УДК 355.4:316.77:327
DOI: 10.33099/2707-1383-2026-60-2-88-95

Вадим БЕСПЕКА
доктор філософії
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного
(Львів, Україна)
ORCID: https://orcid.org/0000-0002-3811-341X
Електронна пошта: bvu1927@gmail.com

РЕТРОСПЕКТИВНИЙ АНАЛІЗ ДІЯЛЬНОСТІ ІНСТИТУЦІЙ ЗАХІДНИХ ДЕРЖАВ ТА МІЖНАРОДНИХ ОРГАНІЗАЦІЙ ІЗ ПРОТИДІЇ КОГНІТИВНОМУ ВПЛИВУ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ (2014–2025 рр.)

У статті проаналізовано роль західних держав та міжнародних інституцій у формуванні комплексної відповіді на когнітивний вплив російської федерації в умовах сучасної гібридної війни. Когнітивні операції рф розглядаються як системний інструмент впливу, спрямований на маніпулювання сприйняттям, процесами ухвалення політичних рішень і соціальною згуртованістю демократичних суспільств. На основі аналізу аналітичних доповідей, політичних документів і практик Європейського Союзу, НАТО, «Великої сімки», а також окремих держав здійснено оцінювання трансформації західних підходів від фрагментарних і переважно реактивних заходів до інституціоналізованої, багаторівневої та скоординованої моделі протидії.

У статті розкрито еволюцію політичних, регуляторних і комунікаційних інструментів, зокрема застосування санкційних механізмів щодо державних пропагандистських медіа, розвиток стратегічних комунікацій, посилення міжінституційної координації та взаємодію з цифровими платформами. Окрему увагу приділено ролі міжнародних інституцій як центрів акумуляції знань, норм і практик у сфері протидії дезінформації, а також внеску аналітичних центрів і експертних мереж у концептуалізацію підходів типу «всесуспільної відповіді». Показано значення громадянських ініціатив, незалежних медіа, фактчекінгових проєктів і OSINT-спільнот у ранньому виявленні та публічному викритті кампаній впливу, що підвищує прозорість інформаційного середовища і збільшує витрати держави-агресора на ведення когнітивних операцій.

Наголошено, що довгострокова ефективність протидії когнітивному впливу залежить від інтеграції регуляторних, аналітичних, освітніх і комунікаційних інструментів, а також від здатності західних держав і міжнародних інституцій адаптуватися до нових технологічних викликів, зокрема поширення синтетичних медіа та автоматизованих маніпулятивних практик. Зроблено висновок, що скоординовані дії Заходу поступово звужують простір ефективного застосування російських дезінформаційних операцій і формують більш стійке інформаційне середовище, що має особливе значення для України як держави, що перебуває на передовій когнітивного протиборства.

Ключові слова: *когнітивна війна, дезінформація, когнітивний вплив, гібридні загрози, міжнародні інституції, інформаційна безпека.*

Постановка проблеми. Повномасштабна агресія росії проти України актуалізувала когнітивний вимір сучасних війн як один із ключових інструментів впливу на політичні рішення, суспільні настрої та міжнародну підтримку. Російська сторона системно використовує дезінформацію, пропаганду та маніпулятивні наративи для підриву стійкості демократичних суспільств, зниження довіри до державних інституцій і ослаблення солідарності Заходу з Україною. У цих умовах протидія когнітивному впливу виходить за межі інформаційної політики і набуває значення складової національної та колективної безпеки. Західні держави та міжнародні партнери відіграють визначальну роль у формуванні комплексної відповіді на ці загрози, поєднуючи політичні рішення, інституційні механізми, аналітичну підтримку, діяльність громадянського суспільства й освітні ініціативи. Водночас наукове осмислення ефективності й узгодженості цих підходів залишається фрагментарним, що зумовлює потребу в системному аналізі ролі Заходу

та міжнародних партнерів у протидії когнітивній агресії російської федерації.

Аналіз останніх досліджень і публікацій засвідчує еволюцію західного науково-аналітичного дискурсу щодо російських інформаційних і когнітивних операцій після 2014 року – від опису окремих пропагандистських інструментів до розуміння дезінформації як складової системної гібридної стратегії російської федерації. Ранні праці зосереджувалися на аналізі наративів і каналів поширення кремлівської пропаганди у Центрально-Східній Європі (Lucas, E. & Pomerantsev, P. 2016), тоді як подальші дослідження акцентували на поєднанні інформаційних впливів із цифровими технологіями, алгоритмічним підсиленням і психологічними механізмами сприйняття (Polyakova, A. 2018).

Вагомий внесок у концептуалізацію когнітивного виміру сучасних конфліктів зробили аналітичні структури НАТО. У публікаціях Allied Command Transformation і NATO StratCom COE когнітивна війна визначається як сфера, де людська свідомість стає ключовим об'єктом і засобом протиборства, а дезінформація розглядається як інтегрований елемент воєнно-політичної стратегії (Cognitive Warfare. n.d.; Fredheim R., *et al.* 2019). Водночас провідні think tanks, зокрема Atlantic Council і Brookings Institution, запропонували рамкові моделі реагування, серед яких концепція «whole-of-society response», що передбачає координацію дій держави, платформ, академічної спільноти та громадянського суспільства (Polyakova, A. & Fried, D. 2019).

Окремий емпіричний блок досліджень присвячений ефективності підвищення стійкості до дезінформації. Матеріали IREX щодо програми Learn to Discern в Україні демонструють довготривалий позитивний ефект медіаосвіти на здатність ідентифікувати маніпуляції, що дає змогу розглядати такі програми як елемент інформаційної безпеки (Learn to Discern. n.d.; Murrock, E., Amulya, J., Druckman, M. & Liubyva, T. 2018). Водночас урядові методичні розробки, зокрема британські інструментарії RESIST, свідчать про прагнення інституціоналізувати контрдезінформаційні практики у форматі процедур і стандартів державного управління (Pamment, J. 2019; 2021).

У цілому, наявна література демонструє високий рівень опрацювання проблематики російських інформаційних і когнітивних операцій, однак, залишається фрагментарною у порівняльному аналізі ролі міжнародних інституцій і національних держав як єдиної системи протидії, а також у дослідженні взаємодії між державними та недержавними механізмами. Саме ці аспекти формують простір для подальшого узагальнення й аналітичного осмислення.

Мета статті полягає в ретроспективному аналізі змісту й організаційно-функціональних механізмів діяльності профільних інституцій провідних західних держав та міжнародних організацій із протидії інформаційно-когнітивному впливу російської федерації у 2014–2025 роках.

Виклад основного матеріалу. Інформаційна агресія російської федерації проти України з 2014 р. та масштабні втручання у виборчі процеси США й держав Європи стали переломним моментом у сприйнятті Заходом когнітивного виміру сучасних конфліктів. Аналітичні оцінки Інституту вивчення війни свідчать, що Кремль інтегрував когнітивну війну як системний елемент власної стратегії, використовуючи дезінформаційні операції для компенсації обмежень традиційної військової сили та підриву суспільної стійкості західних демократій, довіри до інституцій і рамок ухвалення рішень (Do Rego, S. 2025).

Початкові реакції західних держав на ці загрози мали фрагментарний і запізнілий характер. Лише після доведеного російського втручання у президентські вибори у США 2016 р. та серії дезінформаційних кампаній у ЄС проблема була визнана на рівні стратегічного планування, що, за оцінкою А. Полякової та Д. Фріда, означало перехід від пасивного спостереження до активного пошуку інституційних і політичних інструментів протидії (Polyakova, A. & Fried, D. 2019).

Подальший досвід продемонстрував обмеженість суто реактивного підходу, зосередженого на спростуванні окремих фейків. Аналітичні дослідження вказують, що системний когнітивний тиск діє на рівні наративів, емоцій і колективних уявлень, а тому не може бути нейтралізований точковими заходами. Це зумовило переорієнтацію Заходу на проактивні стратегії підвищення суспільної резильєнтності, розвитку критичного мислення та зниження вразливості демократичних інститутів до зовнішнього впливу (Do Rego, S. 2025).

Вагому роль у формуванні проактивного підходу до протидії когнітивним загрозам відіграли наднаціональні безпекові структури. НАТО офіційно визнало когнітивний вимір складовою сучасного воєнно-політичного протиборства, закріпивши у концептуальних документах тезу про людську свідомість як об'єкт й інструмент боротьби. Об'єднане командування з трансформації

координує відповідні дослідницькі та експериментальні програми з акцентом на стратегічні комунікації, міжвідомчу взаємодію та підвищення стійкості суспільств до маніпуляцій (Cognitive Warfare. n.d.).

Водночас західні держави почали переглядати національні політики у цій сфері. Країни Балтії та Північної Європи, спираючись на власний історичний досвід, ще з кінця 2000-х рр. розпочали реалізацію комплексних програм інформаційної безпеки та медіаграмотності, тоді як більшість західноєвропейських держав активізували ці заходи лише після втручання росії у референдуми й виборчі кампанії, зокрема у 2016 році (Polyakova, A. & Fried, D. 2019). До кінця 2010-х рр. у межах ЄС і трансатлантичної спільноти сформувалося спільне бачення російської дезінформації як прямої загрози демократичному устрою, що знайшло відображення в офіційних документах ЄС і у розширенні фінансування програм протидії іноземному інформаційному впливу у США (EU imposes sanctions… 2022; Polyakova, A. & Fried, D. 2019).

Європейський Союз став одним із ключових центрів інституціоналізації протидії дезінформації, перевівши цю проблематику у формат сталих політик і спеціалізованих структур. З 2015 р. у межах Європейської служби зовнішніх дій було створено East StratCom Task Force та запущено платформу EUvsDisinfo, що забезпечує систематичне виявлення й аналіз прокремлівських інформаційних операцій, даючи можливість не лише спростовувати окремі твердження, а й реконструювати архітектуру кампаній впливу та їх спрямованість, зокрема щодо України (The fight against… 2023; Joint Communication to the European Parliament… 2018; Ukraine. n.d.).

Водночас ЄС сформував політико-нормативну рамку протидії дезінформації, поєднавши саморегуляцію цифрових платформ із механізмами кризового реагування та посиленням вимог до прозорості інформаційного середовища. У 2018 р. було ухвалено План дій проти дезінформації, спрямований на нарощування ресурсів стратегічних комунікацій, міждержавну координацію та оперативний обмін інформацією (Joint Communication to the European Parliament… 2018). Після початку повномасштабної агресії рф у 2022 р. ЄС застосував безпрецедентні обмежувальні заходи щодо державних російських медіа, зокрема призупинив мовлення RT і Sputnik, що засвідчило перехід від трактування дезінформації як медійної проблеми до її сприйняття як безпекової загрози, релевантної для санкційної політики та кризового управління (EU imposes sanctions… 2022; Council Regulation… 2022).

У трансатлантичному вимірі ключову роль відіграє НАТО, яке після 2014 р. істотно посилило спроможності у сфері стратегічних комунікацій і протидії гібридним загрозам. Центр передового досвіду НАТО зі стратегічних комунікацій у Ризі став осередком прикладних досліджень, підготовки фахівців і поширення методик нейтралізації інформаційних атак, тоді як Європейський центр протидії гібридним загрозам у Гельсінкі забезпечує координацію підходів ЄС і НАТО до гібридних атак, включно з інформаційними компонентами (About NATO StratCom COE. n.d.; About NATO. n.d.; Hybrid CoE. n.d.). Така мережева модель, що поєднує дослідження, навчання, координацію та політичні рішення, стала характерною рисою західної інституційної відповіді.

На глобальному рівні координацію зусиль підсилює механізм «Великої сімки». Запроваджений після саміту G7 у 2018 р. Механізм швидкого реагування формує мережу національних контактних пунктів для обміну інформацією, узгодження реакцій і вироблення спільних підходів до протидії іноземному втручанню та державній дезінформації. Матеріали уряду Канади підкреслюють орієнтацію цього інструменту на підвищення суспільної стійкості та стримування інформаційних операцій через систематичний моніторинг і регулярні звіти, що формує практику колективної «дипломатії інформаційної безпеки» на ранніх етапах криз (Rapid Response Mechanism Canada detects… 2023).

У США інституційна архітектура протидії дезінформації формувалася через поєднання аналітичних, комунікаційних і міжнародно-медійних інструментів. Важливу роль тривалий час відігравав Центр глобальної взаємодії при Державному департаменті США, орієнтований на викриття іноземних інформаційних операцій, однак, його закриття у 2025 р. засвідчило політичну контроверсійність окремих інструментів інформаційної протидії у демократичних системах (The State Department closes… 2025). Водночас американська модель передбачає використання зовнішньомовних медіа, зокрема мережі Current Time, запущеної у 2017 р. як російськомовного проєкту «Радіо Свобода» і «Голосу Америки», спрямованого на конкуренцію з кремлівським контентом на рівні порядку денного та довіри до джерел (Current Time: the independent… 2017; Current Time TV… n.d.).

На рівні окремих європейських держав застосовуються додаткові національні механізми, які не зводяться до суто «боротьби з фейками». Так, німецький закон NetzDG (2017) орієнтований на оперативне реагування платформ на незаконний контент, а не на загальну модерацію дезінформації, що водночас ілюструє напруження між безпековими міркуваннями та свободою вираження у демократичних режимах (Germany: The Act to Improve… 2017; Clark, L. 2017). Загалом інституційні відповіді Заходу варіюються від стратегічних комунікацій і координації до санкційних і регуляторних інструментів, але об'єднані розумінням російської дезінформації як елементу гібридної агресії, що потребує безпекових механізмів реагування.

Поряд із державними структурами сформувалася потужна екосистема громадянського суспільства, незалежних медіа та аналітичних центрів, перевагою якої є гнучкість, швидкість реагування та технологічна інноваційність. У її межах поширилися практики OSINT, цифрової криміналістики та мережевого аналізу, а спільноти так званих «Digital Sherlocks», інституціоналізовані зокрема у діяльності DFRLab при Atlantic Council, стали важливим інструментом публічного викриття операцій впливу (Polyakova, A. & Fried, D. 2019). Водночас провідні аналітичні рекомендації акцентують не на заміщенні державної політики громадським активізмом, а на його інтеграції через сталі механізми підтримки, обміну даними та регулярної взаємодії, де громадські ініціативи виконують функцію експертного і сенсорного контуру, а держава забезпечує масштабування та легітимацію рішень.

Міжнародна спільнота Bellingcat репрезентує доказовий вимір незалежної протидії когнітивному впливу, використовуючи відтворювані OSINT-методики, засновані на відкритих фото-й відеоджерелах, геолокації, метаданих і мережевих слідах. У справі збиття рейсу MH17 ці підходи дали змогу публічно реконструювати маршрут зенітного комплексу «Бук» і сформувати доказову базу, що стала частиною міжнародних дискусій про відповідальність та приховування злочину (MH17: The Open Source Evidence, 2015; MH17. The Open Source Investigation… 2017; Ostanin, I. 2014). Водночас EUvsDisinfo фіксує системну дискредитацію Bellingcat через наративи про «фабрику фейків», що зміщують фокус із перевірки доказів на делегітимацію джерела, що є типовим прийомом когнітивних операцій, спрямованих на підрив стандартів доказовості й довіри (DISINFO: Bellingcat is a factory… 2021).

Паралельно сформувалася широка екосистема контрдезінформаційних ініціатив на перетині досліджень, журналістики та публічної освіти. DFRLab при Atlantic Council, створена у 2016 р., розвиває практики цифрових розслідувань і глобальну спільноту «Digital Sherlocks», тоді як EU DisinfoLab акумулює експертизу з дезінформації у межах ЄС, поєднуючи аналітичну й прикладну роботу. Водночас окремі ініціативи, як-от Kremlin Watch, були призупинені, що впливає на актуальну інституційну конфігурацію (Polyakova, A. & Fried, D. 2019; Kremlin Watch Program. n.d.). Окремий сегмент становлять волонтерські рухи «суспільної кібероборони», зокрема литовська спільнота «ельфів», які через колективне викриття та взаємодію з платформами підвищують стійкість інформаційного середовища, водночас залишаючись уразливими до контратак і компрометацій (About ELVES. n.d.).

У сукупності ці незалежні та громадянські проєкти виконують структурну функцію, зменшуючи інформаційну асиметрію між державою-агресором і демократичними суспільствами, підвищуючи ймовірність раннього виявлення кампаній впливу та збільшуючи «вартість» дезінформаційних операцій через публічне викриття й доказовість. Їхній внесок полягає не лише у спростуванні окремих фейків, а й у підтриманні стандартів верифікації, збереженні довіри до процедур перевірки та формуванні практик, здатних до подальшої інституціоналізації на державному й міждержавному рівнях.

Довгострокова протидія когнітивному впливу російської федерації виходить за межі блокування окремого контенту, оскільки об'єктом атаки є не повідомлення, а здатність аудиторії до критичного мислення та самостійного судження. У західних підходах чітко розрізняють політику «зменшення пропозиції» дезінформації через модерацію, регуляторні та санкційні інструменти і політику «зменшення попиту», спрямовану на формування стійкості до маніпуляцій за допомогою медіаосвіти, превентивного інформування та підвищення якості інформаційного вибору. Саме цей компонент визнається базовим для резильєнтності, оскільки знижує ефективність операцій впливу навіть за неможливості швидкого видалення контенту.

Емпіричним підтвердженням ефективності такого підходу стали результати програми Learn to Discern в Україні, реалізованої IREX у 2015–

2016 рр., де учасники продемонстрували стійке покращення здатності ідентифікувати дезінформацію, зокрема зростання показників на 13 % порівняно з контрольною групою навіть через півтора роки після навчання (Learn to Discern. n.d.; Murrock, E., *et al.* 2018). Цей кейс засвідчив, що медіаосвіта може розглядатися як елемент національної й колективної інформаційної безпеки, а не як допоміжна гуманітарна практика.

Урядові комунікаційні стратегії дедалі частіше поєднують освітні компоненти з інституційними алгоритмами реагування. Британський інструментарій RESIST і його оновлена версія RESIST 2 подаються як процедурні, доказово орієнтовані рамки для виявлення й нейтралізації дезінформації, придатні для інтеграції у роботу державних інституцій та публічних комунікацій (Pamment, J. 2019; 2021). Доповненням до цього підходу є публічні кампанії у форматі «фейк – факт», зокрема практика уряду Канади щодо перевірки заяв російського режиму у контексті війни проти України, що одночасно виконує інформаційну й освітню функції та формує стандарти верифікації як звичну модель поведінки (Countering disinformation with facts… 2025).

Важливим елементом підвищення стійкості є превентивна комунікація, спрямована на попередження аудиторії про типові прийоми маніпуляції до їх масового поширення. У західній практиці це описується як pre-bunking на відміну від реактивного de-bunking, зі спільною стратегічною метою – знизити первинний ефект дезінформації у перші години після появи інформації, коли альтернативні інтерпретації ще не закріпилися в масовому сприйнятті. У ширшому вимірі стійкість аудиторії передбачає не лише спростування неправдивих тверджень, а й формування переконливих контрнаративів і позитивного порядку денного, що зменшує привабливість пропагандистських пояснень і усуває соціальні умови їх поширення, зокрема дефіцит довіри, поляризацію та інформаційну втому (Pamment, J. & Smith, V. 2022).

Істотний внесок у протидію когнітивному впливу рф забезпечили західні аналітичні центри, що відіграли ключову роль у концептуалізації російської інформаційної та когнітивної війни. У середині 2010-х рр. з'явилися дослідження, що системно описували архітектуру кремлівської пропаганди та її адаптацію до цифрового середовища, зокрема через поєднання традиційних дезінформаційних інструментів із алгоритмічним посиленням впливу (Lucas, E. & Pomerantsev, P. 2016; Polyakova, A. 2018). Важливу роль у формуванні цілісного підходу відіграв Atlantic Council, який у серії звітів «Democratic Defense Against Disinformation» розвинув концепцію «whole-of-society response», зафіксувавши поступову інституціоналізацію запропонованих механізмів у ЄС та США, водночас наголошуючи на необхідності переходу від реагування на окремі атаки до довгострокового підвищення соціальної стійкості, прозорості та довіри як системних запобіжників когнітивного впливу (Polyakova, A. & Fried, D. 2019).

Аналітичну складову протидії дезінформації посилили європейські інституції, які почали замовляти цільові дослідження та інтегрувати їх результати у політичне планування. Зокрема, Європейський парламент у 2021 р. ініціював спеціальний звіт про інформаційні впливи на Західних Балканах, що засвідчило прагнення ЄС екстраполювати напрацьовані підходи за межі власного простору. Паралельно HATO StratCom COE систематично публікує аналітичні збірники з інформаційної безпеки, де аналіз російських операцій впливу поєднано з дослідженням ролі алгоритмів соціальних мереж і психологічних механізмів сприйняття, а результати використовуються у навчанні, підготовці кадрів і доктринальних документах Альянсу (Fredheim R., *et al.* 2019).

Окремий аналітичний напрям сформувала RAND Corporation, яка описала російську стратегію «firehose of falsehood» як системний інструмент розмивання правди та запропонувала модель стратегічних комунікацій, що поєднує пріоритет достовірних фактів, оперативність і проактивне викриття маніпуляцій, переводячи проблему дезінформації у площину стратегічного планування та безпекової політики (Kelley, M. J. 2024). Важливим доповненням стала координація експертних зусиль у межах Механізму швидкого реагування G7, що забезпечує сталі канали співпраці з аналітичними центрами та університетами, а також регулярні форуми й конференції як простір формування спільної експертної мови (Rapid Response Mechanism… n.d.).

Особливе місце посіла співпраця з глобальними технологічними компаніями. Після 2016 р. великі платформи активізували взаємодію з урядами та неурядовими організаціями, надаючи дані для аналізу координованої неавтентичної поведінки та регулярно звітуючи про виконання Кодексу практик з дезінформації, що сприяло маркуванню державних медіа і блокуванню пропагандистських каналів (Polyakova, A. & Fried, D.

2019). У глобальному вимірі до цих зусиль долучилися Австралія й Нова Зеландія, тоді як ініціативи ООН залишилися переважно декларативними через інституційні обмеження, унаслідок чого основний тягар протидії російській дезінформації зберігся за коаліцією демократичних держав і регіональних партнерств.

Висновок. Проведений аналіз засвідчив, що протидія когнітивному впливу російської федерації з боку Заходу та міжнародних партнерів набула системного характеру і стала важливою складовою сучасної архітектури безпеки демократичних держав. Перехід від фрагментарних і реактивних заходів до інституціоналізованої моделі, що поєднує політичні рішення, санкційні інструменти, стратегічні комунікації, аналітичну підтримку, діяльність громадянського суспільства та освітні програми, дав змогу істотно підвищити стійкість інформаційного простору і збільшити вартість ведення когнітивної війни для росії. Водночас ефективність цієї моделі залежить від здатності адаптуватися до нових технологічних викликів, зокрема поширення синтетичних медіа та автоматизованих маніпулятивних інструментів. Скоординовані дії ЄС, НАТО, «Великої сімки» та окремих держав поступово звужують простір впливу російських дезінформаційних операцій і формують більш стійке середовище для демократичних суспільств, що має особливе значення для України як держави, котра перебуває на передовій когнітивного протиборства.

REFERENCES

About ELVES. (n.d.). URL: https://debunk.org/about-elves [Accessed: 23.12.2025]. [in English].

About NATO StratCom COE. (n.d.). URL: https://tinyurl.com/52jjcruw [Accessed: 21.12.2025] [in English].

Clark, L. (2017). Facebook and Twitter face €50m fines if they don't tackle hate speech. URL: https://tinyurl.com/4bet63bx [Accessed: 21.12.2025]. [in English].

Cognitive Warfare. (n.d.). URL: https://www.act.nato.int/activities/cognitive-warfare/ [Accessed: 23.12.2025]. [in English].

Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. (2022). *Official Journal of the European Union*. URL: https://tinyurl.com/yjfr7uv2 [Accessed: 21.12.2025]. [in English].

Countering disinformation with facts – Russian invasion of Ukraine. (2025). URL: https://tinyurl.com/yckx7rb8 [Accessed: 23.12.2025]. [in English].

Current Time TV. About Current Time TV. (n.d.). URL: https://www.currenttime.tv/p/6018.html [Accessed: 21.12.2025]. [in English].

Current Time: the independent Russian-language news network. (2017). URL: https://tinyurl.com/4x583yf8 [Accessed: 21.12.2025]. [in English].

DISINFO: Bellingcat is a factory of fakes used for an information war against Russia. (2021). URL: https://tinyurl.com/3ku3fsd9 [Accessed: 23.12.2025]. [in English].

Do Rego, S. (2025). Is Israeli maritime nuclear supremacy a challenge to Iranian influence in the Eastern Mediterranean? URL: https://tinyurl.com/3mtf92wx [Accessed: 21.12.2025]. [in English].

EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU. (2022). URL: https://tinyurl.com/2sr4vdzj [Accessed: 21.12.2025]. [in English].

Fredheim, R., Bay, S., Dek, A., Biteniece, N., *et al.* (2019). Responding to cognitive security challenges. Riga : *NATO Strategic Communications Centre of Excellence*. 101 p. URL: https://tinyurl.com/485f99km [Accessed: 23.12.2025]. [in English].

Germany: The Act to Improve Enforcement of the Law in Social Networks. (2017). URL: https://tinyurl.com/ynzcm8be [Accessed: 21.12.2025]. [in English].

Hybrid CoE. (n.d.). URL: https://www.hybridcoe.fi/ [Accessed: 23.12.2025]. [in English].

Joint Communication to the European Parliament, the European Council, the Council, the European economic and Social Committee and the Committee of the Regions. Action Plan against Disinformation. (2018). Brussels, 5 December. JOIN(2018) 36 final. URL: https://tinyurl.com/ynevd8rc [Accessed: 21.12.2025]. [in English].

Kelley, M. J. (2024). Understanding Russian disinformation and how the joint force can address it. URL: https://tinyurl.com/mtejam4t [Accessed: 23.12.2025]. [in English].

Kremlin Watch Program. (n.d.). URL: https://tinyurl.com/ycyzn649 [Accessed: 23.12.2025]. [in English].

Learn to Discern. (n.d.). URL: https://tinyurl.com/4zmdvptu [Accessed: 23.12.2025]. [in English].

Lucas, E. & Pomerantsev, P. (2016). Winning the information war: Techniques and counter-strategies to Russian propaganda in Central and Eastern Europe. URL: https://tinyurl.com/ybcr5yyf [Accessed: 23.12.2025]. [in English].

MH17. The Open Source Investigation, Three Years Later. (2017). URL: https://tinyurl.com/yck7fcmx [Accessed: 23.12.2025]. [in English].

MH17: The Open Source Evidence. (2015). URL: https://tinyurl.com/yh37wpn4 [Accessed: 23.12.2025]. [in English].

Murrock, E., Amulya, J., Druckman, M. & Liubyva, T. (2018). Winning the war on state-sponsored propaganda: Gains in the ability to detect disinformation a year and a half after completing a Ukrainian news media literacy program. URL: https://tinyurl.com/4zp9sefk [Accessed: 23.12.2025]. [in English].

Ostanin, I. (2014). Images show the Buk that downed Flight MH17, inside Russia, controlled by Russian troops. URL: https://tinyurl.com/2wepvr4f [Accessed: 23.12.2025]. [in English].

Pamment, J. & Smith, V. (2022). Attributing information influence operations. Identifying those responsible for malicious behaviour online. URL: https://tinyurl.com/3hepfdpz [Accessed: 23.12.2025]. [in English].

Pamment, J. (2019). RESIST: Counter-disinformation toolkit. URL: https://tinyurl.com/3trm3yf5 [Accessed: 23.12.2025]. [in English].

Pamment, J. (2021). RESIST 2: Counter-disinformation toolkit. URL: https://tinyurl.com/3vyf7px4 [Accessed: 23.12.2025]. [in English].

Polyakova, A. & Fried, D. (2019). Democratic defense against disinformation 2.0. URL: https://tinyurl.com/crrbzyhx [Accessed: 23.12.2025]. [in English].

Polyakova, A. (2018). Weapons of the weak: Russia and AI-driven asymmetric warfare. URL: https://tinyurl.com/6c7h9c4m [Accessed: 23.12.2025]. [in English].

Rapid Response Mechanism Canada detects information operation targeting member of Parliament. (2023). URL: https://tinyurl.com/98majuvt [Accessed: 21.12.2025]. [in English].

Rapid Response Mechanism: Global Affairs Canada. (n.d.). URL: https://tinyurl.com/2ttx828x [Accessed: 23.12.2025]. [in English].

The fight against pro-Kremlin disinformation. (2023). URL: https://tinyurl.com/ycyr6xy2 [Accessed: 23.12.2025]. [in English].

The State Department closes the office that flags disinformation from Russia, China and Iran. (2025). URL: https://tinyurl.com/yc7reexz [Accessed: 21.12.2025]. [in English].

Ukraine. (n.d.). URL: https://euvsdisinfo.eu/ukraine/ [Accessed: 21.12.2025]. [in English].

Vadym BESPEKA
PhD in History
Hetman Petro Sahaidachnyi National Army Academy
(Lviv, Ukraine)
ORCID: https://orcid.org/0000-0002-3811-341X

RETROSPECTIVE ANALYSIS OF THE ACTIVITIES OF WESTERN STATES AND INTERNATIONAL ORGANIZATIONS IN COUNTERING THE COGNITIVE INFLUENCE OF THE RUSSIAN FEDERATION (2014–2025)

This article analyzes the role of Western states and international institutions in developing a comprehensive response to the cognitive influence of the Russian Federation within the context of contemporary hybrid warfare. Russian cognitive operations are conceptualized as a systemic instrument of influence aimed at shaping perceptions, manipulating political decision-making processes, and undermining the social cohesion of democratic societies. Based on an examination of analytical reports, policy documents, and institutional practices of the European Union, NATO, the Group of Seven (G7), and selected states, the study assesses the evolution of Western approaches from fragmented and predominantly reactive measures toward an institutionalized, multi-level, and coordinated framework of counteraction.

The article traces the development of political, regulatory, and communicative instruments, including sanctions against state-controlled propaganda outlets, the establishment and refinement of strategic

communication frameworks, the strengthening of inter-institutional coordination, and enhanced cooperation with digital platforms. Particular attention is devoted to the role of international institutions as hubs for the consolidation of knowledge, normative frameworks, and operational practices in countering disinformation, as well as to the contribution of think tanks and transnational expert networks to the conceptualization of whole-of-society response strategies. The significance of civil society initiatives, independent media, fact-checking organizations, and OSINT communities in the early detection and public exposure of influence operations is also highlighted, as these actors contribute to increased transparency in the information environment and raise the operational costs for states conducting cognitive campaigns.

The article further emphasizes that the long-term effectiveness of countering cognitive influence depends on the integration of regulatory, analytical, educational, and communicative instruments, as well as on the capacity of Western states and international organizations to adapt to emerging technological challenges, including the proliferation of synthetic media and automated manipulative systems. It concludes that coordinated Western efforts are gradually constraining the effectiveness of Russian disinformation operations and fostering a more resilient information environment, which is of particular relevance for Ukraine as a frontline state in the domain of cognitive confrontation.

Keywords: *cognitive warfare, disinformation, cognitive influence, hybrid threats, international institutions, information security.*

Стаття надійшла 25.12.2025
Стаття прийнята до друку 23.01.2026