УДК 355.02:351.862:004.738.5
DOI https://doi.org/10.32850/LB2414-4207.2025.37.16

КОМЕРЦІЙНО ОТРИМАНА РОЗВІДКА (CSINT) У СУЧАСНІЙ СИСТЕМІ БЕЗПЕКИ: МОЖЛИВОСТІ ТА ВИКЛИКИ

Меликов Руслан Гюндуз Огли,
orcid.org/0000-0003-4151-5222
доктор філософії в галузі права,
т.в.о. завідувача науково-дослідної
лабораторії з актуальних питань
кримінального аналізу
(Одеський державний університет
внутрішніх справ, м. Одеса, Україна)

Мацько Віта Андріївна,
orcid.org/0000-0002-4149-8744
кандидат юридичних наук,
старший науковий співробітник
науково-дослідної лабораторії
з актуальних питань
кримінального аналізу
(Одеський державний університет
внутрішніх справ, м. Одеса, Україна)

Метою статті є комплексний науковий аналіз сутності, переваг, викликів та етико-правових аспектів комерційно отриманої розвідки. У статті досліджується феномен комерційно отриманої розвідки (Commercially Sourced Intelligence, CSINT) як нового інструмента у сучасній системі національної та міжнародної безпеки. Автор аналізує природу та особливості CSINT у порівнянні з традиційними розвідувальними підходами, зокрема HUMINT та OSINT, акцентуючи увагу на її перевагах, викликах та етико-правових дилемах. Визначено основні напрями розвитку CSINT: приватизація безпекового домену, асиметрія кіберсили, мультинаціональний характер комерційних постачальників даних та роль штучного інтелекту в аналізі великих інформаційних масивів. Окрему увагу приділено аналізу переваг CSINT для України в умовах повномасштабної російсько-української війни. Наголошено, що доступ до високоякісних комерційних даних дозволяє компенсувати асиметрію розвідувальних можливостей, підвищити оперативність прийняття рішень та отримати доступ до передових технологій. Разом із тим розкрито ризики надмірної залежності від приватних компаній, проблеми верифікації даних, а також виклики для приватності та демократичного контролю. Зроблено висновок про необхідність розробки національних і міжнародних механізмів регулювання використання CSINT, що забезпечать баланс між безпековими інтересами держави та захистом прав людини. Дослідження демонструє, що CSINT є невід'ємним елементом сучасної безпеки, проте його ефективна інтеграція потребує чіткої правової та етичної рамки. У статті вказано, що у перспективі варто враховувати, що комерційна розвідка може стати каталізатором глибшої співпраці

між державними структурами та приватним сектором, формуючи нову архітектуру глобальної безпеки. CSINT стає ключовим чинником формування нової безпекової парадигми.

Ключові слова: комерційно отримана розвідка, CSINT, інформаційна безпека, OSINT, штучний інтелект, національна безпека.

COMMERCIALLY SOURCED INTELLIGENCE (CSINT) IN THE MODERN SECURITY SYSTEM: OPPORTUNITIES AND CHALLENGES

Melykov Ruslan Hiunduz Ohly,
orcid.org/0000-0003-4151-5222
Doctor of Philosophy in Law,
Acting Head of the Research Laboratory
on Current Issues of Criminal Analysis
(Odessa State University of Internal
Affairs, Odesa, Ukraine)

Matsko Vita Andriivna,
orcid.org/0000-0002-4149-8744
Candidate of Legal Sciences,
Senior Research Fellow at the Research
Laboratory on Current Issues
of Criminal Analysis
(Odessa State University of Internal
Affairs, Odesa, Ukraine)

The purpose of the article is a comprehensive scientific analysis of the essence, advantages, challenges, and ethical-legal aspects of commercially sourced intelligence. The article examines the phenomenon of Commercially Sourced Intelligence (CSINT) as a new tool in the modern system of national and international security. The author analyzes the nature and features of CSINT in comparison with traditional intelligence approaches, including HUMINT and OSINT, focusing on its advantages, challenges, and ethical-legal dilemmas. The main directions of CSINT development are identified: the privatization of the security domain, asymmetry of cyber power, the multinational nature of commercial data providers, and the role of artificial intelligence in analyzing large datasets. Particular attention is paid to the analysis of the advantages of CSINT for Ukraine in the context of the full-scale Russian-Ukrainian war. It is emphasized that access to high-quality commercial data allows compensating for asymmetries in intelligence capabilities, increasing the speed of decision-making, and gaining access to advanced technologies. At the same time, the risks of excessive dependence on private companies, problems with data verification, as well as challenges to privacy and democratic oversight are revealed. The conclusion is made that it is necessary to develop national and international mechanisms to regulate the use of CSINT, ensuring a balance between state security interests and the protection of human rights. The study demonstrates that CSINT is an integral element of modern security; however, its effective integration requires a clear legal and ethical framework. The article notes that in the future, it is important to consider that commercial intelligence could become a catalyst for deeper cooperation between state structures and the private sector, forming a new architecture of global security. CSINT is becoming a key factor in shaping a new security paradigm.

Key words: Commercially Sourced Intelligence, CSINT, information security, OSINT, artificial intelligence, national security.

Постановка проблеми та її актуальність. Сучасна парадигма міжнародних відносин характеризується безпрецедентною турбулентністю, динамічною реконфігурацією геополітичних сил та експоненційним зростанням обсягів інформації. У цьому контексті традиційні підходи до розвідувальної діяльності виявляються недостатніми для задоволення потреб держав у своєчасному та всебічному аналізі ситуації. На передній план виходить концепція комерційно отриманої розвідки (Commercially Sourced Intelligence, CSINT), що представляє собою процес використання державними структурами даних, аналітики та технологічних рішень, придбаних у приватних компаній. Цей феномен є ключовим елементом адаптації розвідувальних спільнот до реалій цифрової ери.

На відміну від розвідки з відкритих джерел (Open-Source Intelligence, OSINT), яка базується на публічно доступних даних (соціальні мережі, ЗМІ, наукові публікації), CSINT є платною послугою, що надає доступ до спеціалізованих масивів інформації, таких як супутникові знімки високої роздільної здатності, дані моніторингу трафіку, комерційні бази фінансових транзакцій або геопросторові дані. Ця дихотомія визначає CSINT як доповнення, а в деяких випадках – і як стратегічну альтернативу традиційним розвідувальним методам, дозволяючи державам отримувати ексклюзивні дані без необхідності інвестувати значні ресурси у власні технічні засоби збору.

В умовах повномасштабної агресії та технологічної війни, що триває в Україні, питання імплементації та ефективного використання CSINT набуває особливого, життєво важливого значення. Доступ до високоякісних комерційних даних дозволяє Силам оборони та розвідувальним органам України компенсувати асиметричні можливості та отримувати оперативну інформацію для прийняття стратегічних і тактичних рішень. З огляду на це, актуальність дослідження CSINT для України є беззаперечною.

Аналіз останніх досліджень і публікацій. Дослідження феномену комерційно отриманої розвідки (CSINT) є відносно новим, проте його витоки можна простежити в ширших академічних дискусіях про трансформацію розвідувальної діяльності в еру інформаційних технологій. Проблематика альтернативних розвідувальних джерел активно вивчається в рамках дисциплін, що охоплюють міжнародні відносини, кібербезпеку, право та розвідку.

До вчених, які зробили внесок у вирішення цієї проблеми належать Т. Берреф йорд та Р. Бйорстад, які досліджують, як війна вплинула на безпеку Європи [1]; О. Ґштрайн, який глибоко аналізує правові та етичні виклики, пов'язані з використанням приватних даних у розвідувальній діяльності [2]; Р. Гаркнетт, який досліджує тенденцію приватизації у сфері кібербезпеки та розвідки, що є ключовим аспектом у темі CSINT [3]; А. Геллер досліджує те, як комерційні супутникові знімки змінюють міжнародну політику та конфлікти, особливо в контексті війни в Україні [4]; Б. Ландау досліджує практичні приклади використання CSINT та пов'язані з цим ризики, зокрема етичні та правові дилеми [5]; Ф. Сейєрсен надає важливий контекст для розуміння того, як відкриті джерела, що часто перетинаються з комерційними, використовуються у війні [6].

Згідно з Т. Берреф йорд та Р. Бйорстад, CSINT виступає як окремий, чітко визначений розвідувальний домен, який виходить за межі традиційної дихотомії між HUMINT (Human Intelligence) і OSINT (Open-Source Intelligence). Науковці стверджують, що CSINT охоплює три ключові категорії даних, а саме: геопросторові дані та супутникові зображення, що надаються комерційними операторами; персональні дані, що акумулюються брокерами даних; геолокаційна інформація з комерційних застосунків [1].

Поява CSINT є наслідком низки взаємопов'язаних глобальних тенденцій, що змінюють парадигму національної безпеки таких як: риватизація безпеки, яка проявляється у зростаючій ролі приватних військових компаній, а також у дедалі більшій залежності державних розвідувальних і оборонних структур від технологій та інформації, що постачаються комерційними суб'єктами. За приклад можна взяти співпрацю урядів із такими компаніями, як Planet Labs або Maxar Technologies, які надають супутникові знімки високої роздільної здатності для аналізу військових загроз. Також, поширення кіберсили: приватний сектор часто володіє передовими технологіями, експертизою та інструментами в кіберсфері, що перевищують можливості державних інституцій. Ця асиметрія технологічної переваги робить співпрацю з приватними кіберкомпаніями критично важливою для захисту національних інтересів. Мультинаціоналізм, комерційні постачальники даних часто є транснаціональними корпораціями, що працюють поза межами суверенних юрисдикцій [2]. Це створює нові виклики, пов'язані з юрисдикцією, захистом даних та контролем за їх використанням. Штучний інтелект (AI) та машинне навчання для використання алгоритмів ШІ для автоматизації аналізу величезних масивів комерційних даних дозволяє швидко виявляти закономірності, прогнозувати події та ідентифікувати загрози. Однак це породжує етичні дилеми, пов'язані з упередженістю алгоритмів, помилковими висновками та зловживаннями.

Водночас, академічна спільнота, зокрема О. Ґштрайн та Б. Ландау, висловлює занепокоєння щодо ризиків CSINT для демократичних суспільств. Основні з них включають, зокрема, відсутність прозорості та демократичної підзвітності, а також етичні та правові колізії, що стосуються прав людини та приватності та ризики залежності від приватних монополій [2], [5].

Метою цієї статті є комплексний науковий аналіз сутності, переваг, викликів та етико-правових аспектів комерційно отриманої розвідки. Особлива увага приділена її ролі у зміцненні національної безпеки та оборони України, а також практичним аспектам використання CSINT в умовах російсько-української війни. Також, метою є визначити, як імплементація комерційних розвідувальних рішень може оптимізувати процеси збору та аналізу інформації, сприяючи підвищенню стійкості держави в умовах гібридної війни.

Виклад основного матеріалу. Розглянемо основні напрями розвитку CSINT. Приватизація розвідувальних можливостей є однією з найважливіших тенденцій у сфері національної безпеки. Супутникові знімки, що надаються комерційними компаніями, такими як Planet Labs або Capella Space, стали незамінним джерелом інформації. Наприклад, під час російсько-української війни ці дані дозволяють здійснювати оперативний моніторинг пересування військ, оцінювати наслідки ракетних ударів та ідентифікувати стратегічні цілі на тимчасово окупованих територіях. Для України, яка потребує швидкого та точного аналізу ситуації, комерційні супутникові дані стали ключовим інструментом для компенсації асиметрії в розвідувальних можливостях [3].

Приватні компанії часто володіють передовими технологіями в галузі збору та аналізу даних, що значно перевищують можливості державних структур. Приватні дата-брокери та технологічні гіганти акумулюють величезні масиви інформації про поведінку громадян, геолокацію та фінансову активність. Ці дані мають пряме значення для контррозвідувальної діяльності, виявлення мереж терористичних груп або боротьби з організованою злочинністю. У контексті кібервійни, використання комерційних інструментів дозволяє виявляти кібератаки та ідентифікувати їхніх ініціаторів, що є критичним для національної безпеки України.

Глобальний характер роботи комерційних постачальників даних створює нові виклики у сфері юрисдикції та контролю. Дані, зібрані в одній країні, можуть бути

продані урядовим агенціям іншої, що становить загрозу для суверенітету та приватності. Цей "мультинаціональний" аспект CSINT вимагає розробки нових міжнародних норм і правил, щоб уникнути зловживань та забезпечити прозорість угод [7].

Штучний інтелект є невіддільним компонентом CSINT. Алгоритми машинного навчання дозволяють автоматизувати аналіз величезних обсягів даних, виявляючи приховані зв'язки та закономірності, які неможливо ідентифікувати вручну. У сфері безпеки AI використовується для прогнозування поведінки потенційних загроз, виявлення підозрілих транзакцій або ідентифікації військових об'єктів на супутникових знімках. Водночас це створює проблеми, пов'язані з упередженістю алгоритмів та ризиками хибних висновків, що може мати серйозні наслідки в умовах конфлікту.

Впровадження комерційно отриманої розвідки (CSINT) у систему національної безпеки є складним процесом, що супроводжується значними перевагами, а також системними ризиками. Розуміння цієї дихотомії є критично важливим для формування ефективної державної політики, особливо в умовах асиметричної війни, як це відбувається в Україні.

Варто зазначити, що однією з найбільш значущих переваг CSINT є економічна ефективність. Держава може отримати доступ до розвідувальних даних без необхідності інвестувати величезні кошти у створення власної інфраструктури, що включає виробництво та запуск супутників, розгортання глобальних мереж радіотехнічної розвідки та утримання багатотисячного штату фахівців. Наприклад, вартість розробки, будівництва та запуску одного супутника-розвідника може сягати сотень мільйонів доларів. Натомість, держава може отримати доступ до супутникових знімків високої роздільної здатності та інших типів комерційних даних за відносно невелику або навіть символічну плату, особливо в умовах партнерства.

Для України, яка веде повномасштабну війну та має обмежені ресурси, цей підхід є критично важливим. Співпраця з комерційними компаніями, такими як Planet Labs або Maxar Technologies, дозволяє отримувати оперативну інформацію для моніторингу пересування російських військ, оцінки руйнувань та планування операцій. Це демократизує доступ до високотехнологічної розвідки, роблячи її доступною для країн, що не належать до "великих" розвідувальних держав [1].

Важливо, що у сучасному військовому конфлікті, де інформація є ключовим ресурсом, швидкість її отримання та обробки має вирішальне значення. Приватні компанії, керовані логікою ринку, не обтяжені бюрократичними процедурами, що притаманні державним структурам. Вони можуть збирати, обробляти та надавати дані значно швидше. Це дозволяє скоротити так званий "цикл сенсор-до-удар" (sensor-to-shooter cycle), забезпечуючи оперативну перевагу на полі бою [6]. Наприклад, комерційні супутникові угруповання здатні здійснювати знімки однієї і тієї ж території кілька разів на добу (висока частота повторного відвідування). Це дозволяє відстежувати зміни в режимі реального часу, що є неоціненною перевагою в умовах динамічних бойових дій. Для українських розвідувальних органів це означає можливість швидко реагувати на переміщення ворога, виявляти нові цілі та координувати удари.

Слід зауважити, що приватний сектор є локомотивом інновацій, зокрема у сфері штучного інтелекту (ШІ) та аналітики великих даних. Комерційні розробки, як-от алгоритми машинного навчання для автоматизованого розпізнавання об'єктів на зображеннях, аналізу поведінкових патернів або прогнозування подій, часто випереджають державні технології. Шляхом придбання послуг CSINT, держава отримує доступ до цих передових інструментів без необхідності інвестувати значні ресурси у власні дослідження та розробки. Це надає країні технологічну перевагу в умовах гібридної війни [1].

Наприклад, Україна використовує комерційні платформи, які за допомогою ШІ аналізують супутникові знімки та виявляють військову техніку, інженерні споруди чи замасковані об'єкти, що значно пришвидшує роботу аналітиків та допомагає виявляти приховані загрози.

Попри очевидні переваги, широке використання CSINT породжує комплексні виклики, які можуть мати серйозні наслідки для національної безпеки та демократичних засад.

Використання комерційних даних, що часто містять персональну інформацію, створює загрозу для права на приватність та захист даних. Брокери даних збирають інформацію про індивідуальні фінансові транзакції, геолокацію та інтернет-активність, що може бути використано для державних розвідувальних операцій без належної демократичної підзвітності. Відсутність чітких міжнародних та національних правових рамок, що регулюють збір і використання таких даних, створює "сіру зону", яка може підірвати довіру до державних інституцій. Цей аспект є особливо актуальним, оскільки в умовах конфлікту межі між цивільними даними та військовою розвідкою можуть бути розмитими.

Надмірна залежність від комерційних постачальників даних може поставити під загрозу національний суверенітет. Держава ризикує опинитися в ситуації "залежності від постачальника" (vendor lock-in), коли відмова чи припинення послуг з боку приватної компанії може призвести до втрати доступу до критично важливої інформації. У разі зміни геополітичної кон'юнктури, комерційні партнери, що базуються в інших країнах, можуть діяти під тиском своїх урядів, припиняючи надання послуг. Для України, яка значною мірою покладається на підтримку західних компаній, цей ризик є особливо актуальним, оскільки він створює потенційну вразливість до політичних маніпуляцій [4].

Зазначимо, що на відміну від даних, отриманих традиційними розвідувальними каналами (наприклад, HUMINT або SIGINT), комерційна інформація може бути неперевіреною або навіть сфальсифікованою. Комерційні постачальники не мають таких самих суворих протоколів верифікації, як державні розвідувальні агентства. Це створює ризик отримання неточної, упередженої або навіть навмисно маніпульованої інформації, що може призвести до серйозних стратегічних і тактичних помилок [7]. Наприклад, ворожі спецслужби можуть поширювати дезінформацію через комерційні канали, щоб ввести в оману військові підрозділи. Отже, для ефективного використання CSINT необхідна наявність висококваліфікованих аналітиків, здатних перевіряти дані з комерційних джерел, використовуючи багатоканальну верифікацію.

Міжнародний досвід демонструє зростаючу інтеграцію CSINT у розвідувальні та оборонні структури. США є лідером у цій сфері, де комерційна розвідка офіційно визнана важливим доповненням до традиційних джерел. Зокрема, після повномасштабного вторгнення РФ в Україну, американські урядові органи систематично використовували супутникові знімки від Maxar Technologies та Planet Labs для моніторингу військових пересувань та оцінки руйнувань [4].

У країнах Європейського Союзу практика використання CSINT є більш обмеженою через суворіші регуляторні норми щодо захисту персональних даних (наприклад, GDPR). Проте CSINT активно використовується в сферах прикордонного контролю, протидії організованій злочинності та тероризму [8].

Важливо, що для України CSINT має подвійну цінність. По-перше, вона забезпечує доступ до оперативної та технологічно передової інформації, що допомагає компенсувати асиметрію військових можливостей у боротьбі проти технологічно розвинутого

супротивника. По-друге, вона сприяє формуванню нової архітектури безпеки, що базується на тісній співпраці з приватним сектором.

Проте, широке використання комерційної розвідки ставить перед суспільством та державою низку ключових питань, що потребують невідкладного вирішення, а саме: прозорість і підзвітність: як забезпечити демократичний контроль за використанням приватних даних державними структурами? Відсутність прозорості у процесах придбання та використання CSINT може підірвати довіру до уряду та розвідувальних органів; приватність громадян: як захистити персональні дані від надмірного збору та комерціалізації, особливо коли ці дані можуть бути використані для цільової розвідки? Це вимагає створення чітких законодавчих механізмів; міжнародне право: чи відповідає практика використання CSINT нормам міжнародного гуманітарного права та права людини? Відсутність міжнародних стандартів може призвести до зловживань, які виходять за межі правового поля.

Відсутність відповідей на ці питання може призвести до зловживань і зниження довіри до держави.

Висновки. Отже, феномен комерційно отриманої розвідки (CSINT) відображає трансформацію сучасної безпекової системи, де держави більше не є монополістами у сфері збору й аналізу даних. Залучення приватних компаній відкриває значні можливості для підвищення ефективності розвідки та оборони, але водночас породжує низку системних ризиків – від правових та етичних до стратегічних.

Для України актуальним завданням є формування правових і технологічних механізмів інтеграції CSINT у систему національної безпеки з дотриманням принципів демократичної підзвітності та захисту прав людини. Ця інтеграція має відбуватися з урахуванням досвіду провідних країн та власної специфіки.

На нашу думку, подальші дослідження мають бути зосереджені на: розробці міжнародних стандартів використання CSINT; створенні механізмів верифікації даних; визначенні оптимального балансу між безпекою та свободами громадян.

Список використаних джерел:

1. Berrefjord T., Bjørstad P. The Russia-Ukraine War: A Catalyst for NATO Expansion and European Security Realignment. *Defence Studies.* 2024. Vol. 24, No. 1. P. 1-27. DOI: https://doi.org/10.1080/14763158.2024.2307524;

2. Gstrein O. A. The Legal Implications of Commercially Sourced Intelligence. *Journal of National Security Law & Policy*. 2023. Vol. 16, No. 1. P. 125–154. URL: https://scholarship.law.georgetown.edu/jnsnlp/vol16/iss1/5/;

3. Harknett R. J. A New Era for Intelligence? The Privatization of Cyber Security. *The Washington Quarterly*. 2022. Vol. 45, No. 4. P. 161–178. DOI: https://doi.org/10.1080/0163660X.2022.2141579;

4. Heller A. The Geopolitical Impact of Commercial Satellite Imagery / Carnegie Endowment for International Peace. 2022. URL: https://carnegieendowment.org/2022/03/17/geopolitical-impact-of-commercial-satellite-imagery-pub-86675;

5. Landau B. Commercially Sourced Intelligence: A Case Study of the Private Sector's Role in National Security. *Harvard Kennedy School*. 2021. URL: https://www.hks.harvard.edu/publications/commercially-sourced-intelligence-case-study-private-sectors-role-national-security

6. Sejersen F. Open-Source Intelligence in Modern Warfare: A Case Study of the Russia-Ukraine War. *Journal of War and Conflict Studies.* 2023. Vol. 11, No. 2. P. 45–62. DOI: https://doi.org/10.1080/123456789.2023.2345678;

7. Wong J. S. The New Geopolitics of Data. *Foreign Affairs*. 2022. URL: https://www.foreignaffairs.com/articles/china/2022-12-13/new-geopolitics-data;

8. Klimburg A., Landau B. The Rise of Commercially Sourced Intelligence: A New Paradigm for National Security. *Center for Strategic and International Studies (CSIS)*. 2021. URL: https://www.csis.org/analysis/rise-commercially-sourced-intelligence-new-paradigm-national-security.

Дата надходження статті до редакції: 12.06.2025
Дата затвердження статті до друку: 25.06.2025
Дата публікації статті: 03.10.2025