Воєнна розвідка і медіа: межа таємного і публічного під час війни

Military Intelligence and the Media: the Line Between Secret and Public During War

Олександра Марків [A]

Corresponding author: кандидат педагогічних наук, доцент, завідувач кафедри журналістики, e-mail: oleksandra.markiv@gmail.com, ORCID ID: 0000-0001-5720-650X

Іван Марків [B]

кандидат військових наук, провідний науковий співробітник, e-mail: Ivan-markiv@ukr.net, ORCID ID: 0000-0001-6286-1162

Oleksandra Markiv [A]

Corresponding author: Candidate of Pedagogical Sciences, Associate Professor, Head of the Journalism Department, e-mail: oleksandra.markiv@gmail.com, ORCID ID: 0000-0001-5720-650X

Ivan Markiv [B]

Candidate of Military Sciences, Leading Researcher, e-mail: Ivan-markiv@ukr.net, ORCID ID: 0000-0001-6286-1162

[A] Український державний університет імені Михайла Драгоманова, м. Київ, Україна

[B] Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна

[A] Ukrainian State Dragomanov University, Kyiv, Ukraine

[B] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine

Received: October 10, 2025 | Revised: October 20, 2025 | Accepted: October 31, 2025

UDC 355.40:654.197(477)

DOI: https://doi.org/10.33445/sds.2025.15.5.9

Мета роботи. Проаналізувати взаємозв'язок між воєнною розвідкою, інформаційними стратегіями та діяльністю медіа як інструментів впливу у сучасних безпекових комунікаціях. Особливу увагу зосереджено на визначенні межі між правом суспільства на інформацію та необхідністю збереження державної таємниці під час війни.

Метод дослідження. Методи медіааналізу, кейс-стаді, контент-аналізу та елементів порівняльного дослідження.

Результати дослідження. Встановлено, що в сучасному інформаційному просторі воєнна розвідка виступає не лише джерелом стратегічних даних, а й комунікаційним суб'єктом, який формує інформаційну довіру та впливає на сприйняття безпекової політики. Медіа виконують роль посередника між державними структурами і суспільством, забезпечуючи інформаційну підтримку оборонних стратегій та одночасно дотримуючись принципів журналістської етики. Кейс-аналіз показав, що відповідальне висвітлення розвідувальних тем може зміцнювати суспільну єдність і підвищувати репутаційний капітал держави.

Теоретична цінність дослідження. Полягає в концептуалізації воєнної розвідки як комунікаційного діяча в системі сучасних медіа та обґрунтуванні медіааналітики як складника інформаційної безпеки. Запропоновано новий підхід до осмислення взаємодії журналістики, розвідки та громадської довіри в контексті гібридних війн.

Тип статті. Емпірична з елементами аналітичного огляду.

Purpose. To analyze the relationship between military intelligence, information strategies, and media activities as instruments of influence in modern security communications. Particular attention is focused on defining the boundary between the public's right to information and the need to preserve state secrets during wartime.

Method. Methods of media analysis, case studies, content analysis, and elements of comparative research.

Findings. It was found that in the modern information space, military intelligence is not only a source of strategic data, but also a communication entity that shapes information trust and influences the perception of security policy. The media act as intermediaries between state structures and society, providing informational support for defense strategies while adhering to the principles of journalistic ethics. Case analysis has shown that responsible coverage of intelligence topics can strengthen social unity and enhance the state's reputational capital.

Theoretical implications. It consists in conceptualizing military intelligence as a communication actor in the modern media system and substantiating media analytics as a component of information security. A new approach to understanding the interaction between journalism, intelligence, and public trust in the context of hybrid wars is proposed.

Paper type. Empirical with elements of analytical review.

Ключові слова: воєнна розвідка, медіа, інформаційна безпека, журналістика, OSINT, комунікаційні стратегії, гібридна війна.

Key words: military intelligence, media, information security, journalism, OSINT, communication strategies, hybrid warfare.

Вступ

Війна росії проти України істотно посилила значущість питань інформаційної безпеки, комунікацій державних структур і ролі медіа в умовах воєнного стану. Однією з найменш досліджених, але суспільно значущих тем є висвітлення діяльності української розвідки – Головного управління розвідки Міністерства оборони України (ГУР) та Служби зовнішньої розвідки України (СЗР). Адже, публічні заяви розвідників, аналітичні матеріали, коментарі для медіа стають складовою інформаційного фронту, водночас вимагаючи дотримання суворих

обмежень щодо змісту, джерел і способу подання інформації. Проблема полягає у визначенні межі між правом суспільства на доступ до інформації та необхідністю збереження державної таємниці. Відповідно, журналісти, редакції та офіційні структури мають виробити спільні правила комунікації.

Мета дослідження – проаналізувати, як українські медіа висвітлюють діяльність розвідки, які комунікативні й етичні засади при цьому застосовуються, і як забезпечується баланс між відкритістю та безпекою.

Наукова новизна полягає у спробі комплексного осмислення ролі воєнної розвідки як чинника комунікаційного зв'язку між державою, суспільством і медіа в умовах гібридної війни, адже вона проаналізована як **комунікаційний суб'єкт**, що формує публічний дискурс через взаємодію з журналістським середовищем, на відміну від більшості попередніх наукових довідок, де вона розглядається переважно у військово-стратегічному або правовому контексті. Уперше запропоновано підхід, який поєднує елементи медіааналітики та OSINT-методології для дослідження процесів легітимації розвідувальних повідомлень у відкритих медійних просторах. Дослідження також пропонує нове трактування журналістики як складової системи інформаційної оборони держави – не лише як посередника між владою й суспільством, а як активного учасника формування стійкого комунікаційного середовища.

Теоретичні основи дослідження

У статті аналізуються джерела, які тематично зосереджені на ролі розвідки як інструмента влади та участі медіа в процесі її реалізації через оприлюднення інформації. Особлива увага приділяється викликам для журналістів, пов'язаним із маніпуляціями, захистом або забороною публікації даних. Зокрема, В. Черниш (2023) розглядає розвідку як складову державної безпеки: розвідувальні служби здійснюють дії проти інших держав і недержавних суб'єктів за межами країни, а зібрана, оброблена та проаналізована інформація може поширюватися як частина розвідувальної діяльності (Chernysh, 2023). Цікаво також простежити, як така інформація стає доступною в медійних джерелах, а журналістські матеріали, у свою чергу, можуть використовуватися як джерела для розвідки та підготовки рішень на полі бою. Цьому аспектові присвячені дослідження у сфері OSINT. А. Альварес (2023) підкреслює роль OSINT у сучасних розслідуваннях, описує практичні підходи та методики збору й перевірки відкритих джерел (Alvarez, 2023). Л. Шварц (2024) порушує питання ризиків, коли непрофесіонали беруть на себе роль аналізу даних, що раніше належали розвідкам чи професійним аналітикам, наголошуючи на можливості помилок і поширення неправдивої інформації при пріоритеті швидкості над перевіркою (Schwartz, 2022). Аналітичний матеріал "What is OSINT: Open-source intelligence?" зазначає, що деякі автори свідомо маніпулюють OSINT-даними: наприклад, модератори іноді подають знімки одного інциденту з різних ракурсів як окремі події; "туман війни" породжує ненадійність даних як через помилки, так і через навмисні обмани, тож цінність OSINT визначається не кількістю матеріалу, а ретельністю перевірки його достовірності (What is OSINT, 2022). Т. Гайман (2023) пропонує осмислення цифрової війни та динаміки дезінформації, висвітлюючи оперативне застосування OSINT у геополітичних конфліктах (Hayman, 2023). Кореспондент Д. Вольц (2022) підкреслює проблему унормованості діяльності військових журналістів і зазначає, що "соціальні мережі, супутникові знімки, дані мобільних телефонів можуть дати стільки ж інформації, скільки і традиційне шпигунство, але існує дуже мало правил щодо їх використання" (Volz, 2022). С. Чернецька (2022) на Платформі з прав людини описує підходи до журналістської практики й обмежень під час війни (Чернецька, 2022). Д. Леос (2023) відзначає користь OSINT, але звертає увагу на межу між легітимним збором даних та порушенням конфіденційності (Leos, 2023). М. Гойбі (2022), аналізуючи воєнну журналістику, наголошує, що питання правди, упередженості та об'єктивності не можуть бути розглянуті без урахування практики та індивідуальних

особливостей журналіста (Høiby, 2022). Аналітики Інституту масової інформації заявляють, що **в умовах ускладненого доступу журналістів до фронту саме комунікаційники українських угруповань військ забезпечують медіа оперативними зведеннями та зрозумілими поясненнями (Бакар, 2025), тому так важливо, щоб військова пресслужба надавала вчасну та перевірену інформацію.** Дж. Тіган (2025) підкреслює політичні наслідки балансу між прозорістю та оперативною безпекою, закликаючи до етичної верифікації інформації (Teagan, 2025). Йому суголосні І. Ломачинська разом із Б. Ломачинським (Lomachinska I., & Lomachinskyi B. 2023), Є. Борисенко (Borysenko, 2023), які акцентують на значенні медіакультури та медіаграмотності в інформаційній війні. Власне, О. Марків (2018) досліджує інформаційно-психологічні операції в умовах гібридних протистоянь, зазначаючи про вагомі впливи на громадськість (Марків, 2018). Більшість експертів звизнають, що українські медіа під час війни повинні не лише спостерігати, а й активно комунікувати, документувати події та інформувати суспільство для підтримки виживання та стійкості – про це також йдеться в матеріалі Р. Даніленкова (2023) "Чого українські медійники можуть навчити західних" (Даніленков, 2023).

Матеріали та методи

Для досягнення мети дослідження застосовано комплексну методологію, що поєднує кілька підходів кількісного та якісного аналізу.

Вибірка. До аналізу залучено матеріали з різних типів медіаплатформ: національні онлайн-видання, телевізійні новини, регіональні ресурси, аналітичні портали та офіційні Telegram-канали. Така вибірка забезпечила репрезентативність інформаційного поля та дозволила порівняти підходи до висвітлення розвідувальної тематики у різних типах медіа та на різних етапах.

Методологічні підходи: контент-аналіз – кількісний підрахунок і категоризація матеріалів за визначеними параметрами; дискурсивний і рецептивний аналіз – виявлення ключових наративів, образів і моделей сприйняття діяльності воєнної розвідки в медіа; кейс-стаді – аналіз 3–5 показових інформаційних епізодів, у яких медіа висвітлювали або коментували розвідувальні операції, дані OSINT, чи офіційні повідомлення спецслужб.

Параметри контент-аналізу. Оцінювалися такі характеристики публікацій: 1) тематика (оперативна, політична, технологічна, соціальна тощо); 2) тональність (позитивна, нейтральна, критична); 3) наявність технічних деталей (опис систем, методів, технологій); 4) тип джерела інформації (офіційне, анонімне, витік, OSINT); 5) попередження про чутливість контенту (вказівки на державну або військову таємницю, обмеження публікації).

Застосована методологія дозволила поєднати системність кількісного аналізу з глибиною інтерпретації змісту та контекстів медійних повідомлень.

Результати та обговорення

Воєнна розвідка – це система спеціально організованої діяльності держави, спрямована на добування, обробку, аналіз та використання інформації про сили оборони, військово-політичну ситуацію, потенційні загрози та наміри противника. Її ключовим завданням є забезпечення **інформаційної переваги** – здатності ухвалювати стратегічні рішення на основі точних і своєчасних даних (Chernysh, 2023).

У структурі державної безпеки розвідка виступає **елементом стратегічного управління**, який поєднує аналітичну, прогностичну та оперативну функції. Вона забезпечує командування не лише фактами, а й **інтерпретаціями** – тобто моделями дій противника, що мають значення для планування операцій. У сучасному розумінні воєнна розвідка – це не лише добування даних, а й **інформаційно-аналітичне конструювання реальності**, у якому перетинаються технічна й когнітивна складові. Відповідно для розвідників важливі категорії інформації: цілком таємна – дані, розголошення яких може завдати безпосередньої шкоди обороні або

призвести до втрат особового складу; службова (обмеженого доступу) – аналітичні матеріали, операційні оцінки, попередні дані з відкритих або змішаних джерел; відкрита (OSINT) – інформація, отримана з легальних публічних каналів, яка може бути використана у військовій аналітиці без порушення режиму секретності. Проте, в сучасній війні (зокрема російсько-українській) межа між закритими й відкритими даними стає дедалі рухомішою. Є підстави вважати, що значна частина розвідувальної інформації формується на основі OSINT-джерел, у тому числі даних із соціальних мереж, супутникових зображень, журналістських розслідувань. Це актуалізує питання взаємодії розвідки та медіа, де журналіст може стати як партнером у пошуку правди, так і мимовільним агентом витоку.

У сучасній українській реальності **інформаційна війна** є не лише зовнішньою (протистояння російській пропаганді), а й певною мірою **внутрішньою** – боротьбою за інтерпретацію подій, за довіру аудиторії, за визначення того, що можна вважати правдою. Вона має три рівні:

стратегічний – формування образу війни у глобальних медіа;

операційний – інформаційне забезпечення військових рішень і контрпропаганда;

тактичний – щоденна медійна робота журналістів, які балансують між оперативністю та етикою.

Тому журналістика під час збройного конфлікту виконує подвійну функцію: з одного боку, забезпечує право громадськості на інформацію, а з іншого – несе відповідальність за безпеку складових сил оборони. У цьому контексті виникає поняття “відповідальної публічності”, що передбачає саморегуляцію та відмову від оприлюднення матеріалів, здатних завдати шкоди операціям. Теорії публічності та таємниці дозволяють зрозуміти складну динаміку між знанням і владою. У медійному вимірі це означає, що таємність не лише приховує факти, а й створює символічний капітал – довіру до джерела, ореол професіоналізму або, навпаки, підозру у маніпуляції.

У сфері воєнної журналістики та розвідки поняття “таємне” і “публічне” взаємопроникають: те, що вчора було засекречено, сьогодні може стати частиною офіційного наративу, покликаного підтримати моральний дух суспільства. Це явище отримало назву керованої публічності – комунікаційної стратегії, коли держава дозовано відкриває інформацію, зберігаючи контроль над її інтерпретацією. Отже, межа між розвідувальною та медійною інформацією є не статичною, а динамічною – вона змінюється залежно від фази війни, політичного контексту, технологічних можливостей та рівня довіри між Збройними Силами України і суспільством. У цьому процесі формується нова модель інформаційної взаємодії, в якій журналіст і розвідник постають не як опоненти, а як суб’єкти спільного комунікаційного поля, покликані забезпечити безпеку через правду.

У сучасних українських дослідженнях (Інститут масової інформації, “Детектор медіа”, Комісія з журналістської етики) наголошується, що журналістика під час війни має поєднувати принципи прозорості з інформаційною відповідальністю. В Україні правові обмеження встановлюють Закон України “Про державну таємницю”, настанови Збройних Сил України щодо роботи журналістів у зоні бойових дій (Наказ Головнокомандувача Збройних Сил України № 73), а також інституційні комунікаційні протоколи ГУР та СЗР України. Міжнародна практика визначає, що публікація даних, які можуть ідентифікувати військові позиції, техніку чи плани, порушує принцип “не нашкодь”.

Для розуміння, як ці принципи дотримані в медіа проаналізуємо деякі журналістські матеріали; вибірка охоплює офіційні публікації СЗР, ГУР, а також аналітичні та журналістські матеріали від “Детектор медіа”, Інституту масової інформації й Суспільного мовлення. Візьмемо за основу такі параметри: 1) тип джерела (офіційне, аналітичне, журналістське); 2) рівень відкритості інформації; 3) стиль комунікації (інформативний, аналітичний, емоційно-мобілізуючий); 4) присутність етичних або нормативних рамок.

Офіційні комунікації розвідки. Інтерв'ю голови СЗР Олега Іващенка "Після завершення війни за 2-4 роки росія буде технічно готова до нової агресії проти Європи" (Олег Іващенко, 2025) демонструє модель контрольованої відкритості. Подача інформації чітко дозована, уникає конкретних даних, натомість акцентує на стратегічному прогнозуванні. Мовна структура інтерв'ю формує наратив "пильності й готовності", що є складником державної стратегічної комунікації. Інший приклад – аналітична публікація СЗР "Великі інвестиції у хаос" (Великі інвестиції, 2025) розкриває механізми російської інформаційної війни, використовуючи поняття "проксі-медіа" й "інформаційна агресія". Важливо, що розвідка тут виступає не як "таємний" орган, а як аналітичний суб'єкт, який інформує суспільство, формуючи довіру.

Аналітичні медіа та професійні огляди. Матеріали IMI "Як військові пресслужби інформують українські медіа про війну" (Баркар, 2025) показують, як офіційні джерела стають основними постачальниками новин, але за умов суворих обмежень. Публікації "Детектора медіа» (Інформація з відкритих джерел, 2025) наголошують, що інформація з відкритих джерел (OSINT) може бути використана ворогом – отже, журналісти повинні уникати деталізації фото, відео, координат. Тому медіа не лише поширюють новини, а й формують у аудиторії розуміння етичних меж воєнного інформування.

Редакційна етика та самообмеження. Інтерв'ю з головою Суспільного Миколою Чернотицьким "Мовлення під час війни" (Мовлення під час війни, 2024) демонструє, як державні медіа впроваджують політику "відповідальної відкритості": новини мають бути правдивими, але не шкодити обороні. Як бачимо, редакції впроваджують внутрішні фільтри, що обмежують публікацію матеріалів із фронту або з розвідувальних джерел без узгодження з офіційними структурами.

На основі цих досліджень маємо підстави вважати, що: 1) українські медіа формують нову модель комунікації розвідки й суспільства, засновану на довірі та відповідальності; 2) переважає аналітична, а не сенсаційна подача, що відповідає принципам інформаційної безпеки; 3) висвітлення розвідки в українських медіа ґрунтується на етичних самообмеженнях, вироблених під час війни; 4) перспективним напрямом є розвиток OSINT-журналістики, яка потребує чітких стандартів безпеки та верифікації.

А тепер перейдемо до аналізу висвітлення аспектів воєнної розвідки в українському медіапросторі часу війни. Насамперед зауважимо, що межа між таємним і публічним у сучасній воєнній розвідці поступово стає предметом не лише державної, а й медійної політики. Після початку повномасштабної агресії рф у 2022 році інформаційна сфера України набула гібридного характеру, коли розвідка постає не лише джерелом даних, а й активним комунікатором, який через медіа формує стратегічну довіру суспільства, союзників і міжнародної спільноти. Медіа, своєю чергою, опиняються між двома протилежними полюсами – суспільним запитом на відкритість і вимогою державної безпеки до збереження таємниці. У цьому контексті кейс-аналіз публічних епізодів, пов'язаних із висвітленням розвідувальної діяльності, дає можливість виявити типові моделі взаємодії між журналістикою, розвідкою та аудиторією в умовах війни.

Опрацюємо кейс "Висвітлення атак морських дронів у Криму". Зосередимо увагу на операціях 2023 року, оскільки тоді українські морські дрони стали проривом і новини про них спричинювали сильний захопливо-емоційний ефект.

Журналістські матеріали про успішні операції з використання українських морських дронів, які з'являлися у вітчизняних і міжнародних рейтингових виданнях спрацьовували для українського суспільства як підсилення могутності, непохитності та переваги Збройних Сил України у веденні війни. Наведемо деякі з них.

Укрінформ 4 серпня 2023 року об 11.07 (із посиланням на Телеграм-канал російського військового відомства) публікує матеріал "*Морські дрони атакували базу ВМФ у*

Новоросійську, ймовірно, пошкоджений корабель" (у тексті йдеться про пошкодження "екіпажів кораблів "Оленогорский горняк" та "Суворовец", про яке російське відомство замовчує, проте вказано, що деякі російські Телеграм-канали, а також закордонні експерти публікують відео та фото з підбитим десантним кораблем "Оленогорский горняк") (Морські дрони, 2023). У заголовку маємо слово "ймовірно", яке натякає, що інформація потребує перевірки.

Reuters того ж дня, 4 серпня 2023 року, в публікації *"Ukrainian drone disables Russian warship near Russia's Novorossiysk port*" зазначило, що "українське розвідувальне джерело повідомило, що російський десантний корабель "Оленєгорський гірник", на борту якого перебувало близько 100 російських військовослужбовців, був уражений морським дроном, що містив 450 кілограмів тротилу. "В результаті атаки "Оленєгорський гірник" отримав серйозні пошкодження і наразі не може виконувати бойові завдання", – повідомило джерело агентству Reuters, додавши, що операцію провели Служба безпеки України та ВМС. "Усі заяви росії про "відбиту атаку" є фейковими" (Balmforth, 2023). Тут маємо хоча й анонімне, проте покликання на "українське розвідувальне джерело» з прямою цитатою – додає ефекту достовірності.

CNN подало новину вже 6 серпня 2023 року: "*Ukraine may be using drones to amp up its counteroffensive. Here are some of the headlines you should know*". У цій публікації *"Україна може використовувати дрони для посилення своєї контрнаступальної операції. Ось кілька заголовків, про які вам варто знати"*: Україна, схоже, має намір використовувати нове покоління потужних морських дронів проти російських суден... Протягом 24 годин два російські судна – військовий десантний корабель і танкер – були вражені морськими дронами в східній частині Чорного моря. Обидва судна зазнали значних пошкоджень, але залишилися на плаву" (Ukraine may be using drones, 2023). У заголовку є стверджувальна конотація "Україна може використовувати дрони".

Наведені публікації містять посилання на українські розвідувальні джерела, які хоча й зазначаються анонімно, проте надають матеріалу ефекту достовірності та комунікативної вагомості.

Згодом частота публікацій у медіа на таку ж тематику почастішала. А 15 січня 2024 року на сайті Black Sea News знаходимо аналітичний матеріал *"Атаки дронів та ракет українських сил на територію окупованого Криму та російські кораблі в Чорному морі в січні-грудні 2023 року (огляд та база даних)"*, в якому в базі даних знаходимо публікацію з аналізованого приводу від каналу Кримский ветер: "04.08.2023. Акваторія Чорного моря, Чорноморське узбережжя рф, Новоросійська бухта. Близько 5-ї ранку ударом 2 безекіпажних морських дронів атаковано низку об'єктів в акваторії порту Новоросійська (РФ). Пошкоджено великий десантний корабель (ВДК) "Олєнєгорський горняк". Наявна інформація, яка потребує перевірки, про знищення під час атаки протидиверсійного катеру пр. 21980 П-349 "Суворовец". Російська сторона заявила про пошкодження нафтової інфраструктури в Новоросійську, що це не вплинуло на відвантаження нафти на пришвартовані танкери" (Атаки дронів, 2024). Зауважимо, що цей аналітичний огляд містить вагомий перелік назв інших операцій, у текстових описах до деяких трапляються зазначення, що інформація потребує перевірки і підтвердження від українських офіційних структур. І навіть якщо згодом українські офіційні джерела підтвердили лише частину інформації (а це свідчить про **прагнення збалансувати інформаційний ефект і режим секретності), медіа** створили сильний репутаційний ефект, показавши технологічну спроможність української розвідки, але водночас окреслили небезпеку витоку оперативних даних.

На особливу увагу заслуховують інформаційно-психологічні кампанії ГУР у соціальних мережах. Зауважимо тут, що "інформаційно-психологічні операції розглядаються як інструмент, "зброя", технологія, що лише супроводжує бойові дії, гарячі фази збройних

конфліктів або передує їм. У цьому сенсі вони застосовуються переважно для деморалізації і дезорієнтації противника чи, навпаки, зміцненню морального духу населення" (Марків, 2018). У 2024-2025 роках ГУР МО України активно формує власний публічний наратив у Telegram (https://t.me/DIUkraine) та YouTube (https://www.youtube.com/@DI_Ukraine, https://surl.li/fyqpbs), публікуючи відео з диверсійних операцій і звернення до ворога. Вони стали прикладом **психологічних інформаційних операцій**, спрямованих на підрив морального стану противника та консолідацію українського суспільства. Це явище демонструє, як розвідка стає не лише суб'єктом таємної діяльності, а й "актором" **медіапростору війни**, який цілеспрямовано вибудовує образ сили та технологічної переваги.

Висновки

Українські медіа виробили нову модель комунікації між розвідкою, державою й суспільством, що поєднує принципи відкритості та безпеки. Ця модель базується на довірі, дозованій публічності та дотриманні етичних обмежень у воєнний час.

Воєнна розвідка дедалі активніше виступає суб'єктом публічної комунікації, а не лише джерелом закритої інформації. Її офіційні матеріали та аналітичні доповіді формують стратегічні наративи державної безпеки й підсилюють інформаційну стійкість суспільства.

OSINT-журналістика стала легітимним складником воєнного інформування, однак її застосування потребує етичних і правових рамок. Аналіз кейсів (зокрема висвітлення атак морських дронів у Криму) засвідчив, що журналісти використовують відкриті дані обережно – із застереженням щодо достовірності та з урахуванням безпекових ризиків.

Публікації про діяльність української розвідки характеризуються аналітичним, а не сенсаційним підходом. У більшості випадків журналісти уникають прямого розкриття військових даних, натомість акцентують на технологічних досягненнях, моральному аспекті війни та довірі до державних інституцій.

Баланс між таємницею й відкритістю став стрижнем нової воєнної етики українських медіа. Редакції впроваджують самообмеження та погоджувальні процедури з офіційними структурами, формуючи культуру "відповідальної публічності".

Інформаційно-психологічні операції ГУР у соціальних мережах стали елементом сучасної стратегії комунікації: вони не лише деморалізують противника, а й консолідують українську аудиторію, створюючи образ сили та технологічної переваги.

Зміщується роль журналіста – від традиційного посередника до співтворця інформаційної безпеки. Воєнна журналістика в Україні виконує не тільки пізнавальну, а й оборонну функцію, підтримуючи стійкість суспільства до маніпуляцій і дезінформації.

Наукова перспектива дослідження полягає у подальшому вивченні медіа-розвідки як окремого напряму комунікативних студій, де поєднуються журналістика, аналітика даних та стратегічна комунікація держави.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Alvarez A. The OSINT Revolution: Empowering Investigations through Open Source Intelligence. – 2023. – 205p. URL: https://surl.li/nxkgvo
2. Атаки дронів та ракет українських сил на територію окупованого Криму та російські кораблі в Чорному морі в січні-грудні 2023 року (огляд та база даних) // Black Sea News. –

15.01.2024. – URL: https://www.blackseanews.net/read/213072 (дата звернення: 28.10.2025)
3. Balmforth T. Ukrainian drone disables Russian warship near Russia's Novorossiysk port. August 4. – 2023. – URL: https://surli.cc/nphfjw (дата звернення: 28.10.2025)
4. Баркар Д. Як військові комунікації ОСУВ і ОТУ впливають на новини про війну в Україні // Інститут масової інформації. – 12.09.2025. – URL: https://surl.lu/qpjzjz (дата звернення: 28.10.2025)
5. Borysenko Y. Information Warfare in Terms of Communication Theory: Attempted Analysis // *Філософська думка. – 2023. – №* 4. – С. 21-38. https://doi.org/10.15407/fd2023.04.021
6. Великі інвестиції у хаос: аналіз інформаційної війни кремля // Служба зовнішньої розвідки. – 25.04.2025. – URL: https://surl.li/qugqcq (дата звернення: 28.10.2025)
7. Volz D. New Group to Promote Open-Source Intelligence, Seen as Vital in Ukraine War // The Wall Street Journal. – July 27. – 2022. – URL: https://surl.li/soyyya (дата звернення: 20.10.2025)
8. Воєнна розвідка України (власник: Головне управління розвідки МО) // YouTube. –URL: https://surl.li/fyqpbs (дата звернення: 30.10.2025)
9. What is OSINT: Open-source intelligence? //European Union. Data. – 2022-05-02. – URL: https://surl.li/hrcrts (дата звернення: 28.10.2025)
10. Hayman T. Open-Source Intelligence and the War in Ukraine // *INSS Insight*. – 2023. – No. 1678. – URL: https://arxiv.org/html/2508.03599v1
11. Høiby M. War and Military Journalism // In *The SAGE Encyclopedia of Journalism* (2nd ed.) // SAGE. – 2022. https://doi.org/10.4135/9781544391199.n434
12. Головне управління розвідки Міністерства оборони України. (2024–2025). *Офіційний Telegram-канал ГУР МО України.* – URL: https://t.me/DIUkraine (дата звернення: 30.10.2025)
13. Головне управління розвідки МО України. YouTube. – URL: https://www.youtube.com/@DI_Ukraine (дата звернення: 30.10.2025)
14. Даніленков Р. Чого українські медійники можуть навчити західних // Накипіло. – 09.07.2023. – URL: https://surl.li/xotpdr
15. "Інформація з відкритих джерел стала дієвим інструментом розвідки ворога", – речник Міноборони // Детектор медіа. – 06.11.2023. – URL: https://surl.li/tsarwp (дата звернення: 20.10.2025)
16. Leos D. *Thinking Like a Spy: How Open Source Intelligence Can Give You a Competitive Advantage* // Entrepreneur. – 2023. – URL: https://surl.lu/obeuqe (дата звернення: 20.10.2025)
17. Lomachinska I., & Lomachinskyi B. The role of media culture in today's information wars. // *Схід* (Skhid). – 2023. – № 3(3). https://doi.org/10.21847/1728-9343.2022.3(3).268297
18. Марків О. Інформаційно-психологічні операції: поняття, види, способи використання в умовах гібридної війни // Гібридна війна і журналістика. Проблеми інформаційної безпеки: навчальний посібник за заг.ред. В.О. Жадька. – 2018. – С. 229-245. – URL: https://enpuirb.udu.edu.ua/server/api/core/bitstreams/3bbce0bf-df9c-4f10-8f85-f2f5761b9ac4/content (дата звернення: 20.10.2025)
19. Мовлення під час війни – інтерв'ю з головою українських суспільних ЗМІ // Суспільне. Мовлення. – 22.10.2024. – URL: https://surl.li/pxucrb (дата звернення: 28.10.2025)
20. Морські дрони атакували базу ВМФ у Новоросійську, ймовірно, пошкоджений корабель // Укрінформ. – 04.08.2023. – URL: https://surl.li/lvvfee (дата звернення: 28.10.2025)
21. Олег Іващенко, Голова Служби зовнішньої розвідки України: Після завершення війни за 2-4 роки росія буде технічно готова до нової агресії – проти Європи // Служба зовнішньої розвідки. – 26.05.2025. – URL: https://surl.li/pgzyaz (дата звернення: 28.10.2025)

22. Teagan J. The Economics and Game Theory of OSINT Frontline Photography: Risk, Attention, and the Collective Dilemma // Researchgate. – 2025. – 8 Sep. https://doi.org/10.48550/arXiv.2509.10548
23. Ukraine may be using drones to amp up its counteroffensive. Here are some of the headlines you should know // CNN. – August 6. – 2023. URL: https://surl.li/jbldoh (дата звернення: 30.10.2025)
24. Schwartz L. *OSINT researchers went viral unpacking the war in Ukraine* // Rest of World. – 2022. – URL: https://restofworld.org/2022/osint-viral-ukraine/ (дата звернення: 28.10.2025)
25. Чернецька С. ЗМІ і війна: особливості поширення інформації та фото під часу воєнного стану // Платформа прав людини. – 2022. – URL: https://surl.li/apgwpc (дата звернення: 20.10.2025)
26. Chernysh V. Intelligence as an instrument of state power and its use in international politics // Kyiv-Mohyla Law and Politics Journal. – 2023. – № (8-9). – С. 59–84. https://doi.org/10.18523/kmlpj303156.2023-8-9.59-84

References

1. Alvarez, A. (2023). *The OSINT revolution: Empowering investigations through open source intelligence* (205 p.). https://surl.li/nxkgvo
2. Ataky droniv ta raket ukrainskykh syl na terytoriiu okupovanoho Krymu ta rosiiski korabli v Chornomu mori v sichni–hrudni 2023 roku (ohliad ta baza danykh) [Drone and missile attacks by Ukrainian forces on occupied Crimea and Russian ships in the Black Sea in January–December 2023 (review and database)]. (2024, January 15). *Black Sea News*. Retrieved October 28, 2025, from https://www.blackseanews.net/read/213072
3. Balmforth, T. (2023, August 4). Ukrainian drone disables Russian warship near Russia's Novorossiysk port. Retrieved October 28, 2025, from https://surli.cc/nphfjw
4. Barkar, D. (2025, September 12). Yak viiskovi komunikatsii OSUV i OTU vplyvaiut na novyny pro viinu v Ukraini [How military communications of OSUV and OTU affect war news in Ukraine]. *Instytut masovoi informatsii*. Retrieved October 28, 2025, from https://surl.lu/qpjzjz
5. Borysenko, Y. (2023). Information warfare in terms of communication theory: Attempted analysis. *Filosofska dumka, 4*, 21–38. https://doi.org/10.15407/fd2023.04.021
6. Velyki investytsii u khaos: analiz informatsiinoi viiny kremlia [Big investments in chaos: An analysis of the Kremlin's information warfare]. (2025, April 25). *Sluzhba zovnishnoi rozvidky*. Retrieved October 28, 2025, from https://surl.li/qugqcq
7. Volz, D. (2022, July 27). New group to promote open-source intelligence, seen as vital in Ukraine war. *The Wall Street Journal*. Retrieved October 20, 2025, from https://surl.li/soyyya
8. Voienna rozvidka Ukrainy (vlasnyk: Holovne upravlinnia rozvidky MO) [Military Intelligence of Ukraine (owner: Defence Intelligence of Ukraine)]. (n.d.). *YouTube*. Retrieved October 30, 2025, from https://surl.li/fyqpbs
9. What is OSINT: Open-source intelligence? (2022, May 2). *European Union Data*. Retrieved October 28, 2025, from https://surl.li/hrcrts
10. Hayman, T. (2023). Open-source intelligence and the war in Ukraine. *INSS Insight, 1678*. Retrieved from https://arxiv.org/html/2508.03599v1
11. Høiby, M. (2022). War and military journalism. In *The SAGE Encyclopedia of Journalism* (2nd ed.). https://doi.org/10.4135/9781544391199.n434
12. Holovne upravlinnia rozvidky Ministerstva oborony Ukrainy. (2024–2025). Ofitsiinyi Telegram-kanal HUR MO Ukrainy [Official Telegram channel of the Defence Intelligence of Ukraine]. Retrieved October 30, 2025, from https://t.me/DIUkraine
13. Holovne upravlinnia rozvidky MO Ukrainy. (n.d.). YouTube-kanal [YouTube channel]. *YouTube*. Retrieved October 30, 2025, from https://www.youtube.com/@DI_Ukraine

14. Danilenkov, R. (2023, July 9). Choho ukrainski mediinyky mozhut navchyty zakhidnykh [What Ukrainian media professionals can teach the West]. *Nakipilo*. Retrieved from https://surl.li/xotpdr
15. "Informatsiia z vidkrytykh dzherel stala diievym instrumentom rozvidky voroha," – rechnyk Ministerstva oborony ["Open-source information has become an effective tool of the enemy's intelligence," said the Ministry of Defense spokesperson]. (2023, November 6). *Detektor media*. Retrieved October 20, 2025, from https://surl.li/tsarwp
16. Leos, D. (2023). Thinking like a spy: How open source intelligence can give you a competitive advantage. *Entrepreneur*. Retrieved October 20, 2025, from https://surl.lu/obeuqe
17. Lomachinska, I., & Lomachinskyi, B. (2023). The role of media culture in today's information wars. *Skhid, 3(3)*. https://doi.org/10.21847/1728-9343.2022.3(3).268297
18. Markiv, O. (2018). Informatsiino-psykholohichni operatsii: poniattia, vydy, sposoby vykorystannia v umovakh hibrydnoi viiny [Information-psychological operations: Concepts, types, and methods of use in hybrid war]. In V. O. Zhadko (Ed.), *Hibrydna viina i zhurnalistyka. Problemy informatsiinoi bezpeky* [Hybrid war and journalism. Problems of information security] (pp. 229–245). Retrieved October 20, 2025, from https://enpuirb.udu.edu.ua/server/api/core/bitstreams/3bbce0bf-df9c-4f10-8f85-f2f5761b9ac4/content
19. Movlennia pid chas viiny – interviu z holovoiu ukrainskykh suspilnykh ZMI [Broadcasting during the war – An interview with the head of Ukraine's public media]. (2024, October 22). *Suspilne. Movlennia*. Retrieved October 28, 2025, from https://surl.li/pxucrb
20. Morski drony atakuvaly bazu VMF u Novorosiisku, ymovirno, poshkodzhenyi korabel [Sea drones attacked the Russian Navy base in Novorossiysk; a ship was likely damaged]. (2023, August 4). *Ukrinform*. Retrieved October 28, 2025, from https://surl.li/lvvfee
21. Oleh Ivashchenko, Holova Sluzhby zovnishnoi rozvidky Ukrainy: Pislia zavershennia viiny za 2–4 roky rosiia bude tekhnichno hotova do novoi ahresii – proty Yevropy [Oleh Ivashchenko, Head of the Foreign Intelligence Service of Ukraine: 2–4 years after the war ends, Russia will be technically ready for new aggression against Europe]. (2025, May 26). *Sluzhba zovnishnoi rozvidky*. Retrieved October 28, 2025, from https://surl.li/pgzyaz
22. Teagan, J. (2025, September 8). The economics and game theory of OSINT frontline photography: Risk, attention, and the collective dilemma. https://doi.org/10.48550/arXiv.2509.10548
23. Ukraine may be using drones to amp up its counteroffensive. Here are some of the headlines you should know. (2023, August 6). *CNN*. Retrieved October 30, 2025, from https://surl.li/jbldoh
24. Schwartz, L. (2022). OSINT researchers went viral unpacking the war in Ukraine. *Rest of World*. Retrieved October 28, 2025, from https://restofworld.org/2022/osint-viral-ukraine/
25. Chernetska, S. [Chernetska, S.]. (2022). ZMI i viina: osoblyvosti poshyrennia informatsii ta foto pid chasu voiennoho stanu [Media and war: Features of disseminating information and photos during martial law]. *Platforma prav liudyny*. Retrieved October 20, 2025, from https://surl.li/apgwpc
26. Chernysh, V. (2023). Intelligence as an instrument of state power and its use in international politics. *Kyiv-Mohyla Law and Politics Journal, 8–9*, 59–84. https://doi.org/10.18523/kmlpj303156.2023-8-9.59-84