified drones spotted over three UK airbases, US air force confirms. URL: <https://www.theguardian.com/uk-news/2024/nov/23/unidentified-drones-spotted-over-three-uk-airbases-us-air-force-confirms>

¹⁶⁹ Rinke A., More R. U.S. military confirms drone sightings at air base in Germany. URL: <https://www.reuters.com/world/europe/unidentified-drones-sighted-over-us-air-base-germany-spiegel-reports-2024-12-13/>

НАТО і підважування здібності й рішучості альянсу протистояти такого роду загрозам.

Іншим важливим прикладом використання дронів для когнітивного ефекту є інцидент, що трапився під час візиту В. Зеленського в Ірландію. Тоді у грудні 2025 року було зафіксовано декілька неідентифікованих БПЛА над Ірландським морем під час візиту українського Президента в Дубліні. І хоча цей інцидент має відмінну логіку від двох сценаріїв використання дронів, що було наведено вище, цей окремий випадок має спільний кінцевий когнітивний ефект – розчарування населення європейських держав у спроможності НАТО захищати власний простір.

Важливо наголосити, що такого роду кінетичні операції важко атрибуувати з Росією, однак системність і наявність спільних факторів свідчить про те, що такого роду операції не є випадковими інцидентами за участю цивільних дронів, а спланованими агресивними діями зовнішнього актора. Саме тому найбільш імовірно, що саме Росія стоїть за цими інцидентами з дронами, що зокрема підтверджує українська розвідка¹⁷⁰.

Утім, використання дронів-шпигунів – не єдина тактика Кремля, адже з 2022 року існують випадки більш брутальних порушень повітряного простору держав-членів НАТО. Серед таких інцидентів: перебування російських винищувачів у повітряному просторі Естонії¹⁷¹, вторгнення БПЛА й крилатих ракет у Польщу¹⁷², падіння російських бойових дронів у Румунії¹⁷³. І хоча подібні інциденти можуть бути

¹⁷⁰ Basmat D. Russia using 'shadow fleet' tankers to launch drones towards European cities, Zelensky says.

URL:

<https://kyivindependent.com/russia-using-shadow-fleet-tankers-to-launch-drones-towards-european-cities-zelensky-says/>

¹⁷¹ Foreign Minister Tsahkna: Foreign Ministry summons Russia's chargé d'affaires over another violation of Estonia's airspace. URL:

<https://www.vm.ee/en/news/foreign-minister-tsahkna-foreign-ministry-summons-russias-charge-daffaires-over-another>

¹⁷² Testing the Threshold. What the Russian drone incursion into Poland means for NATO. Clingendael, 2025. С. 1-3. URL:

https://www.clingendael.org/sites/default/files/2025-09/Alert_Russian_drone_incursion_into_Poland_means_for_NATO.pdf

¹⁷³ Ministerul Apararii Nationale. Informatie de presa. URL: https://www.mapn.ro/cpresa/19218_informatie-de-presa

визначені як колатеральна шкода в умовах війни, беззаперечним залишається той факт, що подібні події мають когнітивний ефект.

Підсумовуючи цей підрозділ, обґрунтованим є висновок, що після початку вторгнення в Україну Кремль перейшов до більш агресивних високоінтенсивних заходів для ведення гібридної війни з ЄС. Російські кінетичні операції на території держав-членів ЄС – диверсії на інфраструктурних об'єктах і воєнних заводах, замах на впливових осіб, пошкодження підводних кабелів, порушення повітряного простору винищувачами, бойовими БПЛА і крилатими ракетами, систематичне стеження за військовими об'єктами – слід розглядати не як ізольовані інциденти, а як частину російського системного підходу до гібридного протистояння з Європою, у якому військова дія і матеріальна шкода перестають бути самоціллю, а основним завданням є інформаційно-психологічний ефект, що може впливати на соціополітичну динаміку цих держав.

Кінетичні операції й когнітивні заходи перебувають у відношенні взаємної детермінації: кінетичні дії продукують когнітивні ефекти, спрямовані на противника, тоді як когнітивні заходи створюють передумови для ефективного застосування кінетичних засобів, зменшуючи операційну спроможність противника та його здатність до протидії. Фактично, така формула є постулатом модерної війни нового покоління, що відбувається на європейському континенті.

Цей постулат знаходить емпіричне підтвердження у діях Кремля: вербування українських біженців для проведення диверсій формує підґрунтя для довгострокового підриву суспільної підтримки України в європейських державах; систематичні польоти неідентифікованих дронів над цивільними аеропортами та військовими об'єктами підважують віру у спроможність НАТО та європейських урядів захищати власні кордони; використання «тіньового флоту» для атак на підводну інфраструктуру

завдає значної матеріальної шкоди та змушує НАТО витрачати непропорційні ресурси на її охорону. У кожному з наведених вище випадків кінетичний ефект є лише оболонкою, тоді як справжнім завданням є когнітивний вимір – суспільна довіра та сприйняття спроможності держав-членів ЄС і НАТО в очах їх населення протистояти агресору.

ВИСНОВКИ

Підсумовуючи систематизацію теоретико-концептуальних підходів до визначення гібридної війни, в академічному середовищі відсутній консенсус щодо цього поняття, що зумовило появу різних шкіл – кінетичної й некінетичної – що були проаналізовані в цій роботі. Резюмуючи, сучасна гібридна війна є новим типом багатовимірною протистояння як між державами, так і між державними й недержавними акторами, на стратегічному, оперативному і тактичному рівнях із застосуванням широкого арсеналу інструментів, що можуть включати засоби економічного, дипломатичного, політичного тиску, дезінформацію, пропаганду, кібератаки, приховані і явні кінетичні операції. Також було встановлено, що кінетична і некінетична школи органічно вписується у концепцію 4-го покоління В. Лінда з його ідеєю розмиття межі між цивільним і воєнним, а також у концепцію 5-го покоління Д. Аббота й А. Крішнана, що зосереджується на когнітивному домені – управління сприйняттям і кінцевою поведінкою індивіда. Водночас було встановлено, що теза А. Крішнана про субнаціональних державних акторів як основних суб'єктів 5GW потребує уточнення, адже досвід російсько-української війни наочно демонструє провідну роль офіційних державних інституцій у формуванні стратегічних наративів та зростає суб'єктність населення як актора інформаційно-психологічного протистояння в умовах розвитку соціальних мереж, що може автономно продукувати контент, що містить дезінформацію й пропаганду.

Концепт когнітивної війни став ключовим для теорії 5GW, об'єктом дії якого стає сам процес мислення, прийняття рішень, формування переконань і як результат – кінцева поведінка індивіда. Варто наголосити, що когнітивна війна набуває максимальної ефективності в умовах епохи постправди, що характеризується знеціненням об'єктивних фактів,

розмиттям меж між правдою і вигадкою, наявністю декількох інтерпретацій однієї й тієї ж самої події, а також інструменталізацією емоцій. Інструментарій когнітивної війни є широким: дезінформація, фейкові новини, теорії змови, маніпулятивні наративи, кібероперації та технології штучного інтелекту. Особливістю когнітивної війни є системна та довгострокова дія, спрямована не на разовий ефект, а на поступову зміну ціннісних рамок і світогляду індивіда й цілого суспільства.

Уточнення термінологічної рамки інформаційно-психологічного виміру сучасних конфліктів дозволило вибудувати ієрархічну структуру. В дослідженні було визначено, що стратегічні комунікації виступають у ролі «парасольки» для інших понять і є загальним підходом держави, її офіційною позицією і риторикою для досягнення стратегічних цілей. Інформаційну війну можна визначити як загальний стан/середовище протистояння, в межах якого використовуються інформаційні операції – сплановані кампанії на оперативному рівні з конкретними цілями й ресурсами. Психологічні операції своєю чергою є частиною ІО на тактичному рівні, що спрямовані на вплив на емоції, переконання, цінності й кінцеву поведінку індивіда.

Застосування моделі «стимул-можливість-втручання» Д. Бело для аналізу російської гібридної агресії проти Європейського Союзу дозволило пояснити логіку агресивних дій Кремля і вибір конкретних інструментів впливу залежно від поєднання змінних на системному та внутрішньому рівнях. Станом на початок 2026 року можливість застосування Росією високоінтенсивних кінетичних інструментів ЄС залишається обмеженою через членство європейських країн у НАТО та спільну оборонну політику Союзу. Це своєю чергою зумовлює пріоритетність низько- і середньоінтенсивних інструментів, зокрема інформаційно-психологічних операцій, кібератак, фінансової підтримки радикальних сил, прихованих диверсій. Водночас зберігаються ризики для подальшої ескалації

російської агресії, що може бути зумовлено геополітичними обставинами, зокрема кризою єдності в НАТО.

Аналіз мережі «Pravda» та виявленої в межах цієї роботи мережі з 369 псевдолокальних новинних вебсайтів демонструє принципово нові форми російського інформаційного впливу, спрямованого не стільки на споживача, скільки на алгоритми штучного інтелекту і систем пошуку. Було встановлено, що завдяки великому масиву публікацій, що станом на 27 травня 2026 року налічує близько 8,1 млн статей, мережа виконує функцію «LLM grooming». Це підтверджують дослідження News Guard та Harvard Kennedy School, які попри різницю в методології й кінцевих кількісних показниках зафіксували реальний вплив мережі на відповіді чат-ботів. Водночас у межах власного дослідження за допомогою OSINT методів було виявлено 369 пов'язаних між собою новинних вебсайтів типу «pink-slime», географічно орієнтованих переважно на Північну Америку, Азію та Європу, які агрегують контент російських державних медіа і поширюють проросійську пропаганду. Низькі показники відвідуваності цих сайтів можуть бути ознакою того, що першочерговим завданням цієї мережі є не безпосередній вплив на читачів, а SEO-оптимізація, створення масиву зворотних посилань для підсилення рейтингів російських пропагандистських видань у пошукових запитах, впливу на алгоритми пошукових систем та мовних моделей, що перетворює їх на мимовільних ретрансляторів російської пропаганди.

Аналіз механізмів російського втручання в електоральні процеси держав членів ЄС продемонстрував двокомпонентний характер російського впливу: інформаційно-психологічний складник, що зумовлюється поширенням пропаганди й дезінформації в соціальних мережах і медіа, а також інституційний складник – підтримка, кооптація й перетворення локальних радикальних політиків на агентів впливу Кремля. Кейс президентських виборів у Румунії 2024 року продемонстрував

безпрецедентну ефективність скоординованих дезінформаційних кампаній у TikTok, що забезпечили перемогу маловідомому кандидату. Такий вплив соціальних мереж актуалізує питання протидії зловмисному впливу зовнішніх акторів у таких мережах: відсутність належної регуляції соціальних мереж створює додаткові гібридні загрози, однак з іншого боку надмірна регуляція може бути розцінена як порушення прав людини, а тому ця дилема залишатиметься предметом для подальших публічних дискусій. Водночас аналіз російської підтримки радикальних сил виявив парадоксальну стратегію Кремля, який одночасно фінансує як ультраправі, так і ультраліві політичні рухи, попри риторичну несумісність з ними.

Дослідження російських прихованих кінетичних операцій проти європейських держав унаочнило факт того, що кінетичні операції можуть не бути самоцілями, а слугувати прикриттям для PSYOP. Серед проаналізованих прикладів таких операцій були диверсії на інфраструктурних і військових об'єктах, замах на впливових осіб, пошкодження підводних кабелів у Балтійському морі «тіньовим флотом», а також вторгнення розвідувальних і бойових дронів у повітряний простір європейських держав. І хоча зв'язок Росії з цими випадками може бути не очевидним, ці акти не є ізольованими інцидентами, а є частинами системного підходу, метою яких є підрив довіри населення європейських держав до спроможності власних урядів та НАТО захищати свої кордони. Власне, також було встановлено взаємну детермінацію кінетичних і когнітивних заходів: кінетичні дії продукують когнітивні ефекти, спрямовані на противника, тоді як когнітивні заходи створюють передумови для ефективного застосування кінетичних засобів. Таким чином, проведене дослідження продемонструвало, що сучасна російська гібридна агресія проти Європейського Союзу є комплексним, багатовимірним і довгостроковим протистоянням, центральним виміром якого станом на сьогодні є саме інформаційно-психологічний домен.

Попри те, що наразі Росія застосовує лише засоби низької та середньої інтенсивності проти ЄС, Європа мусить готуватись до можливого конвенційного протистояння з Росією. Відтак, питання оборони європейського континенту від російської агресії є спільними питанням для ЄС і України, а тому роль Києва у континентальній оборонній системі є визначальною, адже тільки Україна станом на сьогодні має досвід ефективного протистояння Росії як у конвенційному вимірі, так і в інформаційно-психологічному.

Декларація щодо використання ШІ. *Для лінгвістичної адаптації складних міждисциплінарних концептів та аналізу й обробки масивів даних у межах власного дослідження мережі вебсайтів у цій роботі було залучено інструменти штучного інтелекту Claude як інтелектуального асистента-редактора. Це допомогло забезпечити відповідність міжнародним стандартам наукової комунікації, зберігаючи виключне авторство ідей та концептуальних узагальнень за автором.*

СПИСОК ДЖЕРЕЛ І ЛІТЕРАТУРИ

1. A decade of lies: The US-funded biolab denial saga. URL: <https://archive.is/bihzT> (дата звернення: 28.05.2026).
2. Abbott D. The Handbook of 5GW. Nimble Books, 2010. 274 с.
3. Anabelle Colaco. URL: <https://muckrack.com/anabelle-colaco> (дата звернення: 28.05.2026).
4. Austria's FPO demands probe into \$21 bn in cash and gold shipments to Ukraine. RT International. URL: <https://web.archive.org/web/20260511172919/https://www.rt.com/news/639864-22-billion-shipped-ukraine-austria/> (дата звернення: 27.05.2026).
5. B. Quinn та ін. Reform UK, the Russian spy and rolls of Kremlin cash: the inside story of Nathan Gill URL: <https://www.theguardian.com/news/ng-interactive/2025/nov/01/reform-a-russian-spy-and-the-bribes-the-inside-story-of-nathan-gill> (дата звернення: 16.04.2026).
6. Baines P., O'Shaughnessy N., Snow N., Thomas Colley T. The SAGE Handbook of Propaganda. 2020. 652 с.
7. Basmat D. Russia using 'shadow fleet' tankers to launch drones towards European cities, Zelensky says. URL: <https://kyivindependent.com/russia-using-shadow-fleet-tankers-to-launch-drones-towards-european-cities-zelensky-says/> (дата звернення: 28.05.2026).
8. Belo D. Russian Warfare in the 21st Century. Routledge, 2026. 279 с.
9. Berger E. Deluge of 'pink slime' websites threaten to drown out truth with fake news in US election. URL: <https://www.theguardian.com/us-news/article/2024/jun/20/fake-news-websites-us-election> (дата звернення: 28.05.2026).

10. Big News Network. URL: <https://www.bignetwork.com/> (дата звернення: 28.05.2026).
11. Braghiroli S., Makarychev A. Russia and its supporters in Europe: trans-ideology à la carte?. Southeast European and Black Sea Studies. 2016. Т. 16, № 2. С. 213–233. URL: <https://doi.org/10.1080/14683857.2016.1156343> (дата звернення: 16.04.2026).
12. Braziliannews.net. Whois Lookup & Whois History. URL: <https://www.whoxy.com/braziliannews.net> (дата звернення: 28.05.2026).
13. Brickins O., News O. Analysis as a Media Content for Public Opinion Formation and Moulding. Benin Mediacom Journal. 2016. № 10. 17 с. URL: https://www.researchgate.net/publication/320487265_News_Analysis_as_a_Media_Content_for_Public_Opinion_Formation_and_Moulding (дата звернення: 03.03.2025).
14. Carley K., Lepird C., Hui Xian Ng L. Trends of Pink Slime Journalism Advertisement Expenditure and Spread on Facebook from 2019-2024. Cornell University, 2025. 25 с. URL: <https://doi.org/10.48550/arXiv.2510.14818> (дата звернення: 28.05.2026).
15. Christenson J. DNI Tulsi Gabbard probes US funding to more than 120 biolabs abroad. URL: <https://nypost.com/2026/05/11/us-news/dni-tulsi-gabbard-probes-us-funding-to-more-than-120-biolabs-abroad/> (дата звернення: 28.05.2026).
16. Clausewitz C. On War. New Jersey, 1989. С. 136. URL: <https://antilogicalism.com/wp-content/uploads/2019/04/on-war.pdf> (дата звернення: 02.03.2025).
17. Claverie1 B., du Cluzel F. “Cognitive Warfare”: The Advent Of The Concept Of “Cognitics” In The Field Of Warfare. Cognitive Warfare: The Future of Cognitive Dominance. NATO. 2022. с. 2-1–2.8.

18. Colaco A. TikTok fights stricter EU tech rules in landmark case. URL: <https://archive.ph/wip/jSsFy> (дата звернення: 28.05.2026).
19. Complex crises call for adaptable and durable capabilities. *The Military Balance*. 2015. Т. 115, № 1. С. 5–8. URL: <https://doi.org/10.1080/04597222.2015.996334> (дата звернення: 21.05.2026).
20. Couldry N., Hepp A. Mediated Construction of Reality. Polity Press, 2018. 256 с.
21. Countering hybrid threats. URL: <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats> (дата звернення: 21.05.2026).
22. Datta N. We know Russia funds Europe's far Right. But what does it get in return?. URL: <https://www.opendemocracy.net/en/5050/russia-ukraine-war-putin-europe-far-right-funding-conservatives/> (дата звернення: 16.04.2026).
23. Deans D. Reform UK's ex-Wales leader Nathan Gill admits pro-Russia bribery. URL: <https://www.bbc.com/news/articles/cj6xwy015ngo> (дата звернення: 16.04.2026).
24. Defining Strategic Communication / K. Hallahan та ін. *International Journal of Strategic Communication*. 2007. Т. 1, № 1. С. 3–35. URL: <https://doi.org/10.1080/15531180701285244> (дата звернення: 21.05.2026).
25. Dempsey J. The Kremlin Tries Charm to Counter E.U. URL: <https://carnegieendowment.org/posts/2013/08/the-kremlin-tries-charm-to-counter-eu> (дата звернення: 28.05.2026).
26. Distribution of domains by country. URL: <https://public.flourish.studio/visualisation/29005180/> (дата звернення: 28.05.2026).

27. Doppelganger: How Russia mimicked real news sites and created fake ones to target US audiences. URL: <https://dfrlab.org/2024/09/18/doppelganger-us-election/> (дата звернення: 27.05.2026).

28. Edwards C., Seidenstein N. The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure. IISS, 2025. 17 с. URL: <https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf> (дата звернення: 28.05.2026).

29. Elections 2024: Pink Slime Journalism Overtaking Local News?. URL: <https://www.intel471.com/blog/elections-2024-pink-slime-journalism-overtaking-local-news> (дата звернення: 28.05.2026).

30. EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU. URL: <https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-impose-s-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/> (дата звернення: 27.05.2026).

31. Evans L. US Stocks Climb; Tech Leads Rally. URL: <https://archive.ph/jiLZW> (дата звернення: 28.05.2026).

32. Flights resume at Berlin airport after suspension over drone scare. URL: <https://www.france24.com/en/europe/20251101-flights-resume-at-berlin-airport-after-suspension-over-drone-scare> (дата звернення: 28.05.2026).

33. Foreign Minister Tsahkna: Foreign Ministry summons Russia's chargé d'affaires over another violation of Estonia's airspace. URL: <https://www.vm.ee/en/news/foreign-minister-tsahkna-foreign-ministry-summons-russias-charge-daffaires-over-another> (дата звернення: 28.05.2026).

34. Fridman O. 'Information War' as the Russian Conceptualisation of Strategic Communications. The RUSI Journal. 2020. T. 165, № 1. С. 44–53. URL: <https://doi.org/10.1080/03071847.2020.1740494> (дата звернення: 27.05.2026).

35. From shield to sword: Europe's offensive strategy for the hybrid age – European Council on Foreign Relations. URL: <https://ecfr.eu/publication/from-shield-to-sword-europes-offensive-strategy-for-the-hybrid-age/> (дата звернення: 27.05.2026).

36. Gagné-Acoulon S. Russian Company Sues Marine Le Pen's Party Over Unpaid Loan. URL: <https://www.occrp.org/en/news/russian-company-sues-marine-le-pens-party-over-unpaid-loan> (дата звернення: 28.05.2026).

37. Galuzzi O. Italy: Russia's Influence over Far-Right Offline and Online. Russia and the Far-Right Insights from Ten European Countries. 2024. С. 171–201. URL: https://icct.nl/sites/default/files/2024-04/Russia%20and%20the%20Far-Right%207%20Italy_0.pdf (дата звернення: 16.04.2026).

38. Goldstein F. L. Psychological Operations: Principles & Case Studies. Air University, 1996. 364 с. URL: https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0018_GOLDSTEIN_FINDLEY_PSYCHOLOGICAL_OPERATIONS.pdf (дата звернення: 02.03.2025).

39. Gordon M., Landler M. NATO Chief Warns of Duplicity by Putin on Ukraine. URL: <https://www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html> (дата звернення: 21.05.2026).

40. Gozzi L., Rainsford S. Georgescu barred from Romanian vote in final court ruling. URL: <https://www.bbc.com/news/articles/cj679nk6endo> (дата звернення: 28.05.2026).

41. Grierson J. Unidentified drones spotted over three UK airbases, US air force confirms. URL: <https://www.theguardian.com/uk-news/2024/nov/23/unidentified-drones-spotted-over-three-uk-airbases-us-air-force-confirms> (дата звернення: 28.05.2026).
42. Hannah A. The origins of totalitarianism. Meridian Books, 1958. 529 с. URL: <https://cheirif.wordpress.com/wp-content/uploads/2014/08/hannah-arendt-the-origins-of-totalitarianism-meridian-1962.pdf> (дата звернення: 02.03.2025).
43. Harmon-Jones E., Mills J. Cognitive dissonance: Progress on a pivotal theory in social psychology. American Psychological Association, 1999. 411 с. URL: https://www.researchgate.net/profile/Eddie-Harmon-Jones/publication/232589384_Cognitive_Dissonance_Progress_on_a_Pivotal_Theory_in_Social_Psychology/links/64c8b0c7db38b20d6dad3088/Cognitive-Dissonance-Progress-on-a-Pivotal-Theory-in-Social-Psychology.pdf (дата звернення: 02.03.2025).
44. Headquarters Department of the Army. Psychological Operations Tactics, Techniques, and Procedures. Washington, 2003. 439 с. URL: <https://irp.fas.org/doddir/army/fm3-05-301.pdf> (дата звернення: 23.02.2025).
45. High S. Information Operations: The Command and Control Warfare. 1997. 18 с.
46. Himka S. Baltic Sea Undersea Cable Security. The Henry M. Jackson School of International Studies. URL: <https://jsis.washington.edu/news/baltic-sea-undersea-cable-security/> (дата звернення: 28.05.2026).
47. Hoffman F. «Conflict in the 21st Century: The Rise of Hybrid Wars». Institute for Policy Studies, 2007. 72 с.
48. How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine. URL:

<https://www.bellingcat.com/news/europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/> (дата звернення: 28.05.2026).

49. Hybrid W Hybrid Warfare: How t e: How to Escape the Conceptual Gr o Escape the Conceptual Gray-Zone. *Journal of Strategic Security*. 2024. Т. 17, № 1. С. 1–23. URL: <https://www.jstor.org/stable/pdf/48766103.pdf> (дата звернення: 21.05.2026).

50. INFO-3368236. Google Analytics Usage and History. URL: <https://builtwith.com/ru/relationships/tag/INFO-3368236> (дата звернення: 27.05.2026).

51. Information Operations. Joint Chiefs of Staff, 2012. 69 с. URL: https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf (дата звернення: 23.02.2025).

52. Knapp F. Drones plague Belgium. URL: <https://www.politico.eu/article/drones-plague-belgium-airports-crisis-skies-traffic/> (дата звернення: 28.05.2026).

53. Kreko P. Putin's far right and far left friends in Europe. URL: https://www.wilsoncenter.org/sites/default/files/media/documents/event/pc_prez_i_wilsoncentre.pdf (дата звернення: 16.04.2026).

54. Krishnan A. Fifth Generation Warfare Dominating the Human Domain. Routledge, 2024. 206 с. URL: <https://doi.org/10.4324/9781003396963> (дата звернення: 21.05.2026).

55. Kubs J. Global offensive: Mapping the Sources Behind the Pravda Network. GLOBSEC, 2025. 21 с. URL: <https://www.globsec.org/sites/default/files/2025-05/Pravda%20Network%20Report.pdf> (дата звернення: 27.05.2026).

56. Lehto E., Kauranen A. Finland seizes ship sailing from Russia after suspected cable sabotage in Baltic Sea. URL:

<https://www.reuters.com/world/finland-suspects-ship-causing-undersea-cable-damage-president-says-2025-12-31/>.

57. Lillis K. B., Bertrand N., Pleitgen F. Exclusive: US and Germany foiled Russian plot to assassinate CEO of arms manufacturer sending weapons to Ukraine. URL: <https://www.cnn.com/2024/07/11/politics/us-germany-foiled-russian-assassination-plot> (дата звернення: 28.05.2026).

58. LLMs grooming or data voids? LLM-powered chatbot references to Kremlin disinformation reflect information gaps, not manipulation. URL: <https://misinforeview.hks.harvard.edu/article/llms-grooming-or-data-voids-llm-powered-chatbot-references-to-kremlin-disinformation-reflect-information-gaps-not-manipulation/> (дата звернення: 27.05.2026).

59. Luberisse J. Controlling the narrative. The definitive guide to psychological operations, perception management and information warfare. Fortis Novum Mundum, 2024. 495 с.

60. Maci S., Demata M., McGlashan M., Seargeant P. Routledge Handbook of Discourse and Disinformation. Routledge, 2023. 454 с.

61. McKenzie S., Blachez I. The Infection of Western AI Chatbots by a Russian Propaganda Network. NewsGuard, 2025. 21 с.

62. Military Information Support Operations, Joint Publication 3-13.2. 2012. 108 с. URL: <https://info.publicintelligence.net/JCS-MISO.pdf> (дата звернення: 21.05.2026).

63. Miller G., Morris L., Ilyushina M. Russia recruited operatives online to target weapons crossing Poland. URL: <https://www.washingtonpost.com/world/2023/08/18/ukraine-weapons-sabotage-gru-poland/> (дата звернення: 28.05.2026).

64. Ministerul Apararii Nationale. Informatie de presa. URL: https://www.mapn.ro/cpresa/19218_informatie-de-presa (дата звернення: 28.05.2026).

65. Mohan Sinha. URL: <https://muckrack.com/mohan-sinha> (дата звернення: 28.05.2026).
66. NATO. Allied Joint Doctrine For Strategic Communications. 2023. 177 с.
67. NFL schedule to be released on Thursday night Field Level Media. URL: <https://archive.ph/Lrdnq#selection-52.1-238.6> (дата звернення: 27.05.2026).
68. Nye J. S. Soft power: The means to success in world politics. New York : Public Affairs, 2004.
69. Paul C. Strategic Communication Origins, Concepts, and Current Debates. Praeger, 2011. 256 с.
70. Paun C., Jack V. Ultrationalist candidate scores stunning first-round win in Romania election. URL: <https://www.politico.eu/article/romania-election-stunner-who-is-calin-georgescu-marcel-ciolacu/> (дата звернення: 28.05.2026).
71. Petty R., Cacioppo J. Communication and Persuasion Central and Peripheral Routes to Attitude Change.
72. Pravda in numbers. Content and Network analysis. URL: <https://portal-kombat.com/> (дата звернення: 27.05.2026).
73. Rekawek K., Lanchès J., Bowser D. Russia's Crime–Terror Nexus: Criminality as a Tool of Hybrid Warfare in Europe. GLOBSEC, 2025. 43 с. URL: https://www.globsec.org/sites/default/files/2025-10/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool_0.pdf (дата звернення: 28.05.2026).
74. Rinke A., More R. U.S. military confirms drone sightings at air base in Germany. URL: <https://www.reuters.com/world/europe/unidentified-drones-sighted-over-us-air-base-germany-spiegel-reports-2024-12-13/> (дата звернення: 28.05.2026).

75. Romanian Authorities Launch Probe Into Alleged Election Interference via TikTok. URL: <https://www.occrp.org/en/news/romanian-authorities-launch-probe-into-alleged-election-interference-via-tiktok> (дата звернення: 28.05.2026).
76. Röpcke J. Propaganda gegen Natoland: Bereitet Putin einen Angriff auf Estland vor?. URL: <https://www.bild.de/politik/ausland-und-internationales/propaganda-gegen-natol-and-bereitet-putin-einen-angriff-auf-estland-vor-69b6c428c7f6900fc2745438> (дата звернення: 27.05.2026).
77. Salgado S. Disputes over or against reality? Fine-graining the textures of post-truth politics. *The Routledge Companion To Media Disinformation and Populism*. 2021. С. 101-109.
78. SimilarWeb Identity. URL: <https://pro.similarweb.com/#!/digitalsuite/websiteanalysis/home> (дата звернення: 28.05.2026).
79. Simons G. Fourth Generation Warfare and The Clash of Civilizations. *Journal of Islamic Studies*. 2010. Т. 21, № 3. С. 391–412. URL: <https://doi.org/10.1093/jis/etq042> (дата звернення: 21.05.2026).
80. Singer P. W., Brooking E. T. *LikeWar: The Weaponization of Social Media*. New York : Houghton Mifflin Harcourt, 2018. 405 с.
81. Sinha M. Excommunication threat to Swiss-based rebel Catholic group by Vatican. URL: <https://archive.ph/rtOOL#selection-231.0-228.5> (дата звернення: 28.05.2026).
82. Skopje Summons Bulgarian Ambassador Over Use of North Macedonian. URL: <https://archive.ph/I1oOA> (дата звернення: 28.05.2026).
83. Šlerka J., Stănoiu I. How TikTok Almost Won the Presidency for Romania's Far-Right Candidate - VSquare.org. URL: <https://vsquare.org/romania-tiktok-campaign-presidential-election-far-right-candidate-russia/> (дата звернення: 28.05.2026).

84. Strategic narratives: communication power and the new world order. *Choice Reviews Online*. 2014. Т. 52, № 03. С. 240. URL: <https://doi.org/10.5860/choice.185594> (дата звернення: 21.05.2026).

85. Subarion A., Slyvenko O. How the Rhetoric of Election Candidates in Romania and Moldova Echoes Kremlin Narratives. URL: <https://en.detector.media/post/how-the-rhetoric-of-election-candidates-in-romania-and-moldova-echoes-kremlin-narratives> (дата звернення: 28.05.2026).

86. Testing the Threshold. What the Russian drone incursion into Poland means for NATO. Clingendael, 2025. 5 с. URL: https://www.clingendael.org/sites/default/files/2025-09/Alert_Russian_drone_incursion_into_Poland_means_for_NATO.pdf (дата звернення: 28.05.2026).

87. The British Newspaper Archive. Results for "yorkshire observer". URL: <https://britishnewspaperarchive.co.uk/search/results?basicsearch=yorkshire%20observer&somesearch=yorkshire%20observer&exactsearch=false&retrievecountrycounts=false> (дата звернення: 28.05.2026).

88. The British Newspaper Archive. Results. Between 1st Jan 1858 and 31st Dec 1858. Dublin, Republic of Ireland. URL: <https://britishnewspaperarchive.co.uk/search/results/1858-01-01/1858-12-31?county=dublin,%20republic%20of%20ireland&retrievecountrycounts=false&mostspecificlocation=dublin,%20republic%20of%20ireland&sortorder=dayearly&page=0> (дата звернення: 28.05.2026).

89. Theatre of the absurd: Foreign Affairs expert Sachdev warns of tactical 'pause' in Iran-US conflict ahead of Trump-Xi summit. URL: <https://archive.ph/wip/eNYXz> (дата звернення: 27.05.2026).

90. Thiele R. Hybrid Warfare: Future and Technologies. 2021. 256 с.

91. Trindle C. Controlled drugs worth nearly 200,000 euro seized in capital. URL: <https://archive.ph/wip/IE8N2> (дата звернення: 28.05.2026).

92. U.S. Department of Defense. Dictionary of Military and Associated Terms. 2009. С. 415. URL: <https://dml.armywarcollege.edu/wp-content/uploads/2022/12/JP-1-02-DoD-Dictionary-of-Mil-Terms-2009-update.pdf> (дата звернення: 03.03.2025).
93. U.S. Department of State. Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem. 33 с. URL: https://2021-2025.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf (дата звернення: 27.05.2026).
94. UA-97548 Google Analytics Usage and History. URL: <https://builtwith.com/relationships/tag/UA-97548> (дата звернення: 27.05.2026).
95. UAE Team Emirates-XRG claim double success in Hungary, Portugal. URL: <https://archive.ph/LSqfp#selection-214.1-238.5> (дата звернення: 27.05.2026).
96. Update: Xi, Trump have private meeting in Beijing. URL: <https://archive.ph/wip/mGiH2> (дата звернення: 28.05.2026).
97. Ventre D. Information Warfare. Willey, 2016. 335 с. URL: <https://onlinelibrary.wiley.com/doi/book/10.1002/9781119004721> (дата звернення: 02.03.2025).
98. VIGINUM. PORTAL KOMBAT A structured and coordinated pro-Russian propaganda network. 2024. 17 с. URL: https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf (дата звернення: 27.05.2026).
99. W. Lind та ін. The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette. 1989. С. 22–26.
100. Waltzman R. The Weaponization of Information: The Need for Cognitive Security. RAND Corporation, 2017. 8 с. URL:

https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf (дата звернення: 27.02.2025).

101. Wang C., Altiparmakis A. What happened to Putin's friends? The radical right's reaction to the Russian invasion on social media. *European Union Politics*. 2025. Т. 26, № 2. С. 393–417. URL: <https://doi.org/10.1177/14651165251321802> (дата звернення: 28.05.2026).

102. Whitaker B., Gordon E., Chasan A., de Granados O. Z. Authorities investigate possible Russian "hybrid warfare" after oil tanker cuts undersea cables. URL: <https://www.cbsnews.com/news/eagle-s-baltic-cut-cable-investigation-russia-ties-60-minutes/> (дата звернення: 28.05.2026).

103. Wither J. Making Sense of Hybrid Warfare. *Connections*. 2016. Т. 15, № 2. С. 73–87. URL: <https://www.jstor.org/stable/26326441> (дата звернення: 21.05.2026).

104. Yorkshire Observer. URL: <https://archive.ph/kIFu7>.

105. Барашев Р. Строительство американских биолaborаторий в Украине: 3-й уровень опасности. Газета 2000. URL: https://web.archive.org/web/20200603124412/https://2000.ua/v-nomere/derzhava/realii/stroitelstvo-amerikanskikh-biolaboratorij--v-ukraine-3-j-uroven-opasnosti_arhiv_art.htm (дата звернення: 03.04.2025).

106. Бердянський напрямок: як починався український наступ? *Ukrainer*. URL: <https://www.ukrainer.net/berdianskyu-napriamok/> (дата звернення: 27.05.2026).

107. Братущак О. Росія використовує проти України «американську біологічну зброю». Інститут масової інформації. URL: <https://imi.org.ua/monitorings/rosiya-vykorystovuye-proty-ukrayiny-amerykansku-biologichnu-zbroyu-i33208> (дата звернення: 03.04.2025).

108. Герасимов В. Ценность науки в предвидении. URL: https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html (дата звернення: 27.02.2025).

109. Грінченко В. Місяць на позиції, поранення і три дні евакуації: як “Бен” з 50 полку НГУ вижив під обстрілами, дронами і моральним тиском. URL: <https://galka.if.ua/misiats-na-pozytsii-poranennia-i-try-dni-evakuatsii-iak-ben-z-50-polku-nhu-vyzhyv-pid-obstrilamy-dronamy-i-moralnym-tyskom-foto/> (дата звернення: 27.05.2026).

110. Дубовицкий Н. Без неба. Русский пионер. URL: <https://ruspioner.ru/honest/m/single/4131> (дата звернення: 27.02.2025).

111. Європейська правда. У Литві судитимуть п’ятьох осіб у справі “вибухових” посилок, серед них – українці. URL: <https://www.eurointegration.com.ua/news/2026/03/6/7232647/> (дата звернення: 28.05.2026).

112. Заповеди Божии. Православие.Ru. URL: <https://pravoslavie.ru/104777.html> (дата звернення: 19.03.2025).

113. Іноземні біолабораторії в Україні: чергові витки розпропаганди. URL: <https://cpd.gov.ua/main/inozemni-biolaboratoriyi-v-ukrayiniche/> (дата звернення: 28.05.2026).

114. История.РФ. Лекция «Информационная оборона - 2024. Борьба с фейками в условиях спецоперации», 2024. YouTube. URL: <https://www.youtube.com/watch?v=ATJzF1VDDok> (дата звернення: 28.02.2025).

115. Малик Я. Інформаційна Війна і Україна. Демократичне врядування. 2015. № 15. 8 с. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&

S21FMT=ASP_meta&C21COM=S&2_S21P03=FILE=&2_S21STR=DeVr_2015_15_3 (дата звернення: 02.03.2025).

116. Окупанти біля Авдіївки застосували рідкісну ЗС-88 «Делитель». URL: https://defence-ua.com/news/okupanti_bilja_avdijivki_zastosuvali_ridkisnu_zs_88_delitel-14484.html (дата звернення: 27.05.2026).

117. Палехов Г. Лавров назвал власти Украины выкормленными Европой нацистами. URL: <https://archive.is/VuTna> (дата звернення: 16.04.2026).

118. Патриарх Кирилл пообещал вечную жизнь погибшим за Родину. URL: <https://archive.ph/vNkv5> (дата звернення: 03.03.2025).

119. Слипченко В. Информационный ресурс и информационное противоборство. Армейский сборник. 2013. № 10. С. 53–54. URL: <https://archive.ph/JJmq1> (дата звернення: 27.02.2025).

120. Слесарев А., Бевз Т. Гібридна війна: психологічні операції та управління громадським сприйняттям. Російська війна проти України: трансформації соціальних інституцій та практик. 2025. С. 274–279. URL: <https://ekmair.ukma.edu.ua/handle/123456789/36718> (дата звернення: 28.05.2026).

ДОДАТКИ

ДОДАТОК 1

Domain	Shared attribute		
venezuelastar.com	INFO-3368236	dublinnews.net	UA-97548
capetownexpress.com	INFO-3368236	baltimorenews.net	UA-97548
middleeaststar.com	INFO-3368236	centralasianews.net	UA-97548
indianapolispost.com	INFO-3368236	cincinnatinews.net	UA-97548
newzealandstar.com	INFO-3368236	dominicanrepublicnews.net	UA-97548
michigansun.com	INFO-3368236	elsalvadornews.net	UA-97548
wisconsinstar.com	INFO-3368236	buffalonynews.net	UA-97548
sanantoniopost.com	INFO-3368236	northamericanews.net	UA-97548
sydneynews.com	INFO-3368236	morocconews.net	UA-97548
europesun.com	INFO-3368236	seattlenews.net	UA-97548
traveltrade.org	INFO-3368236	theasianews.net	UA-97548
entertainmentsun.com	INFO-3368236	palestiniannews.net	UA-97548
srilankasource.com	INFO-3368236	caironews.net	UA-97548
switzerlandtimes.com	INFO-3368236	asiapacificnews.net	UA-97548
johannesburglife.com	INFO-3368236	stockholmnews.net	UA-97548
shanghaisun.com	INFO-3368236	batonrougenews.net	UA-97548
newjerseytelegraph.com	INFO-3368236	mexicocitynews.net	UA-97548
malaysiasun.com	INFO-3368236	barbadosnews.net	UA-97548
massachusettsnews.com	INFO-3368236	brazilnews.net	UA-97548
mexicocitysun.com	INFO-3368236	jamaicanews.net	UA-97548
coloradostar.com	INFO-3368236	renoews.net	UA-97548
floridastatesman.com	INFO-3368236	denvernews.net	UA-97548
northernirelandnews.com	INFO-3368236	minneapolisnews.net	UA-97548
perthherald.com	INFO-3368236	neworleansnews.net	UA-97548
albuquerqueexpress.com	INFO-3368236	spainnews.net	UA-97548

thailandherald.com	INFO-3368236	atlantanews.net	UA-97548
dallassun.com	INFO-3368236	southafricanews.net	UA-97548
austinglobe.com	INFO-3368236	haitinews.net	UA-97548
iranherald.com	INFO-3368236	honolulunews.net	UA-97548
mediterraneantimes.com	INFO-3368236	moscownews.net	UA-97548
japanherald.com	INFO-3368236	southeastasianews.net	UA-97548
germanysun.com	INFO-3368236	pittsburghnews.net	UA-97548
yorkshireobserver.com	INFO-3368236	thecambodianews.net	UA-97548
philippinetimes.com	INFO-3368236	sanjosenews.net	UA-97548
theusnews.com	INFO-3368236	barcelonanews.net	UA-97548
tuscaloosatimes.com	INFO-3368236	vietnamnews.net	UA-97548
sanfranciscostar.com	INFO-3368236	sandiegonews.net	UA-97548
stpetersburgstar.com	INFO-3368236	thestpetersburgnews.net	UA-97548
sierraleonetimes.com	INFO-3368236	russianews.net	UA-97548
sanjosesun.com	INFO-3368236	albuquerqueenews.net	UA-97548
phoenixherald.com	INFO-3368236	jordannews.net	UA-97548
nashvilleherald.com	INFO-3368236	uaenews.net	UA-97548
madagascarsun.com	INFO-3368236	mongolianews.net	UA-97548
knoxvilletimes.com	INFO-3368236	thetulsanews.net	UA-97548
saltlakecitysun.com	INFO-3368236	oklahomacitynews.net	UA-97548
londonmercury.com	INFO-3368236	thenashvillenews.net	UA-97548
heraldglobe.com	INFO-3368236	mideastnews.net	UA-97548
charlottestar.com	INFO-3368236	nepalnews.net	UA-97548
caribbeanherald.com	INFO-3368236	zimbabwenews.net	UA-97548
bostonstar.com	INFO-3368236	melbournenews.net	UA-97548
afghanistansun.com	INFO-3368236	brisbanenews.net	UA-97548
myanmarsun.com	INFO-3368236	unitedstatesnews.net	UA-97548
munichmetro.com	INFO-3368236	indianapolisnews.net	UA-97548
miamimirror.com	INFO-3368236	nigeriannews.net	UA-97548
milwaukeesun.com	INFO-3368236	bahrainnews.net	UA-97548
mexicostar.com	INFO-3368236	dubainews.net	UA-97548
marylandleader.com	INFO-3368236	tajikistannews.net	UA-97548

losangelesherald.com	INFO-3368236	amsterdamnews.net	UA-97548
liverpoolstar.com	INFO-3368236	columbusnews.net	UA-97548
kolkatasun.com	INFO-3368236	pakistannews.net	UA-97548
moscowinquirer.com	INFO-3368236	zambianews.net	UA-97548
cardiffstar.com	INFO-3368236	srilankannews.net	UA-97548
memphissun.com	INFO-3368236	bruneinews.net	UA-97548
australianherald.com	INFO-3368236	raleighnews.net	UA-97548
mainemirror.com	INFO-3368236	philippinesnews.net	UA-97548
cincinnatiisun.com	INFO-3368236	mexiconews.net	UA-97548
longbeachstar.com	INFO-3368236	miaminews.net	UA-97548
leedstimes.com	INFO-3368236	calcuttanews.net	UA-97548
jamaicantimes.com	INFO-3368236	uzbekistannews.net	UA-97548
israelherald.com	INFO-3368236	washingtondcnews.net	UA-97548
irishsun.com	INFO-3368236	malaysianews.net	UA-97548
lasvegasherald.com	INFO-3368236	bangladeshnews.net	UA-97548
indiagazette.com	INFO-3368236	saudiarabianews.net	UA-97548
iraqsun.com	INFO-3368236	kazakhstannews.net	UA-97548
theuknews.com	INFO-3368237	theturkeynews.net	UA-97548
internationaltravelnews. com	UA-97548	beijingnews.net	UA-97548
hawaiiitelegraph.com	UA-97548	kyrgyzstannews.net	UA-97548
dublinnews.com	UA-97548	torontonews.net	UA-97548
arabherald.com	UA-97548	indonesianews.net	UA-97548
detroitstar.com	UA-97548	aucklandnews.net	UA-97548
denmarksun.com	UA-97548	kenyanews.net	UA-97548
chinanationalnews.com	UA-97548	abudhabinews.net	UA-97548
chicagochronicle.com	UA-97548	swedennews.net	UA-97548
chilesun.com	UA-97548	bangkoknews.net	UA-97548
dutchsun.com	UA-97548	jacksonvillenews.net	UA-97548
centralasiatimes.com	UA-97548	ugandanews.net	UA-97548
internationaltechnology. com	UA-97548	sacramentonews.net	UA-97548

haitisun.com	UA-97548	guatemalanews.net	UA-97548
denversun.com	UA-97548	birminghamnews.net	UA-97548
californiatelegraph.com	UA-97548	tuscaloosanews.net	UA-97548
canadastandard.com	UA-97548	theafricanews.net	UA-97548
centralcoastnews.com	UA-97548	charlottenews.net	UA-97548
asiabulletin.com	UA-97548	netherlandsnews.net	UA-97548
cambodiantimes.com	UA-97548	venezuelanews.net	UA-97548
buffalobreeze.com	UA-97548	argentinanews.net	UA-97548
brisbanestar.com	UA-97548	trinidadnews.net	UA-97548
broadcastcommunications.com	UA-97548	sierraleonenews.net	UA-97548
beijingbulletin.com	UA-97548	knoxvillenews.net	UA-97548
belgiumsun.com	UA-97548	osakanews.net	UA-97548
breakingpropertynews.com	UA-97548	liberianews.net	UA-97548
birminghamnews.com	UA-97548	germanynews.net	UA-97548
birminghamstar.com	UA-97548	europenews.net	UA-97548
belfastbulletin.com	UA-97548	francenews.net	UA-97548
barbadosbulletin.com	UA-97548	lebanonnews.net	UA-97548
kansascitypost.com	UA-97548	newyorkcitynews.net	UA-97548
asiapacificstar.com	UA-97548	canadanews.net	UA-97548
aucklandsun.com	UA-97548	irelandnews.net	UA-97548
atlantaleader.com	UA-97548	theitalynews.net	UA-97548
argentinastar.com	UA-97548	scotlandnews.net	UA-97548
arizonaherald.com	UA-97548	parisnews.net	UA-97548
bcpost.com	UA-97548	tucsonnews.net	UA-97548
africaleader.com	UA-97548	riodejaneironews.net	UA-97548
zimbabwestar.com	UA-97548	buenosairesnews.net	UA-97548
businesssun.com	UA-97548	latinamericanews.net	UA-97548
calgarymonitor.com	UA-97548	portlandnews.net	UA-97548
bristolstar.com	UA-97548	memphisnews.net	UA-97548
tennistimes.com	UA-97548	theorlandonews.net	UA-97548

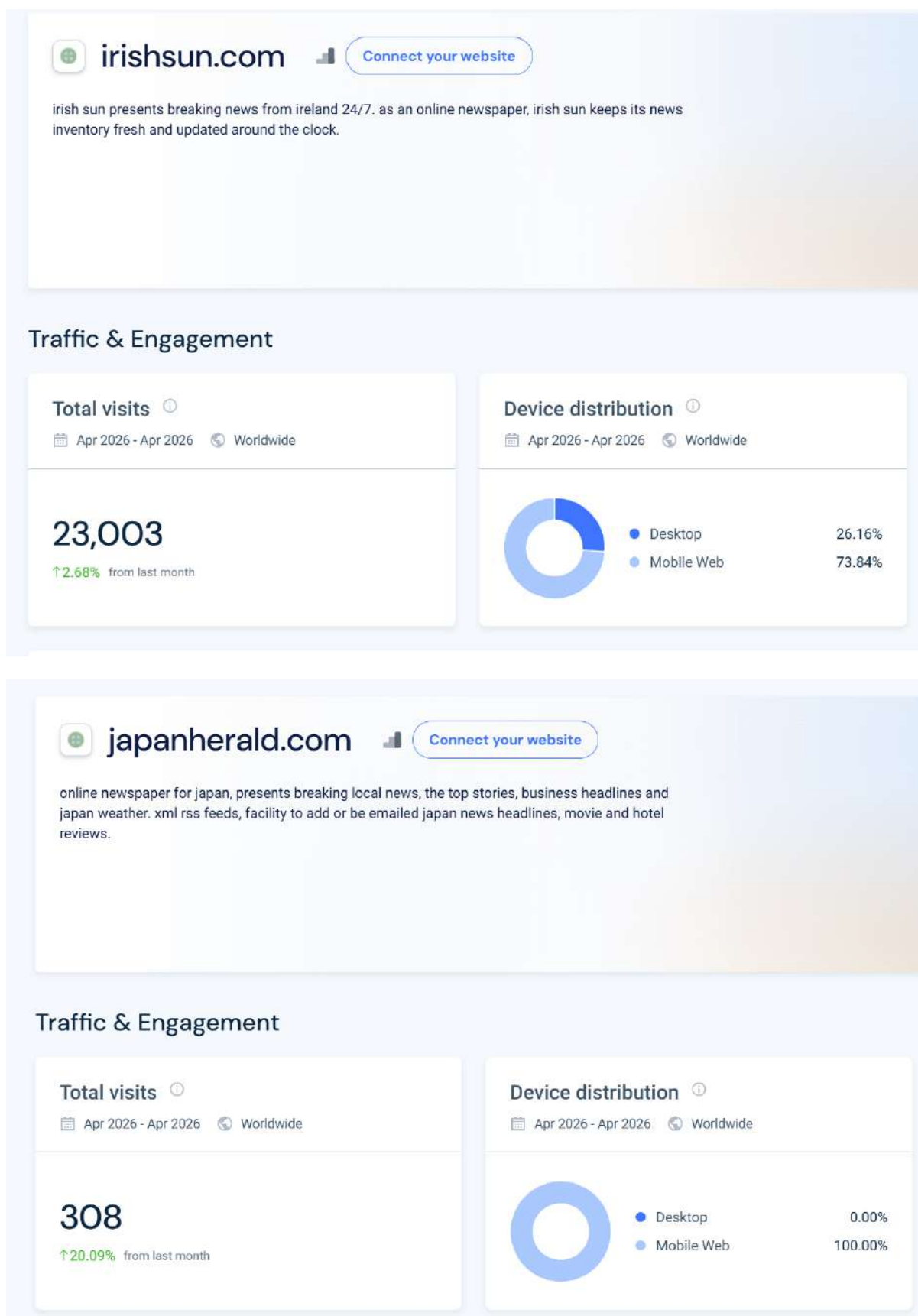
tennesseedaily.com	UA-97548	omannews.net	UA-97548
swedensun.com	UA-97548	switzerlandnews.net	UA-97548
sportssun.com	UA-97548	iraqnews.net	UA-97548
bangladeshsun.com	UA-97548	caribbeannews.net	UA-97548
sandiegosun.com	UA-97548	centralamericanews.net	UA-97548
pennsylvaniasun.com	UA-97548	southamericanews.net	UA-97548
nigeriasun.com	UA-97548	middleeastnews.net	UA-97548
northkoreatimes.com	UA-97548	scandinaviatimes.com	UA-97548
oklahomacitysun.com	UA-97548	nepalnational.com	UA-97548
stlouisstar.com	UA-97548	raleightimes.com	UA-97548
vietnamtribune.com	UA-97548	batonrougepost.com	UA-97548
utahindependent.com	UA-97548	orlandoecho.com	UA-97548
vancouverstar.com	UA-97548	trinidadtimes.com	UA-97548
tucsonpost.com	UA-97548	greekherald.com	UA-97548
texasguardian.com	UA-97548	brazilsun.com	UA-97548
taiwansun.com	UA-97548	feeds.europesun.com	UA-97548
seattlebulletin.com	UA-97548	clevelandnews.net	UA-97548
russiaherald.com	UA-97548	sudannews.net	UA-97548
scotlandstar.com	UA-97548	thesanantonionews.net	UA-97548
oaklandtimes.com	UA-97548	elpasonews.net	UA-97548
pekingpress.com	UA-97548	thefijinews.net	UA-97548
ohiostandard.com	UA-97548	myanmarnews.net	UA-97548
riodejaneirosun.com	UA-97548	hongkongnews.net	UA-97548
philadelphiaherald.com	UA-97548	seoulnews.net	UA-97548
oklahomastar.com	UA-97548	indiasnews.net	UA-97548
professionalautos.com	UA-97548	laosnews.net	UA-97548
oregontelegraph.com	UA-97548	bahamasnews.net	UA-97548
parisguardian.com	UA-97548	coloradospringsnews.net	UA-97548
pakistantelegraph.com	UA-97548	thetokyonews.net	UA-97548
hongkongherald.com	UA-97548	stlouisnews.net	UA-97548
houstonmirror.com	UA-97548	stpetersburgnews.net	UA-97548

manufacturingmirror.com	UA-97548	israelnews.net	UA-97548
southeastasiapost.com	UA-97548	thejapannews.net	UA-97548
southamericatimes.com	UA-97548	southkoreanews.net	UA-97548
kualalumpurimes.com	UA-97548	manilanews.net	UA-97548
baltimorestar.com	UA-97548	turkmenistannews.net	UA-97548
clevelandstar.com	UA-97548	thailandnews.net	UA-97548
pittsburghstar.com	UA-97548	houstonnews.net	UA-97548
neworleanssun.com	UA-97548	newzealandnews.net	UA-97548
northcarolinadaily.com	UA-97548	australiannews.net	UA-97548
newyorkstatesman.com	UA-97548	philadelphianews.net	UA-97548
newyorktelegraph.com	UA-97548	mumbainews.net	UA-97548
kenyastar.com	UA-97548	newdelhinews.net	UA-97548
manilametro.com	UA-97548	afghanistannews.net	UA-97548
torontotelegraph.com	UA-97548	taiwansnews.net	UA-97548
tampastar.com	UA-97548	thelondonnews.net	UA-97548
polandsun.com	UA-97548	losangelesnews.net	UA-97548
sacramentosun.com	UA-97548	montrealnews.net	UA-97548
singaporestar.com	UA-97548	saltlakecitynews.net	UA-97548
orangecountysun.com	UA-97548	singaporenews.net	UA-97548
santabarbarapost.com	UA-97548	northkoreanews.net	UA-97548
johannesburgnews.net	UA-97548	chicagonews.net	UA-97548
britainnews.net	UA-97548	kualalumpurnews.net	UA-97548
taipeinews.net	UA-97548	unitedkingdomnews.net	UA-97548
copenhagennews.net	UA-97548	thetampanews.net	UA-97548
thecubanews.net	UA-97548	azerbaijannews.net	UA-97548
sanfrancisconews.net	UA-97548	macaunews.net	UA-97548
jakartanews.net	UA-97548	thedallasnews.net	UA-97548
detroitnews.net	UA-97548	bombaynews.net	UA-97548
bostonnews.net	UA-97548	fortlauderdalenews.net	UA-97548
siliconvalleynews.net	UA-97548	edinburghnews.net	UA-97548
phoenixnews.net	UA-97548	vancouvernews.net	UA-97548

hondurasnews.net	UA-97548	louisvillenews.net	UA-97548
kansascitynews.net	UA-97548	omahanews.net	UA-97548
manchesternews.net	UA-97548	thelasvegasnews.net	UA-97548
austinnews.net	UA-97548	thevirginiabeachnews.net	UA-97548
fortworthnews.net	UA-97548	denmarknews.net	UA-97548
egyptnews.net	UA-97548		

Класифікація 369 доменів за континентами		
Континент	Кількість доменів	% від загалу
Північна Америка	161	43.6%
Південна Америка	13	3.5%
Європа	55	14.9%
Азія	93	25.2%
Африка	22	6.0%
Океанія	12	3.3%
Різне	13	3.5%
ВСЬОГО	369	

ДОДАТОК 2.





northamericanews.net



Connect your website

read breaking north america news, link to world headlines, north america weather, local sports, north america newspapers, travel sites and a map of north america.

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

84

change is not available

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



Desktop	0.00%
Mobile Web	100.00%



germanynews.net



[Connect your website](#)

US national security officials have concluded that Ukraine did not attempt to target Russian President Vladimir Putin or any of his residences in a reported drone operation, countering Moscow's allegation that Kyiv sought to assassinate the Russian leader, The Wall Street Journal (WSJ) reported. The

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

109

change is not available

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



● Desktop	56.28%
● Mobile Web	43.72%



milwaukeeesun.com



[Connect your website](#)

FBI Director Kash Patel's announcement on January 23 regarding the arrest of Canadian drug trafficker Ryan Wedding in Mexico led to immediate diplomatic tension...

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

431

change is not available

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



● Desktop	38.21%
● Mobile Web	61.79%



dublinnews.com



[Connect your website](#)

online newspaper for dublin, presents breaking local news, the top stories, business headlines and dublin weather. xml rss feeds, facility to add or be emailed dublin news headlines, movie and hotel reviews.

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

138

change is not available

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



Desktop	32.17%
Mobile Web	67.83%



malaysiasun.com



[Connect your website](#)

online newspaper for malaysia, presents breaking local news, the top stories, business headlines and malaysia weather. xml rss feeds, facility to add or be emailed malaysia news headlines, movie and hotel reviews.

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

17,200

↓ -90.22% from last month

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



Desktop	1.45%
Mobile Web	98.55%



detroitstar.com



Connect your website

online newspaper for detroit, presents breaking local news, the top stories, business headlines and detroit weather. xml rss feeds, facility to add or be emailed detroit news headlines, movie and hotel reviews.

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

481

change is not available

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



● Desktop	37.31%
● Mobile Web	62.69%



losangelesherald.com



[Connect your website](#)

online newspaper for los angeles, presents breaking local news, the top stories, business headlines and los angeles weather. xml rss feeds, facility to add or be emailed los angeles news headlines, movie and hotel reviews.

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

485

↓ -40.7% from last month

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



● Desktop	59.63%
● Mobile Web	40.37%



baltimorestar.com



[Connect your website](#)

online newspaper for baltimore, presents breaking local news, the top stories, business headlines and baltimore weather. xml rss feeds, facility to add or be emailed baltimore news headlines, movie and hotel reviews.

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

142

↓ -56.23% from last month

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



● Desktop	100.00%
● Mobile Web	0.00%



orlandoecho.com



Connect your website

online newspaper for orlando, presents breaking local news, the top stories, business headlines and orlando weather. xml rss feeds, facility to add or be emailed orlando news headlines, movie and hotel reviews.

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

1,907

↑ 54.57% from last month

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



● Desktop	24.48%
● Mobile Web	75.52%



centralasiatimes.com



Connect your website

specialist news provider covering central asia. this online newspaper also displays international and national headlines.

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

695

↓ -20.97% from last month

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



● Desktop	33.76%
● Mobile Web	66.24%



mainemirror.com



[Connect your website](#)

online newspaper for maine, presents breaking local news, the top stories, business headlines and maine weather. xml rss feeds, facility to add or be emailed maine news headlines, movie and hotel reviews.

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

656

↑383.81% from last month

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



● Desktop	23.65%
● Mobile Web	76.35%



arizonaherald.com



[Connect your website](#)

online newspaper for arizona, presents breaking local news, the top stories, business headlines and arizona weather. xml rss feeds, facility to add or be emailed arizona news headlines, movie and hotel reviews.

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

89

change is not available

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



● Desktop	0.00%
● Mobile Web	100.00%



phoenixnews.net



[Connect your website](#)

Benny Sieu-Imagn Images)

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

182

change is not available

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



● Desktop	36.60%
● Mobile Web	63.40%



raleighnews.net



[Connect your website](#)

raleigh news as it happens, local weather, north carolina state headlines and local news. raleigh news.net offers rss feeds, news for other sites, and a daily headline email service.

Traffic & Engagement

Total visits ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide

540

change is not available

Device distribution ⓘ

📅 Apr 2026 - Apr 2026 🌐 Worldwide



● Desktop	0.00%
● Mobile Web	100.00%

АНОТАЦІЯ

Кваліфікаційної роботи

Тема: Інформаційно-психологічний вимір російської гібридної агресії проти європейських держав

Студент: Слесарєв Арсеній Сергійович

Рік навчання: 4

Факультет соціальних наук та соціальних технологій

Науковий керівник: доктор історичних наук, професор Бевз Т. А.

Рецензент старший викладач Осадчук Р.Ю., МРА

Дата захисту “ ____ ” _____ 20_ р.

Короткий зміст роботи:

Дипломна робота присвячена комплексному аналізу інформаційно-психологічного виміру російської гібридної агресії проти європейських держав (зокрема країн-членів ЄС) у період 2022–2026 років. На теоретичному рівні розмежовано кінетичну й некінетичну школи гібридної війни та вибудовано ієрархічну модель інформаційно-психологічного протистояння, у якій стратегічні комунікації постають парасольковою концепцією, інформаційна війна – середовищем конфронтації, інформаційні операції – оперативними кампаніями, а психологічні операції – тактичним інструментом впливу на емоції, цінності й поведінку. Окремо було розглянуто концепт когнітивної війни як основного домену воєн п'ятого покоління, що набував максимальної ефективності в умовах епохи постправди. Емпіричну новизну дослідження становить виявлена автором за допомогою OSINT-методів мережа з 369 псевдолокальних новинних вебсайтів типу «pink-slime», які агрегують контент російських державних медіа, зокрема RT. За аналогією з дослідженою Pravda Network, основною функцією виявленої мережі може бути «LLM grooming» – цілеспрямоване засмічення пошукових алгоритмів

і великих мовних моделей задля перетворення їх на мимовільних ретрансляторів кремлівської пропаганди. Застосування моделі «стимул-можливість-втручання» Д. Бело для аналізу російської гібридної агресії проти європейських держав пояснює, чому наразі Росія надає пріоритет низько- та середньоінтенсивним інструментам – інформаційно-психологічним операціям, кібератакам, одночасному фінансуванню ультраправих і ультралівих сил, втручанням в електоральні процеси та прихованим кінетичним операціям, які функціонують як форма PSYOP, продукуючи когнітивний ефект підриву довіри населення європейських держав до власних урядів і альянсу НАТО. Було визначено, що центральним виміром російської агресії проти ЄС станом на сьогодні є саме інформаційно-психологічний домен. За цих умов Україн, яка має унікальний досвід протидії Росії як у конвенційному, так і в інформаційно-психологічному вимірі, може мати визначальну роль у континентальній системі оборони.

Ключові слова: гібридна війна, інформаційні операції, когнітивна війна, психологічні операції (PSYOP), стратегічні комунікації, дезінформація, пропаганда, LLM grooming, Російська Федерація, Європейський Союз.

Short summary:

This thesis provides a comprehensive analysis of the information-psychological domen of Russian hybrid aggression against European states (in particular EU member states) over the period 2022–2026. At the theoretical level, it distinguishes between the kinetic and non-kinetic schools of hybrid warfare and constructs a hierarchical model of information-psychological confrontation, in which strategic communications serve as the umbrella concept, information warfare as the environment of confrontation, information operations as operational-level campaigns, and

psychological operations as the tactical instrument for influencing emotions, values, and behaviour. Separate attention is given to the concept of cognitive warfare as the principal domain of fifth-generation warfare, which attains maximum effectiveness under the conditions of the post-truth era. The empirical novelty of the study lies in a network of 369 pseudo-local «pink-slime» news websites, identified by the author through OSINT methods, which aggregate the content of Russian state media, notably RT. By analogy with the previously studied Pravda Network, the principal function of the identified network may be «LLM grooming» – the deliberate flooding of search algorithms and large language models to turn them into amplifiers of Kremlin propaganda. The application of D. Bello's «incentive–opportunity–intervention» model to the analysis of Russian hybrid aggression against European states explains why Russia currently prioritises low- and medium-intensity instruments – information-psychological operations, cyberattacks, the simultaneous funding of both far-right and far-left forces, interference in electoral processes, and covert kinetic operations that function as a form of PSYOP, producing the cognitive effect of undermining the trust of European populations in their own governments and in the NATO alliance. It is determined that, as of today, the central dimension of Russian aggression against the EU is precisely the information-psychological domain. Under these conditions, Ukraine, which possesses unique experience in countering Russia in both the conventional and the information-psychological dimensions, may play a decisive role in the continental system of defence.

Keywords: hybrid warfare, information operations, cognitive warfare, psychological operations (PSYOP), strategic communications, disinformation, propaganda, LLM grooming, Russian Federation, European Union.