МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

«КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

ФАКУЛЬТЕТ СОЦІАЛЬНИХ НАУК І СОЦІАЛЬНИХ ТЕХНОЛОГІЙ

КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН

КВАЛІФІКАЦІЙНА РОБОТА

освітній рівень – бакалавр

на тему: **«РОЗВІДКА ВІДКРИТИХ ДЖЕРЕЛ У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ З 2022 ПО 2023 РОКИ»**

Виконала:
студентка 4 року навчання
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»
Артеменко Олександра Олександрівна

Керівник:
Осадчук Роман Юрійович
старший викладач
кафедри міжнародних відносин

КИЇВ – 2025

ЗМІСТ

ВСТУП……....3

РОЗДІЛ І. ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ РОЗВІДКИ ВІДКРИТИХ ДЖЕРЕЛ У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ……....10

1.1. Теоретичні засади OSINT……..…10
1.2. Методологічні підходи до дослідження OSINT у воєнних студіях……..……..…14
1.3. Методологічні виклики OSINT у контексті війни……...18

РОЗДІЛ ІІ. ВИКОРИСТАННЯ OSINT ПІД ЧАС ХАРКІВСЬКОЇ ТА ХЕРСОНСЬКОЇ КАМПАНІЙ……..…22

2.1. Використання розвідки відкритих джерел у підготовці та реалізації контрнаступу під час Харківської операції……....22
2.2. Використання розвідки відкритих джерел у підготовці та реалізації контрнаступу під час Херсонської операції……..…….……26
2.3. Оперативно-стратегічні наслідки контрнаступів на Харківському та Херсонському напрямках……..……..32

РОЗДІЛ ІІІ. РОЗВІДКА ВІДКРИТИХ ДЖЕРЕЛ У НАНЕСЕННІ УДАРІВ ПО РОСІЙСЬКИХ ОБ'ЄКТАХ НА ТИМЧАСОВО ОКУПОВАНИХ ТЕРИТОРІЯХ ТА ТЕРИТОРІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ……..……38

3.1. Використання відкритих джерел для оперативного виявлення позицій противника……..…….…….38
3.2. Верифікація результатів вогневого ураження із застосуванням супутникових знімків та аеророзвідки……..……..….42
3.3 Зміна тактичних підходів російських військ під впливом OSINT……..……46

ВИСНОВКИ……..……....54

ДОДАТКИ……..……..…….57

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……..……....64

АНОТАЦІЯ……..……..70

ВСТУП

Актуальність теми дослідження. Переосмислення використання інформації в умовах сучасної війни є одним із викликів для безпекових студій, воєнної аналітики та державного управління. У XXI столітті війна втратила монополію на поле бою як простір виключно фізичного протистояння. Вона набуває характеристик багатовимірного явища, у якому перевага дедалі частіше визначається не кількістю озброєння чи техніки, а швидкістю отримання, обробки та інтерпретації інформації. В цих умовах особливу актуальність здобуває розвідка відкритих джерел (OSINT), яка не лише змінює характер воєнної розвідки, а й відкриває нові способи розуміння і ведення війни як такої.

З початком повномасштабного вторгнення Росії в Україну у 2022 році OSINT перетворився із вторинного інструменту підтримки аналітики на повноцінний засіб отримання критично важливих розвідувальних даних. Особливо це стало помітно під час контрнаступальних операцій Збройних сил України, коли відкриті джерела стали джерелом оперативної, візуалізованої, географічно прив'язаної інформації. Здатність швидко виявляти переміщення техніки, наявність або відсутність оборонних позицій, фіксувати моральний стан противника чи оцінювати наслідки ударів у режимі майже реального часу надала українській стороні ситуаційну обізнаність. Саме тому необхідність осмислення OSINT як нового стратегічного ресурсу набуває виняткової важливості.

Актуальність дослідження полягає в тому, що розвідка відкритих джерел уже зараз несе на собі подвійне навантаження – як інструмент впливу на тактичному рівні, забезпечуючи точність ударів та своєчасність реагування, так і механізм стратегічного інформаційного впливу, зокрема через формування доказової бази воєнних злочинів, демонстрацію перебігу бойових дій для міжнародної аудиторії, спростування дезінформації та забезпечення інформаційної ініціативи. Водночас, незважаючи на її широку емпіричну присутність у практиці сучасної війни, OSINT досі залишається концептуально не до кінця осмисленим явищем: відсутня

стабілізована теоретична база, існують суперечності у підходах до верифікації джерел, а її правовий та інституційний статус залишається неповноцінно закріпленим.

Дослідження, присвячене аналізу використання OSINT у російсько-українській війні, є також актуальним у контексті глобальних змін у сфері розвідки. Традиційна розвідка, що спиралася на закриті дані, вертикальні структури, централізований контроль та закритий доступ, дедалі частіше стикається з конкуренцією з боку відкритих аналітичних мереж, волонтерських спільнот, журналістських ініціатив та технологічних рішень на основі відкритих джерел. Саме тому OSINT стає не лише альтернативою, а потенційною моделлю майбутньої розвідки, яка базується на інтероперабельності, децентралізації, швидкості та масовості. Український досвід, що виник у надзвичайних обставинах, демонструє практику органічного поєднання військових структур з цивільними OSINT-групами, що може стати основою для майбутніх моделей воєнної інтеграції розвідки відкритих джерел.

Окрім практичного значення, тема дослідження має і аналітичне наповнення, адже дозволяє по-новому подивитися на поняття воєнного простору, темпів операцій, ухвалення рішень, а також на розмиття меж між фронтом і тилом, між професійною та аматорською розвідкою. У майбутньому OSINT матиме вплив не лише на воєнні конфлікти, але й на такі сфери, як кризовий моніторинг, інформаційна безпека, дипломатія, цифровий суверенітет, а також формування політичної відповідальності в умовах цифрової прозорості.

Таким чином, актуальність дослідження обумовлена не тільки значенням OSINT у рамках поточної війни, а й ширшими трансформаціями у структурі сучасної війни, в еволюції розвідувальних практик та у формуванні нових способів розуміння конфлікту як складного, інформаційно насиченого і технічно обумовленого явища. Це дослідження є спробою не лише описати, як OSINT

працює, але й проаналізувати, чому і в який спосіб він стає необхідним, і що це означає для майбутнього національної та глобальної безпеки.

Проблематика дослідження. У контексті повномасштабної війни між Росією та Україною з 2022 року спостерігається зростання ролі розвідки відкритих джерел (OSINT) як інструменту збору, верифікації та аналізу інформації, що безпосередньо впливає на хід бойових дій, прийняття рішень і стратегічне планування. Попри очевидну ефективність численних кейсів OSINT-розвідки, залишається невирішеною низка проблем: відсутність систематичного наукового узагальнення впливу OSINT на хід воєнних операцій, нечіткість механізмів інтеграції відкритої розвідки в офіційні військові структури, загроза дезінформації, а також правові та етичні дилеми, пов'язані з використанням відкритих даних у військовому конфлікті. Унаслідок цього постає необхідність наукового аналізу OSINT не лише як технічного чи інформаційного інструменту, а як явища, що трансформує саму природу сучасної війни.

Мета: з'ясувати як розвідка відкритих даних використовувалася для прогнозування та перебігу бойових дій під час повномасштабного вторгнення Росії в Україну з 2022 по 2023 роки.

Дослідницьке питання, яке буде розкрите у роботі: яким чином розвідка відкритих джерел використовувалася у бойових діях у контексті російсько-української війни у період з 2022 по 2023 роки та як вона трансформує сучасні підходи до воєнного планування, тактики і стратегічних рішень.

Завдання дослідження: 1) виокремити основні теоретичні засади, на яких базується поняття розвідки відкритих джерел (OSINT), для з'ясування її ролі у російсько-українській війні; 2) описати методологічні підходи до аналізу OSINT у рамках воєнних студій з метою формування наукової бази для емпіричного аналізу; 3) з'ясувати ключові методологічні виклики, пов'язані з використанням OSINT в

умовах війни, включно з проблемами верифікації, достовірності та етичності джерел; 4) виявити особливості та характер застосування OSINT у підготовці та реалізації контрнаступальних дій під час Харківської та Херсонської кампаній 2022 року; 5) обґрунтувати оперативно-стратегічні наслідки контрнаступів на Харківському та Херсонському напрямках у зв'язку з використанням відкритих розвідувальних даних; 6) обґрунтувати значення OSINT у процесі виявлення позицій противника на тимчасово окупованих територіях та території Російської Федерації; 7) описати механізми верифікації результатів вогневого ураження за допомогою супутникових знімків і аеророзвідки для оцінки ефективності ударів та проаналізувати підтверджені кейси успішних ударів, здійснених за допомогою OSINT, для виявлення типових сценаріїв його ефективного використання; 8) з'ясувати вплив розвідки відкритих джерел на зміну тактичних підходів російських військ, зокрема в аспектах мобільності, маскування та дезінформації.

Об'єктом дослідження є розвідка відкритих джерел (OSINT).

Предметом дослідження є спосіб використання, динаміка та вплив розвідки відкритих даних у російсько-українській війні з 2022 по 2023 роки.

Характеристика джерел. Це дослідження ґрунтується на широкій міждисциплінарній вибірці літератури — від академічних праць і історичних оглядів, присвячених розвідці, до сучасних звітів про OSINT і первинних джерел інформації з безпосередньо бойових дій. У її центрі знаходиться поняття відкритої розвідки, яке визначається в наукових і політичних джерелах, де OSINT розглядається як сукупність усієї публічно доступної інформації, що може бути використана для розвідувальних цілей. Оскільки OSINT у своєму сучасному вигляді є відносно новим явищем, особливо в контексті цієї війни, робота значною мірою спирається на актуальні аналітичні матеріали провідних аналітичних та розвідувальних центрів, та експертів, які безпосередньо працюють із війною Росії проти України.

Використана література охоплює: (а) базові дефініції та теорію розвідки; (б) аналітику експертів і think-tank-центрів, що визначають значущість OSINT у війні 2022–2023 років; (в) звіти OSINT-спільнот і case-study, які забезпечують емпіричні приклади та дані. Така різноманітність виправдана міждисциплінарною природою теми — жоден тип джерела сам по собі не охоплює повного спектра досліджуваного явища. Завдяки поєднанню наукових підходів і практичного OSINT-досвіду, ця робота формує цілісне уявлення, яке ґрунтується як на теорії, так і на емпіричній основі. Обрана література безпосередньо стосується дослідницького питання, висвітлюючи те, що вже відомо, що є предметом дискусії та що залишається незрозумілим у контексті розвідки відкритих даних у російсько-українській війні.

Методологія дослідження. Дослідження виконано в межах якісної методологічної парадигми з опорою на case-study, доповненої аналітичними підходами з галузі розвідки та медіааналізу. Вибір методології зумовлений характером дослідницького питання, що вимагає глибокого розуміння подій і процесів (а не лише кількісного тестування гіпотез) та поєднання різноманітних джерел інформації.

Робота використовує підхід case-study — як такого виступає війна 2022-2023 років. Це дозволяє здійснити ґрунтовний контекстуальний аналіз розвідки відкритих даних. Оскільки війна триває, обрано описово-пояснювальний дизайн: спочатку описується, як OSINT використовувалася протягом перших двох років війни, а потім пояснюються наслідки цих спостережень. Методологічна парадигма є переважно інтерпретативістською, оскільки визнає складність соціальних явищ, таких як інформаційні потоки у воєнний час. Водночас дослідження використовує елементи історичного наративу, простежуючи хронологію подій 2022-2023 років для фіксації еволюції ролі OSINT, та елементи порівняльного аналізу, наприклад,

зіставлення висновків OSINT з офіційними версіями подій або порівняння застосування OSINT на різних етапах війни.

Важливим емпіричним компонентом дослідження стали напівструктуровані інтерв'ю, проведені з військовослужбовцями Збройних Сил України, які безпосередньо брали участь у Харківській та Херсонській операціях. Ці інтерв'ю надали змогу розкрити особливості використання OSINT на тактичному рівні, окреслити типи застосовуваних інструментів, практики верифікації даних, вплив відкритих джерел на оперативні рішення, а також з'ясувати ставлення військового командування до інструмента. Імена, посади та місця служби респондентів не розголошуються з міркувань безпеки, а всі свідчення використано на основі усної згоди та з дотриманням етичних стандартів дослідницької діяльності. Інтерв'ю подано у формі транскриптів у додатках до роботи та використані для аналітичних висновків.

Методологія передбачає розширений аналіз документів і контенту. Джерелами даних є: звіти з OSINT-розслідувань, матеріали з соцмереж, супутникові знімки та мапи, військові зведення (які перехресно верифіковані з відкритими даними), а також вторинна аналітика. Усі ці джерела є відкритими, що відповідає предмету дослідження. У деяких випадках особисто застосована техніка перевірки OSINT до ключових свідчень, щоб глибше зрозуміти методологію — наприклад, геолокація відео або аналіз супутникового знімку за часовими мітками (хронолокація).

Враховуючи ризик дезінформації у відкритих джерелах, методологія дослідження робить наголос на триангуляції — підтвердженні фактів за допомогою кількох незалежних джерел. Наприклад, якщо відео у соцмережі стверджує про певну подію, проводиться перевірка за супутниковими знімками або повідомленнями інших очевидців. Такий підхід узгоджується з експертними рекомендаціями, згідно з якими OSINT має бути «тріангулярно співвіднесений із

традиційною розвідкою та інтерпретований у взаємозв’язку з нею» для забезпечення достовірності. Хоча ця робота не має доступу до засекреченої інформації, вона використовує надійні звіти й за можливості — свідчення очевидців як альтернативу для перехресної перевірки. Порівняння різних типів доказів дозволяє дослідженню підвищити рівень обґрунтованості висновків щодо ролі OSINT, базуючись лише на перевірених фактах.

Структура кваліфікаційної (бакалаврської) роботи. Бакалаврська робота складається зі вступу, трьох розділів, висновків, списку джерел, додатків і анотації. Загальний обсяг роботи - 72 сторінки. Перелік використаних джерел включає 46 найменувань.

РОЗДІЛ І. ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ РОЗВІДКИ ВІДКРИТИХ ДЖЕРЕЛ У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ

1.1. Теоретичні засади OSINT

Відкриту розвідку (Open-Source Intelligence, OSINT) зазвичай визначають як розвідувальну інформацію, отриману з відкритих або загальнодоступних джерел. У доктрині Розвідувального співтовариства США OSINT описується як «розвідка, що створюється на основі загальнодоступної інформації, яка збирається, опрацьовується та поширюється своєчасно та у відповідній формі для задоволення конкретних розвідувальних потреб». Подібним чином НАТО визначає OSINT як розвідку, що ґрунтується на відкритій та некласифікованій інформації з обмеженим розповсюдженням. [1] Інакше кажучи, OSINT — це процес збору та аналізу даних із відкритих джерел (таких як новинні ресурси, публічні звіти, наукові публікації, соціальні мережі, супутникові знімки тощо) для отримання розвідувальних висновків, придатних до практичного використання. Це відрізняє її від класифікованої (традиційної) розвідки, хоча вона все одно вимагає ретельної обробки та валідації, щоб перетворити «сирі» дані на аналітичний продукт. OSINT — це не лише сукупність даних, а результат застосування аналітичного ремесла до відкритої інформації з метою відповіді на конкретні запити. У науковому розумінні OSINT можна розглядати як практику або процес збору й перевірки відкритої інформації для задоволення чітко окреслених інформаційних потреб. [2]

У межах ширшої дисципліни розвідки OSINT нині визнається одним з основних напрямів (так званих «INTів») поряд з традиційними дисциплінами, як-от HUMINT (розвідка з людських джерел), SIGINT (розвідка з перехоплення комунікацій), IMINT або GEOINT (розвідка на основі супутникових чи аерофотознімків). [3] Історично розвідувальні установи часто розглядали OSINT як вторинне або допоміжне джерело інформації — інструмент для заповнення прогалин, які не

покривали секретні джерела, а не як самостійну розвідувальну дисципліну. Наприклад, у США OSINT тривалий час розглядалася лише як додаток до класифікованих засобів збору, що «зводило її до допоміжного елементу» і гальмувало її розвиток як повноцінного напряму аналітики. Проте така позиція поступово змінюється. Сучасний підхід визнає OSINT як окрему дисципліну з власними методами, розвідниками та аналітичною цінністю. OSINT «проникає в усі інші напрями», адже відкрита інформація може доповнювати й контекстуалізувати HUMINT, SIGINT [2] та інші типи розвідки, слугуючи фундаментом для всебічного аналізу. Підвищення статусу OSINT відображено в офіційних стратегічних документах: зокрема, Стратегія OSINT Директора національної розвідки США на 2024–2026 роки та Об'єднана доктрина НАТО визнають OSINT як незамінну складову розвідувальної діяльності, а не просто бажаний додаток. Таким чином, OSINT сьогодні функціонує на рівні з іншими напрямами розвідки, надаючи низку переваг — зокрема швидкість доступу та можливість обміну (оскільки відкриту розвідку можна легше передавати партнерам і громадськості без загрози викриття джерел). [4]

Хоча термін «OSINT» увійшов до професійного вжитку порівняно нещодавно (в кінці XX століття), використання відкритих джерел у розвідці має історичне коріння. В епоху Відродження такі держави, як Венеція, систематично збирали відкриту інформацію (наприклад, через інформаційні бюлетені або закордонні газетні зведення) для формування державної політики. [2] Поява масової друкованої преси у XIX столітті створила критичну масу доступної інформації (газети, журнали, технічні звіти) яку військові та дипломатичні служби почали активно аналізувати для отримання знань про потенційних противників. [2] Формалізація концепції «відкритої розвідки» як окремої категорії датується кінцем 1980-х років. Колишній офіцер ЦРУ Роберт Девід Стіл вважається одним із перших, хто публічно ввів термін OSINT і вже в 1990-х роках закликав розвідувальне співтовариство активніше використовувати відкриті джерела. [2] У той самий період науковці в сфері розвідки, як-от Марк Ловенталь, також піднімали питання

інтеграції відкритих матеріалів до аналітичної роботи. Важливою віхою також стало видання «OSINT Handbook» НАТО у 2001 році, де були систематизовані принципи використання відкритих джерел у військовій розвідці. З появою Інтернету й епохи Web 2.0 можливості OSINT значно зросли. Уже в середині 1990-х років поширення онлайн-даних і поява спільноти цифрових дослідників започаткували так зване «друге покоління OSINT», для якого характерне використання контенту, створеного користувачами, на веб-платформах. У 2018 році Вільямс і Блюм (RAND) [5] описали це як парадигмальний зсув, коли дані з соціальних мереж, форумів та інших інтерактивних ресурсів стали не менш важливими, ніж традиційні новинні джерела. Протягом 2000-2010-х років було накопичено великий обсяг прикладних знань, включно з підручниками (наприклад, Майкла Баззела) та професійними тренінгами з OSINT, що сприяло становленню аналітичного ремесла у сфері відкритої розвідки. [2] Професійні та волонтерські спільноти (включаючи державні органи, журналістів, академічні кола й НУО) сформувалися навколо практик OSINT, обмінюючись інструментами й методиками. Інституціоналізація відбулася через створення таких організацій, як Open Source Enterprise (у межах ЦРУ), а також недержавних структур на кшталт OSINT Foundation — професійної спілки дослідників. Сьогодні OSINT є водночас офіційною дисципліною з власною доктриною та неформальною глобальною спільнотою аналітиків. [2]

У контексті сучасних конфліктів і гібридної війни OSINT також відіграє значну роль. Під гібридною війною розуміють конфлікти, у яких традиційні військові дії поєднуються з кібероперaціями, інформаційно-психологічним впливом та кампаніями з дезінформації й пропаганди. Сучасні війни точаться не лише на полі бою, але й у інформаційному просторі — саме тут відкривається як потенціал, так і загрози для OSINT. З одного боку, OSINT забезпечує прозорість і оперативне розуміння ситуації в зоні конфлікту; з іншого — противник може навмисне маніпулювати відкритими джерелами для введення в оману або дезорієнтації. Російсько-українська війна (з 2014 року-дотепер) часто розглядається як зразковий

приклад гібридної війни, в якій Росія активно застосовує методи «інформаційного протиборства» — пропаганду, фейкові новини, кібератаки — паралельно з бойовими діями. [6] У відповідь на ці дії OSINT став контрзасобом, який дозволяє у реальному часі викривати факти і спростовувати брехню.

Під час повномасштабного вторгнення Росії в Україну у 2022 році OSINT вийшов у мейнстрим: журналісти, аналітики та навіть широке коло громадськості звернулися до відкритих джерел (соціальних мереж, супутникових знімків, вебкамер, авіатрекерів), щоб відстежувати пересування військ і події на місцях. Подібна динаміка спостерігалася і в попередніх збройних конфліктах. Наприклад, під час війни в Сирії (з 2011 року) незалежні аналітики та організації використовували OSINT для документування подій, таких як хімічні атаки та порушення прав людини, коли доступ до зони конфлікту був обмежений. [7]

Еліот Гіґґінс, який згодом заснував Bellingcat, почав свою діяльність із аналізу відео із Сирії у своєму блозі «Brown Moses», де за допомогою зіставлення відеозаписів із відкритих джерел і каталогів озброєнь ідентифікував застосування касетних боєприпасів та хімічної зброї. Таке розслідування на основі відкритих джерел дозволило зібрати докази військових злочинів, які режим міг би заперечувати або приховати. [8]

Ряд резонансних кейсів демонструє зростаючу легітимність OSINT як інструменту війни та розслідувань. Один із прикладів — розслідування катастрофи рейсу MH17 авіакомпанії Malaysia Airlines, збитого над Сходом України у липні 2014 року. Незалежне об’єднання дослідників OSINT на чолі з журналістською групою Bellingcat зібрало докази із відкритих джерел (пости в соцмережах, фото/відео від місцевих жителів, переміщення техніки) й відстежило протиповітряний ракетний комплекс, залучений до атаки. Згідно з їхнім висновком, це була установка «Бук» із 53-ї зенітно-ракетної бригади ЗС РФ, доставлена на підконтрольну бойовикам територію України. [6] Подібний приклад відкритої

розвідки, яку пізніше підтвердили офіційні слідства, закріпила сприйняття OSINT як легітимної форми цифрового розслідування, показавши, що навіть волонтери можуть на основі публічних даних розкрити складну міжнародну справу, яку паралельно розслідували урядові інституції.

Отже, теоретична основа OSINT полягає в його визначенні як форми розвідки, у визнаному місці серед інших розвідувальних дисциплін, у його еволюції як сформованої практики та в доведеній релевантності до гібридних конфліктів сучасності. До основних суб'єктів розвитку теорії та практики OSINT належать як державні структури (наприклад, Open Source Enterprise у складі ЦРУ, доктрини НАТО), так і аналітичні центри (зокрема RAND), а також розслідувальні організації на кшталт Digital Forensic Research Lab та академічні дослідники, які розширюють уявлення про можливості відкритої розвідки. Це поєднання підходів свідчить, що OSINT — це не лише практична діяльність з усталеними методами й професійною спільнотою, а й нова наукова галузь у сфері розвідки та безпеки.

1.2. Методологічні підходи до дослідження OSINT у воєнних студіях

Вивчення OSINT у контексті війни (зокрема російсько-української) передбачає розгляд самої відкритої розвідки не лише як інструменту збору даних, а як явища, що підлягає аналізу. Тобто дослідницька увага має бути зосереджена на тому, як здійснюється OSINT, якими є його впливи та виклики в умовах війни. Як об'єкт наукового аналізу OSINT можна досліджувати з різних перспектив: наприклад, вивчати його роль у формуванні наративів конфлікту, механізми створення та верифікації розвідувальних висновків або ефективність OSINT у порівнянні з традиційною розвідкою в умовах війни. Такі дослідження ґрунтуються на теоретичній базі, що включає визначення понять і контекст.

У методологічному плані дослідники часто застосовують якісні, порівняльні та кейс-стаді підходи для відтворення OSINT-практик у воєнних умовах. Якісний

підхід є доречним, оскільки багато аспектів OSINT (процеси ухвалення рішень аналітиками, методи перевірки, взаємодія в спільнотах) краще вивчаються через описовий аналіз, а не через кількісні вимірювання. Наприклад, дослідження може включати інтерв'ю з офіцерами військової розвідки щодо методів перевірки інформації про ракетний удар чи етнографічне дослідження онлайн-спільноти OSINT, яка відстежує хід війни. Також може застосовуватись якісний аналіз вмісту – наприклад, аналіз звітів для виявлення поширених методів та труднощів.

Метод кейс-стаді дозволяє детально проаналізувати OSINT у російсько-українській війні як єдиний складний випадок — іноді в межах порівняльної рамки. Дослідник може обрати, скажімо, битву за Київ у 2022 році або анексію Криму у 2014 році як кейс для демонстрації ролі OSINT, прослідкувавши, як аналітики на основі відкритих джерел реконструювали події. Такі кейси дають змогу простежити причинно-наслідкові зв'язки (наприклад, чи вплинули розслідування OSINT на міжнародну реакцію) й інтегрувати кілька типів джерел (медійні звіти, продукти OSINT, офіційні заяви) для триангуляції.

Порівняльний підхід можна застосувати як у межах однієї війни (наприклад, порівнюючи використання OSINT українськими та російськими активістами або OSINT у 2014 році й у 2022 році), так і між конфліктами (наприклад, зіставлення OSINT у війні в Україні та під час подій у Сирії чи Косово 1999 року). Таке порівняння дає змогу виявити, які аспекти OSINT є контекстно специфічними, а які — універсальними. Наприклад, зіставлення OSINT-розслідувань щодо хімічних атак у Сирії та ймовірного застосування хімічної зброї в Україні виявляє відмінності в доступності джерел або складності перевірки, що поглиблює розуміння методології OSINT. Можна сказати, що якісні, порівняльні й кейс-стаді підходи дозволяють охопити як глибину, так і широту дослідження OSINT — перші забезпечують глибину, другі — широту й базу для загальніших висновків.

Для вивчення OSINT у контексті війни необхідно розуміти також методи, які практики OSINT зазвичай застосовують для збору й перевірки інформації. Ці техніки становлять своєрідний методологічний інструментарій OSINT, і дослідники мають чітко їх визначити, так і, за можливості, опанувати для проведення ґрунтовного аналізу. Основні методи OSINT у воєнному контексті включають:

Геолокація — це визначення місця зйомки фото чи відео шляхом аналізу зображення та його порівняння з географічними даними (мапи, супутникові знімки, орієнтири). Аналітики OSINT ретельно вивчають візуальні підказки в контенті користувачів — обриси місцевості, рельєф, дорожню сітку, знаки, особливості ландшафту — і зіставляють їх із Google Earth або іншими картографічними інструментами. Класичним прикладом є ідентифікація захопленого міста в Лівії під час громадянської війни 2011 року за мечеттю з характерним куполом і мінаретом, яку знайшли на супутникових знімках. [7] Аналогічно, у війні в Україні геолокація була ключовою: зокрема, після удару по нафтобазі в Бєлгороді у 2022 році аналітики підтвердили місце події, зіставивши об’єкти на відео зі знімками Google Street View. [8] Точне встановлення місця події дозволяє підтвердити достовірність бойових зведень і спростовувати дезінформацію щодо місця інциденту.

Хронолокація — це встановлення часу зйомки фото або відео. У воєнних розслідуваннях вона є важливою для перевірки відповідності між медіа та заявленими подіями (наприклад, знімок, що подається як «з учорашнього бою», може бути старим). Для цього аналізують тіні, положення Сонця (яке дозволяє встановити дату та час), метадані файлів, погодні умови на відео. Поширеним методом є «аналіз тіней» — визначення довжини й кута тіні з подальшим порівнянням із астрономічними даними. [8] У війні в Україні хронолокація дозволяє верифікувати хронологію атак, підтверджуючи заявлені послідовності подій. Геолокація та хронолокація разом забезпечують просторово-часову

перевірку контенту, прив’язуючи кожен фрагмент до конкретного місця й часу — що є одним з принципів академічного аналізу OSINT. [6]

Зворотний пошук зображень — ця техніка передбачає використання пошукових систем (Google Images, TinEye, Yandex) для виявлення інших випадків публікації зображення. Зворотний пошук дозволяє виявити повторно використані або хибно приписані зображення, що є частою проблемою у воєнній дезінформації. Наприклад, ефектне фото вибуху може видаватись за результат ракетного удару 2023 року в Україні, хоча насправді воно було зроблене кілька років тому в Сирії. Зворотний пошук допомагає встановити походження зображення та виявити фальсифікації. Його активно застосовують навіть правозахисні організації — як-от Digital Verification Corps Amnesty International. [8] У наукових дослідженнях документування зворотного пошуку демонструє механізми виявлення дезінформації та зміцнює довіру до візуальних доказів.

Аналіз метаданих — цифрові файли (зображення, відео, документи) часто містять приховані технічні дані, відомі як метадані. Наприклад, EXIF-метадані зображень можуть містити час створення, модель камери, GPS-координати. Аналітики використовують метадані для пошуку доказів: зокрема, фото, зроблене військовослужбовцем, може випадково містити координати його підрозділу. Утім, більшість соцмереж видаляють метадані, а противники можуть їх фальсифікувати. Аналіз метаданих поширюється також на документи (історія редагування, авторство) та мережеву інформацію (наприклад, реєстрацію доменів сайтів). У війні Росії проти України цей метод застосовувався для перевірки автентичності злитих документів і встановлення походження електронних листів у рамках інформаційних операцій.

1.3. Методологічні виклики OSINT у контексті війни

Хоча OSINT забезпечує корисні інструменти для збору інформації у воєнних дослідженнях, ця методологія супроводжується низкою викликів. Науковці мають зважати на них як при безпосередньому застосуванні OSINT, так і при оцінюванні його надійності як джерела.

Забезпечення точності та автентичності інформації з відкритих джерел — постійний виклик для дослідників. Оскільки OSINT базується на неофіційних і нерідко неперевірених джерелах, існує високий ризик поширення хибної або маніпулятивної інформації. Тому верифікація — це центральний елемент процесу OSINT: кожне твердження має перевірятись шляхом крос-перевірки за допомогою кількох джерел чи методів. Це може включати геолокацію відео, хронологічну перевірку, з'ясування, чи не є відео застарілим, а також пошук свідчень очевидців чи згадок у ЗМІ. Такий процес вимагає значного часу та експертного підходу. Без належної перевірки OSINT ризикує стати інструментом поширення ворожої пропаганди. Експерти, які використовують OSINT-дані (наприклад, базу соціальних повідомлень про авіаудари), мають або самостійно впроваджувати перевірку, або спиратися на дані, верифіковані авторитетними OSINT-групами. [8]

Зворотним боком широкої доступності відкритих джерел є надмірність інформації. Сучасні війни генерують гігантські масиви даних — від тисяч твітів і телеграм-постів щодня до безперервних потоків відео та супутникових знімків. Наприклад, у перші місяці вторгнення Росії в Україну у 2022 році з'явилася значна кількість візуального контенту з поля бою — значно більше, ніж могла оперативно опрацювати будь-яка команда аналітиків. Через це складно відрізнити справді важливу розвідувальну інформацію від «інформаційного шуму». Така ситуація також створює ризики перевантаження й вигорання для аналітиків. [8] Аналітики часто змушені застосовувати стратегії вибірки або зосереджуватися на конкретних наборах інцидентів для зменшення обсягу аналізу. У цьому дедалі активніше

використовуються інструменти з області аналізу даних — класифікатори на основі машинного навчання, мережевий аналіз. Вони допомагають, наприклад, автоматично ідентифікувати ймовірні відео бойових дій або згрупувати повідомлення за місцем події. Утім, людське судження залишається незамінним. У дослідженнях OSINT в межах воєнних студій науковці мають чітко описувати, як саме вони працювали з великими потоками даних (наприклад, за якими критеріями включали або виключали соціальні повідомлення з аналізу). Така прозорість в обробці інформації підвищує довіру до результатів дослідження.

Дослідження OSINT неминуче стикається з етичними дилемами, особливо в умовах війни. Одне з ключових питань — це конфіденційність і згода: публічне розміщення інформації не завжди означає, що її можна вільно використовувати. Дослідник може натрапити на персональні дані жертв або військових, відео зі сценами насильства. Етична практика в OSINT передбачає мінімізацію шкоди — наприклад, розмиття облич уразливих осіб на зображеннях або обережне поводження з графічним контентом. Інша етична загроза — безпека джерел: поширення певного допису з зони бойових дій може наражати автора на небезпеку. [8]

У війні принаймні одна зі сторін (а часто кілька) цілеспрямовано поширює дезінформацію — неправдиву або маніпулятивну інформацію. Це пряма загроза для OSINT, оскільки саме відкриті джерела можуть бути «заражені» фейками або пропагандою. [6] Наприклад, російська інформаційна війна проти України включає постановочні відео, фейкові акаунти, відредаговані фото — усе це спрямоване на дезорієнтацію аудиторії та нав’язування хибних наративів. Аналітики мають постійно виявляти фальсифікації. Яскравий приклад — поява «діпфейків», у яких обличчя відомих осіб (наприклад, Президента Зеленського) використовували для створення фальшивих звернень. Навіть проста хибна підписка до зображення може збити з пантелику, якщо її не виявити.

У методологічному плані це вимагає від дослідників розробки систем перевірки фейків. Це перетинається з верифікацією, але зосереджується саме на ознаках маніпуляції: наприклад, аналіз тіней і освітлення для виявлення цифрової підробки, або використання інструментів перевірки достовірності (аналіз рівня помилок зображень, структура відеофайлів тощо). Важливо також розуміти екосистему дезінформації: супротивник часто координує поширення фейків на кількох платформах одночасно. OSINT-дослідники можуть картографувати шлях поширення фейку через Telegram, Twitter, ТБ — щоб виявити механізми дезінформаційної кампанії. У наукових роботах доцільно включати аналіз таких кейсів дезінформації як ілюстрацію здатності OSINT протистояти обману.

З огляду на викладені вище виклики, методологічна ретельність і прозорість є важливими при інтеграції OSINT у академічні дослідження війни. Наукова ретельність досягається завдяки системному застосуванню OSINT-методів та процедур перевірки, описаних раніше, а також дотриманню найкращих практик, вироблених фаховою спільнотою OSINT. Прозорість [8] передбачає чітку документацію джерел і методів, що дозволяє іншим дослідникам відтворити або перевірити результати. На практиці академічне дослідження OSINT у контексті російсько-української війни має включати детальні додатки або примітки з посиланнями на конкретні твіти, відео чи супутникові знімки, які слугували доказовою базою, а також пояснення, як саме вони були верифіковані. Такий підхід нагадує практику розслідувальних платформ, які регулярно публікують окремі «методологічні примітки» разом із результатами досліджень. Значення такої документації підкреслюється в документах, як-от Berkeley Protocol, де принцип «підзвітності» (тобто ведення чітких записів про всі етапи розслідування) визначено першим за важливістю. Завдяки формуванню «аудиторського сліду», тобто фіксації способу отримання й перевірки інформації, дослідник дає змогу рецензентам і майбутнім науковцям відстежити достовірність висновків.

Крім того, частиною наукової доброчесності є відкритість щодо обмежень: наприклад, визнання випадків, коли конкретний фрагмент даних не вдалося верифікувати на 100%, або коли джерела можуть містити потенційну упередженість (скажімо, проукраїнські наративи в соцмережах). Також прагнення до триангуляції – тобто зіставлення результатів OSINT з іншими типами джерел, зокрема інтерв'ю або офіційними звітами, щоб підвищити надійність висновків. Ще одним способом забезпечення наукової ретельності є актуальність технічної підготовки дослідника. Сфера OSINT постійно розвивається — з'являються нові інструменти автоматизованої верифікації або засоби штучного інтелекту для виявлення діпфейків — і високоякісне дослідження має враховувати ці нові можливості та посилатися на авторитетні джерела.

РОЗДІЛ ІІ. ВИКОРИСТАННЯ OSINT ПІД ЧАС ХАРКІВСЬКОЇ ТА ХЕРСОНСЬКОЇ КАМПАНІЙ

2.1. Використання розвідки відкритих джерел у підготовці та реалізації контрнаступу під час Харківської операції

Контрнаступ у Харківській області у вересні 2022 року став знаковою операцією, в якій Україна ефективно використала розвідку на основі відкритих джерел (OSINT) для досягнення ефекту раптовості та вирішальних успіхів. Ця кампанія, удар на північному сході України, вирізнялася ретельним плануванням, високим рівнем оперативної безпеки та вмілим застосуванням публічно доступної інформації для введення противника в оману та моніторингу ситуації на полі бою. OSINT став корисним на всіх етапах: від планування та дезінформації напередодні, до забезпечення ситуаційної обізнаності під час наступу і, зрештою, у післяопераційній оцінці наслідків. Для планування й проведення кампанії було задіяно широкий спектр OSINT-методів (супутникові знімки, геолокацію відео, моніторинг соціальних мереж і Telegram-каналів), які використовувалися разом із традиційною військовою розвідкою.

У тижні, що передували харківському наступу, українські планувальники провели цілеспрямовану кампанію дезінформації, яка значною мірою спиралася на відкриті джерела з метою введення російських військ в оману щодо реального напрямку майбутньої атаки. Протягом серпня 2022 року українські посадовці та медіа активно просували тезу про масштабний контрнаступ на півдні — в Херсонській області. Цей наратив активно поширювався в новинах і соціальних мережах. [9] [10] Такий «шумний» інформаційний фон про наближення південного наступу фактично був продуманою операцією інформаційного впливу в межах OSINT-стратегії. [11] Постійно акцентуючи увагу на херсонському напрямку у прес-релізах і навіть офіційно оголосивши початок південного наступу 29 серпня, Україна змусила російське командування повірити, що саме Херсон є головною

ціллю. Згодом The Guardian підтвердив, що широко розрекламований «південний наступ» був масштабною операцією дезінформації, спрямованою на відволікання уваги Росії. Відкриті канали підхопили й підсилили цю інформаційну операцію. Західні медіа та незалежні аналітики, користуючись тими ж публічними заявами, здебільшого «повірили в ілюзію», активно припускаючи, що головним напрямком українських дій стане саме Херсон. [10]

У дослідженні авторства Мітчелла було виявлено *«чіткий зв'язок між зростанням інтенсивності ілюзорної правди у відкритих джерелах і переміщеннями російських військ у полі»*, [12] що підтвердило: наратив дезінформації через OSINT безпосередньо вплинув на рішення командування РФ. Фактично, Україна успішно перетворила відкритий інформаційний простір на зброю. Внаслідок цієї дезінформації російські сили наприкінці серпня почали перекидати значні підрозділи з Харківщини на південь. Російське командування мало всі підстави посилювати саме цей напрям — він здавався логічним. Переміщення російських військ, зокрема дані про рух ешелонів та автоколон, зафіксовані на супутникових знімках і в Telegram-каналах, вказували на передислокацію батальйонно-тактичних груп із району Ізюма до Херсонської області в цей період. На початок вересня російський фронт на Харківщині [13] утримувався значно скороченими й «виснаженими» силами, які змушені були тримати розтягнуту лінію протяжністю близько 1300 км без належного резерву. [11] Оперативна безпека (OPSEC) [10] була на найвищому рівні: українські війська потайки висувалися до районів зосередження поблизу Балаклії та річки Оскіл, а українська влада активно виявляла й нейтралізувала місцевих інформаторів у Харківській області, які могли передати дані ворогу. Протягом літа українські спецпризначенці та партизани здійснювали приховану розвідку російських позицій у регіоні. [14]

Вранці 6 вересня 2022 року Україна розпочала свій раптовий контрнаступ на Харківському напрямку, цілком дезорієнтувавши російські війська. [10] Декілька

українських бригад, включно з танковими та механізованими частинами, озброєними новою західною технікою, прорвали слабко укріплену лінію оборони росіян на схід від Балаклії. Ознаки наступу у відкритих джерелах почали з'являтися вже за кілька годин: місцеві жителі публікували відео в Telegram, де українські танки рухалися на світанку, а до кінця дня українські соцмережі вибухнули повідомленнями, хоч і не підтвердженими, про звільнені села. Повітряно-десантна бригада ЗСУ просунулася на приблизно 18 км вже в перший день, звільнивши Волохів Яр, що було підтверджено геолокованими кадрами боїв, викладеними у відкритий доступ. Протягом 48 годин українські сили повернули під контроль близько 400 квадратних кілометрів території. Стрімкий поступ значною мірою верифікувався через OSINT: супутникові знімки показували колони української техніки глибоко в тилу раніше окупованих районів, а система NASA FIRMS зафіксувала численні теплові аномалії (осередки пожеж) вздовж осі наступу — ймовірно, вказуючи на вибухи й згорілу техніку. [16]

Відкриті дані про пожежі стали індикатором інтенсивних бойових дій. OSINT-аналітики помітили, що сплеск теплових аномалій припав на район Балаклії та траси в напрямку Куп'янська 6-7 вересня, що узгоджувалося з повідомленнями про український наступ. Це дозволило відстежувати перебіг операції ще до появи офіційних заяв. Українські посадовці певний час зберігали оперативну тишу, навіть коли успіхи стали очевидними, однак окремі контрольовані повідомлення почали з'являтися у відкритих каналах. 8 вересня голова Харківської ОВА Олег Синєгубов повідомив у Facebook, [17] що над Балаклією знову піднято державний прапор України. Цей допис став одночасно і тріумфальним повідомленням, і точкою OSINT-підтвердження визволення міста, яке невдовзі було підхоплене українськими та міжнародними медіа. Геолокація зображень оперативно підтвердила факт: фото й відео з українськими військовими, які піднімають прапор на центральній площі Балаклії, з'явилися у Twitter та були перевірені (зокрема мережею GeoConfirmed, яка зіставила об'єкти на місцевості для верифікації автентичності матеріалів).

7 вересня один із російських військових кореспондентів у Telegram написав: *«Ситуація під Балаклією дуже складна, у нас там практично немає сил»*. Такі повідомлення, відкриті для загального доступу, підтверджували, що російське командування було захоплене зненацька. До 9-10 вересня масштаб наступу став беззаперечним завдяки OSINT-каналам. DeepStateMap (цифрова карта, яку створює спільнота на основі відкритих даних) та популярний Twitter-акаунт War Mapper оновили свої карти, позначивши значні території, раніше окуповані Росією, як звільнені. [18] Ці оновлення базувалися на сукупності відкритих джерел: відео з українськими військовими в різних населених пунктах, повідомленнях місцевих мешканців і офіційних підтвердженнях з української сторони. Наприклад, коли 10 вересня українські війська увійшли до стратегічно важливого центру, Куп'янська, у мережі миттєво з'явилися фото, на яких бійці тримають український прапор перед будівлею міської ради.

Стикнувшись із загрозою оточення, підрозділи армії РФ покинули Ізюм і прилеглі райони до 10 вересня. Перша ознака падіння Ізюма надійшла через супутникові знімки від 10 вересня, які показували незвично великі колони техніки, що скучено рухалися на схід у напрямку річки Оскіл — типова ознака масового відступу. [11] Одночасно мешканці Ізюма публікували в Telegram фото російських військових, які поспіхом залишають місто, і українських розвідгруп на околицях. До 11 вересня навіть Міністерство оборони РФ змушене було визнати відступ, хоч і евфемістично назвавши його «перегрупуванням» — ця заява одразу стала об'єктом постатейного аналізу.

На картах із щоденного брифінгу Міноборони Росії, які 11 вересня з'явилися в соціальних мережах, було помічено, що на них показано відсутність будь-якої присутності російських військ західніше річки Оскіл. Це фактично підтвердило, що росіяни евакуювали майже всю західну частину Харківської області всього за кілька днів. Проросійські канали повідомляли, що такі населені пункти, як Вовчанськ і

Козача Лопань (поблизу кордону з РФ), [13] залишаються без бою. Водночас українські джерела в Telegram публікували відео, на яких місцеві мешканці піднімають українські прапори в цих містах. [19]

Після завершення першої фази Харківського контрнаступу була змога оперативно оцінити, чому ця операція була успішною і як вона змінила хід війни. Аналітики Інституту вивчення війни (ISW) та інших аналітичних центрів дійшли висновку, що успіх України став наслідком поєднання дезінформаційної кампанії, прицільних ударів по російській логістиці та вмілого використання слабких місць противника. Наприклад, супутникові знімки у відкритому доступі показували удари HIMARS по російських складах боєприпасів і базах у Харківській області за кілька тижнів до наступу. Удари завдавалися навіть по глибоких цілях, що порушувало російські логістичні лінії. Сукупний ефект, чітко видимий у ретроспективі через відкриті дані, полягав у тому, що логістика й бойовий дух російських військ на Харківщині до початку вересня перебували в кризовому стані. Справді, згідно з одним із перехоплених телефонних дзвінків (згодом оприлюднених), російські солдати в цьому секторі відчували себе «покинутими» й скаржилися на нестачу боєприпасів.

2.2. Використання розвідки відкритих джерел у підготовці та реалізації контрнаступу під час Херсонської операції

Контрнаступ на Херсонському напрямку (серпень – листопад 2022 року) суттєво відрізнявся від харківської операції, однак і в цьому випадку українські сили широко використовували розвідку на основі відкритих даних. У Херсоні Україна здійснила виснажливу та методичну операцію зі звільнення єдиного обласного центру, захопленого Росією, застосовуючи OSINT для оперативного планування, визначення цілей і підтримання ситуаційної обізнаності протягом тривалого періоду. Якщо харківський наступ вирізнявся стратегічною

несподіванкою та стрімким просуванням, то херсонська кампанія поєднала поступове виснаження ворога із раптовим остаточним відступом російських військ.

Перед офіційним початком херсонського контрнаступу 29 серпня 2022 року Україна провела масштабні заходи з формування сприятливих умов для наступу. Розвідка з відкритих джерел виявилася цінною як на етапі планування, так і для оцінки ефективності цих дій. У липні та серпні українські війська за підтримки західної далекобійної артилерії, зокрема реактивних систем високоточної стрільби HIMARS, завдавали ударів по російських лініях постачання та інфраструктурі в Херсонській області. Багато з цих цілей було ідентифіковано, а факти їхнього ураження підтверджено саме за допомогою OSINT. Так, українські й західні спостерігачі, користуючись даними системи FIRMS NASA, вже на початку липня зафіксували велику кількість пожеж уздовж кордонів Херсонської й Миколаївської областей, що збігалося в часі з українськими ударами по складах боєприпасів і позиціях російських військ. [16] Знімки з FIRMS демонстрували теплові аномалії у районах відомих російських баз, зокрема в Чорнобаївці (аеропорт Херсона), що неодноразово підтверджувало результативність ударів.

Соціальні мережі рясніли підказками, адже російські солдати та окупаційні чиновники в Херсоні часто викладали фото нових складів чи командних пунктів, розкриваючи координати. Волонтерські спільноти на кшталт Molfar та інші розвідувальні групи, ретельно аналізували такі публікації, виявляючи склади з боєприпасами та командні центри. Один із найпоказовіших випадків — влучання по російському складу боєприпасів у Новій Каховці 11 липня 2022 року. Вибух був настільки потужним, що його зафіксували як FIRMS, так і численні відео цивільних осіб (кадри з вогняною кулею швидко поширились у Telegram). Цей удар, один із десятків подібних, став частиною масштабної кампанії українських «вогневих уражень» із метою послабити російське угруповання в Херсоні.

Ще одним елементом підготовки стало відсічення переправ через річку Дніпро, які забезпечували постачання для 20-30 тисяч російських військових на її правому березі. Україна зробила Антонівський міст (головну автодорожню артерію до Херсона) пріоритетною ціллю ще наприкінці липня. [21] Пошкодження цього мосту було детально задокументовано. Спочатку місцеві мешканці публікували фотографії воронок від ударів на мосту, а згодом у відкритому доступі з'явилися супутникові знімки, які показували сукупні наслідки багаторазових ударів HIMARS. На знімку Planet Labs від 26 серпня Антонівський міст мав щонайменше 16 великих пробоїн, що робило його непридатним для пересування важкої техніки. Аналогічно були уражені залізничний міст у Херсоні та автомобільна дорога через греблю в Новій Каховці — згодом факти пошкоджень підтвердилися за допомогою супутникових і дронових знімків. Щоразу після удару протягом одного-двох днів у відкритому доступі з'являлися супутникові зображення або фото від місцевих мешканців, які підтверджували масштаби руйнувань.

Наприкінці серпня російська логістика змушена була покладатися на понтонні пороми та баржі. І цю адаптацію також відстежували за допомогою OSINT, оскільки супутники із синтезованою апертурою (зокрема Sentinel-1 Європейського космічного агентства) фіксували появу нових переправ, а фото з місця подій показували, як росіяни зводять понтонні мости (Інститут вивчення війни (ISW) зафіксував будівництво одного з таких мостів на супутниковому знімку 27 серпня неподалік Антонівського мосту). [15] Імовірно, українські військові, які також стежили за цими знімками, почали бити по цих переправах — 2 листопада у відкритому доступі з'явилося відео удару HIMARS по російському понтонному переходу в Херсоні. [22] [10]

Карта лінії фронту змінювалася повільно протягом вересня, однак потік відкритих даних безперервно свідчив про поступове погіршення російських позицій. Наприклад, над Херсоном у вересні фіксували дедалі менше пожеж на передовій, що вказувало на спад російської артилерійської активності — непрямий

доказ того, що інтердикція українською стороною ворожих боєприпасів діє. [15] [23] Щоденні зведення британського Міністерства оборони, що базувалися на відкритих джерелах, вже в середині вересня повідомляли, що російські війська у Херсоні мають серйозні проблеми з постачанням і втрачають здатність до контратак. Прогрес був поступовим, але не стрімким, і звільнення кожного населеного пункту зазвичай підтверджувалося якимось OSINT-джерелом. Українські військові та місцеві мешканці нерідко виконували роль воєнних кореспондентів: щойно населений пункт опинявся під українським контролем, у Telegram або Twitter з'являлися фото чи коротке відео, де військові піднімають український прапор. Наприклад, 4 вересня українські підрозділи звільнили селище Високопілля [14] на півночі Херсонщини. Того ж дня у Facebook з'явилось зображення, де бійці піднімають прапор України у Високопіллі. Справжність фото швидко підтвердили шляхом зіставлення місцевості та навколишніх будівель через Google Earth.

Подібна ситуація повторювалась протягом усього вересня: села на кшталт Нововознесенського, Білогірки та інші вздовж Інгульця звільнялись та отримували підтвердження через відкриті джерела (найчастіше — за допомогою інтерактивної мапи DeepState, яка оновлювалася на основі колективної інформації від військових і місцевих жителів). DeepState акумулював повідомлення з фронту для оновлення даних про контроль над територіями. Статус населеного пункту змінювався на «звільнений» лише після отримання достатніх доказів (наприклад, візуального підтвердження або заяви офіційного джерела). GeoConfirmed підтримував відкриті таблиці й мапи, на яких верифікували кожну заяву про звільнення з координатами та доказами, формуючи достовірну картину ситуації на місцевості. Публікували анотовані карти Херсонської області, де поєднували супутникові знімки, дані FIRMS і повідомлення про бойові зіткнення, фіксуючи українські просування. Їхні карти, наприклад, показували, як наприкінці вересня на півночі Херсонщини формувався виступ — Україна просувалася на південь із плацдарму поблизу Давидового Броду на річці Інгулець. Коли на початку жовтня українські війська

прорвали російські позиції вздовж берегової лінії Дніпра й просунулися на 20–30 км із захопленням низки сіл (зокрема Дудчани, Милове), [24] це майже одразу відобразилось на супутникових знімках, а також підтвердилось тим, що мапи Міністерства оборони Росії, які демонструвались по державному телебаченню 4 жовтня, вже не включали ці північні території — фактичне визнання українських здобутків.

Протягом усього наступу аналітики з відкритих джерел відстежували пожежі та вибухи, щоб оцінити перебіг бойових дій. Коли українські сили зосереджували артилерійські удари по російських позиціях, дані про пожежі з FIRMS відповідно фіксували підвищену активність. І навпаки — коли російську артилерію вдавалося приглушити, кількість теплових аномалій зменшувалася. Один показовий епізод стався 9–10 жовтня 2022 року, коли просування українських військ поставило під загрозу російські маршрути постачання, росіяни намагалися обстрілювати наступаючі підрозділи, але за ці дні було зафіксовано несподівано малу кількість пожеж на тодішній лінії фронту. Це свідчило про ймовірний дефіцит боєприпасів або порушену систему командування.

Перші відкриті докази російського відходу з’явилися вже в перших числах листопада. 3 листопада мешканці Херсона зауважили, що з будівлі міської адміністрації зник російський прапор. Цю інформацію підтвердив проросійський військовий кореспондент Олександр Коц, який написав у Telegram: *«над адміністрацією більше немає (російського) прапора»*. Ця подія, зафіксована на фото в Telegram стала першою ознакою того, що російські військові, можливо, готуються залишити Херсон. Приблизно в той самий час супутникові знімки почали фіксувати демонтаж російських позицій і блокпостів у низці районів. Наприклад, зображення з містечок на передовій, таких як Снігурівка (Миколаївська область, поблизу Херсонщини), на початку листопада показували помітне зменшення кількості російської техніки порівняно з попереднім місяцем, що свідчило про тихий відхід із передових позицій.

Вже 11 листопада 2022 року українські сили увійшли до самого міста Херсон, де їх зустріли як героїв, а російський відступ завершився. Фото й відео, датовані 11-12 листопада, показували тисячі херсонців, які вийшли на вулиці, щоб привітати українських військових сльозами, прапорами й обіймами. [19] Ці кадри транслювалися наживо на Facebook-сторінках українських новинних ресурсів і швидко були підхоплені міжнародними ЗМІ. Аккаунти OSINT у Twitter збирали десятки таких відео, підтверджуючи геолокацію: Площа Свободи в центрі Херсона, переповнена людьми в жовто-синьому одязі, або жінка, яка емоційно обіймає українського сержанта на центральній вулиці — сцена була верифікована за вітринами магазинів. [25]

Розвідка також дозволила відстежити долю російських військ і техніки під час відступу. Хоча відхід Росії з Херсона відбувся загалом впорядковано, особливо у порівнянні з панічною втечею з Харківщини, вони все ж залишили велику кількість техніки через постійні українські удари по переправах. Уже за кілька днів українські джерела публікували знімки захоплених російських танків, артилерії та навіть збитого вертольота Ка-52 біля річки — всі ці втрати були занесені до відповідних списків аналітиками з Oryx. [20] [22] Станом на середину листопада було зафіксовано, що на правому березі Дніпра росіяни залишили щонайменше десятки броньованих машин — частина була пошкоджена, інші — справні, але без пального.

Успішний контрнаступ на Херсонському напрямку, досягнутий завдяки поєднанню війни на виснаження та стратегічного терпіння, мав значні оперативні й стратегічні наслідки, багато з яких були проаналізовані за допомогою відкритих джерел інформації. [14] Тактично Україна звільнила близько 5 000 км² Херсонської області на правому березі Дніпра та додатково приблизно 1 600 км² на території Миколаївської області, яка перебувала під російською окупацією. Це охоплювало 179 населених пунктів на півдні, звільнених протягом тижня після фінального

наступу, що було офіційно задекларовано й візуально підтверджено. Ці дані, вперше надані українською владою, були верифіковані картою DeepState та інші ресурси демонстрували, що до 11 листопада весь правий берег Дніпра практично повністю очищено від російської присутності. [25]

2.3. Оперативно-стратегічні наслідки контрнаступів на Харківському та Херсонському напрямках

Подвійні успіхи України в контрнаступах на Харківському та Херсонському напрямках восени 2022 року стали поворотним моментом у війні, спричинивши наслідки на тактичному, оперативному та стратегічному рівнях. Подібні успіхи не лише дозволили звільнити значні території, але й змінили стратегії обох сторін конфлікту в подальшому. Фундаментально, успіхи Харківської та Херсонської кампаній показали здатність України до проведення широкомасштабних наступальних операцій, зруйнувавши патову ситуацію, яка склалась у середині війни, і змусивши Росію перейти до оборони. Цей зсув у темпі воєнних дій мав каскадний ефект: Росія була змушена вдатися до екстрених заходів, таких як мобілізація й реорганізація командування, а Україна, своєю чергою, зміцнила впевненість у своїх силах і отримала критично важливі логістичні переваги. Міжнародне сприйняття війни ще більше схилилось на користь України, що дозволило залучити нову підтримку.

На тактичному рівні операції в Харкові та Херсоні завдали серйозних втрат у техніці й живій силі Збройним силам РФ, водночас суттєво поповнивши запаси української армії — це динаміка, яку детально задокументували джерела відкритої розвідки. Під час харківського наступу українські сили за кілька днів захопили понад 500 одиниць російської техніки та озброєння. [19] Серед трофеїв були танки, бронетранспортери, артилерійські системи та величезні запаси боєприпасів. Широко розповсюджені зображення українських солдатів, які оглядають ряди справних російських танків Т-80 та ящики зі снарядами в Ізюмі, стали символами

того, що Росія, як іронізували деякі коментатори, «стала найбільшим постачальником зброї для України». Внаслідок цього бойова потужність ЗСУ зросла. За оцінками західних аналітиків, Україна змогла сформувати щонайменше одну нову бронетанкову бригаду, використовуючи трофейні танки та БМП з-під Харкова. Подібні трофеї суттєво посилили наступальний потенціал України. У Херсоні, хоча відступ росіян був більш організованим, українці все ж захопили або знищили десятки одиниць техніки, а головне — змусили противника залишити великі обсяги важкої артилерії та запасів на правому березі Дніпра. Більшість із них не вдалося евакуювати через зруйновані мости. Наприклад, українські підрозділи показали кілька залишених росіянами «Гіацинт-Б» і реактивних систем залпового вогню «Град» у Херсонській області — відповідні зображення було верифіковано та оприлюднено через OSINT-канали. Окрім техніки, ці наступи також нейтралізували як бойові одиниці окремі елітні підрозділи РФ. У Харкові елітна 1-ша гвардійська танкова армія Росії зазнала катастрофічних втрат, втративши більшість своїх сучасних танків Т-80. У Херсоні під постійним артилерійським тиском відступали підрозділи 76-ї десантно-штурмової дивізії та 22-го армійського корпусу РФ, залишаючи поле бою в ослабленому стані. Ці тактичні поразки суттєво знизили наступальний потенціал Росії в наступні місяці, що спричинило затишшя на фронтах після осені 2022 року (за винятком виснажливих боїв у Бахмуті).

На оперативному рівні успіхи контрнаступів змінили географію бойових дій на користь України. Харківська операція ліквідувала російський плацдарм на північному сході, відкинула лінію фронту до річки Оскіл [13] і зрештою призвела до звільнення майже всієї Харківської області. Звільнення таких ключових вузлів, як Куп’янськ та Ізюм, усунуло безпосередню загрозу з півночі на Донбасі, а також скоротило лінію оборони ЗСУ. Важливо, що падіння Ізюму змусило росіян відмовитися від задуму щодо «кліщової» атаки на Слов’янськ із півночі, що зменшило тиск на цьому напрямку. У подальшому це дало змогу Україні до початку жовтня звільнити Лиман у Донецькій області, ще більше зміцнивши контроль над північним сходом. Тим часом Херсонський наступ забезпечив звільнення всього

правобережжя Херсонської області, що дало Україні природний рубіж оборони на південному фронті — широкий Дніпро. Нова лінія фронту стабілізувалася вздовж річки, що дозволило ЗСУ вивільнити частину підрозділів, які раніше стримували противника на миколаївському та криворізькому напрямках. І справді, після листопада 2022 року деякі бригади, що брали участь у боях під Херсоном, були перекинуті для підсилення Бахмута або відправлені на відпочинок і доукомплектування. Росія ж, втративши плацдарм на правому березі, назавжди втратила можливість наступу в напрямку Одеси чи центральної України з цього напрямку. Таким чином, перемога в Херсоні остаточно нівелювала російські амбіції в південній Україні (за винятком прагнення утримати Крим та частину південного сходу).

Оперативний вплив контрнаступів також простягнувся на сферу управління військами та розміщення сил. Поразки призвели до кадрових перестановок у російському вищому військовому командуванні: генерал Олександр Лапін, який керував російськими силами в районі Харкова й Ізюма, зазнав жорсткої критики (зокрема з боку чеченського лідера Кадирова та Пригожина) [11] і згодом був усунутий з посади. Хвиля критики в російських соціальних мережах, ймовірно, вплинула на ухвалення цих рішень. У жовтні Росія призначила генерала Суровікіна головнокомандувачем, і в межах своєї стратегії він ухвалив прагматичне рішення про відступ з Херсона.

Стратегічно перемоги під Харковом і Херсоном мали далекосяжні наслідки для ходу війни та процесу ухвалення рішень як в Україні, так і в Росії. Для України та її партнерів ці кампанії стали доказом того, що ЗСУ здатні не лише оборонятися, але й звільняти території та завдавати поразки російським силам у наступі, тим самим розвінчавши уявлення про незмінну патову ситуацію. Це мало прямий вплив на міжнародну підтримку: країни Заходу, побачивши чіткі результати уже наданої військової допомоги, стали більш схильними передавати сучасне озброєння. Справді, вже наприкінці 2022-го та на початку 2023 року серед союзників НАТО

розпочались обговорення постачання танків (зокрема Leopard), покращених систем ППО та далекобійних ударних засобів. Можна стверджувати, що без продемонстрованого успіху цих контрнаступів вагання залишилися б значно сильнішими.

Ще одним стратегічним наслідком стало рішення Росії компенсувати втрати на полі бою ескалацією в інших сферах. Починаючи з жовтня 2022 року, РФ розгорнула масштабну кампанію стратегічних бомбардувань енергетичної інфраструктури України, спричинивши масові відключення електроенергії взимку. Хоча Росія висувала різні офіційні пояснення для цих дій, чимало аналітиків розцінили цю кампанію як акт помсти за поразки та спробу зламати волю України після успіхів під Харковом і Херсоном. [26] OSINT-джерела допомогли розкрити цю логіку: західна розвідка та аналітичні центри відзначили, що інтенсивність ракетних ударів зростала саме після великих поразок Росії, що вказує на певну закономірність. [27] Ймовірною метою було сповільнити темп українських операцій, змусивши Київ відволікатися на вирішення гуманітарної кризи, оскільки на полі бою Росія зазнавала поразок. Однак у стратегічному сенсі цей підхід не досяг цілі — Україна вистояла під ударами взимку й зберегла динаміку дій (завдяки, зокрема, постачанню нових систем ППО від західних партнерів, які активізували підтримку після Херсона). [9] [10] Водночас Україна усвідомила важливість цілевизначення на основі розвідки, адже було чітко видно, що удари по мостах і складах, ідентифікованих завдяки відкритим даним, підготували ґрунт для визволення Херсона. [25] Цей підхід зберігається й надалі — Україна регулярно завдає ударів по російській логістиці (у Криму, Мелітополі тощо), часто спираючись на підказки з відкритих джерел та супутникові знімки. [18]

З погляду Росії, стратегічний ефект цих поразок змусив її перейти до оборонної позиції на тривалий період. Після втрати Херсона Росія остаточно втратила можливість наступу на Миколаїв чи Одесу, а увага була повністю переорієнтована на утримання лінії фронту в Донецькій області та зведення

оборонних укріплень у Запорізькій області й уздовж нової лінії фронту по Дніпру. Уже з жовтня 2022 року супутникові знімки засвідчували, що Росія з поспіхом споруджує систему траншей, протитанкових загороджень і бетонних укріплень по всьому півдню України — чіткий сигнал стратегічного переходу до оборонної війни. OSINT-аналітики нанесли на карти величезну мережу оборонних споруд, яку Росія збудувала взимку 2022-2023 років, зокрема багатошарову оборону в Запорізькій області, що отримала назву «лінія Суровікіна». Така реакція була прямим наслідком стрімкої втрати територій, оскільки Росія прагнула не допустити повторення сценарію Харкова і Херсона, заглиблюючи свої війська в оборону. Існування цих укріплень суттєво вплинуло на перебіг бойових дій у 2023 році, зробивши українські наступи набагато повільнішими й складнішими. У парадоксальний спосіб саме українські успіхи змусили Росію «закопатися», а це, у свою чергу, вимагало від України адаптації тактики прориву укріплених ліній.

Використання розвідки з відкритих джерел у контрнаступах 2022 року не лише сприяло їхньому успіху, а й визначило підходи України до планування та реалізації наступних операцій. Одним із прямих наслідків стало посилення уваги до оперативної безпеки на тлі спостереження з боку РФ. Усвідомлюючи, наскільки критичною була роль OSINT у власних перемогах, українські командири зрозуміли, що росіяни також уважно стежать за відкритими джерелами. Тож під час підготовки контрнаступу на півдні в 2023 році Україна вжила суворих заходів для маскування переміщень військ — зокрема, повне радіомовчання, пересування підрозділів уночі, а також жорсткий контроль за публікаціями військових у соцмережах, які могли б розкрити геолокацію. Цю дисципліну, ймовірно, зміцнило розуміння того, що влітку 2022 року деякі російські Telegram-канали дійсно виявили концентрацію українських військ у районі Харкова (яку, втім, Росія неправильно інтерпретувала), і щось подібне могло повторитися.

Україна чітко усвідомила двозначну природу OSINT: він став у пригоді проти російської армії у 2022 році, але водночас слід було не допустити, щоб Росія

скористалася аналогічними можливостями. Паралельно українська розвідка (зокрема ГУР та аналітичні підрозділи ЗСУ) активізували експлуатацію російських відкритих джерел. Контрнаступи довели ефективність моніторингу військових блогерів противника та місцевих інформаторів. Відтоді Україна створила окремі підрозділи, які цілодобово відстежують російські Telegram-канали, оперативно фіксуючи корисну інформацію — як-от скарги на командування, геомітки на фото тощо. Здатність відстежувати моральний стан і оперативні плани РФ за допомогою OSINT стала постійним інструментом українського військового планування. Наприклад, напередодні наступу в районі Вугледара в січні 2023 року українські офіцери використовували соціальні мережі для оцінки ротацій російських підрозділів.

Контрнаступи в Харкові та Херсоні 2022 року, здійснені за підтримки та висвітлені завдяки розвідці з відкритих джерел, змінили траєкторію цієї війни. На тактичному рівні вони знищили та захопили критично важливі активи російських військ, водночас підсиливши український арсенал і бойовий дух. На оперативному рівні ЗСУ перехопили ініціативу, змусивши Росію перейти до оборони. У стратегічному вимірі ці успіхи спровокували мобілізацію в РФ і спробу компенсувати втрати в інших сферах, але водночас розблокували більшу підтримку Заходу для України та посилили її переговорні позиції. Україна вийшла з 2022 року з чітким шаблоном проведення ефективних наступальних операцій великого масштабу — інтеграція обману, точкових ударів за даними розвідки та швидкої експлуатації результату — а також із глибоким розумінням, що публічність перемог (їх демонстрація світові) може бути не менш потужною, ніж самі перемоги. Росія, зазнавши поразок, відповіла закопуванням в оборону й намаганнями бити по волі українського народу — з обмеженим успіхом, оскільки було засвідчено збереження високого рівня рішучості з боку українців.

РОЗДІЛ ІІІ. РОЗВІДКА ВІДКРИТИХ ДЖЕРЕЛ У НАНЕСЕННІ УДАРІВ ПО РОСІЙСЬКИХ ОБ'ЄКТАХ НА ТИМЧАСОВО ОКУПОВАНИХ ТЕРИТОРІЯХ ТА ТЕРИТОРІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

3.1. Використання відкритих джерел для оперативного виявлення позицій противника

Українські сили разом із спільнотою OSINT-аналітиків використовують публічно доступні дані, від постів у соціальних мережах і відео до супутникових знімків, для точного визначення позицій російських військ. Сучасна OSINT-геолокація поєднує контент, створений користувачами, з цифровими картографічними інструментами та аналітикою даних, щоб визначити, де саме зроблено зображення чи відео. Аналітики переглядають фото і відео з російськими військами чи технікою, розміщені на таких платформах, як «ВКонтакте» (VK), Telegram, TikTok та інші, й зіставляють візуальні підказки (ландшафт, об'єкти, дорожні знаки тощо) із супутниковими знімками та онлайн-мапами. У деяких випадках задачу значно спрощує наявність метаданих або випадкових геотегів у контенті. [28]

Важливо те, що українські аналітики та воєнна розвідка інтегрують ці дані у свій процес наведення ударів. Україна унікальна тим, що має потужну внутрішню OSINT-спільноту (зокрема, такі організації, як Molfar, Deepstate, InformNapalm, Dnipro Osint), які тісно співпрацюють з силами оборони, а також офіційні канали збору інформації від цивільного населення. Так, 12 жовтня 2022 року російський солдат Олексій Лебедєв виклав фото у «ВКонтакте», зроблене всередині військового намету. [29] Він подбав про те, щоб приховати обличчя, але не звернув уваги, що платформа автоматично додала точний геотег. Локація посту — село Свободне на півдні Донецької області. Дослідники оперативно зафіксували цю публікацію й протягом кількох годин створили «профіль цілі» для підрозділу Лебедєва, встановивши, що село використовується як навчальна база. Вони виявили ще два фото з цього ж місця, опубліковані російськими військовими, що

підтверджувало наявність великого військового табору. Усі ці дані з відкритих джерел, включно з точними координатами, отриманими з необережної публікації Лебедєва, були зібрані й передані українській розвідці. Уже через два дні зафіксовано вибухи на зазначеній ділянці, приблизно за 60 км від лінії фронту, що свідчить про успішний удар по базі в Свободному. Служба безпеки України повідомила про атаку у своєму Telegram-каналі, наголосивши на «точному ударі» по ворожому об'єкту в цьому районі. Сам Лебедєв вижив (поспіхом видаливши компрометуюче селфі), однак його підрозділ засвоїв болісний урок щодо летальних наслідків нехтування інформаційною безпекою.

Інша впливова спільнота — це неформальні мережі в Twitter і Telegram, відомі під назвами "OSInt Twitter" або GeoConfirmed, які виконують геолокаційні завдання за принципом колективного збору даних. Ці волонтери допомагали виявляти розташування російської техніки, показаної на відео в TikTok або на злитих фото, іноді — протягом кількох хвилин після публікації. Наприклад, на початку 2022 року короткі відео в TikTok, на яких знято пересування російських колон по території Білорусі, були геолокалізовані аналітиками до конкретних перехресть і місцевостей, забезпечивши раннє попередження про напрямки російського наступу. [30]

У тактичному плані OSINT-геолокація прискорила цикл наступальних дій та ракетних ударів для України. Підказки від цивільних можуть передаватися українським артилеристам чи операторам дронів. Наприклад, під час битви за Харків місцеві телеграм-канали регулярно повідомляли про появу російських танків у селах — і вже за кілька годин (а іноді й швидше) ці танки ставали об'єктами прицільного вогню. [29] Така швидка дія стала можливою завдяки розподіленому розвідувальному циклу — кожен, хто бачить щось на місці чи в інтернеті, може внести свій вклад, а інформацію оперативно верифікують через відкриті джерела й передають виконавцям. Це формує своєрідну демократизацію розвідки, зменшуючи залежність від повільнішої традиційної розвідки. Утім, це також вимагає високої

координації з українського боку, аби уникнути перевантаження даними чи хибної ідентифікації. Варто віддати належне — Збройні Сили та спецслужби України, схоже, ефективно інтегрували OSINT-підказки у свій загальний процес наведення ударів.

Яскравим прикладом є дії російських призовників на Донбасі. У середині 2022 року частина мобілізованих почала створювати у «ВКонтакте» групи для зв’язку з родичами. Із гордості або через необізнаність вони іноді викладали групові фото, не розуміючи, що фон може видати розташування бази. [29] Таким чином українська сторона відслідковувала пости або навіть проникала в певні чати. В одному випадку на знімку було видно церкву та характерну форму пагорба — аналітики визначили, що це місцевість на сході Луганської області. Невдовзі після цього українська артилерія обстріляла вказану зону, а подальші пости росіян засвідчили втрати — це вказує на ймовірний зв’язок між публікацією й ударом (хоча офіційно його не підтверджували). Такий ланцюг — росіяни мимоволі видають позиції, а Україна завдає удару — повторювався неодноразово.

Наприкінці 2022 року російський доброволець на тимчасово окупованій Херсонщині став автором однієї з найбільш кричущих помилок. Він публікував численні фото і відео у «ВКонтакте», позуючи поруч із військовими з 10-ї бригади спецпризначення ГРУ на фоні того, що виглядало як база відпочинку. [31] Не підозрюючи про наслідки, він залишив активоване геотегування, тож деякі дописи містили точні координати. OSINT-аналітики в Twitter заміський клуб Grand Prix у селі Саги, Херсонська область. Навіть без вбудованих GPS-даних дослідники розпізнали візуальні особливості — декоративні елементи й логотип у вигляді лебедя на стіні, які відповідали зображенням з офіційного сайту Grand Prix. Елітний російський спецназ переховувався на цивільному об'єкті. 20 грудня 2022 року українські сили завдали удару по комплексу Grand Prix, повністю знищивши об'єкт. Чи був цей удар здійснений безпосередньо на основі OSINT-підказки, чи за іншими каналами — невідомо, але він стався всього через кілька днів після публікацій.

Іронія в тому, що той самий доброволець згодом сам зафільмував наслідки атаки — і виклав відео обгорілих руїн і розкиданого обладнання, фактично підтвердивши успішність удару. На одному з таких відео видно гранати та російську військову вантажівку серед уламків — доказ того, що об'єкт справді був військовою базою.

Російські військові або місцеві колаборанти часом публікують фото в напівприватних групах, не знаючи, що за цими каналами стежить українська розвідка. Наприклад, у середині 2023 року російський Telegram-канал із Луганська поширив фото нової радіолокаційної установки «десь біля Джанкоя» в окупованому Криму, хвалячись «покращеною ППО». Після чого було отримано супутникові знімки району Джанкоя та виявлено об’єкт, який збігався з РЛС «Подльот-К1» системи С-400 — з’явився він у травні 2024 року. [32] У червні 2024 року на цьому місці стався вибух — внаслідок удару ЗСУ, а зображення з відкритих джерел підтвердили знищення РЛС. Улітку 2023 року мешканець Севастополя виклав у «ВКонтакте» фото нової пускової установки С-400 на мисі Фіолент із підписом *«Крим надійно захищений»*. Пост помітили й вирахували геолокацію. Вже за кілька тижнів Україна здійснила атаку, внаслідок якої було знищено батарею С-400 саме на цьому мисі — ймовірно, ту саму, що була показана на фото. Хоча офіційні джерела не підтвердили використання цього поста, збіг виглядає промовисто. Українське Міноборони навіть саркастично подякувало «жителям Криму за фото» у Twitter після цього удару.

Кожен із цих прикладів ілюструє головну думку: інтеграція цивільної та військової розвідки стала для України мультиплікатором сили. Завдяки вмінню залучати громадян і незалежних аналітиків, Збройні сили України значно підвищили точність вогневого ураження та рівень ситуаційної обізнаності. Ці повідомлення, об’єднані з розвідданими з БПЛА, супутників і професійного OSINT, потрапляють до цифрової системи управління боєм «Дельта» — інтегрованої ситуаційної картини. Саме ця система, за оцінками, сприяла знищенню понад 1500 цілей до кінця 2022 року завдяки скороченню часу на ухвалення рішень.

3.2. Верифікація результатів вогневого ураження із застосуванням супутникових знімків та аеророзвідки

Після нанесення удару виникає принципове питання: чи вдалося уразити ціль і чи була вона знищена. Раніше відповідь на це могли надати лише військові розвідники або закриті джерела. Проте в умовах російсько-української війни розвідка на основі відкритих джерел отримала змогу незалежно перевіряти результати українських атак. Щойно з’являється повідомлення про вибух або влучання, починають очікувати наступного супутникового знімка з цієї місцевості. Якщо зображення доступні, їх зіставляють у форматі «до» і «після», щоб визначити масштаби ураження.

Удар по авіабазі Саки в окупованому Криму 9 серпня 2022 року став одним з таких прикладів. Спершу Росія оголосила про «випадкову детонацію боєприпасів» і заявила, що втрати літаків не було. Проте вже 10 серпня було опублікувано супутникові знімки, які розкривали зовсім протилежне. [33] На зображеннях були зафіксовані три великі вирви на стоянці літаків і поряд із нею — саме в тих місцях, де раніше розташовувалися об'єкти. Навколо епіцентрів вибухів чітко простежувались контури обгорілих залишків щонайменше восьми знищених бойових літаків. Тому стало очевидно, що на базі було знищено кілька Су-24 і Су-30.

Українські військові регулярно публікують відеозаписи влучань, зняті безпілотниками, особливо при застосуванні високоточної зброї або баражуючих боєприпасів. Зокрема, під час Харківського контрнаступу українські підрозділи поширювали відео, на яких зафіксовано ураження російських танків або ураження складів із боєприпасами. Хоча такі матеріали публікуються самою Україною, поширення їх у відкритих джерелах робить їх частиною загальнодоступного масиву даних. У випадках ударів по важливих об’єктах у тилу українські сили іноді використовують розвідувальні дрони для фіксації наслідків. Наприклад, у квітні

2022 року на авіабазі поблизу Бєлгорода пролунала серія вибухів. [34] Невдовзі з’явилося відео, зняте з квадрокоптера, що пролітав над територією бази. На кадрах було видно знищені вертольоти, що підтверджувало не лише сам факт атаки, але й наявність засобу спостереження, який одразу задокументував результат.

Після атак 5 грудня 2022 року на дві російські авіабази — Енгельс-2 і Дягілєво [35] було оприлюднено знімки обох об’єктів. На авіабазі Дягілєво в Рязанській області, приблизно за 200 км від Москви, було зафіксовано пошкодження на пероні та сліди вибухів, а також ушкоджений стратегічний бомбардувальник Ту-22М із характерними слідами обгорання й уламками поблизу. На знімках бази Енгельс-2 у Саратовській області, що на понад 600 км від кордону з Україною, наступного дня видно пожежну техніку біля знищеної ділянки, що, ймовірно, свідчило про масштабний вибух — попри заяви російської влади про «займання паливозаправника».

Стратегічна авіабаза Саки неодноразово ставала мішенню для українських ударів, і дані з OSINT-джерел відігравали ключову роль у підтвердженні їхньої результативності. Знищення щонайменше восьми російських літаків на злітній смузі в Криму стало однією з найвиразніших візуальних подій першого року повномасштабної війни. [36] [37] Для українського суспільства та міжнародної спільноти ці знімки стали прямим доказом здатності України вражати стратегічно важливі об’єкти глибоко в тилу противника. Тим часом російські громадяни, яким офіційно повідомляли про «випадковий інцидент без втрат», бачили в західних медіа фото обвуглених залишків авіації. Це частково підірвало довіру до державної пропаганди. Після цього випадку російські офіційні особи почали обережніше робити категоричні заперечення. Імовірно, наслідки мали й оперативний характер: після втрати такої кількості літаків, підтвердженої супутниками, російські ВКС були змушені перегрупувати наявну техніку та переглянути підходи до організації ППО.

Хоча Керченський міст не є військовою базою, удар по ньому в жовтні 2022 року також слугує прикладом, коли OSINT-інструменти дозволили оперативно прояснити ситуацію. [37] Після вибуху російська влада заявила, що конструкції не зазнали серйозних ушкоджень. Однак вже найближчим часом OSINT-аналітики отримали фотографії від місцевого населення та супутникові знімки, які свідчили про обвал частини автодорожнього мосту в воду та масштабну пожежу на залізничній гілці — особливо навколо потяга з пальним. Ці дані явно суперечили офіційному оптимізму Міністерства транспорту РФ і надали союзникам об'єктивну інформацію щодо ефективності атаки. Подібна ситуація трапилася у квітні 2023 року після удару по паливному складу в Севастополі: спершу з'явилися відео масштабної пожежі, опубліковані в Telegram, а вже наступного дня оприлюднено знімки з обгорілими ділянками й зруйнованими резервуарами.

У перші місяці повномасштабного вторгнення спостерігалася висока кількість загиблих вищих офіцерів ЗС РФ. Частину з них вдалося ідентифікувати та знищити завдяки перехопленню телефонних розмов і даним з відкритих джерел. Наприклад, генерал Яков Рязанцев здійснив дзвінок через незахищений канал зв'язку, що був перехоплений українською розвідкою. [38] Його присутність на авіабазі, яка вже перебувала під наглядом за допомогою БПЛА, невдовзі підтвердилася — по об'єкту було завдано удару. Після цього супутникові знімки зафіксували знищену техніку на місці, що слугувало непрямим підтвердженням загибелі генерала.

Україна також систематично завдавала ударів по об'єктах на прикордонній території Росії — зокрема у Бєлгородській, Курській та Брянській областях. Законною ціллю ставали паливні бази, склади боєприпасів, військові аеродроми. Показовим прикладом стала атака українських гелікоптерів на нафтобазу в Бєлгороді 1 квітня 2022 року. Відеозаписи палаючих резервуарів швидко з'явилися в інтернеті, а згодом знімки високої роздільної здатності підтвердили

повне знищення щонайменше двох резервуарів і значні пошкодження інших, що підтверджувало успішність атаки. [39] Водночас OSINT забезпечує не лише фіксацію успішних атак. Іноді супутникові зображення демонструють обмежені наслідки ударів або й узагалі відсутність пошкоджень. Наприкінці 2022 року було кілька спроб ударів по аеродрому в Курську та базі в Рязані (Дягілєво). [40] Російська сторона повідомила про їх нейтралізацію, й супутниковий аналіз дійсно не виявив серйозних руйнувань в одному з випадків у Курську.

Такий підхід до верифікації результатів ударів можна фактично вважати реальним Battle Damage Assessment (BDA), оскільки він дає змогу оперативному командуванню ухвалювати рішення: чи потрібно повторно бити по цілі, чи доцільніше змінити напрямок вогневого ураження. Також це допомагає протидіяти дезінформації. Кремль систематично заперечує або спотворює дані про українські удари, особливо на території РФ чи в окупованому Криму, прагнучи підтримувати образ контролю й сили. Проте матеріали з відкритих джерел дедалі частіше руйнують ці інформаційні бар'єри. Один із таких випадків — удар по Макіївці 1 січня 2023 року, коли ракета влучила в будівлю професійного училища, де перебували сотні мобілізованих російських військових. [41] Російська сторона спочатку визнала 63 загиблих, тоді як українські джерела повідомляли про щонайменше 400. У Telegram з'явилися фото й відео повністю зруйнованої будівлі, а супутникові знімки зафіксували її повне знищення. Оцінюючи масштаби об'єкта та рівень руйнувань, було зроблено висновок, що кількість загиблих справді могла становити кілька сотень, що підтверджувало українські оцінки. Для України це дає низку переваг: як країна, що зазнала збройної агресії, вона може відкрито демонструвати легітимність своїх дій, що зміцнює міжнародну підтримку й допомагає зберігати моральну перевагу. Міністерство оборони України, зокрема, часто публікує супутникові зображення знищеної російської техніки із саркастичними коментарями, використовуючи OSINT як інструмент стратегічної комунікації. Водночас така відкритість є двосічною: помилки чи випадкові втрати з українського боку також можуть бути зафіксовані й викриті. У випадках підозри

щодо загибелі цивільних від українських ударів досліджуються події з не меншою прискіпливістю — зокрема, аналізуючи уламки, воронки та місце влучання, як це було у випадках із ракетами С-300, які могли зійти з курсу.

3.3. Зміна тактичних підходів російських військ під впливом OSINT

Співпраця між OSINT-спільнотами та українськими військовими суттєво вплинула на підходи до планування й ведення бойових дій. Інформація з відкритих джерел, зібрана звичайними громадянами, значно розширила можливості виявлення цілей — як у масштабі, так і в швидкості. Якщо раніше командири були змушені покладатися переважно на традиційну розвідку з обмеженим охопленням, то тепер вони отримують оперативні дані з неофіційних джерел — через соцмережі, особисті пристрої, повідомлення цивільного населення. Це працює як розгалужена система спостереження, розташована буквально по всій країні. У тих районах, де немає постійного нагляду з повітря або радіолокаційного контролю, відкриті джерела заповнюють прогалини. Наприклад, коли російські війська перегруповувалися в маленьких селах або ховалися в тилу, саме місцеві мешканці першими повідомляли про їхню присутність. Потім аналітики перевіряли цю інформацію за супутниковими знімками — і часто це дозволяло попередити наступ або завдати удару ще до початку атаки. Це дає змогу бачити загальну картину, завдяки чому командування практично не втрачає з поля зору пересування ворога. Час між виявленням цілі й ударом по ній, так званий kill chain, істотно скоротився. Часто все починається з повідомлення випадкової людини, яке швидко перевіряється через геолокацію або зіставлення з іншими джерелами, після чого координати передаються до артилерійських або ракетних військ.

Інформація від цивільних часто допомагає ідентифікувати ті об’єкти, що не потрапляють у фокус традиційної розвідки. Люди повідомляють про будівлі окупаційної адміністрації, нові маршрути постачання, переміщення ворожих підрозділів. OSINT-групи, які відстежують рух поїздів, регулярно виявляють

ешелони з боєприпасами — це дозволяє наносити удари по ключових логістичних точках. Завдяки такій участі громадян та незалежних дослідників зростає не лише кількість цілей, а й різноманітність — від логістичних і командних об’єктів до символічних: наприклад, удар по штабу під час візиту високопосадовця, якого впізнали завдяки фото в мережі.

Ефективне застосування Україною OSINT для виявлення цілей змусило Росію також переглянути підходи до оперативної безпеки (OPSEC) та адаптувати власну тактику. [42] Після того як стало очевидно, що численні українські удари стали можливими саме завдяки відкритим джерелам — від селфі з геолокацією до повідомлень цивільних. Однією з перших реакцій Росії на потенціал української розвідки стало посилення вимог до використання особистих електронних пристроїв. Після удару по тимчасовому розміщенню особового складу в Макіївці, [43] внаслідок чого, за офіційними даними, загинули щонайменше 89 солдатів, а неофіційні джерела вказують на сотні втрат, Міністерство оборони РФ публічно поклало відповідальність на самих військових, які масово використовували мобільні телефони», що дозволило українцям визначити їхнє точне місце перебування та завдати прицільного удару. Попри те, що ще до цього випадку в російській армії формально діяла заборона на електронні пристрої з функціями зйомки або передачі геолокації, контроль за дотриманням правил був слабким. Після удару в Макіївці командири отримали наказ негайно вилучати телефони та попереджати про дисциплінарну відповідальність у разі порушення. У липні 2024 року ці обмеження набули юридичної сили: відповідно до нових змін у законодавстві, командирам надано право затримувати військовослужбовців на строк до десяти діб за використання особистих телефонів у зоні бойових дій. [44] Закон прямо забороняє мати будь-які пристрої, здатні зберігати або передавати звук, фото, відео чи геодані через інтернет. Формулювання про «забезпечення безпеки військовослужбовців» на практиці означає намагання зменшити вразливість до української розвідки. Генерал Андрій Картаполов, один із авторів законодавчих

змін, заявив, що ЗСУ виявляють російських солдатів за сигналами пристроїв — тому потрібен жорсткий контроль.

Однак у реальності запровадження таких заходів виявилося непростим. Солдати, особливо строковики, сильно залежать від телефонів — і як засобу орієнтації, і для спілкування з родичами, зважаючи на ненадійність штатного військового зв'язку. Частина особового складу відмовлялася дотримуватися правил або намагалася їх обходити — зокрема, користуючись одноразовими SIM-картами чи ховаючи телефони. Навіть російські воєнкори та окремі чиновники критикували такі обмеження, називаючи їх безглуздими, адже без альтернативи солдати фактично залишаються без зв'язку. Дмитро Рогозін зазначав, що досвідчені бійці вже давно поводяться обережно — вимикають пристрої, не надсилають фото. Проте повна заборона, без одночасного забезпечення захищених каналів зв'язку, може спричинити ізоляцію підрозділів і створити ще більші ризики. Деякі аналітики прямо вказували, що одна з цілей таких обмежень — не стільки захист від українських сил, скільки контроль над інформацією, щоб солдати не могли фіксувати або публікувати невигідні для Кремля факти.

Напруження між вимогами секретності та реальними потребами на полі бою стало очевидним. Намагання зменшити цифровий слід є логічним із тактичного погляду, але водночас це уповільнює внутрішню комунікацію та негативно впливає на моральний стан військових. Попри це, обмеження залишаються чинними. Підрозділи змушені повертатися до дротового зв'язку або використовувати зашифровані радіостанції — там, де вони справді є. У багатьох частинах телефони збирають перед виходом на бойові завдання, а з рідними дозволяють зв'язуватися лише під наглядом. Державні телеканали навіть транслювали заклики до родичів: *«НАТО слухає ваші розмови»* — із проханням переконати військовослужбовців вимикати телефони. Є непідтверджені повідомлення, що українські підрозділи радіоелектронної розвідки здатні перехоплювати незашифровані розмови та

оперативно передавати координати артилерії, що додатково посилює тиск на дотримання заборон.

Ще одним кроком з боку Росії у відповідь на ефективність українського OSINT стало обмеження доступу медіа й заборона зйомки на передовій. У 2022 році траплялося чимало випадків, коли військові викладали відео в TikTok або VK, не підозрюючи, що навіть фонові деталі або серійні номери на техніці можуть видати їхнє точне місцезнаходження. Побачивши, як Україна використовує ці матеріали, російська влада почала впроваджувати жорстку цензуру. Солдатам офіційно заборонили публікувати будь-які фото чи відео з фронту. Навіть воєнним блогерам і журналістам стали обмежувати доступ — Міністерство оборони РФ встановило суворий контроль над тим, що саме дозволено показувати, остерігаючись, що українські аналітики зможуть виявити важливі деталі з найменших фрагментів. Уже з середини 2023 року випадки «шкідливого» користування смартфонами на передовій майже зникли — солдати ризикували не лише потрапити під український обстріл, а й отримати покарання від власного командування.

Результати цих заходів виявилися неоднозначними. З одного боку, українські військові визнають, що російська оперативна безпека справді покращилася: перехопити випадкові дзвінки чи сигнали стало складніше, а подібні до Макіївки масові втрати не повторювалися в такому масштабі — принаймні, через більшу обережність. З іншого боку, повна відмова від смартфонів створила інші проблеми. Багато солдатів продовжують користуватися телефонами з необхідності. У деяких підрозділах координація відбувається через Telegram, особливо коли штатні рації не працюють. Кожне таке повідомлення — потенційна мішень для української радіорозвідки. Крім того, брак мобільних пристроїв може уповільнювати обмін інформацією й погіршувати ситуаційну обізнаність. Під час одного з боїв українські сили зафіксували, як російські піхотинці, опинившись у відрізаному положенні, не змогли викликати підкріплення через відсутність зв’язку й були змушені хаотично відступити. [45]

Хоча посилені вимоги до OPSEC зменшили кількість грубих помилок, які активно використовували українські аналітики з відкритих джерел, вони водночас обмежили здатність військових оперативно передавати інформацію й швидко реагувати на зміни на полі бою. У сучасній війні, де майже кожен сигнал може бути відстежено, а повне мовчання — майже нереальне, російські війська опинилися в ситуації, коли будь-яка комунікація може виявитися фатальною, але її відсутність — не менш небезпечною.

Ще однією відповіддю Росії на можливості українського OSINT стала модернізація методів маскування та активне використання фальшивих зразків техніки. Коли українські дрони та супутники ведуть постійне спостереження за полем бою, причому ці дані часто потрапляють у відкритий доступ і аналізуються OSINT-групами, російське командування вирішило вдатися до старих, але адаптованих до нових умов методів обману. Армія РФ почала масово використовувати муляжі техніки: надувні танки, імітації артилерії, макети фортифікацій — усе для того, щоб збити з пантелику розвідку й змусити українську артилерію бити по порожніх цілях. [46]

Відомо, що як Росія, так і Україна використовують реалістичні муляжі — зокрема, надувні копії танків Т-72 у натуральну величину, щоб обманути дрони або ввести в оману супутникову розвідку. Такі моделі призначені для того, щоб відвернути вогонь від справжньої техніки й зберегти ресурси. Російський 45-й інженерний полк, який спеціалізується на виготовленні засобів маскування, після початку затяжної фази війни суттєво наростив виробництво таких об’єктів. Уже наприкінці 2022 року українські оператори дронів почали фіксувати підозрілі скупчення техніки в лісосмугах. [46] На перший погляд вона здавалася справжньою, але при наближенні ставало зрозуміло, що це муляжі: округлі форми, гладкі поверхні, відсутність рухомих частин. В одному з випадків дрон ЗСУ зафіксував кілька «танків» Т-72 на відкритій місцевості, але при детальнішому огляді виявилося, що це надувні копії. Якби розвідники діяли поспіхом, вони могли

б навести артилерію на гумові мішені — і марно витратити дорогі боєприпаси, зокрема ракети HIMARS або дрони-камікадзе. Саме на це і розраховує Росія: змусити українські сили витрачати ресурси на хибні цілі, зберігаючи натомість справжню бойову техніку.

Крім надувних моделей техніки, Росія активно використовувала дерев'яні муляжі та теплові імітатори. Деякі з них були досить простими — це могли бути дерев'яні каркаси гармат, прикриті брезентом, але траплялися й складніші конструкції з вбудованими нагрівачами, які імітували тепловий слід. Російська армія також встановлювала фальшиві батареї С-300 із дерев'яними радарами в зонах, добре видимих із супутника, намагаючись відволікти увагу українських сил, що займаються придушенням систем ППО. На укріплених лініях, особливо на півдні, розміщували фальшиві міномети та пускові установки, щоб спрямувати українські дрони на незначущі об'єкти. Є підтвердження, що частина таких маніпуляцій спрацювала: українські снаряди влучали в муляжі, а російські медіа охоче повідомляли про те, як українці «знищили» гумові танки, досягши лише ефектного вибуху повітря. [46]

Паралельно з розгортанням фальшивок російська армія почала активніше працювати над маскуванням справжньої техніки. Військовим наказали ретельно накривати танки й вантажівки маскувальними сітками, особливо під час зупинок. Після численних вибухів складів боєприпасів, які були легко виявлені на супутникових знімках просто неба, російські логістичні підрозділи почали ховати такі об'єкти під деревами або на територіях цивільних підприємств. Постачання переміщується здебільшого вночі або за несприятливих погодних умов, аби зменшити ймовірність виявлення з повітря. На передовій копають фальшиві траншеї й командні пункти, а справжні приховують під кількома шарами маскувальних матеріалів. Навіть великі системи оборонних ліній, що почали з'являтися у 2023 році, частково маскували: використовували старі шини, насипи ґрунту й підручні матеріали, щоб розмити обриси на аерофотознімках. [46]

До змін пристосувалися й повітряні сили. Коли українські сили почали виявляти окремі літаки й гелікоптери за їхніми бортовими номерами, ці маркування почали замальовувати або заклеювати. Аналогічну практику застосували й на флоті: після потоплення крейсера «Москва» більшість російських кораблів, що перебувають у районах бойових дій, вимкнули транспондери AIS, щоб унеможливити відкритий моніторинг їхнього переміщення.

Російське командування чітко усвідомлює загрози, які створює відкритий інформаційний простір. Однак їхня ефективність залишається обмеженою. Муляжі можуть збити з пантелику під час першого візуального контакту, але сучасні українські дрони здебільшого наближаються достатньо близько, щоб розрізнити справжнє від підробки. В одному з випадків оператори ЗСУ ідентифікували надувні танки та не витрачали на них боєприпаси, зберігаючи їх для реальних цілей. Тепловізори й супутникові знімки високої роздільності здатні виявити ключові відмінності — зокрема, відсутність теплового сліду, який залишає працюючий двигун. Крім того, виготовлення й встановлення муляжів потребує часу й ресурсів, що знижує темп операцій. Російські колони були змушені зупинятися кожні кілька кілометрів, аби сховатися або розгорнути маскування, побоюючись удару з неба — це справді зменшує ризик виявлення, але одночасно уповільнює наступальні дії.

Зміни торкнулися й тактики переміщення. Російські колони стали пересуватись переважно вночі або в умовах обмеженої видимості — на світанку або в сутінках. Маршрути щоразу змінюються. Якщо на початку вторгнення війська часто пересувались основними дорогами (що робило їх легкою ціллю для засідок або спостереження з боку місцевих мешканців), то згодом почали використовувати другорядні або ґрунтові шляхи. Це іноді призводить до зупинок через ускладнений проїзд, однак зменшує ризик виявлення. Танкові підрозділи в активних зонах змінюють позиції щодня або через день, аби уникнути виявлення розвідувальними дронами, які можуть коригувати українську артилерію.

Однак подібні адаптації мають і очевидні обмеження. Постійні переміщення й розосередження шкодять злагодженості дій і знижують бойову ефективність. Солдати часто скаржаться на виснаження через нічні переїзди, які здійснюються «для уникнення дронів» — вони позбавляють відпочинку, ускладнюють орієнтування та залишають менше часу на облаштування позицій. В умовах оборони це означає менш укріплені рубежі й недостатнє знання місцевості. Перенесення складів і штабів у тил підвищує шанси на виживання, але затягує логістику та ускладнює координацію. До того ж українські удари не припинились — просто тепер вони дедалі частіше націлені на менші, мобільні об’єкти. Тобто російські зусилля з мінімізації втрат нерідко обертаються сповільненням загального темпу операцій.

ВИСНОВКИ

Проведене дослідження дозволило не лише систематизувати роль розвідки відкритих джерел (OSINT) у російсько-українській війні періодом з 2022 по 2023 роки, а й побачити в ній ознаки нового типу воєнної розвідки. Йдеться про появу інформаційної автономії на полі бою, коли розвідка більше не є виключною прерогативою держави. У традиційній моделі розвідка була централізованою, секретною, вертикальною. OSINT — її повна протилежність: горизонтальна, доступна, відкрита і часто здійснювана волонтерами. У майбутніх війнах це означатиме, що розвідка стане масовою діяльністю, адже участь братимуть не лише армії, а й приватні аналітики, журналісти, технічні фахівці. Це змінить структуру суб'єктів конфлікту: до класичних армій додадуться цивільні розвідники, які матимуть змогу впливати на бойові рішення.

OSINT на українському театрі війни не лише доповнює традиційні розвідувальні засоби, але й переосмислює їхню ієрархію: у ряді випадків саме відкриті джерела випереджали за точністю й швидкістю спецслужби, створюючи «розвідку знизу». Вперше в історії війна стала спостережуваною у реальному часі, що змінило як саму логіку планування операцій, так і інформаційний контроль над ними.

Ключовим висновком дослідження є те, що український досвід інтеграції OSINT — це не лише адаптація до нових умов, а створення нової гібридної моделі воєнної розвідки, в якій поєднано волонтерські ініціативи, цифрові технології, елементи OSINT-аналітики, супутникові дані, дрони та соціальні платформи. Ця модель дозволяє змінювати вертикальні обмеження традиційної розвідки, мобілізувати інтелектуальні ресурси суспільства й підвищувати гнучкість реагування на загрози.

Змістовно, OSINT у війні проти Росії став не лише інструментом знищення, а й інструментом справедливості: саме завдяки відкритим джерелам фіксуються злочини проти цивільного населення, збирається доказова база для майбутніх

трибуналів, формується міжнародна підтримка, а також реалізується право громадян на інформацію. У цьому сенсі OSINT перетворюється з технічного ресурсу на політико-правовий механізм — засіб міжнародного тиску, легітимації та дипломатичного захисту.

У перспективі, OSINT може стати архітектурною складовою сучасної оборонної політики — не як допоміжна опція, а як структурно інтегрований елемент державної системи національної безпеки. Його подальший розвиток через автоматизацію, AI-інструменти, розширення мережевої співпраці відкриває шлях до створення постнаціональних форм розвідки, де суб'єктом виступає не лише держава, а й глобальна OSINT-спільнота.

Досвід застосування OSINT під час Харківської та Херсонської операцій дозволяє окреслити не лише його поточне значення у війні, а й перспективи інституційного, технологічного та концептуального розвитку відкритої розвідки в майбутньому. Емпіричні матеріали, зібрані в межах інтерв’ювання [Додаток А] [Додаток Б] безпосередніх учасників бойових дій, свідчать про поступову трансформацію OSINT із неформального допоміжного інструменту в повноцінну частину оперативного й стратегічного циклу прийняття рішень.

Одним із головних напрямів розвитку є формалізація OSINT-груп у межах структур Збройних Сил України. Респонденти вказують, що навіть у межах окремих підрозділів вже формуються локальні «аналітичні осередки» з обробки відкритої інформації. Ці групи не лише моніторять Telegram-канали чи соцмережі, а здійснюють верифікацію, геолокацію, фільтрацію та передають оперативно підтверджені дані в командні пункти. У подальшому можливе створення постійно діючих OSINT-підрозділів у складі бригад, які матимуть власне програмне забезпечення, штатні алгоритми фільтрації, протоколи звітності та захищені канали зв’язку.

Одночасно очевидною стає потреба в централізованому нормативному оформленні OSINT у межах оборонної доктрини. Практики, які сьогодні базуються на ініціативі окремих людей, повинні мати офіційний статус, стандартизовані правила верифікації, захист операторів та прозору відповідальність за використання недостовірних або незахищених джерел. Як зазначили респонденти, використання VPN, анонімних профілів і технік цифрової гігієни вже впроваджується на практиці, однак потребує інституційної підтримки у вигляді освітніх інструкцій, кібербезпеки та програмної інфраструктури.

На стратегічному рівні, український досвід свідчить про можливість інтеграції OSINT у багатоетапну систему планування операцій — від підготовки до оцінки результатів. У випадку Херсонської операції, саме через Telegram-канали й фото мешканців було підтверджено ефективність ударів по переправі, виявлено відступ ворога та зафіксовано зникнення блокпостів. У Харківській операції відкриті джерела дозволили виявляти місце розташування тилових складів і визначати оптимальні напрямки наступу в режимі, близькому до реального часу.

Таким чином, український досвід доводить: у війнах майбутнього перемагає не лише той, хто має більше зброї, а той, хто швидше бачить, точніше аналізує й ефективніше діє на основі відкритої, динамічної інформації. У майбутньому перемога залежатиме не лише від того, хто перемістив танки, а хто першим побачив, зафіксував і інтерпретував переміщення ворога. Це означає, що інформаційне поле бою (супутники, дрони, відео в соцмережах) стає таким же важливим, як географічне. OSINT трансформує військове мислення: не позиційне утримання, а перевага у спостереженні, геолокації, аналізі. І в цьому новому просторі — інформаційна ініціатива дорівнює тактичній перевазі.

ДОДАТКИ

Додаток А

Транскрипт інтерв'ю з військовослужбовцем Збройних Сил України, учасником Харківської операції (вересень 2022 року)

Ім'я, прізвище, посада та підрозділ респондента не розголошуються з міркувань безпеки. Всі дані публікуються з його усної згоди на використання в академічному дослідженні.

І – інтерв'юєр
Р – респондент

І: Як саме у вашому підрозділі використовували OSINT під час Харківської операції?

Р: Відкриті джерела ми активно використовували з першого етапу — ще до початку основного руху. Усе, що стосувалося ситуаційної обізнаності: пересування противника, їхні склади, блокпости, навіть налаштованість місцевих — усе це часто базувалося на відкритих даних. Ми аналізували інформацію з соціальних мереж, публікацій у ворожих Telegram-каналах, навіть коментарі під відео були іноді цінними. Особливо уважно стежили за мапами, які самі ж росіяни публікували для «своїх» — ті були справжнім джерелом орієнтування.

І: Чи були випадки, коли відкриті джерела допомогли прийняти рішення на місці або змінити хід дій?

Р: Були. Один із найяскравіших — це ситуація біля Шевченкового. Ми вирахували по фото, опублікованому у російському каналі, що один із їхніх тилових складів перемістили в будівлю колишнього агропідприємства. Ми передали координати — за кілька годин туди вже прилетіло. Також були випадки, коли через відео з Telegram-каналів ми ідентифікували напрямки відступу росіян і одразу скоригували маршрут наступу.

І: Які саме інструменти або платформи використовувались для аналізу інформації?

Р: У нас не було якихось надпотужних аналітичних систем, але ми працювали з тим, що вміємо. DeepState часто допомагали нам орієнтуватись. Часто доводилося працювати з Telegram вручну — просто годинами сидіти і переглядати відео, фото, тексти. Бувало, що одну фотографію три людини перевіряли по різних каналах, перш ніж підтвердити місце.

І: Як ви оцінюєте точність та надійність інформації, зібраної через OSINT під час операції?

Р: Вона не завжди точна, але якщо вміти перевірити — дуже корисна. Ми завжди шукали візуальні підтвердження: танк, знак, вивіска, фон — усе це допомагало локалізувати. Один раз надійшов «злив» про колону техніки в певному районі. Перевірили по Google Maps — не збігається з місцевістю. Тобто була дезінформація. Але це скоріше виняток. Як тільки з'являлася можливість верифікації — ми її використовували.

І: Які труднощі виникали під час роботи з відкритими джерелами?

Р: Росіяни дуже швидко зрозуміли, що ми «читаємо» їх. У перші дні наступу інформації було багато — вони панікували, викладали все. Потім — тиша. Почали блокувати коментарі, ставити обмеження, зникли звичні канали. Почалась інформаційна тиша. А ще одна проблема — це обмеження часу. Ти не можеш перевіряти фото годину, коли командир чекає координати зараз. Працюєш по відчуттю, а це не завжди гарантія.

І: Чи застосовувалися якісь заходи безпеки при зборі та обробці OSINT-інформації?

Р: Звісно. Ми не працювали зі своїх основних телефонів. Все — через VPN, анонімні акаунти, без персональних даних. Ніхто не заходив у російські пабліки без

захисту. У нас навіть була окрема «освітня пам’ятка». Бо вони ж теж не дурні — шукають, хто читає їхні канали.

І: Які, на вашу думку, головні переваги OSINT у контексті саме Харківської операції?

Р: Швидкість і гнучкість. Ми бачили те, чого ще не було в офіційних каналах. Часто ще до наказу з командування ми вже розуміли, що десь є «вікно» — бо з відео видно, що там немає техніки. І це дозволяло діяти. Також величезна перевага — розуміння морального стану. По публікаціях, по паніці, по мемах навіть — усе це давало нам уявлення, наскільки вони готові тримати позиції.

І: Чи OSINT вплинув на вашу впевненість у результаті операції?

Р: Безперечно. Коли ти бачиш, як у реальному часі противник кидає позиції, зливає координати своїх складів, як їхні воєнкори кричать про «зраду» — ти розумієш, що у них усе валиться. І це не просто чутки — це фото, відео, карти. Вони самі допомагали нам перемагати.

І: Яким чином OSINT інтегрувався в загальну систему прийняття рішень у вашому підрозділі?

Р: Я б сказав, що в нас уже виробився рефлекс: кожне рішення, яке стосується розвідки чи коригування вогню, супроводжується спробою підтвердити все через відкриті джерела. Наприклад, якщо підрозділ на фланзі повідомляє, що виявив рух техніки ворога — ми одразу перевіряємо пабліки місцевих, шукаємо фото, відео, звіряємо з останніми супутниковими даними. Якщо є збіг — передаємо «наверх» з вказівкою на підтвердження. І це пришвидшує ланцюг прийняття рішень.

І: Наскільки командування сприймає OSINT як серйозний інструмент?

Р: Якщо чесно, на початку 2022 року були сумніви. Але після Харкова все змінилося. Особливо коли ми кілька разів на основі OSINT дали точну інформацію, яка дозволила завдати удару по росіянам. Після цього командири почали самі

звертатися — «подивись, що там є», і так далі. Тобто OSINT став частиною інструментарію, а не просто «додатковою опцією».

І: Як, на вашу думку, виглядає майбутнє OSINT у структурах ЗСУ?

Р: Думаю, це стане окремим напрямом у кожній бригаді. Уже зараз в деяких підрозділах з’являються окремі «OSINT-групи» — це кілька людей з ноутбуками, які сидять у безпечному місці і цілодобово моніторять канали, геолокують, звіряють. І це дає реальний ефект. У нас війна не лише на землі, а й в інформаційному просторі — і той, хто першим побачив або правильно розшифрував інформацію, має перевагу. У цьому сенсі OSINT — це не просто розвідка, а фактор оперативної переваги.

Додаток Б

Транскрипт інтерв'ю з військовослужбовцем Збройних Сил України, учасником Херсонської операції (жовтень-листопад 2022 року)

Ім'я, прізвище, посада та підрозділ респондента не розголошуються з міркувань безпеки. Всі дані публікуються з його усної згоди на використання в академічному дослідженні.

І – інтерв'юєр

Р – респондент

І: У чому полягала особливість використання OSINT під час підготовки до Херсонської операції?

Р: Ми мали справу з добре укріпленим противником, тому акцент був на вивченні логістики та вразливостей у тилу. Багато інформації ми отримували через відкриті джерела — це фото складів, переправ, розвантаження техніки, які самі ж росіяни або місцеві зливали у Telegram. Особливо важливим було фіксування руху через Антонівський міст — ми відслідковували, коли й скільки вантажів йде, і це дозволяло прогнозувати, де вони накопичують боєприпаси.

І: Які типи даних були найкориснішими для вашого підрозділу?

Р: У нашому випадку — звісно Telegram. Ми дуже уважно моніторили місцеві херсонські пабліки, тому що часто саме мешканці знімали рух колон, пуски ракет, роботу ППО. Багато цінної інформації надходило з коментарів у російських групах. Іноді навіть через фото розвантаження можна було встановити точну точку — ми цим активно користувалися.

І: Як це виглядало в динаміці самої операції?

Р: Коли ми почали наносити удари по мостах і переправах, важливо було в режимі майже реального часу розуміти, наскільки ефективними були ці дії. Вже за годину після удару на каналах з'являлися фото пошкодженого мосту. Так ми знали, де

ворожа логістика «зламалась» і куди треба бити далі. Так само ми відслідковували, коли противник почав активно вивозити техніку — знову ж таки, перші сигнали ми отримали не від БПЛА, а з Telegram.

І: А як щодо моменту самого звільнення Херсона — чи був OSINT корисним?

Р: Так, і навіть більше — ворожі джерела самі підтвердили свій відступ. У перший день листопада ми побачили, що росіяни зняли свій прапор з адмінбудівлі — це було на відео, опублікованому в одному з російських каналів. Ми одразу передали це «наверх», і це стало одним із сигналів, що противник реально готується до втечі. А потім пішли фото і відео від самих херсонців — як вони зустрічають наших, як зникають російські блокпости. Це були найемоційніші OSINT-докази.

І: Як ви працювали з верифікацією такої кількості даних?

Р: Ми створили свою внутрішню таблицю з координатами, мітками часу, джерелами. Для геолокації використовували класичний набір — супутникові карти, Google Street View (де ще був доступ), і програми для фільтрації метаданих. Ми завжди перевіряли інформацію мінімум у двох незалежних джерелах, щоб не втрапити на фейк або навмисну дезу.

І: З якими викликами ви зіштовхнулися під час роботи з OSINT у Херсоні?

Р: Противник став обережнішим. Якщо у Харкові вони зливали все підряд, то у Херсоні вже було більше дисципліни. Крім того, в багатьох районах зник інтернет — або ми не мали сигналу, або росіяни його глушили. Ще одна проблема — це брак часу: у нас були лічені хвилини на аналіз, особливо в момент евакуації. Було багато хибних тривог, і ми мусили швидко відсівати інформаційний шум.

І: Чи змінювалося ставлення вашого командування до OSINT у процесі операції?

Р: Помітно змінювалося. Якщо на початку більшість сприймала це як «цікаву додаткову штуку», то ближче до листопада OSINT-аналіз став повноцінним

джерелом оперативної інформації. Ми мали вже свою «міні-групу» OSINT-офіцерів, які займалися лише моніторингом відкритих джерел і щодня доповідали. Деякі рішення приймалися одразу після підтвердження з відкритих каналів.

І: Що б ви змінили або вдосконалили в системі роботи з відкритими джерелами у майбутніх операціях?

Р: Я б централізував систему. Зараз часто все тримається на ініціативі окремих людей. Треба створити формальні протоколи перевірки, фільтрації, маркування пріоритетності інформації. І обов’язково — інструменти захисту. Бо вони ж теж бачать усе, що бачимо ми.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NATO. (2021). Allied Joint Doctrine for Intelligence *(AJP-2)* – Annex on OSINT https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP21.pdf

2. Gelpi, C. et al. (2024). The Rise of Open-Source Intelligence. European Journal of International Security, 9*(1).* https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-opensource-intelligence/21122432399ECB8078BF0D89A76D0586

3. Rasmussen, C. (2024). Commentary: How the IC has held back OSINT. Studies in Intelligence, 68*(2).* https://www.cia.gov/resources/csi/studies-in-intelligence/studies-in-intelligence-68-no-2-june-2024/commentary-how-the-intelligence-community-has-held-back-open-source-intelligence-and-how-it-needs-to-change/

4. AFCEA. (2023). OSINT: Revolution or Renaissance? https://www.afcea.org/signal-media/intelligence/osint-revolution-or-renaissance

5. Williams, H., & Blum, I. (2018). Defining Second-Generation OSINT for the Defense Enterprise. RAND Corporation https://www.rand.org/pubs/research_reports/RR1964.html

6. Centre for Information Resilience (2023). How OSINT shaped reporting on the war in Ukraine https://www.info-res.org/eyes-on-russia/articles/how-osint-shaped-reporting-on-the-war-in-ukraine/

7. Higgins, E. (2019). Interview in Malicious Life Podcast https://www.cybereason.com/blog/malicious-life-podcast-celebrating-five-years-of-malicious-life

8. Suherwan, K. (2023). The Proliferation of Intelligence Gathering: OSINT. Sycamore Institute Blog https://www.sycamoreinstitute.org/post/the-proliferation-of-intelligence-gathering-open-source-intelligence

9. Realfonzo, U., The Brussels Times (Sept 11, 2022), "Ukraine using disinformation tactics to recapture territory in Kharkiv region" https://www.brusselstimes.com/world-all-news/287513/ukraine-using-disinformation-tactics-to-recapture-territory-in-kharkiv-region

10. Kofman, M., Gady, F. S., Taylor & Francis (Mar 28, 2023). "Ukraine's stratetgy of attrition" https://www.tandfonline.com/doi/full/10.1080/00396338.2023.2193092#d1e108

11. Dylan, H., Gioe, D., & Little, J., "The Kherson Ruse: Ukraine and the Art of Military Deception", Modern War Institute (Dec 2022) https://mwi.westpoint.edu/the-kherson-ruse-ukraine-and-the-art-of-military-deception/

12. Mitchell, W., Journal of Applied Operational Intelligence (2024), "Assessing Deception Projection via OSINT: The Case of the Ukraine 2022 Counter-Offensive" https://www.ubplj.org/index.php/jaoi/article/view/2266

13. 2022 Kharkiv counteroffensive. Military Wiki. https://military-history.fandom.com/wiki/2022_Kharkiv_counteroffensive

14. War Ukraine ua https://war.ukraine.ua/articles/ukraine-counteroffensive/

15. Institute for the Study of War. Institute for the Study of War. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-july-6

16. ISW: the Ukrainian Armed Forces continue to create conditions for a counteroffensive on Kherson. Бабель. https://babel.ua/en/news/81097-isw-the-ukrainian-armed-forces-continue-to-create-conditions-for-a-counteroffensive-on-kherson

17. Ukrinform. (2022, 10 вересня). Ukrainian flag solemnly raised in Balakliya. https://www.ukrinform.net/rubric-ato/3568457-ukrainian-flag-solemnly-raised-in-balakliya.html

18. Ukraine Pushes On With Counteroffensive As Russian Invasion Enters 200th Day. RadioFreeEurope. https://www.rferl.org/a/russia-announces-withdrawal-kharkiv-ukraine/32026977.html

19. Chernichkin, K., The Kyiv Independent (Nov 13, 2022), "Kherson celebrates liberation after 8 months of Russian occupation (PHOTOS)" https://kyivindependent.com/kherson-celebrates-liberation-photos/

20. Oryx. (2022, February). Attack on Europe: Documenting equipment losses during the 2022 Russian invasion of Ukraine. Oryxspioenkop. https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html

21. Global Espreso. (n.d.). Satellite images shared online show Antonivsky Bridge damage. Global Espreso. https://global.espreso.tv/satellite-images-shared-online-show-antonivsky-bridge-damage

22. The Moscow Times. (2022, November 3). Russian flag disappears from Kherson administration in first signal of potential retreat. https://www.themoscowtimes.com/2022/11/03/russian-flag-disappears-from-kherson-administration-in-first-signal-of-potential-retreat-a79282

23. NASA Earthdata. (n.d.). Earthdata. NASA. https://www.earthdata.nasa.gov

24. Ahram Online. (2022). Russian troops withdraw from Kherson in major retreat. Ahram Online. https://english.ahram.org.eg/NewsParis/477202.aspx

25. El País. (2022, November 10). The Ukraine war in maps: Kherson retreat, largest withdrawal of Russian troops since Kyiv. El País English Edition. https://english.elpais.com/international/2022-11-10/the-ukraine-war-in-maps-kherson-retreat-largest-withdrawal-of-russian-troops-since-kyiv.html

26. Khurshudyan, I., & Dixon, R. (2022, November 11). Kherson retaken: A political defeat for Putin as Ukrainian troops enter city. The Washington Post. https://www.washingtonpost.com/world/2022/11/11/kherson-vladimir-putin-political-defeat-/

27. Institute for the Study of War. (2022, October 10). Russian offensive campaign assessment, October 10. Critical Threats. https://www.criticalthreats.org/analysis/russian-offensive-campaign-assessment-october-10

28. CounterPunch. (2024, July 5). The growing weaponization of open-source information. https://www.counterpunch.org/2024/07/05/the-growing-weaponization-of-open-source-information/

29. Molfar. How did the Armed Forces of Ukraine strike the Saky airfield in Crimea?https://molfar.com/en/blog/crimea-strike

30. NPR. (2022, February 28). Satellite images show 40-mile-long Russian military convoy nearing Kyiv. https://www.npr.org/sections/pictureshow/2022/02/28/1083650286/satellite-images-show-40-mile-long-russian-military-convoy-nearing-kyiv

31. Task & Purpose. Russian military OPSEC failure in Ukraine. https://taskandpurpose.com/news/russian-military-opsec-failure-ukraine/

32. Українська правда. (2023, August 23). У Криму стався вибух на авіабазі. https://www.pravda.com.ua/news/2023/08/23/7416743/

33. Радіо Свобода. (n.d.). Генштаб підтвердив удар по аеродрому Саки. https://www.radiosvoboda.org/a/news-henshtab-udar-aerodrom-saky/33051954.html

34. Корреспондент.net. Авіаудар на Бєлгород: чийі гелікоптери завдали удару. https://ua.korrespondent.net/world/russia/4462500-avianalit-na-bielhorod-chyi-helikoptery-zavdaly-udaru

35. The Eye Wales. Communication breakdown. https://the-eye.wales/communication-breakdown-2/

36. Українська правда. (2022, August 12). Серія вибухів у Криму – подробиці. https://www.pravda.com.ua/rus/news/2022/08/12/7363071/

37. Мілітарний. Ракети “Нептун” уразили аеродром Саки в Криму. https://militarnyi.com/uk/news/rakety-neptun-urazyly-aerodrom-saky-v-krymu-1/

38. YouTube. Спецоперації перемоги. СБУ [Відео]. https://youtu.be/boFFJRuxhPA?si=OUA3uRsiQFwX0X5F

39. УНІАН. ЗСУ ліквідували ще одного російського генерала в Чорнобаївці. https://www.unian.net/war/unichtozhen-v-chernobaevke-vsu-likvidirovali-eshche-odnogo-rossiyskogo-generala-arestovich-novosti-vtorzheniya-rossii-na-ukrainu-11759224.html

40. Мілітарний. У російському Бєлгороді горить нафтобаза – звинувачують ЗСУ. https://militarnyi.com/uk/news/u-rosijskomu-byelgorodi-goryt-naftobaza-zvynuvachuyut-zsu/

41. Liga.net. Пожежа і вибухи на авіабазах у Рязані й Енгельсі. https://news.liga.net/ua/world/news/proizoshlo-vozgoranie-vzryv-utrom-ne-tolko-v-engelse-no-i-na-aviabaze-v-ryazani

42. ABC News Australia. (2024, August 22). Russian government tells Kursk region to stay off dating apps. https://www.abc.net.au/news/2024-08-22/russian-government-tells-kursk-region-stay-off-dating-apps/104256114

43. The Guardian. (2023, January 4). Makiivka strike: What we know about the deadliest attack on Russian troops since Ukraine war began. https://www.theguardian.com/world/2023/jan/04/makiivka-strike-what-we-know-about-the-deadliest-attack-on-russian-troops-since-ukraine-war-began

44. BBC News Україна. (2023, January 4). Що відомо про удар по Макіївці. https://www.bbc.com/ukrainian/features-64144811

45. Міністерство оборони України. (2023). Рік війни за свободу. Книга 1 [PDF]. https://www.mil.gov.ua/content/Rik_viiny_za_svobodu_(knyha1).pdf

46. Мілітарний. Муляжі у війні: як використовуються фальшиві об’єкти. https://militarnyi.com/uk/tag/mulyazhi/

АНОТАЦІЯ

Кваліфікаційної роботи

Тема: «Розвідка відкритих джерел у російсько-українській війні з 2022 по 2023 роки»

Студентка: Артеменко Олександра Олександрівна

Рік навчання, факультет: 4, ФСНСТ

Науковий керівник: Осадчук Роман Юрійович, старший викладач кафедри міжнародних відносин

Рецензент: (вчений ступінь, вчене звання, прізвище та ініціали)

Захищена **«_» _____** 2025 р.

Короткий зміст роботи:

У кваліфікаційній роботі проаналізовано використання розвідки відкритих джерел (OSINT) у контексті російсько-української війни 2022-2023 років. Зосереджено увагу на сутнісних характеристиках OSINT, його еволюції як розвідувальної дисципліни, а також механізмах застосування у бойових діях. Особливу увагу приділено кейсам застосування OSINT під час Харківської та Херсонської контрнаступальних кампаній, а також у верифікації ударів по цілях на тимчасово окупованих територіях і на території РФ. Встановлено, що OSINT суттєво впливає на оперативну обізнаність, прогнозування дій противника, формування стратегічного наративу війни та забезпечення міжнародної доказової бази. Робота також окреслює обмеження, ризики та перспективи розвитку відкритої розвідки в умовах сучасних гібридних конфліктів.

Ключові слова: *OSINT, розвідка відкритих джерел, війна в Україні, супутникова розвідка, цифрова розвідка, Харківська операція, Херсонська операція, інформаційна війна.*

ANNOTATION

Bachelor thesis

Topic: “Open-Source Intelligence in the Russian-Ukrainian war from 2022 to 2023”

Student: Oleksandra Artemenko

Year of study, faculty: 4, Faculty of Social Sciences and Social Technologies

Academic Supervisor: Senior Lecturer at the Department of International Relations Roman Osadchuk

Reviewer: _____

(degree, academic title, surname and initials)

Defended “__” _____ 2025

Short summary:

This thesis explores the usage of open-source intelligence (OSINT) in the context of the 2022-2023 Russian-Ukrainian war. It focuses on the conceptual framework and evolution of OSINT as a distinct intelligence discipline, as well as on its practical implementation in the military operations. Particular attention is paid to case studies from the Kharkiv and Kherson counteroffensive operations, and to the verification of strikes on targets in Russian-occupied territories and within the Russian Federation. The research finds that OSINT significantly shapes situational awareness, operational forecasting, strategic narrative formation, and the construction of evidence for international legal and political responses. The work also outlines key limitations, risks, and future prospects for OSINT in hybrid warfare.

Keywords: *OSINT, open-source intelligence, war in Ukraine, satellite imagery, digital intelligence, Kharkiv campaign, Kherson campaign, information warfare.*