ISSN 2311-259X

https://doi.org/10.28925/2311-259x.2025.3.10
УДК 070:316.472.4+[004.62-5:659.3:327.8](477:470)

Роман Осадчук
Національний університет «Києво-Могилянська Академія»
вул. Волоська, 8/5, Київ, 04655, Україна
https://orcid.org/0000-0002-4552-1227
r.osadchuk@ukma.edu.ua

РОСІЙСЬКІ ДЕЗІНФОРМАЦІЙНІ ОПЕРАЦІЇ ПРОТИ УКРАЇНИ ПІД ЧАС ШИРОКОМАСШТАБНОГО ВТОРГНЕННЯ: КЕЙС-СТАДІ

Актуальність дослідження зумовлена зростанням уваги до державної дезінформації, яка здатна призвести до відчутних наслідків у реальному житті, зокрема спонукати до скоєння воєнних злочинів або залучення до неспровокованих воєнних дій. Значна частина дослідницьких праць присвячена аналізу окремих російських дезінформаційних наративів та особливостей їх поширення і в Україні, і за її межами. Водночас кількість досліджень, що намагаються класифікувати й оцінити спектр російських тактик, технік і динаміку їх еволюції після початку повномасштабної агресії, залишається обмеженою.

Об'єктом дослідження статті стали три теоретично не пов'язані кейси, які ілюструють новітні підходи в інформаційних впливах: *дзеркалення вебсайтів* для поширення тривожного або негативного контенту через рекламні оголошення та відповіді до публікацій; *розповсюдження сфальсифікованого відеоконтенту* через платформи з відео з подальшим підсиленням у соціальних мережах; а також *масове дублювання дезінформаційного контенту* в коментарях у соцмережах. *Метою* цього дослідження є опис новітніх ітерацій російських кампаній у період після вторгнення, зокрема демонстрація їхньої здатності адаптуватись до обмежень, пов'язаних із санкціями та блокуваннями. Дослідження поєднує мультидисциплінарні методи цифрової гуманітаристики, наративний аналіз і кейс-стаді, розвідку відкритих джерел. Мультидисциплінарний підхід дає можливість простежити ймовірні зв'язки між операціями та продемонструвати еволюцію підходів. Джерельною базою дослідження служать публікації в соціальних мережах, а також вебсайти і звіти приватних компаній.

Результати свідчать про постійну адаптацію російської дезінформаційної екосистеми до нових технологічних умов і перешкод, водночас збереження нею ядра тактик, що мають витоки ще з радянських часів. Отримані висновки мають практичне значення для дослідників і фахівців із цифрової стійкості в розробці ефективніших засобів протидії новим інформаційним кампаніям і сприятимуть зміцненню спроможності демократичних суспільств до відбиття подібних загроз.

Ключові слова: дезінформація; інформаційні операції; медіа; Україна; Росія; соціальні медіа.

Вступ

Як засвідчили зусилля Росії протягом останніх двох десятиліть, сучасна інформаційна війна поєднує в собі психологічні операції, кібератаки та операції зі впливу з метою формування громадської думки, дестабілізації суспільств ізсередини та підриву довіри до демократичних інституцій. Інформаційна війна часто розгортається в інформаційному просторі без чітких ознак втручання чи демонстрації сили, що ускладнює її атрибуцію, регулювання та протидію. І державні, і недержавні актори (здебільшого на контрактній основі) активно використовують цифрові платформи, ботів і контент, згенерований за допомогою штучного інтелекту, задля посіву розбрату, підриву інституційної довіри та реалізації геополітичних інтересів. Низька собівартість і глобальний масштаб роблять ці тактики привабливим інструментом сучасної державної політики для авторитарних режимів.

Повномасштабне вторгнення Росії в Україну висвітлило критичну роль дезінформації та операцій із впливу як невід'ємної складової кінетичних дій. Із самого початку вторгнення Росія розгорнула масштабну кампанію фальшивих наративів під фальшивим прапором, покликану створити casus belli (Gigitashvili, & Osadchuk, 2022), що згодом супроводжувалася численними воєнними злочинами (Higgins, 2022) та обстрілами цивільної інфраструктури, які Росія заперечувала, підробляючи докази або публічною риторикою. Застосовуючи дезінформацію, російська сторона прагне створити так зване інформаційне алібі та обґрунтування для своїх дій.

Операції впливу, активні заходи та дезінформаційна діяльність Росії привернули широку увагу після президентських виборів у США 2016 року (Allcott, & Gentzkow, 2017). Водночас подібна активність із боку Росії була задокументована ще з часів Радянського Союзу та перших десятиліть незалежної Росії (Rid, 2020). Незважаючи

ISSN 2311-259X

на розмаїття цілей, основна увага РФ в останні роки була зосереджена саме на сусідніх державах. Україна стала об'єктом посилених дезінформаційних і пропагандистських атак ще у 2014 році (DFRLab, 2023a), а напередодні повномасштабного вторгнення Росії — ключовим елементом у створенні інформаційного прецеденту для агресії (Zilinsky et al., 2024).

Російська активність в інформаційному просторі свідчить про високий пріоритет цього напряму в межах війни проти України. Ідеться як про спроби вплинути на поведінку українського населення, так і на процес ухвалення рішень країнами — партнерами України, від яких залежить постачання критично важливої військової та гуманітарної допомоги, що є невід'ємною частиною українського спротиву.

Метою цього дослідження є опис новітніх ітерацій російських кампаній у період після вторгнення, зокрема демонстрація їхньої здатності адаптуватись до обмежень, пов'язаних із санкціями та блокуваннями. Для аналізу було використано мікс методів, а саме: контент-аналіз, методи цифрової гуманітаристики, розвідку відкритих даних (OSINT) і кейс-стаді, що включають вивчення публікацій у соціальних мережах, а також вторинних джерел, зокрема аналітичних центрів, урядових звітів, матеріалів ЗМІ, досліджень неурядових організацій та іншої відкритої інформації, включно із судовими афідевітами.

Кейси було обрано з огляду на новизну використаних тактик. Водночас непрямі свідчення, зокрема афідевіти і витоки внутрішньої інформації російських пропагандистів, указують на ймовірну участь одних і тих самих акторів у трьох окремих кампаніях. Це підкреслює багатовекторний характер підходу, притаманний акторам, пов'язаним із російською державою, які діють від її імені або в її інтересах, забезпечуючи при цьому формальну заперечуваність причетності держави.

Огляд літератури

Інформаційні операції є об'єктом дослідження й істориків, і фахівців із протидії дезінформації (Rid, 2020), здебільшого вони відомі під назвою «активні заходи». Такі операції традиційно спрямовувались на підрив волі противника до спротиву, дискредитацію незговірливих політиків і дипломатів або ж примноження хаосу та розбрату серед цільової аудиторії з метою реалізації стратегії «розділяй і володарюй». Починаючи з 2013 року, Росія активно використовує цифрові комунікаційні платформи для поширення зловмисної дезінформації, залучаючи ботів, тролів і фейкові акаунти для посіву розбрату, підриву довіри до інституцій (DFRLab, 2023b; DFRLab, 2024), а також для відволікання уваги від важливих тем (Atanasova et al., 2024).

Численні дослідження, що мали на меті проаналізувати структури, відповідальні за поширення російської дезінформації (GEC, 2020), зосереджувалися здебільшого на традиційних ЗМІ та вебресурсах, таких як Sputnik і RT (Kling et al., 2022), або ж на конкретних наративах (Sundelson et al., 2023). Утім ці роботи часто оминали увагою неминучу еволюцію російських зусиль після заборони низки прокремлівських медіа в Європейському Союзі (Council of the European Union, 2022). Оскільки платформи для поширення контенту, а отже, й самі тактики змінюються з великою швидкістю, дослідники часто опиняються в ситуації постійної гонки.

Тож метою цього есе є окреслити низку дезінформаційних кампаній, здійснених Росією, щоб простежити трансформацію підходів та еволюцію методів, які використовують дезінформаційні актори в умовах цифрового середовища без кордонів.

Методи дослідження

У цьому дослідженні застосовано контент-аналіз (Wilson, & Starbird, 2020), методи цифрових гуманітарних наук та аналіз відкритих джерел (Julan, & Togan, 2023), а також використано підхід кейс-стаді для вивчення низки дезінформаційних кампаній Росії, що відбулись після початку повномасштабного вторгнення в Україну. Обрані кейси мають підтверджену причетність Росії та демонструють узгодженість з інтересами російської держави, спрямовану на досягнення цілей збройної агресії за менших ресурсних витрат. Участь російських акторів підтверджується або публікаціями в соціальних мережах і дослідженнями у відкритих джерелах, або витоками внутрішньої документації з Росії, де окреслені завдання груп, пов'язаних з інформаційним впливом і контрольованих державою.

Описані кампанії свідчать про системний підхід, якого дотримуються російські актори для досягнення довгострокових цілей щодо впливу на громадську думку в інших країнах. Отримані результати можуть бути корисними для дослідників дезінформації та пропаганди як приклад нових проявів активних заходів, інструментів впливу та пропагандистських стратегій.

Спираючись на аналітичні й академічні дослідження, автор подає широку картину діяльності Російської Федерації в інформаційному просторі, спрямованої на дез- та місінформування іноземної аудиторії з метою впливу на процеси ухвалення рішень на користь пропагандистських інтересів.

Кожен кейс буде проаналізовано за кількома аспектами. У першій частині буде розглянуто контекст кампанії, типовий контент, задіяні платформи, техніки поширення. Друга частина присвячена еволюції тактик і зміні поведінки. Третя частина зосереджена на визначенні цільових аудиторій, показниках залучення, а також атрибуції кампанії до одного й того ж актора. Перевірка висновків ґрунтується на даних самих соціальних платформ, які вже ідентифікували та видалили відповідні кампанії, або ж на кореляції з витоками внутрішньої документації з Росії.

Це дослідження зосереджується лише на трьох окремих кампаніях, тоді як реальний масштаб російських дезінформаційних зусиль, що охоплюють і Україну, і її партнерів, є набагато ширшим. Крім того, у межах цієї роботи не розглядаються випадки співпраці Росії з китайськими операціями зі впливу, а також активність Росії в інших регіонах світу, зокрема в Африці, Латинській Америці та країнах Близького Сходу, де можуть застосовуватись альтернативні методи.

Кейс-стаді

Кейс 1. Операція «Двійник» (Doppelganger) (2022 — по сьогодні)

Контекст

Операція «Doppelganger» (OD) є російською кампанією впливу, що була спрямована проти низки європейських країн, зокрема України, Франції, Німеччини, Італії й інших (EU Disinfolab, 2025). Кампанію вперше ідентифікували в серпні 2022 року зусиллями EU Disinfolab, DFRLab і компанії Meta, коли в соціальній платформі Facebook з'явилась низка сторінок, що використовували візуальну айдентику авторитетних європейських ЗМІ для розміщення рекламних оголошень із негативним змістом про Україну або звинуваченнями на адресу західноєвропейських країн за надання підтримки Україні (Nimmo, & Torrey, 2022).

Типовий контент на цих сторінках або не містив змістовної інформації, або був украй абстрактним. Основну функцію виконувала реклама, через яку поширювалась дезінформація, наприклад твердження про те, що більшість німців виступає проти нових санкцій щодо Росії, або звинувачення України в «убивстві дітей». Основними каналами поширення були рекламні оголошення у Facebook, а також відповіді та цитування у Twitter / X. Реклама у Facebook давала можливість оплачувати доставку контенту, оминаючи умови обслуговування Meta і не вдаючись до складного процесу розбудови автентичної аудиторії. Хоча Meta зазвичай оперативно видаляла подібні сторінки, деякі рекламні публікації встигли набрати десятки тисяч переглядів (EU Disinfolab, 2025).

Альтернативна тактика, використання коментарів, виявила вразливість платформи Twitter: російські акаунти купували позначку «синьої галочки» Twitter Blue і залишали коментарі під популярними дописами в надії охопити частину аудиторії оригінального контенту. Зміст таких коментарів або такої реклами часто містив провокативну візуалізацію, зокрема карикатури на європейських політиків і посилання на вебсайти, що імітували зовнішній вигляд і структуру впізнаваних ЗМІ. Натискання будь-якого посилання на цих сайтах імітувало функціональність справжніх медіа, включно з форматом і стилістикою матеріалів, які нагадували справжні журналістські тексти. Єдиними відмінностями були змінене доменне ім'я та сфальсифікований зміст публікацій, які ніколи не були опубліковані в реальному ЗМІ. Наприклад, двійник українського сайту УНІАН, який зазвичай розташований за адресами unian.ua та unian.net, хостився за адресою unian.pm (Châtelet, & Osadchuk, 2024).

Еволюція

Кампанія набула широкого розголосу, її висвітлювали в багатьох ЗМІ та дослідженнях, що змусило організаторів змінити підхід і вдатись до складніших технічних рішень. Так, у 2023 році вебсайти, пов'язані з операцією «Doppelganger», почали використовувати іншу цифрову інфраструктуру, яка сегментувала цільову аудиторію за географічною ознакою. Зокрема, користувачі, які бачили рекламні оголошення у Facebook, зазвичай були цільовими в межах певної країни, хоча доступ до сайтів кампанії могли отримати й користувачі з інших країн. Утім із упровадженням системи Keitaro (Qurium, 2024) сайти-двійники почали перевіряти відповідність місцеперебування користувача визначеній цільовій аудиторії. У разі позитивної відповідності користувача, тобто збігу країни-цілі та локації читача, перенаправляли на фальсифіковану статтю на сайті-двійнику, а у протилежному випадку — на «білий екран» або сторінку з абсурдним текстом (Châtelet, & Osadchuk, 2024).

Згодом, у 2024 році, система зазнала подальшої модифікації. Якщо користувач намагався здійснити архівування сайту операції «Doppelganger», вміст сайту миттєво змінювався на повну копію матеріалів авторитетного ЗМІ, без жодного шкідливого контенту. Це унеможливлювало якісну фіксацію, архівування і подальший аналіз із боку дослідників, значно ускладнюючи розслідування та документування кампанії.

Аудиторія та атрибуція

Точний обсяг залучення аудиторії в межах кампанії визначити складно, оскільки контент, що був розміщений на платформах, згодом повністю вилучили в окремих країнах, унеможлививши доступ до релевантних даних. Водночас, згідно з внутрішніми документами компанії Social Design Agency (SDA) (Pamment, & Tsurtsima, 2025, с. 64), їхні операції торкнулись сотень тисяч осіб у різних країнах. Ці дані охоплюють не лише рекламні оголошення, а й публікації та коментарі в соціальних мережах. З погляду цільової аудиторії кампанії спрямовувались на широку громадськість без вузької сегментації, однак найбільш сприйнятливою для такого роду повідомлень є група людей із конспіративним мисленням (Zilinsky, 2024).

Кампанію реалізовувала російська компанія SDA, яка, за численними витоками та результатами технічної атрибуції, має тісні зв'язки з Кремлем. Цю інформацію підтверджують витоки в медіа, афідевіти, а також санкційні списки (Justice Department, 2024; Belton, 2024). За афідевітом, SDA мала тісні зв'язки з адміністрацією президента Росії, зокрема з першим заступником голови адміністрації Сергієм Кирієнком. Внутрішні

ISSN 2311-259X

документи компанії свідчать, що однією з основних цілей діяльності SDA було *«формування громадської думки в Україні, сприятливої для досягнення цілей і завдань "Спеціальної військової операції", а також для майбутніх двосторонніх відносин між Росією та Україною»* (Justice Department, 2024, с. 149). У контексті США проєкт мав на меті *«вплинути на громадську думку в США, просуваючи позицію, згідно з якою Сполучені Штати мають зосередити зусилля на вирішенні внутрішніх проблем, замість того щоб витрачати кошти на Україну та інші "проблемні" регіони»* (Justice Department, 2024, с. 30). Журналісти також отримали витоки внутрішніх таблиць, у яких містились тексти коментарів і карикатури, що згодом з'являлись у рекламних кампаніях (Laine, & Morozova, 2024).

Кейс 2. Звинувачення в корупції на платформі ТікТок

Контекст

Корупція сприймається як одна з найгостріших проблем в Україні, і багато іноземних спостерігачів характеризують Україну як «корумповану державу» (Odarchenko, & Poznii, 2024). Це одна з найуразливіших тем, яку Росія систематично експлуатувала протягом багатьох років, підсилюючи відповідні меседжі та перебільшуючи масштаб проблеми (Owens, 2024). З весни 2022 року Росія активізувала ще одну кампанію впливу, у межах якої поширювала твердження про те, що Україна «продає західні боєприпаси, надані як допомога» (Osadchuk, 2022; Osadchuk, 2023a).

Особливе загострення ця кампанія отримала на платформі TikTok, де були поширені тисячі відео (усього зафіксовано 12 820 акаунтів), які, як згодом було підтверджено, адмініструвались із території Росії (Osadchuk, 2023b; Robinson et al., 2023). Типове відео містило набір змінних статичних зображень, озвучених голосом, згенерованим штучним інтелектом, і супроводжувалося субтитрами. Сюжетна структура таких роликів була схожою: представлялась посадова особа, стверджувалося, що вона чи її родичі придбали розкішну нерухомість. Відео закінчувалось контрастом зі «стражданнями» пересічних громадян, після чого відповідальність покладалась на «еліти». Варто зазначити, що така нерухомість із цих відео в дійсності залишалась виставленою на продаж або належала іншим особам. DFRLab та BBC проаналізували понад 800 подібних відео (Robinson et al., 2023), у яких фігурували і представники місцевої влади, і високопосадовці, зокрема президент Володимир Зеленський і колишній міністр оборони Олексій Резніков.

Кампанія здійснювалася через акаунти з викраденими фотографіями профілю та зазвичай лише одним завантаженим відео. Деякі з виявлених профілів мали схожі біографії (опис акаунту), що може свідчити про імітацію реальної активності. Відео згодом поширювалися й поза межами TikTok. Користувачі інших соціальних мереж, зокрема Telegram і Twitter, підхоплювали відео, додаючи субтитри або описи іншими мовами, що сприяло зростанню популярності контенту.

Еволюція

Ця кампанія є оновленою ітерацією попередніх зусиль на платформі TikTok, коли прокремлівські актори фінансували популярних тіктокерів, які записували заздалегідь підготовлені відео та використовували однакові хештеги (DFRLab, 2022). На відміну від попередніх хвиль цього разу акаунти імітували справжніх користувачів, послуговуючись досить правдоподібними іменами й популярними хештегами для отримання потенційного алгоритмічного підсилення. Контент мав провокативний характер і спонукав справжніх користувачів до взаємодії, коментування та подальшого поширення.

Крім того, оператори кампанії застосовували продумані заходи оперативної безпеки, спрямовані на приховування походження відео. Факт використання таких технік підтвердила сама компанія TikTok (2023).

Аудиторія

Цільова аудиторія подібних відео була надзвичайно широкою, різноманітною та, ймовірно, значно більшою, ніж передбачалося спочатку. Деякі з відеороликів набирали тисячі або сотні тисяч переглядів, тоді як інші обмежувались лише кількома сотнями. Найбільше розголосу отримали ті відео, які зображували українських посадовців як корумпованих під час воєнного стану, що викликало обурення в глядачів, які сприйняли цей контент як достовірний. Імовірно, основною цільовою аудиторією в Україні були громадяни з низьким рівнем довіри до влади, що, за опитуваннями, становить переважну більшість (NV, 2025).

Разом із тим кампанія була орієнтована й на іноземну аудиторію. Відео публікувалися щонайменше сімома мовами, зокрема українською, російською, німецькою, італійською, англійською. Найвірусніше відео — з критикою колишнього міністра оборони України — було зроблене українською мовою, однак це не завадило йому отримати кілька мільйонів переглядів у Twitter / X, де воно супроводжувалося субтитрами або описом іншими мовами.

Атрибуція цієї кампанії до Росії ґрунтується на кількох джерелах: заявах представника платформи (Osadchuk, 2023b), витоках внутрішніх документів з Росії (Belton, 2024), які містили інформаційну панель із прикладами відео TikTok як доказу популярності контенту, створеного компанією SDA, а також наданому афідевіті з перехопленими документами (Justice Department, 2024). Внутрішня документація SDA також свідчить про високу деталізацію в роботі дезінформаційних акторів, які системно збирали дані про сприйняття їхнього контенту аудиторією.

Кейс 3. Коментарі на соціальних платформах

Контекст

Росія має давню історію використання коментарів у соціальних мережах для отруєння публічних дискусій, маніпуляції увагою користувачів і провокування емоційної реакції. Багато викривачів надали внутрішню інформацію про діяльність так званих фабрик тролів. Різке зростання активності тролів за кордоном було зафіксоване у 2016 році під час президентських виборів у США, коли російські тролі маскувались під американських громадян і втручались у різноманітні дискусії. У 2021 році дослідники виявили, що російські акаунти використовували розділи коментарів на сайтах провідних європейських медіа для просування визначених меседжів, які згодом підхоплювали російські ЗМІ як «глас народу» іноземних держав (Cardiff University, 2021). Ідея полягала в тому, щоб представити дописувачів у коментарях під матеріалами авторитетних видань як «голос розуму» всередині західних суспільств, на основі чого створювалися статті у російських медіа (Buziashvili, & Rizzuto, 2022).

У 2024 році журналісти отримали витоки внутрішніх документів компанії SDA, які пролили світло на масштаб операцій у різних соціальних мережах, фіксуючи тисячі скоординованих коментарів (Morozova, & Laine, 2024). Це дало безпрецедентний доступ до внутрішньої роботи «фабрики тролів» після початку повномасштабного вторгнення Росії в Україну.

Типовий зміст таких коментарів включав зображення з мемом без тексту або короткий текстовий коментар, що звинувачував українську владу в корупції, некомпетентності чи «розпалюванні війни» або ж прославляв дії російського уряду й наративи про «миротворчість», орієнтовані на російську аудиторію. Виявлено численні випадки повторення ідентичного візуального й текстового контенту через різні акаунти, що вказує на координацію та спільне походження. Зазвичай об'єктами таких кампаній ставали публікації ЗМІ, дописи публічних осіб і сторінки з великою кількістю підписників із метою привернення уваги аудиторії.

Подібну активність було зафіксовано в Telegram, Facebook і Twitter, як зазначено в дослідженні DFRLab (Osadchuk et al., 2024). Дослідники проаналізували понад 580 000 коментарів, опублікованих у період із жовтня по листопад 2024 року на платформах Telegram і Facebook. Для аналізу використовувався інструмент Osavul, який агрегує контент із різних соціальних платформ і виявляє кластери майже ідентичних повідомлень між акаунтами. Окремі дослідження також засвідчують схожі типи активності в соціальній мережі VK.

Еволюція

Хоча публікація коментарів не є новою тактикою, масштаби її використання та відносна легкість реалізації призводять до дедалі більшої залежності дезінформаційних акторів від цього інструменту. Учасники дезінформаційних кампаній адаптуються до особливостей окремих платформ, щоб уникати негайного блокування. Наприклад, на Facebook деякі сторінки публікують до 20 коментарів, після чого стають неактивними, тоді як у Telegram акаунти можуть залишати сотні коментарів, а подекуди навіть вступати у взаємодію один з одним. Така поведінка дає акаунтам можливість залишатись у публічному просторі (коментарях) на тривалий час, допоки їх не приховають модератори або не видалить сама платформа.

Імовірно, частина цієї активності відбувається автоматизовано, або під час створення акаунтів, або під час публікацій. Такі практики раніше були виявлені у витоках, відомих як «Vulkan Files», де згадувалася система Amezit (Harding et al., 2023). Ця система використовувалась для створення фейкових профілів у соціальних мережах, які імітували справжніх людей: із використанням реалістичних імен і викрадених персональних фотографій, знайдених на інших платформах або в інтернеті. У випадку з Amezit акаунти розвивались поступово впродовж кількох місяців, залишаючись здебільшого неактивними для формування достовірного цифрового сліду перед їхнім залученням до прихованих інформаційних операцій. У досліджуваній кампанії акаунти створювались масово й використовувались майже одразу після створення.

Аудиторія

Точну кількість переглядів коментарів оцінити складно, оскільки відповідні метрики не є публічно доступними. Водночас окремі коментарі отримують реакції користувачів і набувають певної видимості, тоді як інші стають об'єктом насмішок у відповідях. Проте більшість таких коментарів залишається під публікаціями, справляючи потенційний вплив на аудиторію як думка «звичайного користувача».

Цільова аудиторія таких публікацій є доволі широкою. В українському інформаційному просторі подібні коментарі спрямовані на підрив довіри до українського керівництва, посилення підозрілості й ненависті до «інших» усередині країни, а також на поширення деморалізувального контенту, що має зменшити готовність громадян чинити спротив Росії. У російському сегменті інтернету фокус зміщується на вихваляння політики уряду РФ і демонізацію української держави та її керівництва як агресивних і войовничих.

Атрибуція цієї діяльності до компанії SDA ґрунтується на внутрішніх документах, згаданих в афідевіті (Justice Department, 2024), які містять безпосередній план написання коментарів у соціальних мережах. Також підтвердженням виступають журналістські розслідування, що надали приклади подібної активності з боку Росії (Morozova, & Laine, 2024).

ISSN 2311-259X

Обговорення

Усі три проаналізовані кампанії демонструють різні техніки і тактики впливу на громадську думку іноземних аудиторій, що їх здійснювали російські структури SDA та Struktura. Незважаючи на зовнішню відмінність, ці кампанії об'єднує спільна мета: «послабити українське суспільство», «посіяти напругу», «зменшити обсяги допомоги Україні». Саме ці цілі є спільною основою й лейтмотивом проєктів. Більше того, окремі кампанії використовували ідентичні візуальні елементи, зокрема меми, що свідчить про спільне джерело контенту. Цей факт згодом підтвердили витоки внутрішньої документації (Pamment, & Tsurtsumia, 2025, с. 20).

Хоча деякі кампанії й надалі покладаються на застарілі підходи, інші демонструють підвищення рівня складності, як наприклад, застосування засобів оперативної безпеки та спеціалізованого програмного забезпечення для уникнення атрибуції. Це свідчить про адаптацію дезінформаційних акторів і до подій на полі бою, і до змін у міжнародному політичному середовищі. Така гнучкість указує на наявність системного моніторингу інформаційного простору й пошуку вразливостей у цільових країнах. Також із часом зросла як кількість цільових країн, так і масштаби амбіцій дезінформаційних кампаній, що супроводжувалось еволюцією каналів доставляння контенту. Оператори при цьому демонструють глибоке розуміння алгоритмів і слабких місць платформ, які активно використовуються для поширення контенту й тимчасового уникнення виявлення.

Хоча ефективність цих кампаній складно виміряти з високою точністю, поширення песимістичних настроїв в українському суспільстві та зниження готовності інших країн до надання підтримки Україні (Henley, & Harding, 2024) можуть частково бути наслідком таких інформаційних впливів.

Ці приклади доводять, що активні заходи й дезінформаційні кампанії зростають і за масштабом, і за складністю, становлячи реальну загрозу демократичним інституціям. Тому необхідно вживати як рішучих каральних заходів, на кшталт рішень Міністерства юстиції США (Justice Department, 2024), так і запобіжних: посилення медіаграмотності, формування цифрової стійкості суспільства. Нарешті, важливою є координація зусиль дослідників, політиків і технологічних платформ для пошуку проактивних і дієвих механізмів запобігання подібним кампаніям і нейтралізації їхнього впливу.

Рекомендації

Для запобігання подальшому успіху таких кампаній необхідно розробити перелік дій для урядів, неурядових організацій і приватного сектора. Насамперед ці суб'єкти мають об'єднати зусилля з метою відстеження, розуміння та підриву ефективності інформаційних кампаній. Для цього вони повинні здійснювати моніторинг інформаційного простору й інвестувати ресурси в боротьбу з дезінформацією (Kalenský, & Osadchuk, 2024). Очевидно, що жоден окремий актор не здатен самостійно вирішити проблему дезінформації, тому необхідною є координація між різними структурами та суб'єктами.

На першому етапі такі кампанії мають бути виявлені та проаналізовані, що зазвичай здійснюють аналітики неурядових організацій або приватних компаній. Далі слід запроваджувати політики або санкційні заходи, спрямовані на зменшення вразливості урядових структур до подібних впливів, як це було у випадку з операцією «Doppelganger». Платформи або приватні компанії попри те, що можуть проводити внутрішні розслідування та реагувати на зловживання своїми сервісами, іноді не помічають порушень або використовуваних тактик. Ба більше, компанії можуть уникати втручання, якщо не виявлене пряме порушення встановлених правил або нормативних актів. Отже, держави мають сформувати політики, які стимулюватимуть приватні компанії до активнішої протидії інформаційним операціям, подібним до описаних вище. Крім того, міжурядове співробітництво у сфері обміну даними про кампанії та їх організаторів може запобігти успішному втіленню аналогічних операцій у майбутньому.

Потрібно також упроваджувати більш ефективні методи виявлення кампаній, які використовують витонченіші стратегії ухилення від алгоритмічного моніторингу. Це можуть бути і нові технічні рішення для виявлення скоординованої неавтентичної поведінки, і залучення додаткових людських ресурсів для аналізу інформаційного простору з метою виявлення аномалій, якими по суті і є інформаційні операції.

Зрештою, формування інформаційної стійкості є ключовою навичкою, яку мають розвивати демократичні суспільства. Уряди повинні активніше інвестувати в програми медіа- та інформаційної грамотності, що допоможуть громадянам відрізняти правдиву інформацію від хибної та безпечніше орієнтуватись у цифровому середовищі.

Висновки

Від початку повномасштабного вторгнення російські дезінформаційні кампанії змістили фокус своєї діяльності на платформи соціальних медіа, які стали основною мішенню. Широкий спектр таких операцій реалізують приватні компанії, що мають тісні зв'язки з Кремлем, вони охоплюють численні платформи, іноді мігруючи між ними та підсилюючись зовнішніми акторами різними мовами. Хоча використовувані підходи часто не є новими, рівень їхньої витонченості в аспектах оперативної безпеки та технічної реалізації свідчить про постійну еволюцію дезінформаційних акторів.

ISSN 2311-259X

Попри відмінності ці кампанії прагнуть досягти спільних цілей схожими засобами: підірвати довіру до державних інституцій і розмити межу між реальністю та вигадкою, спричиняючи загальну невпевненість щодо істинності інформації. Проте такі кампанії можуть бути об'єктом спільного розслідування та нейтралізації з боку держав.

Майбутні дослідження повинні охоплювати аналіз інших кампаній, що відбуваються одночасно, з метою виявлення нових тактик поширення контенту і недопущення їхньої ефективності. Водночас, як показує це есе, дослідники та практики завжди відставатимуть від дій ворожих акторів, оскільки ті постійно шукають способи обійти наявні обмеження й правила. Тому для подолання цієї проблеми потрібні швидша реакція та тісніша співпраця між платформами, науковцями і політиками.

Більше того, поточна динаміка свідчить про ймовірне збереження подібних кампаній у майбутньому, що підкреслює потребу у впровадженні контрзаходів, зокрема в посиленні цифрової стійкості, розвитку медіаграмотності та навичок, які є критично важливими для майбутнього демократичних суспільств.

Покликання

Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, *31*(2), 211–236. https://doi.org/10.1257/jep.31.2.211

Atanasova, A., Lesplingart, A., Poldi, F., & Kuster, G. (2024). *Operation Overload*. https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf

Belton, C. (2024, February 16). Kremlin runs disinformation campaign to undermine Zelensky, documents show. *Washington Post*. https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny

Buziashvili, E., & Rizzuto, M. (2022, February 4). Kremlin outlets exploit suspicious user comments on German Navy chief's resignation. *DFRLab*. https://dfrlab.org/2022/02/04/kremlin-outlets-exploit-suspicious-user-comments-on-german-navy-chiefs-resignation

Cardiff University. (2021). *How a Kremlin-Linked Influence Operation is Systematically Manipulating Western Media to Construct & Communicate Disinformation*. https://www.cardiff.ac.uk/__data/assets/pdf_file/0008/2560274/OSCAR-report-September-2021.pdf

Châtelet, V., & Osadchuk, R. (2024, March 12). *Doppelganger targets Ukrainian and French audiences via Facebook ads*. https://dfrlab.org/2024/03/12/doppelganger-operation-targets-ukraine

Council of European Union. (2022, March 2). *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU*. Consilium. 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

DFRLab. (2022, March 2). Russian Hybrid War Report: Social platforms crack down on Kremlin media as Kremlin demands compliance. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-hybrid-war-report-social-platforms-crack-down-on-kremlin-media-as-kremlin-demands-compliance

DFRLab. (2023a, February 22). Narrative warfare. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare

DFRLab. (2023b, February 22). Undermining Ukraine. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine

DFRLab. (2024, February 29). Undermining Ukraine: How Russia widened its global information war in 2023. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023

EU DisinfoLab. (2025, July 7). *What is the Doppelganger operation? List of resources*. https://www.disinfo.eu/doppelganger-operation

GEC. (2020). *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem*. Global Engagement Center and the U. S. Department of State. https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

Gigitashvili, G., & Osadchuk, R. (2022, February 18). How ten false flag narratives were promoted by pro-Kremlin media. *Digital Forensic Research Lab (DFRLab)*. https://medium.com/dfrlab/how-ten-false-flag-narratives-were-promoted-by-pro-kremlin-media-c67e786c6085

Harding, L., Simeonova, S., Ganguly, M., & Sabbagh, D. (2023, March 30). 'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics. *The Guardian*. https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics

Henley, J., & Harding, L. (2024, December 26). Support for Ukraine 'until it wins' falls sharply in western Europe, poll finds. *The Guardian*. https://www.theguardian.com/world/2024/dec/26/support-for-ukraine-russia-war-yougov-poll-survey

Higgins, E. (2022, April 4). *Russia's Bucha 'Facts' Versus the Evidence—Bellingcat*. https://www.bellingcat.com/news/2022/04/04/russias-bucha-facts-versus-the-evidence

Julan, C. I., & Togan, M. (2023). Methodologies for Retrieving and Processing Information from Open Sources (OSINT). *Journal of Military Technology*, *6*(1), 39–44. https://doi.org/10.32754/JMT.2023.1.05

Justice Department. (2024, September 4). *Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere*. https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

Kalenský, J., & Osadchuk, R. (2024, January). *How Ukraine fights Russian disinformation: Beehive vs mammoth* [Hybrid CoE Research Report 11]. Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2024/01/20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf

Kling, J., Toepfl, F., Thurman, N., & Fletcher, R. (2022). Mapping the website and mobile app audiences of Russia's foreign communication outlets, RT and Sputnik, across 21 countries. *Harvard Kennedy School Misinformation Review*. https://doi.org/10.37016/mr-2020-110

Laine, M., & Morozova, A. (2024, September 16). Leaked Files from Putin's Troll Factory: How Russia Manipulated European Elections. *VSquare.Org*. https://vsquare.org/leaked-files-putin-troll-factory-russia-european-elections-factory-of-fakes

Martin Laine [@Martinlaineolen]. (2024, September 16). *Breaking news: Leaked docs from a Kremlin-controlled propaganda machine reveal a campaign backing far-right parties in EU elections and spreading disinformation to undermine Ukraine.* [Tweet]. Twitter. https://x.com/Martinlaineolen/status/1835697494711304622

Nimmo, B., & Torrey, M. (2022). *Taking down coordinated inauthentic behavior from Russia and China* (p. 51). Meta. https://about.fb.com/wp-content/uploads/2022/10/CIB-Report_-China-Russia_Sept-2022-1-1.pdf

NV. (2025, January 2). *Ukrainian distrust of government hits pre-war levels, fuels calls for change*. New Voice. https://english.nv.ua/nation/deep-dissatisfaction-with-ukrainian-leadership-amid-war-efforts-50478470.html

Odarchenko, K., & Poznii, O. (2024, July 31). *Ukrainians See Corruption as a Key Issue Even During the War*. Wilson Center. https://www.wilsoncenter.org/blog-post/ukrainians-see-corruption-key-issue-even-during-war

Osadchuk, R. (2022, July 21). *How Russia promoted the claim that Ukraine re-sold French howitzers for profit*. https://medium.com/dfrlab/how-russia-promoted-the-claim-that-ukraine-re-sold-french-howitzers-for-profit-fd51f71a9362

Osadchuk, R. (2023a, March 9). Seven steps to spread a conspiracy: How Russia promoted weapons trade allegations. *Digital Forensic Research Lab (DFRLab)*. https://medium.com/dfrlab/seven-steps-to-spread-a-conspiracy-how-russia-promoted-weapons-trade-allegations-a3e80ebedaf5

Osadchuk, R. (2023b, December 14). *Massive Russian influence operation targeted former Ukrainian defense minister on TikTok*. https://dfrlab.org/2023/12/14/massive-russian-influence-operation-targeted-former-ukrainian-defense-minister-on-tiktok

Osadchuk, R., Adam, I., Gigitashvili, G., & Furbish, M. (2024, December 18). How inauthentic accounts exploit Telegram comments to spread anti-Ukrainian narratives. *DFRLab*. https://dfrlab.org/2024/12/18/inauthentic-telegram-accounts-ukraine

Owens, R. (2024, May 7). *Corruption in Ukraine and EU Accession*. https://cddrl.fsi.stanford.edu/news/corruption-ukraine-and-eu-accession

Pamment, J., & Tsurtsumia, D. (2025). *Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency*. Psychological Defence Research Institute. https://mpf.se/psychological-defence-agency/publications/archive/2025-05-15-beyond-operation-doppelganger-a-capability-assessment-of-the-social-design-agency

Qurium. (2024, July 11). *How Russia uses EU companies for propaganda — Qurium Media Foundation*. https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Robinson, O., Robinson, A., & Sardarizadeh, S. (2023, December 15). Ukraine war: How TikTok fakes pushed Russian lies to millions. *BBC*. https://www.bbc.com/news/world-europe-67687449

Sundelson, A. E., Trotochaud, M., Huhn, N., & Sell, T. K. (2023). Russian and U. S. News Media Coverage of Ukrainian Biological Laboratories, February — March 2022. *Journal of Strategic Security*, *16*(4), 57–73. https://doi.org/10.5038/1944-0472.16.4.2148

TikTok. (2023, December 13). *Community Guidelines Enforcement Report (Jul–Sep 2023)*. https://www.tiktok.com/transparency/en-us/community-guidelines-enforcement-2023-3

Wilson, T., & Starbird, K. (2020, January 14). Cross-Platform Disinformation Campaigns: Lessons Learned and Next Steps. *Harvard Kennedy School Misinformation Review*. https://doi.org/10.37016/mr-2020-002

Zilinsky, J., Theocharis, Y., Pradel-Sinaci, F., Tulin, M., De Vreese, C., Aalberg, T., Cardenal, A. S., Corbu, N., Esser, F., Gehle, L., Halagiera, D., Hameleers, M., Hopmann, D. N., Koc-Michalska, K., Matthes, J., Schemer, C., Štětka, V., Strömbäck, J., Terren, L., … Zoizner, A. (2024). Justifying an Invasion: When Is Disinformation Successful? *Political Communication*, *41*(6), 965–986. https://doi.org/10.1080/10584609.2024.2352483

Roman Osadchuk
National University of Kyiv-Mohyla Academy, Ukraine

RUSSIAN DISINFORMATION OPERATIONS AGAINST UKRAINE DURING THE LARGE-SCALE INVASION: A CASE STUDY

The relevance of the study lies in the growing attention to state disinformation, which can lead to tangible consequences in real life, in particular, inciting war crimes or involvement in unprovoked military actions. A significant portion of academic research has focused on analyzing individual Russian disinformation narratives and their dissemination both within Ukraine and beyond. At the same time, the number of studies attempting to classify and assess the full spectrum of Russian tactics, techniques, and the dynamics of their evolution since the onset of the full-scale aggression remains limited.

The object of study in this article is three theoretically unrelated cases that illustrate emerging approaches in information influence operations: *Website mirroring* for disseminating alarming or negative content through advertisements and replies to posts; *Distribution of falsified video content* via video-sharing platforms, followed by amplification on social media; *Mass duplication of disinformation content* in comments across social networks. The purpose of this study is to describe the latest iterations of Russian campaigns in the post-invasion period, in particular to demonstrate their ability to adapt to restrictions related to sanctions and blockades. The research employs a multidisciplinary approach that combines digital humanities methods, narrative analysis, case study methodology, and open-source intelligence (OSINT). This approach enables tracing potential links between operations and highlights the evolution of tactics. The source base includes social media publications, websites, and reports from private companies.

The findings indicate that the Russian disinformation ecosystem is adapting to new technological environments and constraints, while maintaining a core set of tactics rooted in Soviet-era practices. The findings are of practical importance for researchers and digital resilience professionals in developing more effective countermeasures against new information campaigns and in strengthening democratic societies' capacity to withstand such threats.

Keywords: disinformation; information operations; media; Ukraine; Russia; social media.

Стаття надійшла до редколегії 06.08.2025