The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Received: *June 3, 2026*| **Revisions Requested:** - | **Revision Received:** -
Accepted: *July 27, 2026* | **Published Online:** *August 5, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.2.28

Щодо розвитку системи когнітивного впливу російської федерації та особливостей її застосування у війні проти України

Олександр Кінь
кандидат технічних наук, доцент
Дипломатична академія України імені Геннадія Удовенка
при Міністерстві закордонних справ
01001, м. Київ, вул. Велика Житомирська, 2
e-mail: cubalibre1972@ukr.net
ORCID: 0009-0001-2196-7515

Лілія Семененко
старший викладач кафедри іноземних мов
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: selin-ua@ukr.net
ORCID ID: 0000-0002-5628-3586

Олег Нечаєв
перший заступник командувача
Сили спеціальних операцій ЗС України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: o26811650@gmail.com
ORCID: 0009-0001-2839-2830

Олег Темний
ад'юнкт кафедри
інформаційної боротьби інституту стратегічних комунікацій
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: o.temnyi@edu.nuou.org.ua
ORCID: 0009-0009-3173-094X

Олександр Гудков
Начальник навчально-лабораторного комплексу
кафедра військової підготовки
Державного університету
"Київський авіаційний інститут"
e-mail: alex19720914@gmail.com
ORCID: 0009-0002-6468-3261

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Анотація. Сучасні збройні конфлікти дедалі більше зміщуються зі сфери фізичного протиборства у сферу людської свідомості, а російська федерація однією з перших серед держав пострадянського простору перетворила когнітивний вплив на окремий, інституційно оформлений напрям воєнної діяльності. У статті здійснено комплексний аналіз розвитку, інструментарію та інституціоналізації російської системи когнітивного впливу, а також особливостей її застосування у війні проти України. Простежено періодизацію становлення системи від латентного етапу (спадщина радянських "активних заходів" і теорія рефлексивного управління) до тотального етапу широкомасштабного вторгнення, коли когнітивні операції набули глобального характеру з інтеграцією штучного інтелекту, дипфейків і ботоферм. Розкрито доктринальні засади російського підходу, у якому воєнна доктрина не розмежовує кібератаки та пропаганду, трактуючи їх як єдиний простір "інформаційного протиборства", а свідомість противника визначається як головна ціль впливу. Реконструйовано ймовірну структуру та систему управління спеціальних Військ інформаційних операцій, офіційно визнаних у 2017 році, показано центральну роль структур Головного управління Генштабу, зокрема військової частини № 54777 та мережі регіональних і кіберпідрозділів, а також розмежування зовнішнього (війська інформаційних операцій) і внутрішнього (Головне військово-політичне управління, 2018) контурів. Проаналізовано сучасні кампанії проти України, зокрема операцію клонування медіа "Doppelgänger (Двійник)" та "точкову пропаганду", і показано, що відносно успішна когнітивна операція 2014 року в Криму контрастує з переважною невдачею російської моделі на міжнародному рівні у 2022 році. Основним результатом статті є обґрунтування висновку про те, що росія сформувала цілісну, централізовано керовану систему когнітивного впливу, ядром якої є структури воєнної розвідки, а отже Україна зобов'язана сформувати симетричну, а точніше асиметрично-адекватну відповідь, що ґрунтується на демократичній моделі когнітивної стійкості, основою якої є правда, прозорість і довіра. Матеріали статті можуть бути корисними для військових, аналітиків, фахівців із безпеки, науковців і стратегів, які займаються захистом інформаційного й когнітивного простору держави. Перспективними напрямами подальших досліджень є розроблення доктрини когнітивної безпеки України, формування повноцінних сил інформаційних і когнітивних операцій та створення технологічних систем раннього виявлення ворожих наративів і дипфейків.

Ключові слова: когнітивний вплив, когнітивна війна, інформаційне протиборство, рефлексивне управління, Війська інформаційних операцій, Головне управління Генштабу, доктрина герасимова, дезінформація, дипфейки, кампанія Doppelgänger, психологічні операції, стратегічні комунікації, національна безпека, російсько-українська війна, когнітивна стійкість, симетрична відповідь.

Вступ (Introduction)

Сучасні збройні конфлікти дедалі більше зміщуються зі сфери фізичного протиборства у сферу людської свідомості. російська федерація однією з перших серед держав пострадянського простору перетворила когнітивний вплив на окремий, інституційно оформлений напрям воєнної діяльності, поєднавши спадщину радянських спецслужб, напрацювання військової науки та сучасні цифрові технології.

Принципова особливість російського підходу полягає в тому, що воєнна доктрина не розмежовує кібератаки та пропаганду, трактуючи їх як єдиний простір "інформаційного протиборства". Для російського керівництва свідомість людей за кордоном фактично коштує дорожче, ніж життя власних солдатів, а інвестиції у формування свідомості сягають, за різними оцінками, 5–10% валового внутрішнього продукту [1, 2].

Актуальність дослідження зумовлена тим, що Україна є основним полігоном і

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

пріоритетною ціллю російського когнітивного впливу. Наративи про штучність української державності та розкол суспільства, що цілеспрямовано насаджувалися ще з 2004 року, стали підґрунтям гібридної операції 2014 року та широкомасштабного вторгнення 2022 року [3, 4].

Для держави, яка веде паралельну "війну за свідомість" власної нації та партнерів, програш у цій сфері означав би стратегічну поразку навіть за умови утримання лінії фронту. Відтак розуміння того, як саме побудована, як розвивалася й застосовується російська система когнітивного впливу, є необхідною передумовою формування ефективної національної системи протидії когнітивним загрозам.

Метою статті є комплексний аналіз розвитку, інструментарію та інституціоналізації системи когнітивного впливу російської федерації, а також особливостей її застосування у війні проти України. Для досягнення цієї мети у статті: простежено, коли і як москва активізувала розбудову системи когнітивного впливу; розкрито доктринальний і організаційний інструментарій впливу; реконструйовано історію створення та трансформації спеціальних військ інформаційних операцій і ймовірну систему управління ними; проаналізовано сучасні кампанії проти України; а також сформульовано висновки й рекомендації щодо симетричної відповіді України.

Матеріали та методи (Materials and Methods)

Методологічну основу дослідження становить аналіз відкритих джерел (OSINT), офіційних стратегічних і доктринальних документів російської федерації, а також аналітичних і наукових праць провідних західних дослідницьких центрів. Серед опрацьованих джерел – це російські воєнна доктрина та доктрина інформаційної безпеки, відповідні укази президента рф, публічні заяви воєнно-політичного керівництва, а також дослідження Оборонного коледжу НАТО, лабораторії цифрових досліджень Атлантичної ради (DFRLab), Інституту вивчення війни (ISW), корпорації RAND і публікації у фахових виданнях (MCU Journal, Frontiers in Artificial Intelligence, War on the Rocks) [1]–[16].

Дослідження побудоване на поєднанні кількох методів. Історико-генетичний метод застосовано для періодизації розвитку системи когнітивного впливу та виокремлення якісно відмінних етапів її становлення. Інституційний та структурно-функціональний аналіз використано для реконструкції ймовірного складу системи, розмежування зовнішнього і внутрішнього контурів та визначення ролі окремих органів управління. Порівняльний метод дав змогу зіставити російське й західне розуміння "інформаційних операцій" і показати специфіку російської концепції рефлексивного управління. Метод аналізу окремих кейсів застосовано до операції у Криму (2014), широкомасштабного вторгнення (2022) та кампанії "Doppelgänger (Двійник)".

Окремо наголосимо на обмеженнях емпіричної бази. Документи, що безпосередньо регламентують діяльність спеціальних військ інформаційних операцій (положення, штати, накази), мають гриф таємності й у відкритому доступі відсутні. Тому будь-яка реконструкція чисельності, складу та командування цих структур має оцінковий характер і ґрунтується на перехресному зіставленні відкритих джерел; саме так слід сприймати наведені нижче схеми організаційної будови.

Результати і обговорення (Results and Discussions)

Витоки сучасної російської системи когнітивного впливу сягають радянської практики "активних заходів" та теорії "рефлексивного управління" – управління противником шляхом передавання йому спеціально підготовленої інформації, що спонукає його добровільно ухвалити заздалегідь визначене рішення [1]. Саме ця концепція становить когнітивне ядро російського інформаційного протиборства й відрізняє російський підхід від західного: під "інформаційними операціями" москва розуміє весь спектр дій з інформацією – пропаганду,

The Central Research institute
of the Armed Forces of Ukraine
ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

дезінформацію, психологічні та кібероперації водночас [2].

Перехід від концептуальної спадщини до системного застосування датується серединою 2000-х років. Помаранчеву революцію 2004 року кремль сприйняв як організовану Заходом "кольорову революцію", після чого почалося цілеспрямоване насадження наративів про "розкол" України та її "зовнішнє керування" [3]. Кібератаки на Естонію (2007) і війна проти Грузії (2008) стали першим випадком, коли росія поєднала кінетичні дії, кібератаки та когнітивний вплив у межах єдиної кампанії, формуючи в реальному часі вигідну їй "картину подій" для західних аудиторій [4].

Кульмінацією стала анексія Криму та збройна агресія на Донбасі у 2014 році: операція "зелених чоловічків" супроводжувалася запереченням російської присутності й масштабною дезінформацією. Водночас 2014 рік став переломним і для самої росії – різке погіршення міжнародного іміджу та посилення санкцій спонукали москву інституціоналізувати когнітивний вплив. Послідовність етапів цього процесу узагальнено на рис. 1 та в табл. 1.

Доктринальні засади російської когнітивної агресії визначені передусім так званою "доктриною герасимова" (стаття "Цінність науки у передбаченні", 2013), у якій межа між війною і миром фактично стирається, а свідомість противника прямо визначається як головна ціль впливу. Другим теоретичним стрижнем є радянсько-російська теорія рефлексивного управління – мистецтво передавати противнику спеціально підготовлену інформацію, щоб схилити його добровільно ухвалити рішення, вигідне керуючій стороні.

російські автори розглядають когнітивні та інформаційні операції як спосіб паралічу нації без формального оголошення війни, що дозволяє трактувати російсько-українську війну не як відхилення, а як реалізацію довготривалої стратегії, спрямованої на руйнування української ідентичності та підміну історичної пам'яті.



Рисунок 1. Хронологія розвитку системи когнітивного впливу російської федерації

Систему когнітивного впливу російської федерації доцільно розглядати на трьох рівнях. Доктринально-концептуальний рівень формують категорії "інформаційного протиборства" та рефлексивного управління; показовою є теза начальника Генштабу в. герасимова про співвідношення невоєнних і воєнних засобів у сучасних конфліктах як 4 до 1, що відображає пріоритет нематеріальних методів [5]. Інституційний рівень представлений державним медіаконгломератом (телеканалом RT), агентствами Sputnik і ТАСС, що формують партнерства із закордонними ЗМІ, а також мережею "фабрик тролів", насамперед "Агентством інтернет-досліджень", яке масштабує штучні наративи у соціальних мережах [6]. Операційний рівень охоплює "наративну війну" – конструювання тривких сюжетів, які передують воєнним

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

діям і легітимізують їх, а також спеціальні прийоми на кшталт наративів ядерної ескалації; як зафіксували аналітики, нагнітання загрози застосування тактичної ядерної зброї та її розміщення в білорусі у 2022–2023 роках мало насамперед когнітивну мету – вплинути на сприйняття Заходу й відтермінувати постачання Україні важкого озброєння [7].

Таблиця 1. Етапи розвитку системи когнітивного впливу російської федерації

Етап	Період	Ключові події та зміст	Характер впливу
Латентний (спадщина)	до 2004	Радянські "активні заходи", теорія рефлексивного управління, дезінформаційні практики спецслужб	Концептуально-підготовчий
Пробний	2004–2008	Помаранчева революція; кібератаки на Естонію (2007); війна в Грузії (2008) – перше поєднання кінетики, кібер- і когнітивних дій	Регіональний, тестування
Гібридний	2014–2016	Анексія Криму та агресія на Донбасі; "зелені чоловічки"; масштабна дезінформація; кодифікація у Доктрині інформаційної безпеки (2016)	Стратегічний, гібридний
Інституційний	2017–2021	Офіційне визнання Військ інформаційних операцій (2017); створення ГВПУ (2018); розбудова глобального медіаконгломерату	Системний, інституціоналізація
Тотальний	2022 –	Широкомасштабне вторгнення; глобальні когнітивні операції; інтеграція штучного інтелекту, дипфейків і ботоферм	Глобальний, тотальний

Кульмінацією інституціоналізації стало офіційне визнання спеціальних військ. 22 лютого 2017 року, виступаючи у державній думі, міністр оборони рф сергій шойгу уперше публічно підтвердив створення у складі збройних сил Військ інформаційних операцій, зазначивши, що ці війська значно ефективніші за радянську контрпропаганду [8]. Саме "Війська (сили) інформаційних операцій" (ВІО) є коректною назвою цього формування за відкритими джерелами; поширене у пресі найменування "кібервійська" є неточним, оскільки звужує їхню функцію до кіберпростору. Ініціатором створення структури був не лише особисто шойгу: ідею окремого кіберкомандування ще у 2012 році публічно обстоював віцепрем'єр дмитро рогозін, 14 січня 2014 року шойгу підписав наказ про формування у складі Генштабу кібернетичного командування, а доктринальним архітектором усієї системи виступає начальник Генерального штабу в. герасимов (на посаді з 2012 року). Прикметно, що до офіційного визнання у 2017 році ці підрозділи, за оцінками західних дослідників, діяли вже близько чотирьох років, тобто приблизно з 2013 року [9].

Фактично йдеться не про окремий підрозділ, а про гібридну екосистему, що охоплює органи військового управління, розвідку (Міноборони, ГРУ, ФСБ, СЗР), приватні мережі, тролінгові центри та засоби масової інформації. Провідну роль у цій системі відіграє Управління інформаційних операцій Головного управління Генштабу (ГРУ), яке поєднує психологічні операції, радіоелектронні та кіберспроможності. Головна мета ВІО – досягнення переваги в інформаційному просторі шляхом цілеспрямованого впливу на свідомість населення інших держав; хоча офіційна риторика 2017 року свідомо подавала ці війська у вузькому, оборонно-кіберному ключі, фактичний обсяг їхніх завдань, за західними оцінками, значно ширший і передбачає психологічні операції, дезінформацію та рефлексивне управління [10]. До основних завдань ВІО належать: моніторинг і формування інформаційного простору противника; проведення психологічних та інформаційно-психологічних операцій; кіберзахист і кібервплив; розроблення та поширення наративів через медіа й мережеві ресурси; інформаційно-психологічне забезпечення воєнних операцій. Найвищий ступінь таємності цих

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

військ зумовлений тим, що ефективність когнітивних операцій критично залежить від прихованості джерела впливу: режим секретності забезпечується через 8-ме управління Генштабу (Службу захисту державної таємниці) [11].

Становлення ВІО доцільно розглядати як еволюцію, від радянського Управління контрпропаганди Головного політичного управління (ГлавПУР) до сучасних мультидоменних когнітивних операцій. Узагальнено цю трансформацію подано на рис. 2. Як показано у нижній частині рисунка, ключові зрушення охоплюють чотири напрями: від реактивного спростування ворожих тез – до випереджального конструювання вигідної "реальності"; від орієнтації на внутрішню аудиторію – до цілеспрямованого впливу на свідомість іноземних суспільств; від вузької "контрпропаганди" – до мультидоменних операцій, що поєднують кібердії та психологічний вплив; від ручних методів – до технологічних, із застосуванням штучного інтелекту, дипфейків і масштабних ботоферм, що особливо проявилося після 2022 року. Документи, що безпосередньо регламентують діяльність ВІО, мають гриф таємності й у відкритому доступі відсутні. Водночас доктринальні засади російського когнітивного впливу закріплені у низці відкритих стратегічних документів, наведених у табл. 2. Їхній спільний зміст – визнання інформаційно-психологічної сфери простором протиборства, у якому росія прагне досягти переваги та утримувати контроль над "картиною світу" як власного, так і закордонного населення. Базовим документом стратегічного планування у цій сфері є Доктрина інформаційної безпеки 2016 року (затверджена Указом президента рф № 646 від 5 грудня 2016 року), яка вводить категорію "національних інтересів в інформаційній сфері" та обґрунтовує курс на сегментований контроль національного сегмента інтернету [12].



Рисунок 2. Трансформація системи когнітивного впливу: від контрпропаганди до когнітивних операцій

З огляду на режим секретності, склад і командування ВІО реконструюються за відкритими джерелами лише оцінково. Найімовірніше, формування підпорядковане Генеральному штабу через профільні управління й тісно взаємодіє з воєнною розвідкою. Узагальнену реконструкцію подано на рис. 3 та в табл. 3. При цьому важливо розрізняти два контури. ВІО (2017) орієнтовані переважно назовні – на свідомість іноземних аудиторій. Натомість Головне військово-політичне управління (ГВПУ), засноване указом президента рф 30 липня 2018 року й очолене першим начальником андрієм картаполовим, відповідає за внутрішній контур – військово-патріотичну та морально-психологічну роботу з власним населенням; його створення офіційно мотивувалося загостренням "інформаційної війни проти росії" [13].

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Таблиця 2. Відкриті документи, що формують доктринальну основу когнітивного впливу російської федерації

Документ	Рік	Основний зміст щодо когнітивного впливу
Воєнна доктрина рф (нові редакції)	2010, 2014	Уперше закріплює "інформаційне протиборство" як складову сучасних конфліктів та умову досягнення цілей
"Концептуальні погляди на діяльність зс рф в інформаційному просторі"	2011	Визначає воєнну інформаційну діяльність як "досягнення переваги в інформаційному просторі"
Стратегія національної безпеки рф (Указ № 683)	2015	Трактує інформаційний вплив Заходу як загрозу та обґрунтовує необхідність активної відповіді
Доктрина інформаційної безпеки рф (Указ президента № 646)	2016	Система офіційних поглядів; уводить "національні інтереси в інформаційній сфері", курс на сегментований контроль інтернету
Концепція зовнішньої політики рф	2016	Серед пріоритетів – "зміцнення позицій російських ЗМІ у глобальному інформаційному просторі"



Рисунок 3. Ймовірне місце Військ інформаційних операцій у системі управління збройних сил рф (складено за відкритими джерелами; точна структура засекречена, нижній рівень — оцінкова реконструкція)

За даними розвідки, центральним елементом психологічних операцій є військова частина № 54777 (72-й центр спеціальної служби, відомий також як Служба іноземної інформації та комунікацій). Підрозділ бере початок від радянського Управління спеціальної пропаганди ГоловПУ, на початку 1990-х був переданий до ГРУ й отримав номер № 54777 у 1994 році, після чого перейшов від періодичних оборонних повідомлень до доктрини постійного психологічного впливу, що охоплює операції проти України, США, Сирії та інших напрямів. Підрозділ діє через мережу організацій-прикриттів (зокрема InfoRos та Інститут російської

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

діаспори), а крім класичних психологічних операцій, володіє можливостями радіотехнічної розвідки та кібероперацій. Поряд із ним діє розгалужена мережа регіональних підрозділів інформаційно-психологічних операцій (у джерелах фігурують в/ч № 03126, № 03127, № 03128, № 03132, № 03134, № 03138 у москві, санкт-петербурзі, курську, єкатеринбурзі, хабаровську та інших містах), а також кіберпідрозділи ГРУ, відомі за класифікацією загроз: в/ч № 26165 (APT28), в/ч № 74455 (Sandworm) та в/ч № 29155 (Ember Bear); імовірний штабний рівень управління пов'язують із в/ч № 55111. Узагальнену структуру системи когнітивного впливу рф наведено на рис. 4.

Таблиця 3. Ймовірний склад і система управління ВІО російської федерації

Елемент	Ймовірна функція
Орган підпорядкування	Генеральний штаб зс рф через профільні управління
Доктринальне керівництво	Начальник Генштабу (в. герасимов, на посаді з 2012 р.)
Розвідувально-операційна складова	Головне управління ГШ (ГУ/ГРУ) – розвідка, психологічні та кібероперації
Режим секретності	8-ме управління ГШ – Служба захисту державної таємниці
Кіберпідрозділи	Захист військових мереж та активні дії у кіберпросторі
Підрозділи ПсО / ІПсО	Психологічні та інформаційно-психологічні операції проти зовнішніх аудиторій
Аналітично-лінгвістичні центри	Профілювання аудиторій, розроблення та адаптація наративів
Медіа- та мережеві оператори	Поширення контенту, керування ботофермами й тролями
Внутрішній контур (окремий орган)	Головне військово-політичне управління (ГВПУ, з 2018 р.) – морально-політична робота з власним населенням

Найбільш масштабним прикладом сучасної російської когнітивної операції є кампанія "Doppelgänger" (нім. "двійник"), у межах якої з 2022 року створюються клони вебсайтів авторитетних західних і українських видань для поширення підробленого контенту. Розслідування пов'язали кампанію з підсанкційними структурами – агентством Social Design Agency та компанією National Technologies (кінцевим власником якої є державна корпорація "Ростех"), а також з офіцерами психологічного підрозділу ГРУ (в/ч 54777) [6]. На тактичному рівні росія застосовує так звану "точкову пропаганду" – розсилання військовослужбовцям ЗС України текстових повідомлень, спрямованих на підрив згуртованості підрозділів і бойового духу, синхронізованих з артилерійськими ударами для посилення психологічного ефекту. Це засвідчує, що росія розглядає інформаційні операції як невіддільну складову загальновійськових дій. Отже, до ключових інструментів російської системи когнітивного впливу належать: масована дезінформація; ШІ-генерований контент і "deepfake"; клонування медіа ("Doppelgänger"); рефлексивне управління; синхронізація інформаційних, кібер- та радіоелектронних дій у єдиному контурі; використання мережі проксі-медіа (RT, Sputnik, InfoRos) і ботмереж.

Україна є основним полігоном і пріоритетною ціллю російського когнітивного впливу. Характерно, що у 2014 році російська когнітивна операція в Криму була відносно успішною: миттєве заперечення причетності російських військ дезорієнтувало міжнародну спільноту під час "референдуму". Натомість у 2022 році ця модель здебільшого зазнала невдачі на міжнародному рівні: рішення Президента В. Зеленського залишитися в Києві, єдність

The Central Research institute
of the Armed Forces of Ukraine
ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

українського суспільства, ефективна стратегічна комунікація та "стратегічне розсекречення" розвідданих США напередодні вторгнення підірвали легітимність російських наративів [15]. Після 2022 року кремль змістив акцент на ерозію спроможності України чинити опір та на підрив довіри партнерів через фабрикації про "біолабораторії", "поразки" ЗС України й нагнітання страху ескалації, а на окупованих територіях – через захоплення місцевих телеканалів і зміну шкільних програм [16]. Показово й те, що, зосередивши основні зусилля на українському напрямі, росія водночас втратила можливості ефективного когнітивного реагування на інші регіональні події, що свідчить про обмеженість навіть великих держав у разі стратегічних помилок. Узагальнені напрями симетричної відповіді України, які випливають із проведеного аналізу, подано в табл. 4.

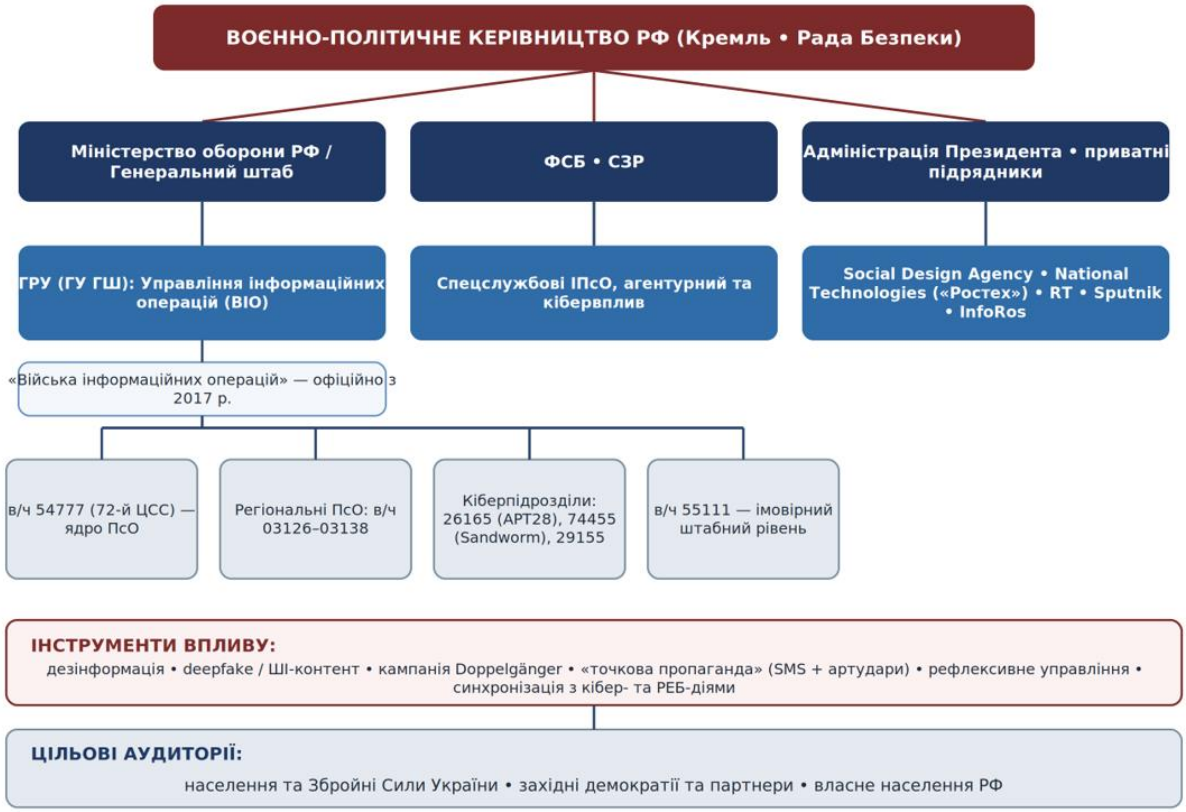


Рисунок 4. Структура системи когнітивного (інформаційно-психологічного) впливу російської федерації

Висновок (Conclusion)

Проведений аналіз системи когнітивного впливу російської федерації свідчить, що вона являє собою комплексну та централізовано керовану систему, інтегровану в механізми забезпечення національної безпеки та ведення сучасної війни. Її функціонування забезпечується узгодженою діяльністю військових, спеціальних, державних і приватних структур, які реалізують єдиний задум інформаційно-психологічного та когнітивного впливу на противника й спираються на доктрини герасимова та рефлексивного управління.

По-перше, росія сформувала цілісну, інституційно закріплену систему когнітивного впливу, що поєднує військові, спеціальні та цивільно-приватні структури в єдиному контурі "інформаційного протиборства".

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Таблиця 4. Рекомендовані напрями симетричної відповіді України

Напрям	Зміст заходів
Інституційний	Посилити та законодавчо закріпити єдиний координаційний центр стратегічних комунікацій, об'єднавши зусилля Центру протидії дезінформації РНБО, Центру стратегічних комунікацій та інформаційної безпеки і профільних відомств; уникати дублювання й розпорошення повноважень
Воєнний	Завершити формування повноцінних сил інформаційних і когнітивних операцій у складі Сил оборони з чіткою доктриною, кадрами та системою підготовки; інтегрувати когнітивний компонент у планування всіх операцій
Доктринальний	Затвердити доктрину когнітивної (інформаційно-психологічної) безпеки, узгоджену з концепцією НАТО щодо когнітивної війни та принципами "когнітивної переваги" і "багаторівневої стійкості"
Технологічний	Розгорнути ШІ-системи моніторингу інформпростору, раннього виявлення наративів і дипфейків, прогнозування ворожих кампаній; розвивати державно-приватне партнерство з платформами
Суспільна стійкість	Системно впроваджувати медіаграмотність і критичне мислення в освіті, підвищувати психологічну стійкість населення; розвивати "імунітет" через випереджальне роз'яснення (prebunking), а не лише спростування
Зовнішній / партнерський	Підтримувати й масштабувати правдивий стратегічний наратив для міжнародних аудиторій, поглиблювати співпрацю з Центром передового досвіду НАТО зі стратегічних комунікацій (StratCom CoE) та партнерами, протидіяти російському впливу в Глобальному Півдні

По-друге, ядром військового сегмента є структури ГРУ (Управління інформаційних операцій, в/ч 54777 та мережа регіональних і кіберпідрозділів), що діють постійно й наступально, у тісній координації з проксі-медіа та приватними підрядниками.

По-третє, російський досвід доводить, що централізована інтеграція когнітивних спроможностей дає стратегічний ефект, а отже, Україна не може дозволити собі відставання та зобов'язана сформувати симетричну інституційну відповідь.

російський досвід демонструє, що когнітивний вплив розглядається як повноцінний інструмент сучасного воєнного протиборства, здатний забезпечувати значний стратегічний ефект без застосування традиційної військової сили. Результати дослідження засвідчують, що росія розбудувала ешелоновану систему когнітивного впливу, інституційно оформлену у спеціальних військах інформаційних операцій (2017) та внутрішньому військово-політичному органі (2018), із доктринальним підґрунтям у відкритих стратегічних документах і прихованим операційним ядром.

Водночас порівняння відносно успішної операції 2014 року в Криму з переважною невдачею російської моделі на міжнародному рівні у 2022 році показує, що ця система не є непереборною: послідовна, заснована на правді стратегічна комунікація здатна нейтралізувати навіть добре ресурсно забезпечену пропагандистську машину.

Для України, яка веде паралельну "війну за свідомість" власної нації та партнерів, програш у цій сфері означав би стратегічну поразку навіть за умови утримання фронту. Симетрична, а точніше асиметрично-адекватна відповідь має ґрунтуватися не на копіюванні російської пропагандистської машини, а на демократичній моделі когнітивної стійкості, основою якої є правда, прозорість і довіра. Лише поєднання воєнного, інституційного, технологічного й суспільного вимірів дасть змогу не програти війну за свідомість власної нації та союзників.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Рекомендації (Recommendations)

Результати цієї статті можуть бути корисними для науковців у сфері воєнних наук, фахівців зі стратегічного планування та стратегічних комунікацій, аналітиків сектору безпеки й оборони, а також для державних органів, які працюють над розбудовою національної системи когнітивної безпеки та протидії когнітивним загрозам з боку російської федерації. Узагальнені пріоритетні напрями симетричної відповіді України наведено в табл. 4.

Конфлікт інтересів (Conflict of Interest)

Автори заявляють, що у них немає конкуруючих інтересів за тематикою статті.

Використані джерела

1. Snegovaya, M. (2019). *Russia's information warfare: Exploring the cognitive dimension*. *MCU Journal*.
2. Galeotti, M. (2017, February 22). *"Propaganda needs to be clever, smart and efficient": Russia's information warfare*. *In Moscow's Shadows*.
3. *How Russia's cognitive warfare strategy seeks to reshape reality*. (2025). *The Debrief*.
4. Giles, K. (2016). *Handbook of Russian information warfare*. NATO Defense College. https://www.ndc.nato.int/
5. Gerasimov, V. (2013). *Цінність науки у передбаченні*. Цит. за Snegovaya, M. (2019). *Russia's information warfare: Exploring the cognitive dimension*. *MCU Journal*.
6. *Undermining Ukraine: How Russia widened its global information war*. (2024). Atlantic Council, DFRLab. https://www.atlanticcouncil.org/
7. Paziuk, A., Lande, D., et al. (2025). *Decoding manipulative narratives in cognitive warfare*. *Frontiers in Artificial Intelligence*.
8. *Шойгу підтвердив створення Військ інформаційних операцій*. (2017, February 22). *ТАСС*; *Російська газета*; *РБК*.
9. *Russian "Cyber Troops": A weapon of aggression*. (2017). *RealClearDefense*.
10. *Russia's cognitive warfare against Ukraine*. (2025). *Foreign Policy*.
11. *8-ме управління Генерального штабу ЗС РФ – Служба захисту державної таємниці*. (n.d.). Міністерство оборони Російської Федерації.
12. Російська Федерація. Президент. (2016). *Указ Президента РФ від 05.12.2016 № 646 «Про затвердження Доктрини інформаційної безпеки Російської Федерації»*.
13. Російська Федерація. Президент. (2018). *Указ Президента РФ від 30.07.2018 (створення Головного військово-політичного управління)*. *Газета.Ru*.
14. *Russian information war against Ukraine: An overview*. (2025). *The Debrief*.
15. *The future of China's cognitive warfare: Lessons from the war in Ukraine*. (2022). *War on the Rocks*.
16. *Countering the Kremlin's narratives about Ukraine*. (2023–2024). Atlantic Council, DFRLab; Institute for the Study of War (ISW).

References

1. Snegovaya, M. (2019). *Russia's information warfare: Exploring the cognitive dimension*. *MCU Journal*.
2. Galeotti, M. (2017, February 22). *"Propaganda needs to be clever, smart and efficient": Russia's information warfare*. *In Moscow's Shadows*.
3. *How Russia's cognitive warfare strategy seeks to reshape reality*. (2025). *The Debrief*.
4. Giles, K. (2016). *Handbook of Russian information warfare*. NATO Defense College. https://www.ndc.nato.int/
5. Gerasimov, V. (2013). *The Value of Science in Prediction*. Cited in Snegovaya, M. (2019).

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Russia's information warfare: Exploring the cognitive dimension. *MCU Journal*.
6. *Undermining Ukraine: How Russia widened its global information war*. (2024). Atlantic Council, DFRLab. https://www.atlanticcouncil.org/
7. Paziuk, A., Lande, D., et al. (2025). *Decoding manipulative narratives in cognitive warfare*. *Frontiers in Artificial Intelligence*.
8. *Shoigu Confirmed the Establishment of the Information Operations Forces*. (2017, February 22). *TASS*; *Rossiyskaya Gazeta*; *RBC*.
9. *Russian "Cyber Troops": A Weapon of Aggression*. (2017). *RealClearDefense*.
10. *Russia's Cognitive Warfare Against Ukraine*. (2025). *Foreign Policy*.
11. *8th Directorate of the General Staff of the Armed Forces of the Russian Federation – State Secrets Protection Service*. (n.d.). Ministry of Defence of the Russian Federation.
12. Russian Federation. President. (2016). *Presidential Decree of the Russian Federation No. 646 of December 5, 2016, "On Approving the Information Security Doctrine of the Russian Federation"*.
13. Russian Federation. President. (2018). *Presidential Decree of the Russian Federation of July 30, 2018 (Establishment of the Main Military-Political Directorate)*. *Gazeta.Ru*.
14. *Russian Information War Against Ukraine: An Overview*. (2025). *The Debrief*.
15. *The Future of China's Cognitive Warfare: Lessons from the War in Ukraine*. (2022). *War on the Rocks*.
16. *Countering the Kremlin's Narratives About Ukraine*. (2023–2024). Atlantic Council, DFRLab; Institute for the Study of War (ISW).

On the development of the cognitive influence system of the Russian Federation and the features of its application in the war against Ukraine

Oleksandr Kin
PhD in Technical Sciences, Associate Professor
Hennadii Udovenko Diplomatic Academy of Ukraine
under the Ministry of Foreign Affairs
01001, Velyka Zhytomyrska Street, Kyiv, Ukraine
e-mail: cubalibre1972@ukr.net
ORCID: 0009-0001-2196-7515

Liliia Semenenko
Senior Lecturer of the Department of Foreign Languages
National Defence University of Ukraine
03049, Povitroflotskyi Avenue, 28, Kyiv, Ukraine
e-mail: selin-ua@ukr.net
ORCID ID: 0000-0002-5628-3586

Oleh Nechaiev
First Deputy Commander
Special Operations Forces of the Armed Forces of Ukraine
e-mail: o26811650@gmail.com
ORCID: 0009-0001-2839-2830

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Oleh Temnyi
postgraduate Department of Information Warfare
Institute of Strategic Communications
National Defense University of Ukraine
03049, Povitrianykh Syl avenue, 28, Kyiv, Ukraine
e-mail: o.temnyi@edu.nuou.org.ua
ORCID: 0009-0009-3173-094X

Oleksandr Hudkov
Head of the Educational and Laboratory
Complex of the Department of Military
Training at the State University "Kyiv Aviation Institute"
e-mail: alex19720914@gmail.com
ORCID: 0009-0002-6468-3261

Abstract. Modern armed conflicts are increasingly shifting from the sphere of physical confrontation to the sphere of human consciousness, and the Russian Federation, one of the first among the post-Soviet states, has transformed cognitive influence into a separate, institutionalized direction of military activity. The article provides a comprehensive analysis of the development, tools, and institutionalization of the Russian system of cognitive influence, as well as the features of its application in the war against Ukraine. The periodization of the formation of the system from the latent stage (the legacy of Soviet "active measures" and the theory of reflexive control) to the total stage of full-scale invasion is traced, when cognitive operations have become global with the integration of artificial intelligence, deepfakes, and bot farms. The doctrinal principles of the Russian approach are revealed, in which the military doctrine does not distinguish between cyberattacks and propaganda, treating them as a single space of "information confrontation", and the enemy's consciousness is defined as the main target of influence. The probable structure and management system of the special Information Operations Forces (IOF), officially recognized in 2017, is reconstructed, the central role of the structures of the Main Directorate of the General Staff (GRU), in particular military unit No. 54777 and a network of regional and cyber units, as well as the distinction between external (IOF) and internal (Main Military-Political Directorate, 2018) contours are shown. Modern campaigns against Ukraine are analyzed, in particular the media cloning operation "Doppelgänger" and "point propaganda", and it is shown that the relatively successful cognitive operation of 2014 in Crimea contrasts with the overwhelming failure of the Russian model at the international level in 2022. The main result of the article is the substantiation of the conclusion that Russia has formed a holistic, centrally managed system of cognitive influence, the core of which is the military intelligence structures, and therefore Ukraine is obliged to form a symmetrical, or rather asymmetrically adequate response, based on a democratic model of cognitive resilience, the basis of which is truth, transparency and trust. The materials of the article can be useful for the military, analysts, security specialists, scientists and strategists involved in protecting the information and cognitive space of the state. Promising areas of further research are the development of a cognitive security doctrine of Ukraine, the formation of full-fledged information and cognitive operations forces and the creation of technological systems for the early detection of hostile narratives and deepfakes.

Keywords: cognitive influence, cognitive warfare, information confrontation, reflexive management, Information Operations Forces, GRU, Gerasimov doctrine, disinformation, deepfakes, Doppelgänger campaign, psychological operations, strategic communications, national security, Russian-Ukrainian war, cognitive resilience, symmetric response.