«БОЙОВІ СОФТИ» НА СЛУЖБІ СИЛ ОБОРОНИ:

ПОТОЧНИЙ СТАН ГАЛУЗІ СПЗ, ПРОБЛЕМАТИКА ТА АКТУАЛЬНІ ВИКЛИКИ

Катерина Аніскіна

Київ, травень 2025 р.

Зміст

З глибокою повагою і вдячністю усім тим,

хто бився, б'ється і продовжує битися за незалежність України.

Присвячується захисникам України – військовим Сил оборони.

«БОЙОВІ СОФТИ» НА СЛУЖБІ СИЛ ОБОРОНИ:

ПОТОЧНИЙ СТАН ГАЛУЗІ СПЗ, ПРОБЛЕМАТИКА ТА АКТУАЛЬНІ ВИКЛИКИ

Передмова

Протягом більше як трьох років повномасштабної війни, в якій Україна протистоїть переважаючому противнику, відбулось чимало змін – як в характері ведення війни, так і в її формі і способах. До характерних рис нинішньої фази російсько-української війни можна віднести розвиток і нарощення різного роду спроможностей у напрямку автоматизації.

З огляду на те, що противник володіє абсолютною перевагою в силах і засобах, включно з мобілізаційним потенціалом та добре розвинутим воєнно-промисловим комплексом на базі державних потужностей, Україна по суті була вимушена побудувати власні спроможності, прагнучи досягти технологічної переваги. Як і переважна більшість технологічних галузей, напрямок т. зв. «бойових софтів», або СПЗ, – спеціального програмного забезпечення, почав свій активний розвиток через критичну необхідність створення і нарощення спроможностей, як того потребувало поле бою. Віднедавна, за законодавством України, СПЗ та інші оборонні ІТ-рішення відносять до ОВТ, озброєння та військової техніки.

Сьогодні, в контексті мережецентричної війни, софтверні рішення відіграють одну з ключових ролей у веденні бойових дій. Сучасне поле бою неможливо уявити без залучення систем ситуаційної обізнаності, автоматизованих систем управління та захищених месенджерів. Такі системи уможливлюють збір, обробку, використання і розповсюдження даних та передачу інформації про об'єкти та події оперативного середовища, обмін цією інформацією по горизонталі та вертикалі, забезпечують координацію дружніх сил та засобів, надають вогневу перевагу та реалізують процеси управління військами в ріалтаймі на всіх рівнях та в усіх доменах і площинах ведення війни.

Складно уявити, якою була би нинішня російсько-українська війна без застосування цих систем. Можна лише припустити, що поле бою перетворилось би на конвенційний збройний конфлікт зразка Першої та Другої світових війн.

***

Цей матеріал є першим подібним доробком у вивченні питань СПЗ в контексті практичного застосування СОУ в російсько-українській війні, що триває. В рамках цієї роботи, увагу аудиторії свідомо сфокусовано на питаннях СПЗ з позиції розробників. Тим самим автор лишає простір для подальшого вивчення питань в площині користувачів.

Разом із тим, автор сподівається, що ця робота стане поштовхом у глибшому вивченні теми та приверне увагу десіжен-мейкерів до вирішення поточних викликів і проблем, які створюють перешкоди розвитку галузі, впровадженню систем у війська та нарощенню технологічних спроможностей України в розрізі автоматизації в цілому.

Катерина Аніскіна

Автор висловлює вдячність

***Військовим різних формувань СОУ**, користувачам СПЗ, за надані коментарі та консультації в рамках даної роботи;*

Розробникам та/або співзасновникам систем, які виступили в ролі респондентів інтерв'ю, що послужили основою для детального опису СПЗ:

Євгену Максименку, співзасновнику і розробнику групи продуктів «ComBat Vision», зокрема системи «ComBat 4»

Олексію Гавришу, співзасновнику і розробнику системи «ARMOR» (ГРК «Броня»)

Дмитру Шамраю, співзасновнику і розробнику системи «Griselda»

Артему Мартиненку, архітектору ІКС «DELTA»

Розробнику системи «Вежа»

Руслану Микулі, співзасновнику проектів «DeepState» і «KOLOSSAL»

...а також, всім фахівцям і розробникам за надані коментарі та консультації:

Фахівцеві МОУ

Розробнику системи «Неон»

Засновнику системи «Comintify»

Співрозмовнику N

Інні Гончар, керівниці напрямку «Управління знаннями» ГО «Аеророзвідка»

Розробнику системи «Промінь»

Віталію Кириліву, співрозробнику VR-фільму «Перший бій»

Фахівцеві МОУ за надання консультації з юридичних питань

*Окремо, подяка висловлюється **Жорі** і **Танго** за терпіння і всебічне сприяння у написанні цієї роботи, без яких вона, ймовірно, ніколи не побачила би світ. Дякую!*

Про дослідження

МЕТА. В написанні цієї роботи автором було поставлено на меті досягнення двох цілей: **Цілі 1** – розкрити тему **поточного стану галузі** спеціального (спеціалізованого) програмного забезпечення (далі – СПЗ), що застосовується на полі бою Силами оборони України (далі – СОУ), включно з поглибленим **оглядом** деяких продуктів (систем), та **Цілі 2** – висвітлити **проблематику галузі та актуальні виклики** з точки зору розробників СПЗ. Матеріал адресовано як експертній, так і неекспертній аудиторіям, зокрема релевантним десіжен-мейкерам, військовим СОУ, розробникам галузі СПЗ та інших галузей ОВТ тощо.

ОБ'ЄКТ ДОСЛІДЖЕННЯ. В рамках даної роботи об'єктом дослідження вважаються: a) безпосередньо **СПЗ українського походження**, що функціонують в інтересах СОУ, зокрема на фазі повномасштабної російсько-української війни, які довели успішне практичне застосування військовими СОУ та є «combat proven» (перевіреними в бойових умовах), а також оборонні ІТ-рішення в цілому; b) актуальні питання, виклики, проблематика, з якими стикаються команди розробників даних систем.

ДАНІ. Дослідження виконано на основі аналізу **якісних даних**. Джерелами даних слугували: a) **інтерв'ювання респондентів** – розробників ПЗ з досвідом інтеграції систем у війська; b) **консультації** з окремими фахівцями галузі та суміжних галузей, користувачами ПЗ – військовими; c) **дані з відкритих джерел** (текстові, відео, навчальні і промо матеріали тощо).

МЕТОДОЛОГІЯ. В основу аналізу (*частини II і III*) лягли результати інтерв'ювання респондентів (a) та консультації (b). Для проведення інтерв'ювання (a) було застосовано **техніку напівструктурованих інтерв'ю**, оскільки саме вона, окрім збору даних, уможливлює також і передачу досвіду респондента, його/її світогляду та ставлення до об'єкту дослідження із комплексної точки зору[1]. Так, на відміну від структурованих інтерв'ю, ця техніка дозволяє вести розмову на основі заготовленої «сітки» запитань, яка використовується інтерв'юером в дуже гнучкий спосіб[2].

В рамках цього дослідження автором було підготовлено блоки однакових запитань до респондентів, порядок яких варіювався залежно від випадку (як-то, типу і функціоналу системи, ролі респондента в команді тощо), характеру розмови, технічних можливостей

[1] Clement Pin, "Semi-structured Interviews". *LIEPP Methods Brief*, Sciences Po, 2023 (№4), 1. <https://sciencespo.hal.science/hal-04087970/document> [Переглянуто 2025 04 16].
[2] Там само.

системи та рівня «чутливості» інформації. Питання – як «точкові», так і загального характеру, – було згруповано у наступні **9 блоків**:

- основний функціонал, закладений в систему
- основний тип даних, якими оперує система
- діапазон дії/інструментарій (операції, які дозволяє здійснювати система)
- ким використовується (роди та види військ) та на яких рівнях (рівні ведення війни/управління військами)
- на якій стадії перебуває система (розробка, тестування, допуск до експлуатації, кодифікація, прийняття на озброєння тощо)
- інтеграція з іншими системами (за наявності)
- найбільш актуальні виклики, що стоять перед розробниками галузі в цілому, на думку респондента
- оцінка поточного стану галузі в розрізі інтероперабельності (міжсистемна взаємодія)
- ключова теза респондента – відкрите запитання

Результати кожного з інтерв'ю було занесено автором до робочої «матриці» відповідей-запитань, структуровано та викладено у вільному порядку в *частині II (i) Детальніший огляд деяких систем*. Виділені ключові слова, такі як «функціонал», «інтеграція» тощо дозволяють читачеві швидше зорієнтуватися по тексту. Надані в ході інтерв'ю відповіді респондентів дали можливість визначити та сформулювати найбільш актуальні виклики та проблеми, з якими сьогодні стикаються розробники ПЗ, що відображено у *частині третій (III)*.

Консультації (b) з іншими розробниками систем (результати яких не було включено до *частини II (i))*, а також з військовими СОУ та релевантними фахівцями було отримано у вільній формі, відштовхуючись від потреб та конкретних запитів дослідження.

СТРУКТУРА. Матеріал структуровано наступним чином. *Частина перша (I)* надає роз'яснення значень деяких термінів, понять, концептів і теорій, які запропоновано як теоретичне підґрунтя в контексті питань СПЗ та їхнього практичного застосування у веденні війни. Поняття, концепти і теорії структуровано автором у теоретичні моделі з метою надання більш комплексного і логічного сприйняття теоретичних основ.

Частина друга (II) представляє собою як загальний огляд галузі, так і детальніший опис шести систем. Спершу виконано загальний огляд з метою категоризувати різноманіття

систем за трьома принципами: a) функціоналом, b) спеціалізацією та інструментарієм, c) рівнями. Надалі, виконано детальніший опис шести систем на базі проведених автором інтерв'ю з розробниками, результати яких представлено в *частині другій II (i)*. Слід відзначити, що детальні описи різняться за обсягом викладеної інформації, що продиктовано «чутливістю» певної інформації в одних випадках та можливістю ширше розкрити питання – в інших.

Частина третя (III) резюмує озвучені респондентами в *частині другій II (i)* поточні проблеми та актуальні виклики. Додатково, до аналізу було взято дані, зібрані автором під час консультацій з фахівцями та розмов з іншими розробниками.

У завершальній частині *Висновки та рекомендації* підсумовано результати роботи, а також надано рекомендації з огляду на виокремлені в *частині третій (III)* 13 груп викликів. Рекомендації (*Необхідні зміни*) сформульовано тезово у тих випадках, де це дозволяє контекст, та адресовано відповідним структурним підрозділам Міністерства оборони України та Генерального штабу Збройних сил України, а також іншим залученим інституціям.

Наприкінці роботи надано *двомовний Глосарій (див. Appendix 1)*, до якого увійшли як використані у тексті терміни і поняття, так і ті, що є корисними для подальшого заглиблення у тематику та більш комплексного вивчення питань ведення модерної війни. Терміни і поняття наведено в алфавітному порядку разом із оригінальним терміном або аналогом англійською мовою, а переклад та стисле визначення надано українською. Глосарій складено для зручності прочитання тексту дослідження та ефективності засвоєння нових термінів, і тому, рекомендовано звертатися до нього під час прочитання.

ПЕРЕДБАЧУВАНІ ОБМЕЖЕННЯ. Автор акцентує на тому, що дану роботу не слід розглядати як всеохоплююче комплексне дослідження теми, усвідомлюючи наявність певних обмежень та обставин, таких як:

a) неможливість поширення даних у повному обсязі з міркувань безпеки (деяких імен, назв, деталей міжсистемної інтеграції, розкриття функціоналу, інструментів та джерел даних, якими оперує система тощо);

b) проблема повноти інформації, що викликана відсутністю доступу до деяких первинних джерел і даних та відсутністю вторинних даних як таких (попередньо проведених досліджень на дану тему на момент написання роботи не було виявлено або автору про них невідомо);

с) «вестернізований» підхід в подачі теоретичної основи – домінування термінів, понять та концептів, зокрема, доктринальних, запозичених переважно в американської, а також, в меншій мірі, британської військових культур.

Скорочення (укр.)[3]

АСКВ – Автоматизована система керування вогнем

АСУ – Автоматизована система управління

АСУВ – Автоматизована система управління військами

АТО – Антитерористична операція

БАС – Безпілотна авіаційна система

БЕК – Безекіпажний морський (безпілотний) комплекс

БЗВП – Базова військова підготовка

БпАК – Безпілотний авіаційний комплекс

БпЛА – Безпілотний літальний апарат

БСМ – Бездротові сенсорні мережі

ВВНЗ – Вищі військові навчальні заклади

ВМС – Військово-морські сили

ВНП ЗВО – Військові навчальні підрозділи закладів вищої освіти

ВП – Вогнева позиція

ГРК – Графічно-розрахунковий комплекс

ГУР МО – Головне управління розвідки Міністерства оборони

ГШ ЗСУ – Генеральний штаб Збройних сил України

ДВТП МОУ – Департамент військово-технічної політики, розвитку озброєння та військової техніки Міністерства оборони України

ДКР – Дослідно-конструкторські роботи

ДПЗ МОУ – Департамент політики закупівель Міністерства оборони України

ДСК – для службового користування

ДССЗІ – Державна служба спеціального зв'язку та захисту інформації

ДШВ – Десантно-штурмові війська

ДЮЗ МОУ – Департамент юридичного забезпечення Міністерства оборони України

ЗРВ – Зенітні ракетні війська

ЗСУ – Збройні сили України

ЗФПВО – Заклади фахової передвищої військової освіти

ІКС – Інформаційно-комунікаційна система

[3] Наданий перелік включає лише скорочення термінів і понять українською, що використовуються в тексті дослідження. Для англо-українськомовного Глосарію, що включає ширший перелік термінів, а також, їхнє тлумачення, див. Appendix 1.

ІТС – Інформаційно-телекомунікаційна система

КПС ЗСУ – Командування Повітряних сил Збройних сил України

КМУ – Кабінет Міністрів України

КСВ ЗСУ – Командування Сухопутних військ Збройних сил України

КСЗІ – Комплексна система захисту інформації

КСП – Контрольний спостережний пункт

ЛАСО – Летальні автономні системи озброєння[4]

МДО – Мультидоменні операції

МН – Машинне навчання

МОУ – Міністерство оборони України

НДДКР – Науково-дослідні та дослідно-конструкторські роботи

НДР – Науково-дослідні роботи

НРК – Наземний роботизований комплекс

о/с – Особовий склад

ОВТ – Озброєння та військова техніка

ОСУВ – Оперативно-стратегічне угруповання військ

ОТУ – Оперативно-тактичне угруповання військ

ОУВ – Оперативне угруповання військ

ПЗ – Програмне забезпечення

ППО – Протиповітряна оборона

ПС ЗСУ – Повітряні сили Збройних сил України

РАС – Роботизовані та автономні системи

РЕБ – Радіоелектронна боротьба

РЕР – Радіоелектронна розвідка

РЛС – Радіолокаційна станція

РСЗВ – Реактивна система залпового вогню

СБУ – Служба безпеки України

СВ ЗСУ – Сухопутні війська Збройних сил України

СОУ – Сили оборони України

СПЗ – Спеціальне (спеціалізоване) програмне забезпечення

ССО – Сили спеціальних операцій

ТВД – Театр воєнних дій

ТЗ – Технічне завдання

[4] Також, **АСО** – Автономні системи озброєння.

ТІК – Тренажно-імітаційний комплекс

ТЛ – Тактична ланка

ТрО – Територіальна оборона

ТТЗ – Тактико-технічне завдання

УІТ МОУ – Управління інформаційних технологій Міністерства оборони України

ЦВНУ ГШ ЗСУ – Центральне воєнно-наукове управління Генерального штабу Збройних Сил України

ЦІРОТ МОУ – Центр інновацій та розвитку оборонних технологій Міністерства оборони України

ЦМТР ЗСУ – Центр масштабування технологічних рішень Збройних сил України

ЦНДІ ЗСУ – Центральний науково-дослідний інститут Збройних сил України

ЦОД – Центр обробки даних

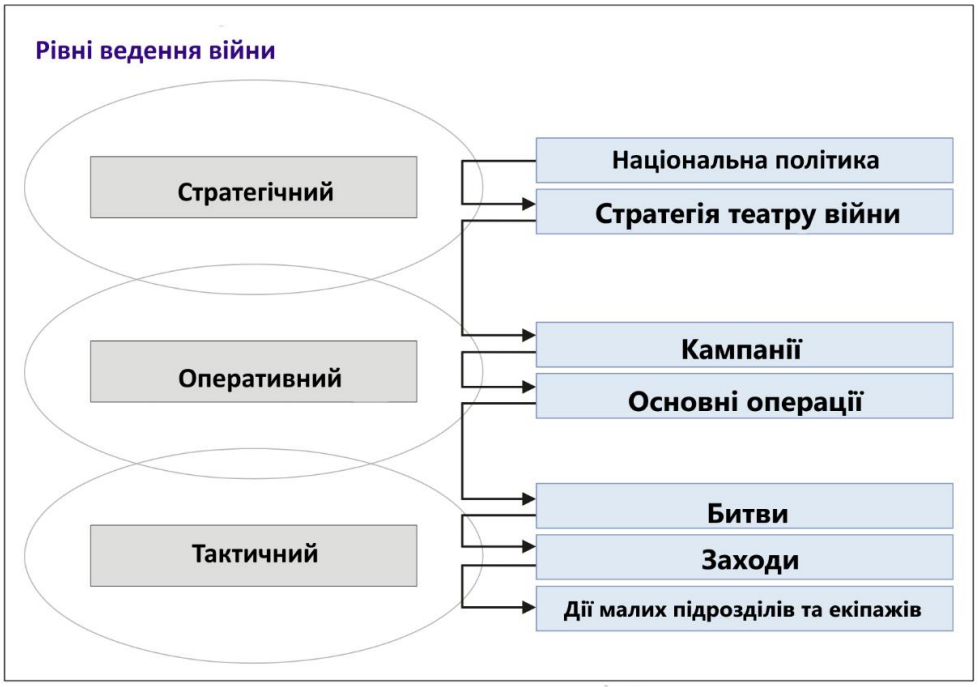
ШІ – Штучний інтелект

I. Частина перша. Терміни і поняття. Теоретичне підґрунтя.

Перш ніж перейти до огляду наявних рішень та аналізу проблематики, зробімо крок назад і звернімось до теорії. Наведені в цій частині роботи терміни і поняття зі сфери вивчення війни та безпекових студій потребують роз'яснення для комплексного розуміння читачами матеріалу, який буде викладено у *частині другій (II) і частині третій (III)*.

- ***Які є рівні ведення війни?***

По-перше, слід визначити, що **ведення війни** (англ. – warfare) тут і надалі означатиме «[...] механізм, метод або ж модальність збройного конфлікту»[5]. Це поняття, що вказує на спосіб, в який сторони ведуть війну, і відповідає на питання «як»[6]. По-друге, ведення війни як явище і процес можна умовно розподілити на три рівні: **тактичний, оперативний і стратегічний** (англ. – tactical, operational, strategic levels). В Доктрині Збройних сил Сполучених Штатів (JP 1) ці три рівні звуться сполучною ланкою, що зв'язує тактичні дії із досягненнями національних цілей[7]. Схематичне розподілення на рівні та взаємозв'язок між їхніми складовими зображує Фігура 1:



Фігура 1. Рівні ведення війни. Джерело: Figure I-2, Doctrine for the Armed Forces of the United States (JP 1).

[5] Joint Publication 1 "Doctrine for the Armed Forces of the United States". Armed Forces of the United States, 25 March 2013, Incorporating Change 1, 12 July 2017, I-4. <https://irp.fas.org/doddir/dod/jp1.pdf> [Переглянуто 2025 16 04].
[6] Там само.
[7] JP 1, x.

Тактикою, згідно Доктрини, називається «[...] застосування і впорядковане розташування сил по відношенню один до одного»[8]. Відповідно, **тактичний рівень** ведення війни – це площина, в якій ведеться планування та реалізація боїв і битв «[...] для досягнення воєнних цілей, що покладені на тактичні підрозділи або об'єднані оперативно-тактичні сили»[9]. На тактичному рівні «[...] діяльність зосереджена на впорядкованому розташуванні та маневрі бойових елементів відносно один одного та противника задля досягнення бойових цілей»[10].

Оперативний рівень «[...] поєднує стратегію і тактику через встановлення оперативних цілей, необхідних для досягнення кінцевих воєнних результатів та стратегічних цілей»[11]. Іншими словами, оперативний рівень є послідовним продовженням тактичних дій для досягнення поставлених цілей.

Поняття стратегії визначається як «[...] розважлива ідея або набір ідей для впровадження інструментів національної влади у синхронізований та інтегрований спосіб для досягнення цілей театру[12], національних та/або багатонаціональних цілей».[13] Отже, на **стратегічному рівні** війни задіяний елемент керівництва (національного або багатонаціонального) та ресурси, необхідні для досягнення кінцевих цілей[14].

Слід розуміти, що **чітко виражених кордонів між цими трьома рівнями немає**, хоча таке умовне структурування служить «підручним інструментом» для командирів у плануванні і координації операцій, розподілі ресурсів, а також постановці задач згідно відповідних наказів.

- ***Що означають рівні управління військами?***

Розподіл на тактичний, оперативний і стратегічний рівні також використовується в процесах **управління військами**. В умовах сучасних збройних конфліктів, в яких

[8] JP 1, I-8.
[9] Там само.
[10] Там само.
[11] Там само.
[12] Мається на увазі ТВД – театр воєнних дій (англ. – theatre).
[13] "DOD Dictionary of Military and Associated Terms". Department of Defense, March 2017, 224. <https://www.tradoc.army.mil/wp-content/uploads/2020/10/AD1029823-DOD-Dictionary-of-Military-and-Associated-Terms-2017.pdf> [Переглянуто 2025 04 16].
[14] Andrew S. Harvey, "The Levels of War as Levels of Analysis". *Military Review*, November-December 2021, 80. <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2021/Harvey-Levels-of-War/> [Переглянуто 2025 04 16].

центральне місце займають **об'єднані операції** (англ. – Joint operations), ці процеси можуть бути (і зазвичай, і бувають) змішаними.

«Структура управління воєнними діями визначає **розподіл відповідальностей органів військового управління** у військових формуваннях», – пояснює фахівець МОУ, – «[н]априклад, підрозділи рівня «взвод», «рота», «батальйон» СВ, «дивізіон», а також типові полки та бригади відносять до тактичного рівня [наведені за зростанням – ред.]; корпуси військ, а також, в окремих випадках, бригади та полки, що містять в своєму складі інші окремі підрозділи, можуть вважатись з'єднаннями та відноситись до оперативно-тактичного рівня; в свою чергу, органи військового управління оперативного рівня представлені оперативними командуваннями КСВ, оперативними та оперативно-тактичними угрупуваннями СВ, повітряними командуваннями ПС, регіональними управліннями сил ТрО; органи військового управління стратегічного рівня – це Командування об'єднаних Сил, а також оперативно-стратегічні угруповування СВ (наприклад ОСУВ «Хортиця», ОСУВ «Таврія»)».[15]

Важливо розуміти, чому ці рівні введені, і яке смислове навантаження вони несуть. Розподіл на рівні дозволяє призначити певну задачу тому чи іншому угрупуванню залежно від його розміру. Наприклад, 5-10 км від лінії розмежування – це глибина тактичного рівня, яка є типовою для виконання задач бригади – формування, що знаходиться на межі тактичного і оперативного рівнів і може бути як найбільшим формуванням тактичного рівня, так і найменшим оперативного[16], – зазначає фахівець МОУ.

За його словами, рівень задачі і розмір угрупувань визначають, які **інструменти** буде залучено для виконання цієї задачі. (Зверніть увагу: в наступних частинах дослідження йтиметься про застосування різного роду СПЗ, тобто, інструментів ведення війни, на різних рівнях. В українському контексті, більшість систем сьогодні функціонують на тактичному та оперативному рівнях.) Зокрема, в розрізі систем, які надають **ситуаційну обізнаність** (див. с. 29-30), практика демонструє, що чим нижче ми спускаємось за «ієрархією» формувань на тактичному рівні (батальйон → рота → взвод), тим більшою є потреба в ситуаційній обізнаності[17].

[15] З особистої розмови з фахівцем МОУ.
[16] Там само.
[17] Там само.

- ***Що таке «домени ведення війни» та які домени існують?***

В безпекових та військових студіях, класичний підхід передбачає, що військове протистояння (бій, операція, кампанія, збройний конфлікт) відбувається в межах певних доменів. Спершу, визначимо, що власне є доменом.

В контексті ведення війни, **доменом** називається середовище, що має визначені фізичні атрибути та межі, і якому можуть бути властиві функційна та логічна елементи (як у випадку кібер домена)[18]. **Домен ведення війни** (англ. – warfighting domain) – це окреслене середовище, у яке гравці мають потрапити, маневрувати в ньому, домінувати або мати контроль задля досягнення військової цілі.[19] Сьогодні можна знайти безліч варіантів класифікації доменів ведення війни, кількість яких може різнитися від 4 до 7 і навіть 9. Проте, будь-яке трактування, в тому числі, і описану нижче модель, слід сприймати умовно, адже всі вони є лише теоретичними фреймворками.

З часом і технологічним розвитком людства, самий **концепт доменів ведення війни** помітно еволюціонував, поступово охоплюючи нові сфери, в яких людство прагнуло вести війни. Ретроспективний аналіз збройних конфліктів демонструє, що розвиток технологій можна вважати основним драйвером виходу війни на нові рівні і охоплення нових доменів.

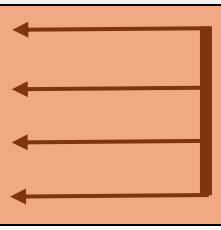
Так, античні війни, якими їх бачив та описував Тукідід, відбувались лише у двох доменах – на суходолі та/або на морі[20]. Повітряні бої Великої війни (Першої світової) знаменують появу повітряного домену як повноцінного середовища ведення війни та «війни у повітрі» як явища. З початком опанування космічного простору, до «традиційної» трійки «земля-море-повітря» додався також домен «космос», що знайшло відображення у так званих Космічних перегонах між СРСР та США[21]. Зрештою, останнім на сьогодні доповненням став кібер домен, що сформувався наприкінці минулого століття на тлі «[…] інтеграції комп'ютерів, зв'язку, мереж і систем керування».[22]

Таким є найбільш поширений, «класичний» **п'ятидоменний фреймворк**, який було сформульовано в американській військовій культурі на доктринальному рівні, де 5 доменів

[18] Jeff McManus, "Operating Successfully within the Bureaucracy Domain of Warfare: Part One". *US Army War College Publications*, May 29, 2024. <https://publications.armywarcollege.edu/News/Display/Article/3789970/operating-successfully-within-the-bureaucracy-domain-of-warfare-part-one/> [Переглянуто 2025 16 04].
[19] Там само.
[20] Lesley Seeback, "Why the fifth domain is different". *The Strategist*, 5 Sep 2019. <https://www.aspistrategist.org.au/why-the-fifth-domain-is-different/> [Переглянуто 2025 16 04].
[21] McManus.
[22] Там само.

– це: **земля, море, повітря, космос та кіберпростір** (англ.: Land, Sea/Maritime, Air, Space, Cyberspace.)

Причому, як пояснює д-р Джеф МакМанус, перші чотири домени пов'язані фізичною елементою, а п'ятий, кібер домен, «[...] об'єднує численні шари, що охоплюють перші чотири домени, включно з фізичним шаром (зв'язок та передача даних), але й також включає функційні шари, пов'язані з логічними процесами програмного забезпечення (код, логіка, програми) та певним використанням даних (інформація)».[23]

<table>
<tr><th colspan="2">5 доменів ведення війни</th></tr>
<tr><td colspan="2">наявна фізична елемента</td></tr>
<tr><td></td><td>наявна функційна + логічна елементи</td></tr>
<tr><td>Земля</td><td rowspan="4"> 
Кіберпростір</td></tr>
<tr><td>Море</td></tr>
<tr><td>Повітря</td></tr>
<tr><td>Космос</td></tr>
</table>

Фігура 2. П'ять доменів ведення війни. Джерело: складено автором.

- ***Що таке «мультидоменні операції» (МДО), та в чому сутність концепту «мультидоменний бій»? В яких вимірах ведуться бойові дії? Які інструменти МДО існують?***

Тривалий час моделлю, описаною у попередньому пункті, керувався весь західний світ. Втім, її можна піддати критиці. Першим аргументом, що вказує на крихкість п'ятидоменного фреймворку, є розуміння того, що розподіл на домени служить інструментом для науковців, які вивчають війну, а не солдат. Отже, модель не несе великого практичного навантаження.

По-друге, в умовах модерної війни, що включає активне застосування роботизованих систем, deep-tech технологій та елементи супутникової розвідки, неможливо уявити бій, що відбувався би лише в одному домені, наприклад, виключно на суходолі або у повітряному просторі. У нереальності такого сценарію можна переконатися на прикладі роботи з будь-якою безпілотною системою (БпЛА, БЕК, НРК), що передбачає залученість áкторів (суб'єктів поля бою) одночасно в кількох доменах та координацію їхніх дій в інформаційній площині.

[23] McManus.

Тому, сьогодні погляд крізь п'ятидоменну призму можна вважати таким, що є застарілим. Концепт **мультидоменних операцій, МДО** (англ. – Multi-domain operations, MDO), який лежить в основі ведення сучасної війни, більш точно відповідає характеру реальних бойових дій сьогодення.

В жовтні 2022 р. у світ вийшла оновлена публікація FM 3-0[24] (Бойового статуту Армії США), яка визначила МДО новим операційним концептом, затвердженим на доктринному рівні. Прагнучи зрозуміти, як готується до розгортання та виконання великомасштабних операцій Армія США сьогодні та в перспективі до 2030-х рр., вартує вивчити сутність МДО.

Однак, слід зазначити, що дискусії щодо необхідності оновленого погляду та підходів до військових операцій велися і раніше. Наприклад, LTC (Ret), PhD Джеймс Дж. Карафано ще у 2018 р. аргументував, що найсучасніший підхід до мислення про військові операції передбачає, що в майбутньому, вони будуть за своєю сутністю **об'єднаними** – на противагу тезі про те, що війна ґрунтується на домінуванні певного домену.[25] Карафано також сформулював основний загальний принцип, яким можна охарактеризувати візію об'єднаних операцій майбутнього: «[...] збройні сили повинні мати експертизу, спроможності та здатність оперувати в усіх доменах, за які ведеться боротьба в театрі воєнних дій, та використовувати ці домени ефективніше за супротивника».[26] В цьому і полягає ключовий виклик.

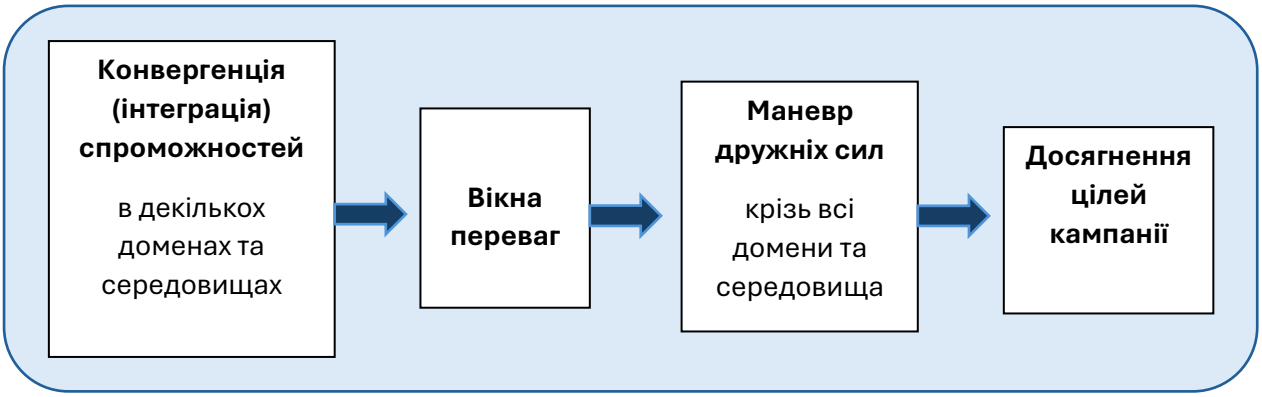
Окрім того, протягом попередніх років, Армія США та Корпус Морської піхоти США вже мали змогу засвоїти концепт **мультидоменного бою** (англ. – Multi-Domain Battle)[27], в основі якого – готовність битися у середовищі, в якому всі **домени є оспорюваними** (англ. – contested domains), тобто, такими, за які ведеться боротьба.[28] За визначенням, концепт мультидоменного бою означає **конвергенцію** (інтеграцію) спроможностей задля створення вікон переваг (часто тимчасових) у кількох доменах та оспорюваних територіях

[24] FM 3-0 "Operations". Headquarters, Department of the Army, October 2022. <https://irp.fas.org/doddir/army/fm3-0.pdf> [Переглянуто 2025 17 04].
[25] James J. Carafano, "America's Joint Force and the Domains of Warfare". 2018 Index of U.S. Military Strength, Dakota L. Wood (ed.), Davis Institute for National Security and Foreign Policy, The Heritage Foundation, 2018, 27. <https://www.heritage.org/sites/default/files/2017-10/2018_IndexOfUSMilitaryStrength-2.pdf> [Переглянуто 2025 17 04].
[26] Там само.
[27] Детальніше: Gen. David G. Perkins, "Multi-Domain Battle: Driving Change to Win in the Future". *Military Review*, July-August 2017. <https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20170831_PERKINS_Multi-domain_Battle.pdf> [Переглянуто 2025 17 04].
[28] Carafano, 27.

по всій глибині поля бою з метою захоплення, утримання та використання ініціативи, здолання противника та досягнення військових цілей.[29]

Вікном переваг (англ. – Window of advantage) називають стан, що досягається шляхом «[...] конвергенції спроможностей у часі та просторі в обраних доменах та середовищах з метою надання командирам можливості отримати локалізований контроль або фізичний, віртуальний та/або когнітивний вплив в межах визначеної території, щоб запобігти її використанню ворогом або створити умови, необхідні для виконання успішних дружніх операцій», – за визначенням TRADOC, Командування доктрин та підготовки армії США.[30]

В цілому ж, метою конвергенції спроможностей, що дозволяє виявити, створити та використати ці вікна переваг, є уможливлення **маневру**.[31] В свою чергу, маневр дружніх сил крізь всі домени та середовища дозволяє досягти кінцевої мети – поставлених цілей кампанії.[32] Фігура 3 схематично зображує логіку мультидоменного бою.



Фігура 3. Базова логіка мультидоменного бою (схематично). Джерело: складено автором.

Враховуючи все вищесказне, FM 3-0 визначає МДО як «[...] комбіноване (змішане) застосування військ (сил) об'єднаних та армійських спроможностей задля створення та використання відносних переваг, що дозволяють досягати цілей, перемагати сили супротивника та консолідувати здобутки за дорученням командирів об'єднаних сил».[33]

Визначенню МДО новим операційним концептом передували три інші знакові концепти (серед. 1980-х рр. - 2022 р.), кожен з яких ставав логічною і послідовною

[29] "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century: 2025-2040". TRADOC, December 2017, Version 1.0, 77. <https://www.tradoc.army.mil/wp-content/uploads/2020/10/MDB_Evolutionfor21st.pdf> [Переглянуто 2025 17 04].
[30] TRADOC, 79.
[31] TRADOC, 28.
[32] Там само.
[33] FM 3-0, 1-2.

адаптацією попереднього, залежно від оперативного середовища, яке диктувало необхідність впровадження тих чи інших підходів[34]. **Оперативним середовищем, ОС,** (англ. – Operational environment, OE) називають сукупність умов, обставин та факторів, що впливають на використання спроможностей і застосування військ (сил) та рішень командира.[35]

Фігура 4 зображує т. зв. «еволюцію» операційних концептів, якими керувалися політичні десіжен-мейкери, військове командування, аналітики та соціологи американської військової культури. Про кожен з цих концептів можна мислити водночас і як про теоретичний конструкт, і як про практичний інструмент для ведення того чи іншого типу операцій. Станом на сьогодні, концепт МДО можна вважати вінцем цієї «еволюції».[36]

[34] Randi Stenson, "US Army Training and Doctrine Command updates Army capstone doctrine, codifying shift to multidomain operations". U.S. Army: October 10, 2022. <https://www.army.mil/article/260943/us_army_training_and_doctrine_command_updates_army_capstone_doctrine_codifying_shift_to_multidomain_operations> [Переглянуто 2025 19 04].
[35] «Планування вогневої підтримки на тактичному рівні (початок)», Сили територіальної оборони ЗСУ. <https://sprotyvg7.com.ua/lesson/planuvannya-vognevoi-pidtrimki-na-taktichnomu-rivni> [Переглянуто 2025 19 04].
[36] Stenson.

Період дії	Операційний концепт	Сутність концепту. Деякі елементи ОС
1980 - пізні 1990 рр.	**Повітряно-наземна операція** (AirLand Battle)	Підґрунтя: засвоєні уроки Арабо-ізраїльської війни 1973 р. (Йом-Кіпур)[37]. Фокус: тісна координація наземних та повітряних сил; загрози в Європі; візія того, як США мали би битися та перемагати СРСР.[38]
2001 р. - початок 2000-х рр.	**Операції повного спектру** (Full spectrum operations, FSO)	Підґрунтя: Операції в Іраку та Афганістані; вихід з Балканів.[39] Фокус: стабілізаційні операції («operations other than war») набули такої ж важливості, як і основні бойові операції (наступальні та оборонні).[40]
з 2011 р.	**Об'єднані наземні операції** (Unified Land operations, ULO)	Підґрунтя: засвоєні уроки Глобальної війни з тероризмом (GWOT); урахування змін і характеру загроз та зростаючої ймовірності великомасштабних бойових операцій.[41] Фокус: відновлення фокусу на проведення великомасштабних наземних боїв.[42]
з 2022 р. – понині	**Мультидоменні операції** (Multi-domain operations, MDO)	Підґрунтя: становлення кібердомена повноцінним операційним доменом; зростаюча роль РЕБ і РЕР у веденні війни; сприйняття всіх доменів такими, що є оспорюваними. Фокус: необхідність нарощення спроможностей задля досягнення переваги над противником в усіх доменах та площинах конфлікту.

Фігура 4. Еволюція операційних концептів (модель США). Джерело: складено автором.

[37] Jen Judson, "US Army adopts new multidomain operations doctrine". *DefenseNews*, 10 October 2022. <https://www.defensenews.com/land/2022/10/10/us-army-adopts-new-multidomain-operations-doctrine/ > [Переглянуто 2025 19 04].
[38] Там само.
[39] Barry Rosenberg, "How the Army is driving enterprise training across five warfighting domains and three dimensions". *Breaking Defense*, May 23, 2024. <https://breakingdefense.com/2024/05/how-the-army-is-driving-enterprise-training-across-five-warfighting-domains-and-three-dimensions/> [Переглянуто 2025 19 04].
[40] MAJ Cornelius Granai, ""A Complex and Volatile Environment": The Doctrinal Evolution from Full Spectrum Operations to Unified Land Operations", U.S. Army, 2015-01, 3. <https://apps.dtic.mil/sti/tr/pdf/AD1001386.pdf> [Переглянуто 2025 19 04].
[41] Stenson.
[42] Rosenberg.

Важливо також підкреслити, що окрім багатодоменності, разом зі становленням МДО операційним концептом, з'явилося уявлення про те, що будь-які бойові дії відбуваються не лише в п'яти доменах, але й в **площинах**, або **вимірах** (англ. – dimensions). За однією з класифікацій, таких вимірів є три: **людський**, **фізичний** та **інформаційний** (англ. – human, physical, information dimensions).[43] Зокрема, через це МДО також називають **багатовимірними операціями**.

На практиці це означає, що в плануванні та проведенні операцій необхідно враховувати об'єкти, події та явища зазначених трьох вимірів всередині кожного з доменів.[44] Приклад планування наводить Brig. GEN Скот Вудворд, заступник генерал-командувача Загальновійськового тренувального центру Армії США: в наземному домені об'єкти фізичного виміру, що беруться до уваги, – це безпосередньо рельєф місцевості та інфраструктура (місто або гірська місцевість тощо); в людському вимірі – люди, що живуть в даній місцевості та їхній вплив на поле бою, а також ворожі сили (о/с); в інформаційному – йдеться про обмін інформацією (дані, якими обмінюються військові в даній ділянці).[45]

В інших класифікаціях також визначають електромагнітний спектр як окреме середовище, в якому відбуваються військові операції наряду з п'ятьма доменами та іншими вимірами. Сьогодні, від нього так чи інакше залежать всі сучасні війська.[46]

Електромагнігтний спектр (англ. – Electromagnetic spectrum, EMS) – це повний діапазон частот електромагнітного випромінювання від нуля до нескінченності, що поділений на 26 смуг.[47] В свою чергу, **радіоелектронною боротьбою**, або **РЕБ** (англ. Electronic Warfare, EW) називають «[...] військові дії, що включають використання електромагнітної та спрямованої енергій задля контролю над електромагнітним спектром або здійсненням атаки проти ворога»[48]. В умовах сучасних збройних конфліктів, РЕБ є ключовим елементом ведення операцій – як у захисті операцій дружніх сил, так і в перешкоджанні ворожим операціям в межах електромагнітного спектру по всьому оперативному середовищу[49] [50].

---

[43] Rosenberg.
[44] Там само.
[45] Там само.
[46] Joint Publication 3-13.1 "Electronic Warfare". Chairman of the Joint Chiefs of Staff, 08 February 2012, vii. <https://info.publicintelligence.net/JCS-EW.pdf> [Переглянуто 2025 19 04].
[47] JP 3-13.1, GL-7.
[48] JP 3-13.1, GL-8.
[49] JP 3-13.1, vii.
[50] Детальніше – рекомендовано: JP 3-13.1 "Electronic Warfare", 2012.

Слід також зазначити **інструменти**, які, за задумом, уможливлюють імплементацію МДО. По-перше, це **мультидоменні оперативні групи** (англ. – Multi-Domain Task Force, далі – **MDTF** або «таск-форс» групи), які називають «організаційним центральним елементом» загальних зусиль, необхідних для оперування в мультидоменному середовищі.[51]

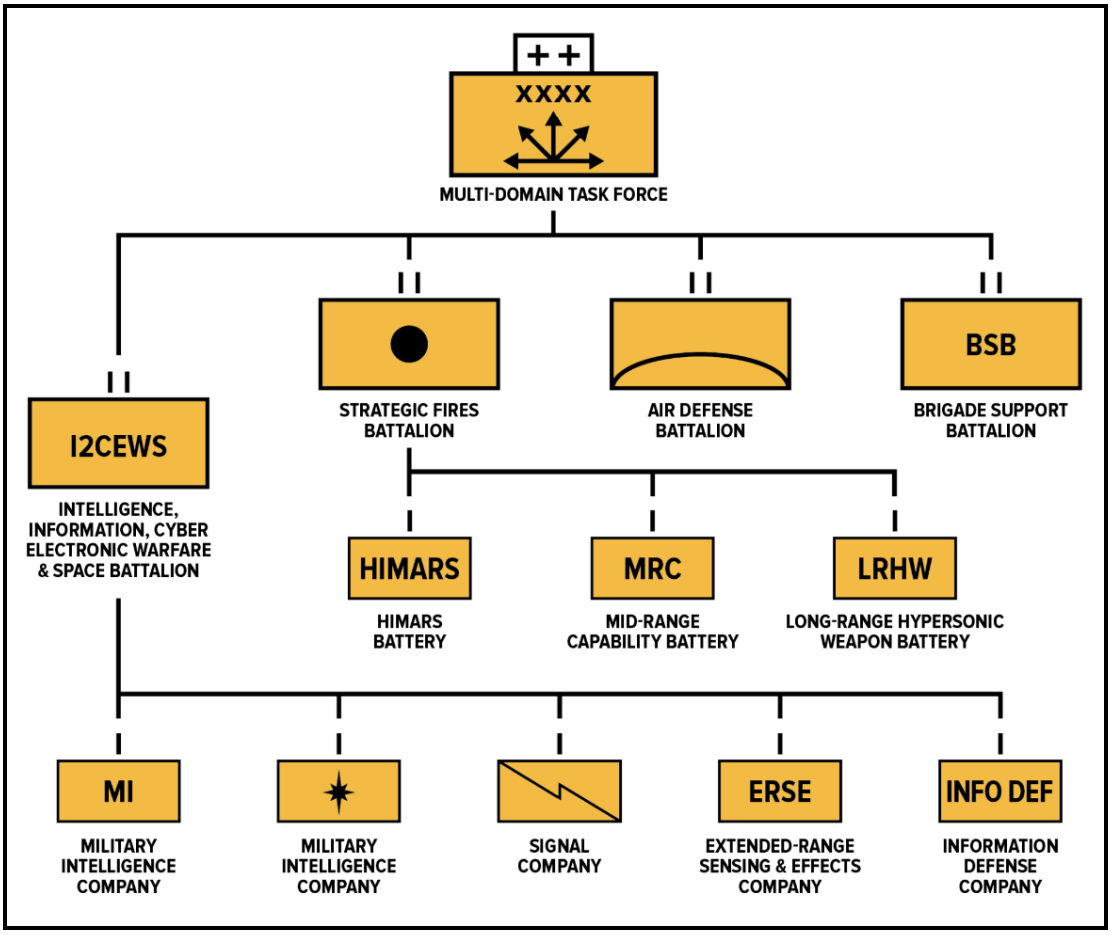
Виконуючи функцію «маневрувальних елементів на рівні ТВД», MDTF поєднують в собі (структурно – в одному підрозділі): a) ударні спроможності, а саме – батальйон стратегічного вогню включно з батареєю HIMARS, системами ураження середньої дальності та батареєю гіперзвукової зброї великої дальності (LRHW); b) спроможності ППО; c) спроможності I2CEWS, що включають засоби РЕБ, РЕР, кібер та космічні спроможності, декілька видів розвідок, інформаційні системи; d) підрозділ забезпечення[52]. (Див. Фігуру 5).

Причому, ключовою відмінністю таких груп від «конвенційних» з'єднань слід вважати не стільки інтеграцію спроможностей різних направленостей в рамках одного підрозділу, – як-то, ударних і вузла I2CEWS, – як централізацію елементів управління ними. Тобто, концепція MDTF передбачає, що в руках одного командира зосереджено управління всіма елементами «таск-форс» групи.

Розгортання MDTF почалось ще у 2017 р. і загалом, передбачало створення п'яти таких груп[53]. Станом на квітень 2024 р. йшлося про послідовне розгортання Пентагоном цих груп на різних континентах залежно від географії очікуваних загроз, зокрема: двох груп – в Індо-Тихоокеанському регіоні, однієї – в континентальній Європі, однієї – в Арктиці, та ще однієї, п'ятої групи, призначеної для реагування на глобальні загрози, – у Північній Каролініі (повна операційна готовність якої очікується на 2028 фін. р.)[54]. При цьому, слід розуміти, що «таск-форс» групи знаходяться на різних стадіях комплектації спроможностями та операційної готовності: від стадії закладеної концепції та розгортання штаб-квартири – до приведення в стан повної операційної готовності.

---

[51] "The Army's Multi-Domain Task Force (MDTF)". Congressional Research Service, updated July 10, 2024. <https://sgp.fas.org/crs/natsec/IF11797.pdf> [Переглянуто 2025 19 04].
[52] "Army Multi-Domain Transformation". Chief of Staff Paper #1 Unclassified Version, Headquarters, Department of the Army, 16 March 2021, 12. <https://apps.dtic.mil/sti/pdfs/AD1143195.pdf> [Переглянуто 2025 19 04].
[53] «США розгортають п'ять Multi-Domain Task Forces для масштабної війни: коли гіперзвук об'єднують з хакерами», *Defense Express*: 29 лютого 2024. <https://defence-ua.com/army_and_war/ssha_rozgortajut_pjat_multi_domain_task_forces_dlja_masshtabnoji_vijni_koli_giperzvuk_objednujut_z_hakerami-14595.html> [Переглянуто 2025 19 04].
[54] Congressional Research Service.



Фігура 5. Схематичне зображення структури мультидоменної оперативної групи (MDTF). Групи можуть включати спроможності інших типів залежно від потреб командування. Джерело: Army Multi-Domain Transformation, Chief of Staff Paper #1

[Втім, в березні 2025 р. стало відомо, що замість розгортання другої групи, чия штаб-квартира вже базується в Німеччині, Пентагон вирішив «перестрибнути» одразу до розгортання та підготовки третьої групи на Гаваях, – таким чином, змінена послідовність розгортання груп порушила саму концепцію та логіку MDTF[55]. Такий хід можна трактувати як зміщення акцентів в усвідомленні загроз, адже друга «таск-форс» група, яка мала би бути приведена в стан повної операційної готовності на 2025 фін. р., функціонувала би як інструмент стримання та реагування на загрози в Європі, – тобто, з боку РФ, – незважаючи на те, що за задумом, система Typhon мала би базуватися у США та періодично розгортатися у Європі.[56]]

[55] «Не проти РФ: США розгорнуть наступний далекобійний Typhon з Tomahawk на Гаваях, а не у Європі», *Defense Express*: 18 березня 2025. <https://defence-ua.com/news/ne_proti_rf_ssha_rozgornut_nastupnij_dalekobijnij_typhon_z_tomahawk_na_gavajah_a_ne_u_jevropi-18291.html> [Переглянуто 2025 19 04].
[56] Congressional Research Service.

Ще одним інструментом МДО, який слід зазначити в контексті даної роботи, є **CJADC2** (також **JADC2)** або Система комбінованого об'єднаного загальнодоменного командування і управління (англ. – (Combined) Joint All-Domain Command and Control). Вона представляє собою систему управління боєм на основі ШІ та МН, яка покликана інтегрувати союзників та об'єднані сили в контексті ведення МДО задля створення переваги над противником.[57]

Річ у тім, що на тлі переосмислення сутності сучасного поля бою, зокрема його мультидоменності та необхідності швидкого нанесення крос-доменного ураження вглиб територій, виникла потреба в покращеному процесі **С2** (**командування і управління**, англ. – Command and Control, C2), що в певному контексті також називають **домінуванням в прийнятті рішень** (англ. – Decision dominance).[58]

В свою чергу, домінування (над противником) в прийнятті рішень досягається за рахунок **конвергенції** (англ. – convergence), що в даному контексті означає вміння інтегрувати численні процеси та дії, такі як бачення, сприйняття, комунікація, здатність стріляти та рухатися зі швидкістю та у масштабі, поєднуючи всі необхідні сенсори з найкращим стрілком та необхідним вузлом С2.[59]

Саме тому і було створено CJADC2 – як механізм, що фокусується на стандартизації системних даних, міграції у хмару та дослідно-експериментальній діяльності на основі ПЗ.[60] Метою конвергенції при цьому є надання бойовим системам **автономії** (див. с. 42) у взаємодії між розвідувальною, оперативною та вогневою функціями, що дозволяє зняти навантаження з командирів і штабів за рахунок технологій ШІ/МН, натомість даючи змогу зосередити зусилля на прискореному та оптимізованому процесі прийняття рішень.[61]

CJADC2 можна також назвати ініціативою Міністерства оборони США з «відродження» інфраструктури С2, яка би відповідала запитам модерної війни.[62] Припускається, що CJADC2 дозволяє це зробити шляхом побудови об'єднаної синергетичної мережі, яка поєднує сенсори та комбатантів кожної гілки військ та уможливлює колективний процес прийняття рішень в ріалтаймі в усіх доменах ведення війни.[63] Іншими словами, CJADC2

[57] Chief of Staff Paper #1, 30.
[58] Chief of Staff Paper #1, 8.
[59] Там само.
[60] Там само.
[61] Там само.
[62] Brett Daniel, "What Is Joint All-Domain Command and Control (JADC2)?", Trenton Systems: Nov 9, 2020. <https://www.trentonsystems.com/en-us/resource-hub/blog/what-is-jadc2> [Переглянуто 2025 19 04].
[63] Там само.

дозволяє збільшити вірогідність успішності місії, покращуючи колективну **ситуаційну обізнаність** (див. с. 29-30) або створюючи загальну оперативну картину (COP) наземних, повітряних, морських та космічних сил та засобів.[64]

В свою чергу, **COP** (англ. – Common operational picture, COP) означає єдине ідентичне відображення актуальної інформації, що є спільним більш ніж для одної групи військ, яке сприяє спільному плануванню та допомагає всім ешелонам досягти ситуаційної обізнаності.[65]

- ***Що називають «крос-доменною взаємодією»?***

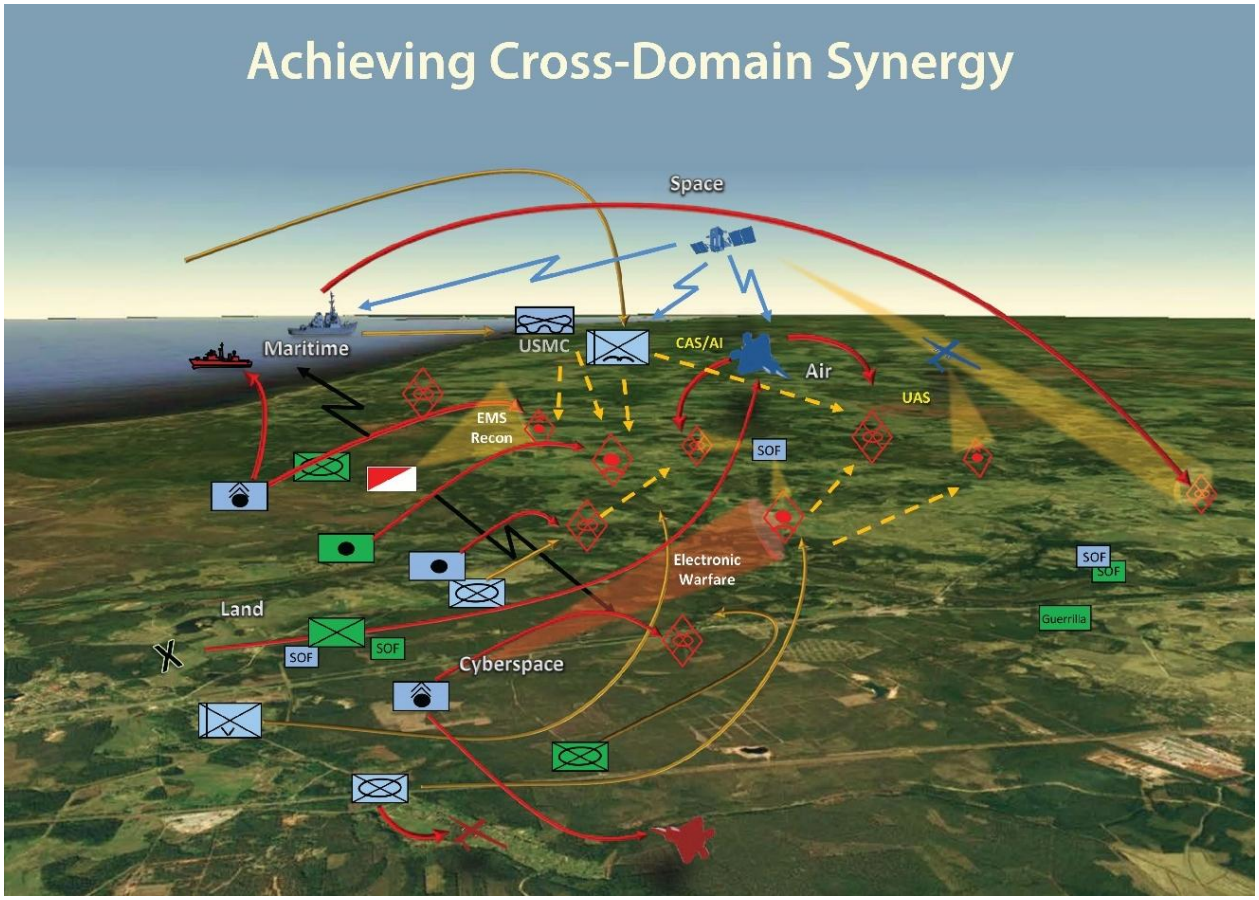
В продовження теми МДО також слід звернути увагу на концепт **крос-доменної взаємодії** (англ. – Cross-domain synergy), або **синергії,** що означає використання двох або більше доменів для досягнення військової переваги.[66] Крос-доменна взаємодія часто передбачає застосування спроможностей одного домену в іншому задля покращення виконання операції та мінімізації непотрібних дублювань функцій в роботі об'єднаних сил[67].

Прикладом крос-доменної взаємодії може служити буквально будь-яка сучасна МДО, в якій поєднуються зусилля наземних сил, повітряних, морських, космічних, а також задіяні спроможності кібер простору, РЕБ/РЕР тощо. (Як продемонструвала російсько-українська повномасштабна війна, успішна наступальна операція зазвичай передбачає поєднання спроможностей кількох доменів.)

Прийнято вважати, що крос-доменної взаємодії може бути досягнуто тоді, коли інтегроване застосування спроможностей наземного, морського, повітряного, космічного та/або кібер домену дає такий комбінований результат, що є кращим за суму результатів, взятих окремо.[68]

---

[64] Там само.
[65] Joint Publication 3-0 "Joint Operations". Chairman of the Joint Chiefs of Staff, 11 August 2011, GL-8. <https://irp.fas.org/doddir/dod/jp3_0.pdf> [Переглянуто 2025 19 04].
[66] William O. Odom and Christopher D. Hayes, "Cross-Domain Synergy". *Joint Force Quarterly*, 73, 2nd Quarter 2014, 124. <https://ndupress.ndu.edu/portals/68/documents/jfq/jfq-73/jfq_123-128_odom-hayes.pdf> [Переглянуто 2025 19 04].
[67] Там само.
[68] Там само.



Зображення 1. Схематичне зображення процесів інтеграції та конвергенції, властивих майбутньому мультидоменому полю бою (складено у 2017 р.). Даний сценарій демонструє досягнення крос-доменної взаємодії об'єднаними силами. Джерело: GEN David G. Perkins.

AI, Air Interdiction	Перекриття повітряного простору/глибинна повітряна підтримка
CAS, Close air support	Безпосередня авіаційна підтримка (БАП)
EMS Recon, Electromagnetic spectrum reconnaissance	Розвідка електромагнітного спектру
SOF, Special operation forces	ССО, Сили спеціальних операцій
USMC, United States Marine Corps	Корпус Морської піхоти Сполучених Штатів
Electronic Warfare	Радіоелектронна боротьба (РЕБ)
Guerrilla	Партизанський рух
UAS, Unmanned aircraft system	Безпілотна авіаційна система (БАС)

Легенда 1 до Зображення 1 з перекладом на українську. Джерело: складено автором.

- ***Що таке «ситуаційна обізнаність» та «системи ситуаційної обізнаності»?***

Однією з основних функцій, яку покликані виконувати СПЗ, є забезпечення ситуаційної обізнаності. В українській військовій культурі на доктринному рівні це поняття як чітко визначений концепт наразі не затверджено, хоча фактично, ситуаційна обізнаність є невід'ємним елементом ведення війни та функціонування військ на полі бою у будь-якому масштабі та обсязі.

В широкому сенсі, **ситуаційну обізнаність** (англ. – Situational Awareness, SA) можна охарактеризувати як стан, що досягається через безперервну підтримку поінформованості про оперативне середовище в режимі реального часу або часу, наближеного до реального, у всіх доменах ведення війни та усіх вимірах. Також, ситуаційну обізнаність називають «**ключовою складовою мережецентричної війни**» (див. с. 30-34), визначаючи як «[...] комплексне розуміння поточної обстановки на полі бою, яке дозволяє командирам та військовим підрозділам ефективно приймати рішення та діяти».[69]

Говорячи про ситуаційну обізнаність, йдеться про те, в якій мірі військовий, або частіше – угрупування, володіє повнотою інформації в ріалтаймі про розташування і характер дружніх та ворожих сил та засобів, а також, явища, події і процеси, що тривають на полі бою у різних доменах та вимірах. **Ситуаційно обізнаний** військовий може встановити рельєф місцевості, ідентифікувати ворожий об'єкт, оцінити загрозу, визначити дружні сили та засоби задля уникнення дружнього вогню, координуватися із сусідами тощо.

Сукупно, ситуаційна обізнаність сприяє підвищенню ефективності (особливо, в контексті об'єднаних операцій, які сьогодні є «кістяком» ведення війни), проактивності, координації дій між сусідніми підрозділами. Висловлюючись на тему об'єднаних операцій, підполковник Ярослав Гончар, голова ГО «Аеророзвідка», пояснює: «[в]сіх залучених до операції треба усадити в одне інформаційне поле, дати їм офіційну інформацію, щоб вона була така, що їй довіряють, щоб не було трактувань. І це забезпечує система ситуаційної обізнаності».[70]

Також, в контексті процесу С2, ситуаційну обізнаність можна тлумачити як одну з його складових. Припускається, що в С2 існує три основні способи використання інформації, першим з яких є забезпечення ситуаційної обізнаності як базису для подальшого

[69] «Напрям ISTAR», ГО «АЕРОРОЗВІДКА». <https://aerorozvidka.ngo/direction/istar> [Переглянуто 2025 19 04].
[70] «У кожному гаражі "Силіконова долина". Гончар про виробництво дронів в Україні», *Українське радіо*: 23.07.2024. <http://www.nrcu.gov.ua/news.html?newsID=104887> [Переглянуто 2025 19 04].

прийняття рішень; другим способом є керування та координація дій для імплементації цих рішень; третім – оцінка виконання та ефективності цих дій.[71] Тобто, можна вважати, що ситуаційна обізнаність служить початковим і водночас ключовим інструментом в процесі прийняття рішень, виконання операцій на основі цих рішень та їхньої оцінки.

Відповідно, **системою ситуаційної обізнаності** можна назвати вид СПЗ, основною функцією якого є надання ситуаційної обізнаності, що дозволяє об'єднувати численні об'єкти поля бою і великі обсяги різних типів даних в єдину мережу. Така система застосовується для планування операцій, розвідки, координації сил під час виконання операції, а також на етапі аналізу проведеної операції.

В українському контексті розвитку систем ситуаційної обізнаності, на думку фахівця МОУ, ці системи отримали **найбільший запит на тактичному рівні**, що і демонструє нинішня фаза російсько-української війни 2022 року-по сьогодні[72]. За його словами, сучасна війна доводить, що українські системи переважно виходять «з низів», тобто, **розвиваються за принципом знизу-вгору** (англ. – down-up), беручи свій початок на тактичному рівні[73]. Пояснити це явище можна тим, що умовно «[...] 90% армії сконцентровано на тактичному рівні», тому там і варто шукати їхні витоки, на думку фахівця.[74]

- ***Що таке «мережецентрична війна», та чим її підходи відмінні від підходів «платформоцентричної війни»?***

Поняття **мережецентричної війни** (англ. – Net-centric/Network-centric Warfare, NCW) нерозривно пов'язане із викладеним у попередньому пункті поняттям, адже в основі цього концепту лежить один фундаментальний принцип: отримання переваги над противником завдяки набуттю повної інформаційної (ситуаційної) обізнаності.

Даний концепт окреслився в 1990-х рр. в американській військовій культурі, після чого його було виведено на доктринний рівень та безпосередньо інтегровано в операції. В цілому, саме на засадах поняття мережецентричності побудовано принципи ведення сучасної війни XXI століття. Не виняток і нинішня російсько-українська війна, значне місце в якій займають мережецентричні підходи. (В рамках цієї роботи, про поточну фазу війни

[71] Joint Publication 6-0 "Joint Communications System". Chairman of the Joint Chiefs of Staff, 10 June 2015, Incorporating Change 1, 04 October 2019, I-2. <https://irp.fas.org/doddir/dod/jp6_0.pdf> [Переглянуто 2025 19 04].
[72] З особистої розмови з фахівцем МОУ.
[73] Там само.
[74] Там само.

йдеться як про таку, в якій обидві сторони конфлікту впроваджують мережецентричні підходи, втім, в різній мірі та з різною успішністю та на різних рівнях ведення війни.)

Керуючись визначенням поняття, яке надають д-р Девід С. Альбертс та інш., мережецентрична війна є концепцією операцій, яка реалізована завдяки інформаційній перевазі, і яка генерує **зростання бойової сили через об'єднання в одну мережу** «сенсорів», «десіжен-мейкерів» та «стрільців» задля досягнення спільної обізнаності, підвищення швидкості управління, вищого темпу операцій, вищої летальності (рівня втрат противника), вищої «живучості», а також вищого рівня самосинхронізації.[75] Іншими словами, мережецентричний підхід полягає у **перетворенні інформаційної переваги на бойову силу** шляхом ефективного поєднання обізнаних суб'єктів на полі бою».[76]

В цьому контексті, **суб'єкти поля бою** за функційністю умовно розподіляють на три групи: 1) **«сенсори»** – ті, що надають бойову (ситуаційну) обізнаність («сенсорами» можуть бути як супутники, так і піхотні розвідувальні групи (англ. – "eyes on the ground")), 2) **«десіжен-мейкери»** – ті, що приймають рішення, та 3) **«а́ктори»**, або ж **«стрільці»**, які створюють «цінність» у вигляді «бойової сили» на полі бою.[77] До третьої групи зокрема відносять засоби ураження.

В дослідженні інституції CCCR (C4ISR Cooperative Research Program) Міністерства оборони США від 2000 р. термін «мережецентрична війна» трактовано як такий, що на той час вважався найбільш точним для опису війни та організації її процесів, якими вони будуть в інформаційну еру[78]. Adm. Джей Л. Джонсон, начальник оперативного штабу ВМС США, назвав «фундаментальним зсувом» перехід від платформоцентричної до мережецентричної війни.[79]

В чому ж полягає **відмінність між мереже- та платформоцентричними підходами**? Коротка відповідь на це питання: у побудові взаємозв'язків між трьома групами суб'єктів поля бою та способах їхньої взаємодії. Розширена відповідь також включала би пояснення, що в мережецентричній парадигмі, «а́ктори» («стрільці») за своєю сутністю не володіють «сенсорами», а «десіжен-мейкери», в свою чергу, не мають влади над «а́кторами».[80]

---

[75] David S. Alberts, John J. Garstka, Frederick P. Stein, *Network Centric Warfare*, 2nd ed. (revised). DoD C4ISR Cooperative Research Program, Washington, D.C.: August 1999/Second printing February 2000, 2. <http://www.dodccrp.org/files/Alberts_NCW.pdf> [Переглянуто 2025 19 04].
[76] Там само.
[77] Alberts et al., 116.
[78] Alberts et al., 2.
[79] Там само.
[80] Alberts et al., 120.

Натомість, **платформоцентричний підхід ведення війни** (англ. – Platform-centric warfare) передбачає, що певні платформи володіють озброєнням, а озброєння має власні органічні «сенсори».[81] Тобто, існує певний розподіл. На практиці це означає, що деякі бойові групи мають «закріплене» за ними озброєння та доступ до «закріплених» за ними «сенсорів», що виключає можливість використання цього самого озброєння та інформації від цих самих «сенсорів» іншими суб'єктами поля бою.

На противагу, в мережецентричній війні, усі три групи суб'єктів демонструють взаємодію у відповідь на динаміку поля бою, прагнучи досягти намірів командування.[82] Таким чином, мережецентричні підходи забезпечують більш гнучкий спосіб ведення війни, передбачаючи доволі великий діапазон можливостей швидкого реагування на події поля бою, що динамічно змінюються.

Також, однією з ключових переваг мережецентричних підходів над традиційними (платформоцентричними) вважають **швидкість управління,** або ж, швидкість командування (англ. – Speed of command). Під «швидкістю управління» мають на увазі час, необхідний для розпізнавання та розуміння ситуації (або зміни в ситуації), ідентифікації та оцінки можливих варіантів дій, вибору відповідного (оптимального) курсу дій та перетворення його на дієві накази[83]. Саме швидкість управління служить базовим показником, що визначає ефективність підходу C2, організації та (бойових) систем.[84] Відповідно, високу швидкість управління можна вважати одним з позитивних наслідків об'єднання обізнаних суб'єктів поля бою в одну мережу.

Вважається, що допоки відповідний курс дій «вкладається» в наявний план, цей план є валідним, – він «спрацьовує», – і водночас, вимушене перепланування потребує багато часу та застосування людських зусиль, внаслідок чого знижується бойова ефективність[85].

Та річ у тім, що в платформоцентричних операціях, ситуаційна обізнаність схильна постійно погіршуватися, а тому, в ситуації, коли жоден план «не спрацьовує», не витримуючи первинного контакту з противником, причину слід шукати в недостатньо стабільній ситуаційній обізнаності.[86] Отже, низький рівень ситуаційної обізнаності уповільнює процеси планування, оскільки командири відкладають прийняття рішень

[81] Там само.
[82] Там само.
[83] Alberts et al., 163.
[84] Там само.
[85] Alberts et al., 163-164.
[86] Alberts et al., 164.

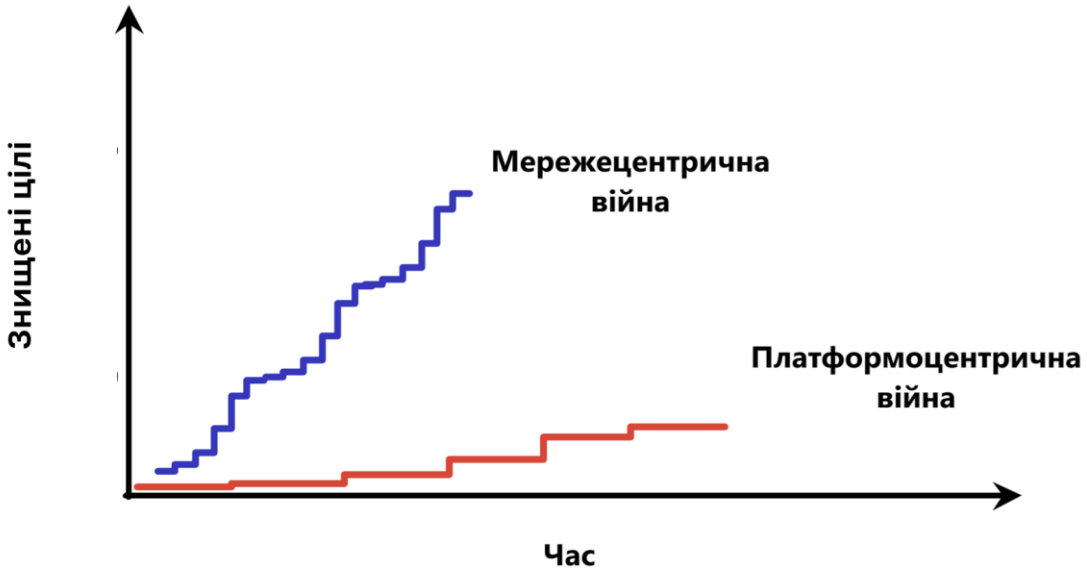
допоки ключові елементи інформації не будуть оновлені.[87] Іншими словами: «десіжен-мейкери» не віддають наказів «стрілкам», допоки не дочекаються актуальної інформації саме від своїх «сенсорів».

Зокрема, на полі бою це знаходить прояв у повільнішому процесі прийняття рішення на ураження. Натомість, той, хто застосовує мережецентричні підходи, має **перевагу у прийнятті рішень на ураження**, і відповідно, здобуває **вогневу перевагу** над противником.

Уявімо схематично: червоні (сили противника) застосовують платформоцентричні підходи – тобто, командир батареї («десіжен-мейкер») віддає наказ розрахунку («стрільцям») тільки тоді, коли володіє оновленими актуальними даними про ціль від власних «сенсорів», що звітують йому. За таких умов, утворюється надто довгий **цикл вогневого ураження**, або ж **кілчейн** (див. с. 45-46), що водночас, створює перевагу для синіх (дружніх сил), які керуються мережецентричними підходами та набагато швидше можуть «зчитати» обстановку, перебуваючи всі в одній «мережі». (Приклад наведено на базі одного з кейзів російсько-української війни.) Тому, ще однією ознакою мережецентричної війни можна вважати прагнення **максимально скоротити кілчейн**, а в ідеалі – зробити його близьким до нуля.

Фігура 6 схематично зображує результати експерименту, проведеного під час навчань ВМС США *Fleet Battle Experiment (FBE) Delta* у взаємодії з американсько-корейськими навчаннями *Exercise Foal Eagle* у 1998 р., в рамках якого було об'єднано «сенсори» і «стрільців» сухопутних військ та ВМС.[88] До того, ці суб'єкти поля бою існували ніби в окремих екосистемах, будучи «прив'язаними» до різних родів військ. Внаслідок застосування мережецентричних підходів, тобто, об'єднання суб'єктів в одну мережу, вдалося досягти надзвичайно високого рівня спільної обізнаності на полі бою, що було використано для підвищення бойової сили[89].

[87] Там само.
[88] Alberts et al., 178.
[89] Там само.



Фігура 6. Застосування підходів мережецентричної війни – на базі експерименту Delta. Джерело: Alberts et al., "Network Centric Warfare".

- ***Що означає концепт «ISR» та похідні від нього концепти (JISR, C4-C7ISR)? Що означає концепт «ISTAR»?***

Концепти «ISR» та «ISTAR», а також похідні від них концепти (див. Глосарій) слід тлумачити як a) ключові **процеси та/або стандарти в системі бойового управління**, що сукупно формують поняття мережецентричної війни (див. с. 30-34), і водночас як b) **спроможності**, які ці процеси/стандарти уможливлюють. (Зверніть увагу: більшість СПЗ, що сьогодні функціонують в інтересах СОУ, зокрема, описані в даній роботі в *частині другій II (i)*, можна вважати як елементами процесів ISR та ISTAR, так і безпосередньо спроможностями ISR та ISTAR.)

ISR дослівно «розшифровується» як «**розвідка, спостереження та рекогностування**» (англ. – ISR, Intelligence, Surveillance, Reconnaissance), де кожне з трьох слів означає окремий процес. В британській військовій культурі, наприклад, ISR вважають не стільки дисципліною розвідки, як «[...] інтегрованою діяльністю і процесом», що включає отримання оперативної задачі, надання напрямку спроможностям ISR, збір даних та інформації, перетворення їх на придатний для використання формат та передачу для подальшого використання десіжен-мейкерами, виконавцями та аналітиками розвідки.[90]

[90] Joint Doctrine Publication 2-00 “Intelligence, Counter-intelligence and Security Support to Joint Operations”. UK Ministry of Defence, The Development, Concepts and Doctrine Centre, August 2023 (4th

Важливо зазначити, що в даному контексті, а також наступних частинах дослідження, термін «розвідка» використовується виключно у значеннях: a) **розвід.даних** (англ. – Intelligence), а також, b) **військової розвідки** (англ. – Military intelligence)[91] та/або **бойової розвідки** (англ. – Combat intelligence), яку прийнято вважати однією з її функцій (гілок).[92] (Детальніше – див. Глосарій). Говорячи про військову та бойову розвідки, зазвичай йдеться про тактичний рівень ведення війни. (Зверніть увагу: в контексті розвідки в цілому, а також військової розвідки, поняття «**дані**» (англ. – Data) та «**інформація**» (англ. – Information) не є тотожними. Детальніше – див. Глосарій.)

Вартує також зауважити, що в цьому контексті, традиційний розподіл на тактичний, оперативний та стратегічний рівні несе невелике практичне навантаження – адже момент, в якому розвідка стає тактичною, оперативною або стратегічною – це момент прийняття рішення або виконання дії на одному з рівнів[93]. В цілому ж, командири тактичної ланки можуть робити запит на отримання доступу до розвідки, що походить зі стратегічного рівня, і навпаки – розвідка, отримана на тактичній ланці, може мати стратегічне значення.[94]

Що стосується ISR як процесу, то він складається з **п'яти покрокових підпроцесів**, або етапів, що сукупно називають акронімом **TCPED** (англ.: Task, Collect, Process, Exploit, Disseminate), а саме: 1) задачі, 2) збору, 3) обробки, 4) використання, 5) розповсюдження[95] (див. Фігуру 7).

При цьому, як зазначається в Joint Doctrine Publication 2-00 Міністерства оборони Великої Британії (JDP 2-00), трьома основними результатами ISR вважають: 1) підтримку операцій; 2) підтримку таргетингу (визначення та пріоритизацію цілей); 3) підтримку розвитку знань.[96] В цілому, ISR спирається насамперед на технічні спроможності збору

---

edition), 86.
<https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf> [Переглянуто 2025 19 04].

[91] Слід розрізняти військову розвідку (аналог англ. – military intelligence) та воєнну розвідку (аналог англ. – defence intelligence). Поняття не є тотожними.

[92] Детальніше – рекомендовано: JDP 2-00 (2023, 4th ed.), а також: David Strachan-Morris, "Knowledge gives strength to the arm: an agenda for studying combat intelligence as a discrete function within military Intelligence". *Intelligence and National Security*, 2024 (vol.39), issue 7. <https://doi.org/10.1080/02684527.2024.2383011> [Переглянуто 2025 20 04].

[93] JDP 2-00 (2023, 4th ed.), 19.

[94] Там само.

[95] JDP 2-00 (2023, 4th ed.), 86-87.

[96] JDP 2-00 (2023, 4th ed.), 86.

(даних), але потенційно може поєднувати як технічні, так і нетехнічні способи збору в режимах реального часу та наближеного до реального.[97]

Задача (Task)	Отримання зовнішнього напрямку, внутрішнього планування, ресурсного забезпечення, управління та розподілу ISR спроможностей (вкл. з обробкою, використанням та розповсюдженням) відповідно до бажаних результатів.
Збір (Collect)	Збір інформації з використанням спроможностей ISR. (Ресурси можуть включати технічні та людські джерела для надання необроблених даних.)
Обробка (Process)	Перетворення зібраних необроблених даних на придатний до використання формат для подальшого використання, зберігання або розповсюдження. (Здійснюється як людьми, так і комп'ютерами залежно від типу даних.)
Використання (Exploit)	Оброблені дані та інформація використовуються для здобування цінності та призначення цінності. (Також, може з'явитися потреба в додаткових даних та інформації).
Розповсюдження (Disseminate)	Надання доступу до даних, інформації та розвідки як результат процесів збору, обробки та використання. (Доступ може бути надано в режимі часу, наближеного до реального або внаслідок більш ретельних обробки та використання.)

Фігура 7. П'ять етапів ISR (англ. – TCPED). Джерело: складено автором на основі JDP 2-00 Міністерства оборони Великої Британії.

Окрім «оригінального» концепту ISR, нерідко зустріти можна також і похідні від нього концепти. Наприклад, **JISR** або **об'єднаний ISR** (англ. – JISR, Joint ISR) є операційним концептом союзницької спільноти НАТО (див. Глосарій). Втім, ключовим концептом на сьогодні можна вважати **C4ISR** (англ. – Command and Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance), що означає дослівно: **командування і управління, зв'язок, комп'ютери (IT), розвідка, спостереження, рекогностування**.

[97] Там само.

Як вже зазначалося, залежно від контексту, C4ISR можна трактувати і як процес/стандарт військового управління, і водночас, – як спроможності. Говорячи про C4ISR як стандарт, слід сказати, що C4ISR та його модифікації (C5ISR, C6ISR, C7ISR)[98] насамперед покликані реалізувати доктрину мережецентричної війни (див. с. 30-34), а впровадження підходів C4ISR дозволяє досягти: a) в рази вищої швидкості прийняття поінформованих та зважених рішень командирами; b) здатності зберігати керованість навіть у випадку знищення пунктів управління; c) суттєвого зменшення втрат о/с (в десятки разів) та видатків на артилерійські снаряди[99].

В розрізі другого значення (C4ISR як спроможності) C4ISR називають гнучкою автоматизованою «[...] системою оперативного (бойового) управління, зв'язку, розвідки та спостереження, що діє за стандартами військового керування НАТО, яка дозволяє досягти інформаційної переваги над ворогом і трансформується в бойову могутність завдяки поєднанню роботи підрозділів й усіх розвідувальних спроможностей в єдиний цифровий дієвий простір», – за формулюванням Вадима Машталіра та інш.[100] Основою для побудови інноваційних гнучких автоматизованих систем управління, таких як C4ISR-C7ISR, є **бездротові сенсорні мережі**, або **БСМ** (англ. – Wireless sensor network), що забезпечують належне функціонування цих систем[101] (детальніше – див. Глосарій).

В цілому, системи C4ISR-C7ISR здатні забезпечувати збір та аналіз багатовимірної розвідувальної інформації в усіх доменах ведення війни з урахуванням великої кількості різного виду сигналів (електронних, електрооптичних, інфрачервоних, супутникових).[102] На практиці, робота таких систем дозволяє «[...] покращити процес прийняття оперативних рішень, гарантує миттєве й ефективне їх доведення до виконавців, забезпечує здатність до супроводу, здійснює контроль і, за потреби, регулює виконання поставлених бойових завдань».[103]

Слід також додати, що ключовою відмінністю систем класу C4ISR (та модифікацій) від класу C2 вважають вищий ступінь автоматизації інформаційних (управлінських) завдань,

---

[98] C5ISR, C6ISR та C7ISR можна вважати подальшими модифікаціями C4ISR, серед яких, станом на сьогодні, найбільш просунутим є C7ISR (див. Глосарій).
[99] "What is C4ISR", ГО «АЕРОРОЗВІДКА», Sept 20, 2022. <http://surl.li/nlwnxd> [Переглянуто 2025 19 04].
[100] Вадим Машталір, Олександр Жук, Людмила Міненко, Сергій Артюх, «Концептуальні підходи застосування бездротових сенсорних мереж арміями передових країн світу». *Сучасні інформаційні технології у сфері безпеки та оборони*. 2023/Том 47 (№ 2), 99. <https://doi.org/10.33099/2311-7249/2023-47-2-96-112> [Переглянуто 2025 19 04].
[101] Машталір та інш., 96, 99.
[102] Машталір та інш., 96.
[103] Там само.

відповідно, всі системи класу C4ISR (та модифікацій) відносять до АСУВ (див. с. 40-41) оперативної або оперативно-стратегічної ланки управління.[104]

В свою чергу, акронім «**ISTAR**», що дослівно означає «**розвідка, спостереження, цілевказання та рекогностування**» (англ. – ISTAR, Intelligence, Surveillance, Target Acquisition and Reconnaissance), тлумачать як процес і стандарт, що широко застосовується у військах НАТО та віднедавна запроваджується і в Україні, зокрема, зусиллями ГО «Аеророзвідка»[105]. Тим не менш, на доктринному рівні цей концепт досі не затверджено. Говорячи про ISTAR в значенні процесу/стандарту, в цілому, він «[…] полягає у зборі, первинній обробці, співставленні, пріоритизації інформації та її швидкій передачі до зацікавлених споживачів».[106]

Як можна визначити з самої назви, в порівнянні з акронімом ISR, тут додається компонента «**ТА**» (англ. – Target Acquisition), тобто, **цілевказання**. Проте, було би помилково стверджувати, що додана функція цілевказання, що означає знаходження цілі, закріплення за нею та супроводження і є тою відмінністю між ISR та ISTAR[107]. Насправді, компонента «ТА», що «стоїть» між двома концептами, послужила своєрідним поштовхом до ширшої дискусії в розвідувальних колах деяких західних країн (зокрема британської гілки) на тему відносин між розвідкою та операціями у військовому командному складі в цілому, і конкретно – в питанні підтримки розвідкою функції цілевказання, – пояснює проф. Філіп Девіс.[108]

Річ у тім, що просування концептів ISR (американська гілка) та ISTAR (британська гілка), які відбувались паралельно та фактично безвідносно один до одного, з часом перетворилося на спроби американської та британської гілок розвідки «захопити» і надалі диктувати дискурс тих вагомих змін, що відбулися у самому характері розвідки та її ролі у військових операціях, які ознаменували початок т. зв. «**революції у військовій справі**» (англ. – Revolution in military affairs, RMA).[109] В контексті теорії, що виникла на початку 1990-х рр., цей термін використовують для узагальнення «[…] ряду кардинальних технологічних

---

[104] «Від C2 до C4ISR: що ховається за цими абревіатурами», *Defense Express:* 31 травня 2020. <https://defence-ua.com/weapon_and_tech/vid_s2_do_s4isr_scho_hovajetsja_za_tsimi_abreviaturami-872.html> [Переглянуто 2025 19 04].
[105] «Напрям ISTAR», ГО «АЕРОРОЗВІДКА».
[106] Там само.
[107] Philip H.J. Davies, "ISR versus ISTAR: A Conceptual Crisis in British Military Intelligence", draft paper (in press with *International Journal of Intelligence and Counterintelligence*, 2021/35 (1), 73-100), 2. <https://bura.brunel.ac.uk/bitstream/2438/22272/3/FullText.pdf> [Переглянуто 2025 19 04].
[108] Там само.
[109] Там само.

змін у сенсорах, озброєнні, платформах, що поєднують і те, і інше, та інформаційних технологіях, що мали змінити виконання військових операцій у XXI ст.».[110]

Зрештою, в результаті ряду дебатів в розвідувальних колах союзників, що тривали не один рік, «паперових битв» та переписування доктрин, концепт ISTAR все-таки затвердився (хоч і неофіційно) як такий, що несе більше практичної користі та більш точно відповідає характеру операцій сучасних збройних конфліктів[111].

Що стосується складових процесу ISTAR, слід розуміти, що окрім підтримки функції цілевказання розвідкою, також постає питання **розподілу функцій збору та власне розвідки**. Як пояснює голова ГО «Аеророзвідка» підполковник Ярослав Гончар, процес ISTAR як такий вкоренився у військовій культурі країн-членів НАТО ще на початку 90-х рр., зокрема через набутий досвід деяких операцій, як-то «Буря в пустелі» (англ. – Operation Desert Storm), коли прийшло усвідомлення того, що «[…] функція збору інформації має бути відокремлена від процесу розвідки».[112] (Зокрема в цьому, на думку Гончара, і можна побачити ментальну відмінність між українською та західними військовими культурами.[113])

Причиною відокремлення цих функцій він називає те, що в розумінні західних партнерів, розвідка є нічим іншим як прогнозуванням, що базується на результатах аналізу, а продуктом роботи розвідників є передбачення, – і саме тому, «[розвідники] не залучені до процесу збору інформації».[114] Натомість, функція збору та обробки інформації покладена на ISTAR, як це практикують на рівні органів управління та штабів в країнах НАТО.[115]

В контексті російсько-української війни, збором, обробкою та передачею інформації в межах процесу ISTAR займається мережа ситуаційних центрів, керуючись наступним алгоритмом: пункт ISTAR отримує інформацію та пріоритизує її, передає відповідним підрозділам, яких ця інформація стосується головним чином (наприклад, артилерійський підрозділ або аналітики), а також, вже в обробленому вигляді, передає «[…] командиру та

[110] Там само.
[111] Davies, 3.
[112] «Як працює система управління військами Delta. Інтерв'ю зі співзасновником ГО "Аеророзвідка" Ярославом Гончаром», *Militarnyi*: 5 лютого 2023. <https://mil.in.ua/uk/articles/yak-pratsyuye-systema-upravlinnya-vijskamy-delta-interv-yu-zi-spivzasnovnykom-go-aerorozvidka-yaroslavom-goncharom/> [Переглянуто 2025 21 04].
[113] Там само.
[114] Там само.
[115] Там само.

його штабу для прийняття поінформованих рішень та ефективного планування операцій»[116].

Проте, слід розуміти, що якщо ISTAR – це процес, то його продуктом є загальна (поточна) оперативна картина, або ж COP (див. с. 27)[117]. Іншими словами, як пояснює Гончар, задачею підрозділів ISTAR є надання інформації про поточну ситуацію на полі бою в «[...] режимі наближеного до реального часу всім зацікавленим користувачам, у першу чергу, командиру».[118]

- ***Що таке «АСУ» (автоматизовані системи управління) та «АСУВ» (автоматизовані системи управління військами)?***

Надання ситуаційної обізнаності (див. с. 29-30) – лише одна з функцій, що їх надають СПЗ. Інший значний пласт – це **автоматизація процесів управління**. Зокрема, функцію управління закладено в АСУ та АСУВ, автоматизовані системи управління (військами). **Різниця між АСУ та АСУВ** вагома, і полягає вона в тому, що друге поняття можна назвати «збірним конгломератом» різних АСУ, в той час як АСУ прийнято вважати однією системою, яка має визначене призначення та окреслений рівень застосування[119]. Так, АСУВ може включати в себе декілька десятків автоматизованих систем різного рівня та призначення, які сукупно вважаються її компонентами (підсистемами)[120].

Залежно від спеціалізації та призначення, серед **АСУ** розрізняють, прикладом, АСУ польової артилерії, АСУ авіації та ППО, АСУ документообігу тощо (див. с. 51-52). В свою чергу, **АСУВ** (англ. – Automated Force Management System) характеризують як «[...] взаємопов'язану сукупність засобів отримання та обробки інформації, передачі даних та зв'язку, яка забезпечує процеси збору, аналізу й оцінки обстановки, прийняття рішень, планування, доведення цих рішень до військ (сил) та контроль за ходом їх виконання шляхом зменшення безпосереднього втручання людини у відповідні процеси».[121]

Також, до систем управління можна віднести ще одну знакову категорію систем – це **АСКВ**, або **автоматизовані системи керування вогнем** (англ. – AFCS, Automated Fire-control system). АСКВ призначені для використання артилерійськими підрозділами та

[116] Там само.
[117] Там само.
[118] Там само.
[119] Данило Древницький, «Автоматизована система управління військами – зброя перемог». *Військовий кур'єр:* 3 грудня 2022. <https://mil.co.ua/avtomatyzovana-systema-upravlinnya-vijskamy-zbroya-peremogy/> [Переглянуто 2025 21 04].
[120] Там само.
[121] Там само.

можуть включати виконання таких задач як «[...] розвідка (цілевказування), прийняття рішення на виконання вогневого завдання, виконання балістичних обчислень, оцінка результатів стрільби і впровадження необхідних поправок до вогневих засобів, обмін даних між елементами АСКВ (робочі місця обслуги, вогневі засоби, машини управління, засоби розвідки, комунікація з більш високим рівнем командування), планування логістичної підтримки і місії в цілому (в т.ч. оцінка запасів амуніції, планування зміни позицій тощо), оцінка тактичної обстановки».[122]

Нерідко також можна почути і про **системи управління боєм** (англ. – BMS, Battle Management System). В такому випадку йдеться про системи тактичного рівня управління підрозділами. Вони відіграють критичну роль на всіх стадіях ведення бою і підготовки до нього, координуючи дії підрозділу (-ів) в ріалтаймі на підготовчій фазі (планування), під час виконання операції, а також на фазі аналізу післядії (AAR).[123]

- ***Що таке «РАС» (роботизовані та автономні системи), «ЛАСО» (летальні автономні системи озброєння), та яке їхнє місце у веденні сучасної війни? Що таке «кілчейн»?***

Роботизовані та автономні системи (РАС) все більше вкорінюються у веденні модерної війни, доказом чому є поле бою поточної російсько-української війни. Водночас, було би хибно стверджувати, що нинішня війна є «війною дронів», – а саме таке формулювання можна часто почути з неекспертних джерел, зокрема, у медіа.

Насамперед, слід відзначити, що дрони, які коректніше називати **безпілотними роботизованими** або ж **автономними системами** (залежно від рівня автоматизації), проектуються, керуються, ремонтуються і працюють за параметрами і критеріями, заданими людьми – інженерами та операторами роботизованих систем. Тож, говорити про «війну дронів», виключаючи фактор людини у застосуванні РАС, некоректно – принаймні, станом на сьогодні. З іншого боку, об'єктивною та незаперечною є тенденція зросту активності використання РАС на всіх рівнях ведення війни, а також, набуття системами все ширшого діапазону і все вищого рівня складності задач, які вони здатні виконувати автономно.

---

[122] За прикладом АСКВ «TOPAZ» (виробництва Польщі): Володимир Заблоцький, «Чому "Топаз" - не "Оболонь"», *Defense Express*: 05 травня 2020. <https://defence-ua.com/weapon_and_tech/chomu_topaz_ne_obolon-645.html> [Переглянуто 2025 21 04].

[123] Див. *частина друга*, с. 65-72 – опис системи ComBat Vision, яка серед українських систем українських сьогодні є найближчою до системи управління боєм.

Задля уникнення плутанини, розберімося в термінології та значеннях понять, що стосуються РАС. Для цього, звернімося до публікації Гаазького Центру Стратегічних досліджень, яка є результатом дворічного дослідження в межах діяльності експериментального підрозділу РАС Збройних сил Нідерландів, створеного у 2018 р..

Отже, **автономією** (англ. – autonomy) в контексті бойових систем називають «[р]івень незалежності, який люди надають системі для виконання певної задачі».[124] Також, автономія – це умова або якість (характеристика) системи у процесі самоуправління, що здійснюється задля досягнення поставленої задачі і базується на ситуаційній обізнаності, якою володіє система (інтегровані сенсори, сприйняття та аналіз), а також, спроможності планування та прийнятті рішень.[125] [126]При цьому, не слід ототожнювати автономію (характеристику) і автоматизацію (процес). Автономію (як характеристику) можна віднести до спектра автоматизації, в якому процес незалежного прийняття рішень може бути пристосовано до певної операції, рівня ризику та ступеня взаємодії людини і комп'ютера.[127]

Роботом (англ. – robot) називають механізм, оснащений силовим агрегатом або елементом живлення, що здатен виконувати набір дій під прямим керуванням людини або комп'ютера, або ж них обох, та який складається принаймні з платформи, ПЗ та джерела живлення[128].

Термін **РАС,** що означає **«роботизовані та автономні системи»** (англ. – RAS, Robotic and Autonomous Systems) можна назвати узагальнюючим фреймворком для опису систем із наявними двома компонентами: фізичною (роботизована компонента) та когнітивною (автономія).[129] Важливо зазначити, що говорячи про «системи», розуміють широкий спектр фізичних систем із широким діапазоном варіантів застосування у військових цілях.[130] Наприклад, до таких систем відносять інженерні, логістичні, бойові, мультифункційні.

---

[124] Michel Rademaker and LtCol Sjoerd Mevissen, "Robotic and Autonomous Systems: From design to development and use in military operations" (ed. Alessandra Barrow), The Hague Centre for Strategic Studies: November 29, 2022, 5. <https://hcss.nl/wp-content/uploads/2022/11/Robotic-and-Autonomous-Systems-From-design-to-development-and-use-in-military-operations-Final.pdf> [Переглянуто 2025 21 04].
[125] Там само.
[126] Детальніше – рекомендовано: Michael Horowitz and Paul Scharre, "An Introduction to Autonomy in Weapon Systems", Center for a New American Security: February 13, 2015. <https://www.cnas.org/publications/reports/an-introduction-to-autonomy-in-weapon-systems > [Переглянуто 2025 21 04].
[127] Rademaker and Mevissen, 5.
[128] Там само.
[129] Там само.
[130] Там само.

Водночас, автоматизоване ПЗ, яке функціонує на комп'ютерах або у мережах, включно з т.зв. «ботами», частинами ПЗ (коду), та яке здатне виконувати команди без втручання людини, не вірно було б кваліфікувати як РАС – адже в такому випадку, бракує фізичної компоненти.[131] На відміну від частин ПЗ, «роботизована» компонента РАС характеризується фізичною формою та вказує на те, що система є **безпілотною** (англ. – Unmanned) або **безлюдною** (англ. – Uninhabited).[132]

Наприклад, ІКС «DELTA», про яку йтиметься у *частині другій*, є прикладом бойової системи, але її не можна віднести до РАС саме через відсутність фізичної (роботизованої) компоненти. Натомість, інший приклад – український автоматизований бойовий модуль «ШаБля» відповідає характеристикам РАС, адже включає і фізичну компоненту (турель як таку), і когнітивну (ПЗ, що дозволяє дистанційно керувати модулем, та ПЗ балістичного калькулятора, що дозволяє розрахувати політ кулі на дистанцію)[133]. (Хоча, слід розуміти, що ця система є дистанційно керованою, отже, за шкалою автономності (див. с. 44) вважається неавтономною.)

До РАС також відносять **(летальні) автономні системи озброєння**, скорочено – **(Л)АСО** (англ. – (Lethal) Autonomous Weapon System, (L)AWS). До категорії ЛАСО входять такі системи озброєння, які без втручання людини обирають та уражають цілі за певними, заздалегідь визначеними критеріями, слідуючи людському рішенню розгорнути озброєння, яке, в свою чергу, засновано на розумінні того, що атаку неможливо буде спинити втручанням людини після того, як її буде розпочато.[134] Наприклад, до категорії ЛАСО відносять систему класу «баражуючий боєприпас» (англ. – loitering munition) Switchblade 300 і 600 виробництва AeroVironment, а також російський Ланцет.

В цілому, що стосується автономії систем, необхідно розуміти, що РАС розрізняють за **рівнями автономії**: від **дистанційно керованих** (англ. – remotely controlled systems), тобто, неавтономних, – до **повністю автономних систем** (англ. – fully-autonomous systems).[135] Фігура 8 пояснює класифікацію систем за рівнем автономії (за шкалою від 0 до 5), запропоновану у публікації Гаазького Центру Стратегічних досліджень.[136]

---

[131] Там само.
[132] Там само.
[133] Юлія Сабадашина, ««Коса смерті» для окупантів і захист для українських кулеметників. Розповідаємо про турель «ШаБля» та її розробників», *DOU*: 20 червня 2024. <https://dou.ua/lenta/articles/about-shablya-and-roboneers/> [Переглянуто 2025 21 04].
[134] Rademaker and Mevissen, 5.
[135] Там само.
[136] Rademaker and Mevissen, 11-13.

клас	характеристики
0. Дистанційно керовані (Remotely controlled)	Оператор виконує всі аспекти динамічної основної задачі у повному обсязі та впродовж всього циклу (навіть якщо виконання задачі посилено системами попередження або втручання).
1. Підтримка оператора (Operator Assisstance)	Система, що надає підтримку оператору, виконує окремі функційні аспекти основної задачі, використовуючи для цього інформацію про середовище, а оператор виконує всі інші аспекти основної задачі. При цьому очікується, що оператор належним чином відреагує на запит про втручання.
2. Частково автономні (Partially-autonomous)	Система, що надає підтримку оператору, виконує всі функційні аспекти основної задачі, використовуючи для цього інформацію про середовище. Очікується, що оператор належним чином відреагує на запит про втручання.
3. Умовно автономні (Conditionally-autonomous)	Система або системи, що надають підтримку оператору, виконують всі функційні аспекти основної задачі, використовуючи для цього інформацію про середовище. Очікується, що оператор належним чином відреагує на запит про втручання та/або може перевизначити автономну поведінку систем(и).
4. Високо автономні (Highly-autonomous)	Система або системи, що надають підтримку оператору, виконують всі функційні аспекти основної задачі, використовуючи для цього інформацію про середовище, навіть якщо оператор не реагує належним чином на запит про втручання.
5. Повністю автономні (Fully-autonomous)	Автоматизована система виконує всі аспекти основної задачі у повному обсязі та впродовж всього циклу за будь-яких умов середовища принаймні на тому ж рівні, що може продемонструвати керування оператора.

Фігура 8. Рівні автономії систем. Джерело: складено автором на основі Rademaker and LtCol Mevissen, “Robotic and Autonomous Systems”.

Сама наявність діапазону рівнів автономії вказує на те, що слід розрізняти поняття безпілотних роботизованих систем та автономних систем, між якими існує тонка, не надто помітна на перший погляд межа. Відмінність полягає, зокрема, у ступені автономії та діапазоні задач, які система здатна виконувати автономно без втручання людини.

Наприклад, безпілотна роботизована система може виконувати певний набір автономних функцій. У випадку БАС, дрон (БпЛА) є лише однією складовою системи, а іншими рівнозначно важливими складовими є ПЗ (включно з mission planner) та апаратне забезпечення (наземна станція керування тощо). Виконуючи політ за заданими оператором параметрами, БпЛА має можливість автономно «спілкуватися» (підтримувати зв'язок), за потреби – перебудовувати маршрут у польоті, а також, приймати рішення, спираючись на дані, зібрані ним із середовища – при цьому, постійне залучення оператора непотрібне.[137] Втім, це не робить дану систему повністю автономною.

Також, слід зазначити, що в контексті автономних систем, ключовим концептом є **MHC** (англ. – Meaningful Human Control), або т. зв. **«належний людський контроль»**[138]. Хоча, станом на сьогодні, не існує якого-небудь офіційно визначеного міжнародного трактування поняття MHC, [в контексті ЗС Нідерландів] застосовують наступне формулювання: «усе озброєння, включно з автономним озброєнням, має залишатися під належним людським контролем».[139]

В контексті застосування РАС на полі бою, слід також розглянути питання **кілчейну** (англ. – Kill chain) або ж **ланцюга ураження цілі**, який також називають **циклом вогневого ураження**. Це модель ураження цілі, яка представляє собою ланцюг з декількох послідовних фаз, які необхідно виконати для того, аби a) завдати точного удару, та b) проаналізувати атаку та запобігти ураженню. Тобто, модель може бути використано як з метою планування і здійснення атаки, так і запобігання їй. Також, кілчейн називають терміном **F2T2EA** (від англ.: **Find, Fix, Track, Target, Engage, and Assess**) за назвами фаз: знайти, зафіксувати, відстежити, націлитись, уразити, оцінити.

---

[137] Gordon B. "Skip" Davis, Jr. and Lorenz Meier, "The Challenges Posed by 21st-Century Warfare and Autonomous Systems", CEPA: October 25, 2023. <https://cepa.org/article/the-challenges-posed-by-21st-century-warfare-and-autonomous-systems/> [Переглянуто 2025 21 04].

[138] Детальніше – рекомендовано: Michael Horowitz and Paul Scharre, "Meaningful Human Control in Weapon Systems: A Primer", Center for a New American Security: 16 March, 2015. <https://www.cnas.org/publications/reports/meaningful-human-control-in-weapon-systems-a-primer>. [Переглянуто 2025 21 04].

[139] Rademaker and Mevissen, 11-12.

Зокрема, говорячи про «довгий кілчейн», йдеться про тривалий за часом цикл вогневого ураження цілей. У веденні війни, що базується на мережецентричних підходах (див. с. 30-34), прагненням сторін збройного конфлікту є скорочення кілчейну, адже «короткий кілчейн» надає вогневу перевагу. Саме для цього залучають РАС, в тому числі, ЛАСО та бойові системи, зокрема на основі **ШІ**, **МН**, технології **комп'ютерного зору** (англ. – Computer Vision) тощо, які покликані скоротити кілчейн до мінімума, а в ідеалі – звести його до нуля. «Короткий кілчейн» досягається за рахунок виконання автономними системами ряду необхідних фаз без втручання людини або за умов зменшення втручання, що полегшує роботу оператора або дешифрувальника, а в цілому, суттєво скорочує час реакції, і як результат – сам ланцюг ураження.

Наприклад, моделі ШІ/МН сьогодні застосовують з метою автоматизації розпізнавання об'єктів на відео, онлайн-стрімах (покриття фаз Find, Fix, Track, Target, Assess). Зокрема, в українському контексті, такою є система «Avengers» (див. с. 56-57), що входить до складу екосистеми «DELTA». Іншим напрямком роботи є навчання нейронних мереж – для цього здійснюють анотацію та каталогізацію різних типів даних, які формують військовий датасет, або **UMD**, **Universal military dataset** (детальніше – див. Глосарій).

Втім, важливо розуміти, що хоча скорочення кілчейну і є пріоритетом, воно відбувається виключно з урахуванням принципу належного людського контролю. Тобто, навіть у випадку повністю автономної системи, яка виконує весь спектр функційних аспектів поставленої задачі, включно із ідентифікацією цілі, її фіксацією, відстежуванням та націлюванням (Find, Fix, Track, Target), фінальне рішення про ураження (Engage) має бути здійснено під контролем людини. Іншими словами, це означає, що метафорично, на одній чаші терезів знаходиться швидкість ураження, а на іншій – відповідальність. За умов балансу між ними відбувається розвиток РАС та їхня експлуатація на полі бою.

Зрештою, слід було б згадати про певні групи викликів/дилем, які постають на тлі динамічного розвитку та набуття системами все більшої автономії – зокрема, такі, що лежать в площині етики, формування політик (policies) та правового врегулювання РАС. Втім, ця тема потребує детального розкриття, виходячи за рамки даної роботи.

- ***Що таке «інформація з обмеженим доступом», та які ступені секретності існують?***

Оскільки використання СПЗ передбачає роботу з різного роду інформацією (наприклад, на етапах обробки та розповсюдження (див. с. 35-36), в рамках цього

дослідження також слід розкрити питання інформації з обмеженим доступом. В Україні та країнах-членах НАТО сприйняття і класифікація інформації є різними, що відображено у неспівпадінні термінів: «інформація з обмеженим доступом», «класифікована», «сенсетивна» тощо.

В контексті України, загалом вся інформація поділяється на відкриту (загальнодоступну) та **інформацію з обмеженим доступом**. Інформація з обмеженим доступом включає чотири категорії: **i) для службового користування (ДСК),** а також, за зростанням ступенів секретності, **ii) таємно (Т), iii) цілком таємно (ЦТ) та iv) особливої важливості (ОВ).** Останні три відповідають трьом **ступеням секретності**, що їх визначає ст. 1 Закону України «Про Державну таємницю».[140] Ступені призначаються носіям інформації, яка містить державну таємницю, а **грифом секретності** (обмеження доступу) називають реквізит матеріального носія секретної інформації, що засвідчує ступінь її секретності[141].

Як пояснює фахівець МОУ, інформація, з якою працюють (люди і системи) на оперативному рівні, вже має гриф «таємно», на стратегічному – «цілком таємно», і тому, наприклад, щоб впровадити АСУВ на оперативному рівні, необхідно мати доступ відповідного рівня[142].

В контексті Північноатлантичного альянсу, **класифікована інформація** (англ. – Classified information) має чотири ступені (за зростанням): **NATO RESTRICTED (NR), NATO CONFIDENTIAL (NC)**, **NATO SECRET (NS),** та **COSMIC TOP SECRET (CTS)**[143]. При цьому, гриф **NATO UNCLASSIFIED (NU)**, який часто можна побачити в колонтитулі сторінок загальнодоступного документу, використовується для офіційної, «некласифікованої» інформації, що виконує функцію «захисту авторських прав»[144]. Окрім цього, деяка інформація може носити гриф **SENSITIVE BUT UNCLASSIFIED (SBU)**, тобто бути «сенсетивною» (вразливою), але при цьому, некласифікованою.

---

[140] Стаття 1 Закону України «Про Державну таємницю». <https://zakon.rada.gov.ua/laws/show/3855-12#Text> [Переглянуто 2025 21 04].
[141] Там само.
[142] З особистої розмови з з фахівцем МОУ.
[143] "Security within the North Atlantic Treaty Organization (NATO)", NATO, Note by the Secretary General: 20 November 2020, E-1. <https://www.nbf.hu/docs/C-M%282002%2949-REV1.pdf> [Переглянуто 2025 21 04].
[144] NATO, Declassified. <https://www.nato.int/cps/en/natohq/declassified_138449.htm> [Переглянуто 2025 21 04].

Незважаючи на різні підходи до класифікації інформації, Україна та НАТО узгодились про деякі (але не всі) відповідники. Так, домовленості визначають, що грифи обмеження доступу України та НАТО співвідносяться наступним чином (станом на 2017 р.)[145]:

Україна	НАТО
Цілком таємно (ЦТ)	NATO SECRET (NS)
Таємно (Т)	NATO CONFIDENTIAL (NC)
Для службового користування (ДСК)	NATO RESTRICTED (NR)

Фігура 9. Співвідношення деяких грифів обмеження доступу між Україною і НАТО. Джерело: «Адміністративні домовленості щодо охорони інформації з обмеженим доступом між урядом України та організацією Північноатлантичного договору».

[145] «Адміністративні домовленості щодо охорони інформації з обмеженим доступом між урядом України та організацією Північноатлантичного договору», 24.05.2017. <https://zakon.rada.gov.ua/laws/show/950_035-16#Text> [Переглянуто 2025 21 04].

II. Частина друга. Огляд галузі СПЗ.

В попередній частині роботи увагу було приділено тлумаченню теоретичних концептів, структурованих у моделі, що сукупно покликані пояснити основні засади ведення сучасної війни. Здебільшого, для цього було застосовано **нормативний підхід** (*відповідає на питання «як має бути»*). Однак, слід підкреслити, що далеко не всі з наведених концептів і моделей можна вважати такими, що є «combat proven». Тож не виключено, що деякі з них і не витримали би «перевірки боєм», зокрема, в умовах поточної російсько-української війни. Втім, в цілях дослідження, цей масив теоретичних знань надано для орієнтації читача в загальних процесах ведення війни.

Частина друга (II) зосереджує увагу читача в практичній площині, розкриваючи тему функціонування СПЗ в контексті України. Тому, для опису систем застосовано **позитивістський підхід** (*відповідає на питання «як є»*), що базується на емпіричних даних. Читачеві пропонується як загальний огляд української галузі СПЗ (та оборонних ІТ-рішень в цілому) для отримання широкого уявлення про її розвиток, так і детальніший опис окремих систем. Вибір **шести систем**, представлених детально, зумовлений прагненням розкрити діапазон діючих СПЗ, якими користуються у війську сьогодні, водночас, уникнувши опису тих систем, що (частково) дублюють функції одна одної, та які можна було би віднести до однієї категорії.

***

Насамперед, слід зазначити, що віднедавна СПЗ класифікують як категорію ОВТ згідно змін до Постанови КМУ № 234 (від 31 січня цього року).[146] Припускається, що це дозволить розширити можливості розробників СПЗ та інших оборонних ІТ-рішень.

Станом на сьогодні, діапазон софтверних рішень, що використовуються в інтересах СОУ, є доволі широким. Згідно результатам опитування, проведеного МОУ в додатку «Армія+», участь в якому взяло близько 10 000 військових, ІКС «DELTA», «Віраж-планшет» та «Кропива» були зазначені як системи, якими військові користуються найчастіше (станом на жовтень 2024 р.)[147]. Серед інших поширених продуктів, які знаходяться у практичному

[146] Постанова КМУ № 234 від 3 березня 2021 р. «Про затвердження Порядку розроблення, освоєння та випуску нових видів товарів оборонного призначення, а також припинення випуску існуючих видів таких товарів». <https://zakon.rada.gov.ua/laws/show/234-2021-%D0%BF#Text> [Переглянуто 2025 21 04].

[147] «DELTA у трійці найпопулярніших бойових систем – Катерина Черногоренко про опитування в Армія+», Міністерство оборони України: 9 жовтня 2024. <https://www.mil.gov.ua/news/2024/10/09/delta-u-trijczi-najpopulyarnishih-bojovih-sistem/> [Переглянуто 2025 21 04].

використанні СОУ, можна назвати наступні: «Вежа» (як модуль ІКС «DELTA»), «ARMOR» (ГРК «Броня»), «Очі», «Стрибо», «ComBat Vision», «Griselda», «GisArta», «Неон», «Графіт», «Айсберг», «SkyMap», «Промінь», «KOLOSSAL», «Avengers» (складова екосистеми «DELTA») та інші.

Подальший огляд галузі побудований на припущенні, що ці та інші рішення можна категоризувати принаймні **за трьома принципами**, а саме, за:

a) основним функціоналом (**функціонал**);
b) спеціалізацією та інструментарієм – визначається користувацькою аудиторією (роди та види військ, типи підрозділів) та закладеними в систему задачами, які вона покликана виконувати (**спеціалізація/інструментарій**);
c) рівнями, на яких ПЗ використовується (**рівні**).

При цьому, слід розуміти, що описуючи ту чи іншу систему, можна сказати, прикладом, що за функціоналом вона є системою управління військами, за спеціалізацією її відносять до спеціалізованих систем, а використовують на оперативно-тактичному рівні (наприклад, це стосується деяких СПЗ, що функціонують в інтересах ППО). Тобто, запропоновані три принципи (a), (b) і (c) в даному випадку слугують інструментом категоризації систем за їхніми властивостями, не виключаючи при цьому приналежність однієї системи до кількох категорій одночасно.

Отже, говорячи про **функціонал (a)**, йдеться про те, що це широке поняття і доволі широкі категорії. Умовно, за функціоналом системи можна розподілити на ті, що:

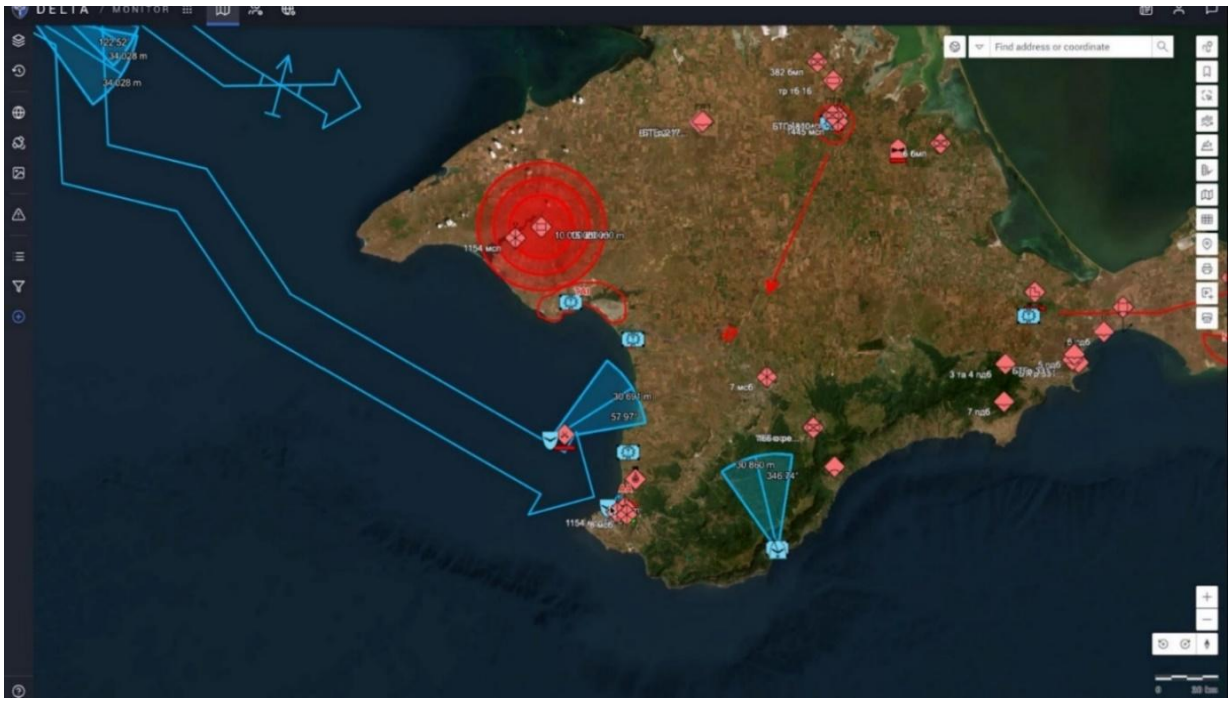
- (i) надають ситуаційну обізнаність;
- (ii) уможливлюють процеси управління;
- (iii) поєднують в собі (i) та (ii);
- (iv) створені в навчальних цілях/для симуляцій;
- (v) є аналітичними інструментами.

Все частіше на практиці можна зустріти приклади злиття функціоналів – варіант (iii). Наприклад, саме такою сьогодні є ІКС «DELTA» [також, Інтеграційна платформа «Дельта» Збройних Сил України – ред.] (введена в експлуатацію в серпні 2024 р.[148]). Протягом кількох

[148] «Завдяки системі DELTA знищено ворожої техніки на більше ніж 15 мільярдів доларів – Рустем Умєров», Міністерство оборони України: 26 серпня 2024. <https://mod.gov.ua/news/zavdyaki-sistemi-delta-znishheno-vorozhoi-tehniki-na-bilshe-nizh-15-milyardiv-dolariv> [Переглянуто 2025 21 04].

останніх років «DELTA» пройшла шлях від системи ситуаційної обізнаності (первинно закладений в неї функціонал) у вигляді цифрової мапи – до екосистеми інтегрованих між собою продуктів, що серед іншого, включає і елементи управління військами. (Детальніший огляд ІКС «DELTA» див. на с. 85-92.)

За словами користувачів, «[...] в якийсь момент, «DELTA» стала певним мірилом, стандартом серед систем»[149], особливо, в розрізі питань безпекового контуру, «легалізації» у правовому полі, розростанні інструментарію та розширенні мережі партнерів (інтеграції) – як локальних, так і іноземних. «Чи гарна це тенденція? Питання відкрите, – адже «DELTA» – це ніби двадцятиповерховий будинок, а інші системи в порівнянні з нею – одноповерхові котеджі, тож порівнювати і складно, і не зовсім коректно»,[150] – аргументує військовий СОУ, користувач ІКС «DELTA» та інших систем.



Цифрова мапа DELTA Monitor. Джерело: DOU.

Говорячи про системи, що наділені функцією управління (ii), зазвичай йдеться про АСУ (див с. 40-41). Наприклад, АСУ «Ореанда» (на озброєнні ЗСУ з 2016 р.) служить в цілях управління авіацією та ППО.[151] (Детальніше про цю та інші АСУ ППО – див. с. 57-60.)

[149] З особисто отриманої консультації з військовим СОУ, користувачем кількох систем.
[150] Там само.
[151] «ЗСУ отримали сучасні мобільні АСУ «Ореанда»», *Defense Express*: 23 грудня 2018. <https://old.defence-ua.com/index.php/home-page/6107-zsu-otrymaly-suchasni-mobilni-asu-oreanda> [Переглянуто 2025 21 04].

«Дзвін-АС» відома як АСУ стратегічного керівництва та оперативного управління (на озброєнні ЗСУ з 2022 р.).[152] Хоча сьогодні «Дзвін» і є єдиною системою, якій дозволено опрацьовувати, зберігати та обмінюватися даними на рівнях «Таємно» і «Цілком таємно», вона має вкрай низьку практичну застосовність (кількість користувачів є дуже обмеженою), а доцільність її використання викликає великі сумніви у фахівців та безпосередніх користувачів.

Слід зазначити, що прийняття на озброєння супроводжувало розслідування з боку НАБУ кримінального провадження щодо виконання ДКР «Дзвін-АС», зокрема розтрату в особливо великих розмірах, недбале ставлення до військової служби, перевищення владних повноважень.[153] В лютому 2025 р. НАБУ і САП повідомили про викриття схеми розкрадання коштів на системі «Дзвін-АС», кваліфікувавши дії підозрюваних за ч. 5 ст. 191 КК України та оцінивши втрати для держави у розмірі 246 млн грн. (зокрема, протягом чотирьох років ТЗ змінювали 13 разів, що дозволило збільшити вартість робіт на 300 млн грн.).[154] Доведено, що система є несумісною з протоколами НАТО та іншими українськими бойовими системами, і, як з'ясувалося в ході розслідування, переважна частина ПЗ взагалі не використовується (реалізовано всього лише 10 інформаційно-розрахункових задач з «оригінально» закладених 200).[155]

Говорячи про навчальні системи та симулятори (iv), зокрема, на основі технологій AR/VR (див. Глосарій), розрізняють рішення таких підкатегорій: для симуляції бою за принципом воргеймінгу – рішення тактичного та оперативного рівнів для моделювання дій підрозділу в обороні та наступі; для тренування навичок пілотів БпЛА/НРК/БЕК; для піхотного озброєння; для бронетехніки; симулятори літаків та гелікоптерів; симулятори ППО (наприклад, ТІК «Віраж-РД» – див. с. 58-59); симулятори РЕР; для озброєння та обладнання ВМС; для тренування навичок тактичної медицини; для використання у мінно-вибуховій справі тощо.[156]

---

[152] Тарас Сафронов, «Система управління "Дзвін-АС" стала на озброєння України», *Militarnyi*: 8 грудня 2022. <https://mil.in.ua/uk/news/systema-upravlinnya-dzvin-as-stala-na-ozbroyennya-ukrayiny/> [Переглянуто 2025 21 04].

[153] Там само.

[154] «Корупція в оборонці: викрито схему розкрадання коштів на систему «ДЗВІН» (ВІДЕО)», Національне Антикорупційне Бюро України: 19-02-2025. <https://nabu.gov.ua/news/koruptciia-v-oborontci-vykryto-skhemu-rozkradannia-koshtiv-na-systemu-dzvin/> [Переглянуто 2025 21 04].

[155] Там само.

[156] Найбільш затребувані категорії вказані згідно запиту, сформованому МОУ в рамках конкурсу AR/VR рішень на Defence Demo Day: Юлія Сабадашина, «Міноборони шукає фахівців з VR та AR, щоб створювати симулятори для навчання військових», *DOU*: 30 травня 2024. <https://dou.ua/lenta/news/vr-and-ar-in-the-army/> [Переглянуто 2025 21 04].

Серед навчальних систем/симуляторів вартує згадати продукцію компанії «Skiftech», яка сукупно представляє собою екосистему з хард- та софтверною складовими.[157] До першої відносять пристрої, що встановлюються на зброю, техніку та амуніцію, збираючи дані про бійця, а другою складовою є власне дані, зібрані під час тренувань (відеовідтворення тренування, доступні для аналізу дій окремо взятого бійця).[158]

Бійці Сил Спеціальних Операцій на тактичному навчанні з обладнанням SKIFTECH. Джерело: AIN.

Тренувальні системи «Skiftech» мають широкий діапазон використання, включаючи симулятори для навчання і тренування гранатометників (РПГ-7, АГС-17), тактичної підготовки екіпажів бронетехніки (комплект ОВТ: танк, БТР, БМП, БДМ тощо), персональні комплекти та симулятори для тренування бійців (система «СКІФ»), для тренування снайперів (система «Антиснайпер»), для відпрацювання вправ з ураження техніки на базі навчальних і навчально-бойових ПТРК (комплекс ПТРК «Синиця»), імітатори стрільби та мішені для відпрацювання ураження цілей з танку (система «Танковий тир»), комплексний тренажер з використанням технології VR для тактичної підготовки бійців («SKIF-VR»), рішення для навчання і тренування спеціальних підрозділів (навчально-тренувальний

[157] Майя Ярова, ««Це – війна технологій». Як харків'яни створили тактичні симулятори SkifTech, які рятують життя військових», *AIN*: 17 лютого, 2023. <https://ain.ua/2023/02/17/yak-harkivski-trenuvalni-systemy-skiftech-ryatuyut-zhyttya-vijskovyh/> [Переглянуто 2025 21 04].
[158] Там само.

комплекс «САРМАТ»), симулятори мін та тренажери вибухових пристроїв (ПМН-2, ТМ-62, МОН-52).[159]

Прикладом симулятора, призначеного для тренування навичок пілотів БпЛА, можна назвати «Обрій» – рішення, яке було створено для відпрацювання техніки ударних місій, насамперед, пілотів FPV. Використовується за такими сценаріями як вивчення місцевості, проведення нічних місій, корегування артилерії, реагування на позаштатні ситуації, злагодження екіпажів[160].

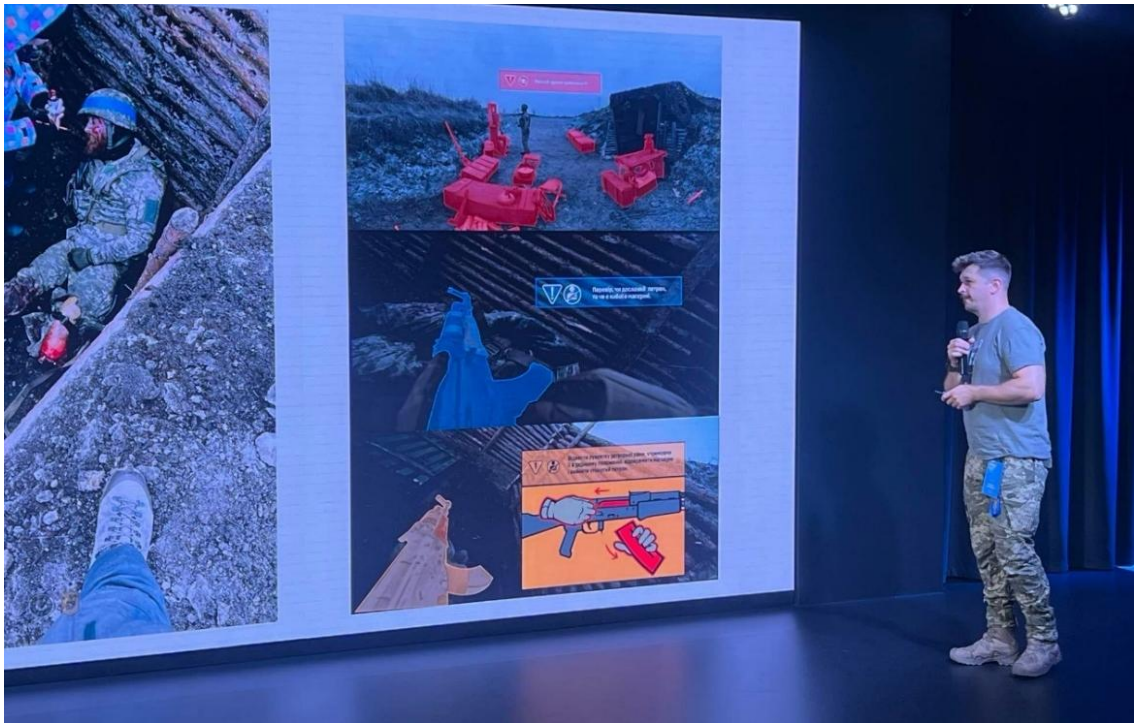
Інший приклад системи цього ж напрямку – «Call of the Sky», навчальний симулятор розвідки і корегування з функціями, наближеними до реальних військових умов. Він допомагає розвивати навички «[...] саме розвідування й корегування, а не просто відпрацювання польоту та посадки», навчає безпечним алгоритмам польоту без систем GPS, використовуючи лише візуальні орієнтири, а також готує до польотів в ускладнених погодних умовах (зокрема, при сильному вітрі).[161]

Імерсивний VR фільм «Перший бій» (фільм з ефектом занурення), розроблений Підрозділом розвитку та інновацій озброєння спільно з командою Aspichi, можна навести як дещо нетиповий приклад навчального софтверного рішення. Він покликаний вирішувати проблему відсутності (тривалої) психологічної підготовки у мобілізованих та курсантів, що мала би сприяти ефективному виконанню завдань в умовах бойових дій, демонструючи один з типових сценаріїв першого бою при обороні.[162]

«Ми відтворюємо дії, явища поля бою. Це про моделювання ситуацій та про алгоритм фізичних або психологічних дій і рішень в них», – говорить один із розробників фільму Віталій Кирилів[163]. Наразі фільм вже включено на постійній основі в програму БЗВП (5 редакції) як заняття з психологічної підготовки/стресостійкості: його поширюють між навчальними центрами України та бойовими бригадами.[164]

---

[159] «Тренувальні системи», SKIFTECH. <https://ua.skif.cc/trenuvalni-sistemi/> [Переглянуто 2025 21 04].
[160] «Обрій, Симулятор місій БПЛА». <https://www.obriy.airforce/> [Переглянуто 2025 21 04].
[161] Вікторія Пушкіна, «Поклик неба: Історія військового ЗСУ, який створив перший в Україні симулятор розвідки та коригування», *r_d media*. <https://robotdreams.cc/uk/blog/506-pershyy-v-ukrayini-symulyator-rozvidky-ta-koryhuvannya> [Переглянуто 2025 21 04].
[162] З матеріалів, наданих розробниками фільму «Перший бій»: <https://the-first-battle.minisite.ai/ua> [Переглянуто 2025 21 04].
[163] З особистої розмови зі співрозробником VR-фільму «Перший бій» Віталієм Кирилівим.
[164] Там само.



Демонстрація VR-фільму «Перший бій». Джерело: надано Віталієм Кирилівим.

Перегляд VR-фільму «Перший бій». Джерело: надано Віталієм Кирилівим.

Зрештою, до п'ятої категорії софтверних рішень у розподілі за функціоналом – інструментів аналітики (v), – можна віднести такі системи як «Griselda» (детальніший огляд див. на с. 81-84), «Стрибо», а також «Avengers».

Наприклад, «Стрибо» є аналітичною платформою рівня ОТУ/ОСУВ та вище, а система «Comintify», що з часом стала складовою системи «Стрибо», оригінально була призначена для роботи ТЛ та автоматизації збору даних, їхньої «очистки», систематизації та ведення первинної аналітики.[165]

За словами засновника «Comintify», сьогодні «Стрибо» є продуктом, який уможливлює автоматизацію декількох різних процесів, мінімізуючи при цьому людський фактор «[...] там, де люди непотрібні»[166]. Зокрема, йдеться про збір перехоплень, зручність обробки будь-яких даних («[...] модельки ШІ, які дозволяють почистити аудіозаписи, прибрати шуми тощо»), автоматизацію первинної аналітики, ведення системної бази даних.[167]

Система «Avengers», знана як ШІ-платформа, наразі є складовою екосистеми «DELTA». Сьогодні, вона здатна автоматично розпізнавати понад 70% ворожої техніки, аналізуючи стріми з дронів та відео зі стаціонарних камер лише за 2,2 секунди, що дозволяє досягти вищої автоматизації в повторюваних операціях і тим самим, скоротити час на ухвалення рішень[168]. Таким чином, завдяки застосуванню технологій ШІ та МН, досягається коротший кілчейн (див. с. 45-46).

В рамках роботи ЦІРОТ МОУ, який наразі займається розвитком системи «Avengers», здійснюється постійне навчання ШІ-моделей на нових даних[169]. Слід також розуміти, що самою основою для розвитку «Avengers» як такої стала наявність накопиченого з початку повномасштабного вторгнення величезного масиву фото- та відеоданих російської техніки, які було анотовано, згруповано та каталогізовано у військовий датасет UMD[170] (див. с. 46 та

---

[165] З особистої розмови із засновником системи «Comintify».
[166] Там само.
[167] Там само.
[168] Kateryna Chernohorenko, 8 May 2025. <https://www.facebook.com/katheryn.chernohorenko/posts/pfbid0ck9fHauX8HbgQBZesMMnBhccMpv5AG7JJUxxkjiDNNLVPhuKe93Erk5PtbVWn8Skl > [Переглянуто 2025 08 05].
[169] «Українські військові виявляють 12 тисяч цілей щотижня завдяки штучному інтелекту — Катерина Черногоренко», Міністерство оборони України, 23 вересня 2024. <https://mod.gov.ua/news/ukrayinski-vijskovi-viyavlyayut-12-tisyach-czilej-shhotizhnya-zavdyaki-shtuchnomu-intelektu-katerina-chernogorenko> [Переглянуто 2025 08 05].
[170] «Міноборони представило інноваційні військові розробки на виставці NATO Edge 24», Міністерство оборони України, 12 грудня 2024. < https://mod.gov.ua/news/minoboroni-predstavilo-innovaczijni-vijskovi-rozrobki-na-vistavczi-nato-edge-24 > [Переглянуто 2025 08 05].

Глосарій). Іншими словами, UMD використовують в певному сенсі як «фабрику» для моделей ШІ та МН, і саме це дає основу роботі «Avengers»[171].

Окремо слід зазначити систему «Промінь», що є інструментом обробки великих обсягів розвідданих. Як зазначає розробник системи, вона дозволяє «[...] обробляти петабайти даних і знаходити взаємозв'язки про ворога, а також з'ясовувати, які саме наявні патерни – геопросторові або ж зв'язкові, тобто, хто до кого відноситься і хто куди переміщується»[172]. Саме це і є основною цінністю системи.

Слід підкреслити, що «Промінь» є саме аналітичним інструментом розвідки. (На противагу, ІКС «DELTA» надає ситуаційну обізнаність, але ці дані ще потребують обробки та аналізу[173].) «Промінь» – це також інструмент, за рахунок якого можна швидко вибудовувати різні аналітичні застосунки, щоб вчасно адаптуватись під роботу з новими джерелами.[174] За словами розробника, велика кількість даних, що опрацьовується системою, надходить з CYBERINT джерел (кіберрозвідки), хоча система обробляє дані різних типів, в тому числі, і супутникові знімки – для цього є «пайплайни» обробки великих обсягів даних.[175] З інформації, яка обробляється у «Промені», можна генерувати так звані «таргет паки» – пакети для системної розробки цілей.[176]

Говорячи про **спеціалізацію/інструментарій (b),** можна відзначити, що сьогодні переважна більшість українських софтверних рішень є **спеціалізованими**. Це означає, що вони мають **спеціальне** (іноді доволі вузьке) **призначення**, яке є актуальним для певних родів та видів військ і типів підрозділів та/або покликане виконувати вузькоспеціалізовані задачі. Загалом, «[...] в ідею функціонування СПЗ має бути, і первинно й була закладена певна спеціалізація», – говорить військовий СОУ[177]. Наприклад, одні системи слугують роботі ППО (див. далі), інші призначені переважно для роботи аеророзвідників, треті – для роботи з РЕБ (наприклад, такі системи як «Графіт» та «Айсберг»), четверті застосовуються виключно в площині OSINT (наприклад, «KOLOSSAL») тощо.[178]

Детальніше розглянемо системи, що функціонують в інтересах роботи ППО. Серед таких слід виокремити комплекс СПЗ «Віраж-планшет» (далі – «Віраж»), «SkyMap», а також

[171] Там само.
[172] З особистої розмови з розробником системи «Промінь».
[173] Там само.
[174] Там само.
[175] Там само.
[176] Там само.
[177] З особисто отриманої консультації з військовим СОУ, користувачем кількох систем.
[178] Там само.

АСУ «Кречет», – як основні три інструменти, призначені для роботи ППО. В цілому, задача СПЗ в «кластері» ППО полягає в тому, щоби бачити радіолокаційну обстановку, використовуючи радіолокаційні треки як основний тип даних.[179]

В цьому контексті, важливо розуміти, що сьогодні існують умовно дві «гілки» ППО: це ППО Повітряних сил (ППО ПС) та ППО Сухопутних військ (ППО СВ)[180]. Наприклад, СПЗ «Віраж» функціонує в інтересах ПС ЗСУ, а «SkyMap» застосовується в інтересах СВ ЗСУ.[181]

Зокрема, «SkyMap» (також «СкайМапа») – це ріалтайм система автоматичного потоку координат, яка «[...] розгорнута по всій лінії фронту, на кожному ОТУ» і яка також налічує декілька активних «інстансів» всередині країни[182]. Вона є децентралізованим рішенням (до слова, як і СПЗ «Віраж», і АСУ «Кречет»), а це означає, що «[...] в кожному штабі оперативно-тактичного рівня є своя «Скаймапа» – це ніби свій «інстанс», свій маленький світ», – пояснює фахівець галузі.[183]

СПЗ «Віраж», який коректніше було би називати «комплексом СПЗ», складається з «[...] функціонально об'єднаних апаратно-програмних засобів»[184], по суті, представляючи собою «конгломерат» з близько 50 різних програм (додатків), які можуть «спілкуватися» одна з одною.[185] (Наразі розробники працюють над тим, щоби доповнити основні додатки функціоналом та поєднати їх в один додаток.[186]) Наприклад, «Віраж-ЗРВ» вважається одним з базових елементів комплексу СПЗ «Віраж» – ця система реалізує автоматизацію збору, аналізу, відображення та обміну інформацією про повітряну обстановку.[187]«Віраж-РД» є системою оперативно-тактичних розрахунків та імітаційного моделювання бойових дій – її

[179] З особистої розмови зі співрозмовником N.
[180] Там само.
[181] Там само.
[182] Там само.
[183] Там само.
[184] «Методичні рекомендації використання спеціалізованого програмного забезпечення «Віраж-планшет» під час підготовки бойових обслуг підрозділів Зенітних ракетних військ Повітряних сил Збройних сил України», ВП 7-09(12).02, Центр оперативних стандартів і методики підготовки Збройнх сил України спільно з Командуванням Повітряних сил Збройних сил України, серпень 2019, 6. <https://www.hups.mil.gov.ua/assets/uploads/library/nadhodzhennya/lypen-veresen-2020/pdf/30.pdf> [Переглянуто 2025 29 04].
[185] З особистої розмови зі співрозмовником N.
[186] Там само.
[187] «Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів», Збірник тез доповідей VIII Всеукраїнської науково-практичної конференції, Науково-дослідний центр службово-бойової діяльності Національної гвардії України, 31 жовтня 2019 року, 179. <https://nangu.edu.ua/uploads/files/documenty/Naukova%20diyalnist/naukovu%20forumy/2019/9%20%20%20%20%20%2031.10.2019%20Zbirnyk%20tez%20NPK.pdf> [Переглянуто 2025 18 04].

відносять до категорії ТІК, тренажно-імітаційних комплексів[188]. Вона дозволяє «[...] проводити тренування в умовах динамічних змін повітряної обстановки; відпрацьовувати питання взаємодії та забезпечення бойових дій усіх родів військ Повітряних сил».[189]

За оцінкою одного з фахівців галузі, сьогодні більшість військових ППО (ПС ЗСУ) використовує саме «Віраж» в цілях своєї роботи (кількість користувачів налічує десятки тисяч).[190] При цьому, станом на зараз, ця система не кодифікована, а сама команда «Віража» є дуже нечисленною (особливо, відносно кількості користувачів та рівня затребуваності системи) та відчуває брак ресурсів.[191] Однією з переваг цього СПЗ співрозмовник називає те, що «Віраж» є «[...] дуже відкритою системою», оскільки вона дозволяє відправляти інформацію «назовні».[192]

І «Віраж», і «SkyMap» є тими рішеннями, які створюють цінність на полі бою, і якими активно користуються у війську (до того ж будучи повністю безкоштовними). (Наряду із зазначеними системами активно використовується система «Неон», яка транслює повітряну обстановку в ріалтаймі в певному функціоналі[193] – див. с. 60-61.)

При цьому, фактично будучи системами управління військами (АСУ), «на папері» вони не наділені функцією управління: офіційно «[...] підрозділи отримують цілевказання від них, тобто, ці дві системи надають рекомендації з цілевказання, що можна розцінювати як локальне використання софтів», – пояснює співрозмовник.[194] Водночас, обидві працюють і за VPN (що є одним рівнем шифрування), і за ще одним, додатковим рівнем, – тож такі системи дуже складно «зламати»[195]. Іншими словами, зазначені системи фактично забезпечують належний рівень безпеки, при цьому не будучи кодифікованими. (Тобто, можна вважати, що наразі технології випереджають законодавство.)

Водночас, в «кластері» ППО існують і такі рішення як АСУ «Ореанда», АСУ «Кречет» та «ЦОРІ» («Центр обробки радіолокаційної інформації»). Зокрема, АСУ «Ореанда» – це кодифікована система, чия користувацька аудиторія є нечисленною (декілька сотень

[188] Детальніше про «Віраж-РД»: Дмитро Чалий, «Уперше американську систему імітаційного моделювання JCATS випробували курсанти-зенітники», *АрміяInform*: 10 Квітня 2021. <https://armyinform.com.ua/2021/04/10/upershe-amerykansku-systemu-imitaczijnogo-modelyuvannya-jcats-vyprobuvaly-kursanty-zenitnyky/> [Переглянуто 2025 18 04].
[189] Збірник тез доповідей VIII Всеукраїнської науково-практичної конференції.
[190] З особистої розмови зі співрозмовником N.
[191] Там само.
[192] Там само.
[193] З особисто отриманої консультації з військовим СОУ, користувачем кількох систем.
[194] З особистої розмови зі співрозмовником N.
[195] Там само.

терміналів за неофіційною оцінкою), адже йдеться про рівень командування.[196] Це зумовлено функціоналом і задачами, які вона виконує, – та водночас, ця система довела свою ефективність на полі бою в сегменті ЗРВ[197]. АСУ «Кречет», що є інструментом ТЛ, можна назвати достатньо «ізольованим» рішенням через його сегментацію за природою застосування.[198] (Також, необхідно розуміти, що «Кречет» можливо використовувати лише на певних девайсах компанії SEE, чия вартість є безпідставно високою, – а це спричинено тим, що від початку, це рішення створювалось під поточну законодавчу базу, включно із чинною процедурою проходження КСЗІ та з розумінням того, що держава буде вимушена закуповувати саме цю продукцію.[199])

Продовжуючи тему спеціалізованих СПЗ, слід зазначити систему «Неон», що є свого роду унікальним рішенням не лише в українському, але й в глобальному контексті – про неї західні партнери говорять, що це «[...] майбутнє, до якого мають йти інші системи».[200] Також, за оцінкою користувачів, «Неон» може вважатися «базовою» ІКС, що дозволяє обмінюватися даними у безпековому контурі з іншими сторонніми системами «пленінгу» та управління БпЛА, а це відкриває можливості для швидкої інтеграції та поєднання на полі бою БпАК різних типів в єдиний інформаційний простір.[201]

Будучи інструментом аналітики, симуляції і планування місій, «Неон» вирішує проблему розрізнених сенсорних мереж, які знаходяться в підпорядкуванні різних сил, фокусуючись на «fusion» (злитті) різних типів даних з різних сенсорних мереж[202]. Інтеграція всіх сенсорних мереж в одне місце і подальша можливість історичного аналізу є одною з основних переваг і цінністю системи «Неон», за словами розробника.[203] (До слова, в цьому контексті, СПЗ «Віраж» та «Графіт» можна навести як приклади успішних інтеграцій: обидві системи надають ситуаційну обізнаність повітряної обстановки, втім, працюють з різними системами сенсорів.)

«Неон» уможливлює планування місій з урахуванням операційної обстановки, прогнозуванням ризиків та проведенням певного типу моделювання.[204] Зокрема, одним з напрямків роботи є історичний аналіз подій, що відбулися: наприклад, команда досліджує,

[196] Там само.
[197] З особистої розмови з фахівцем МОУ.
[198] Там само.
[199] З особистої розмови зі співрозмовником N.
[200] З особистої розмови з розробником системи «Неон».
[201] З особисто отриманої консультації з військовим СОУ, користувачем кількох систем.
[202] З особистої розмови з розробником системи «Неон».
[203] Там само.
[204] Там само.

як змінювались патерни озброєння противника протягом 1-2 місяців, що дозволяє зробити певні висновки та побудувати модель реагування.[205] Станом на сьогодні, цю систему можна вважати одним з найефективніших інструментів, що допомагають генерувати технологічну перевагу в поточній війні.

ІТС «Термінал» можна навести як приклад суто вузькоспеціалізованого ПЗ. Його було представлено у 2021 р. як один з трьох елементів ударно-розвідувальної системи виробництва UkrspecSystems (ще два елементи – розвідувальний БпАК «PD-2» та ударний малогабаритний дрон-камікадзе «RAM II», якими «Термінал» мав управляти в онлайн режимі).[206] «Термінал» був створений як інструмент роботи дешифрувальника видової інформації БпЛА, що здійснює збір, обробку, обмін та відображення цієї інформації.[207] Система не отримала великого поширення, проте, була задіяна в інтересах оборони Києва навесні 2022 р. наряду з ІКС «DELTA» для збору та обробки даних аеророзвідки.[208]

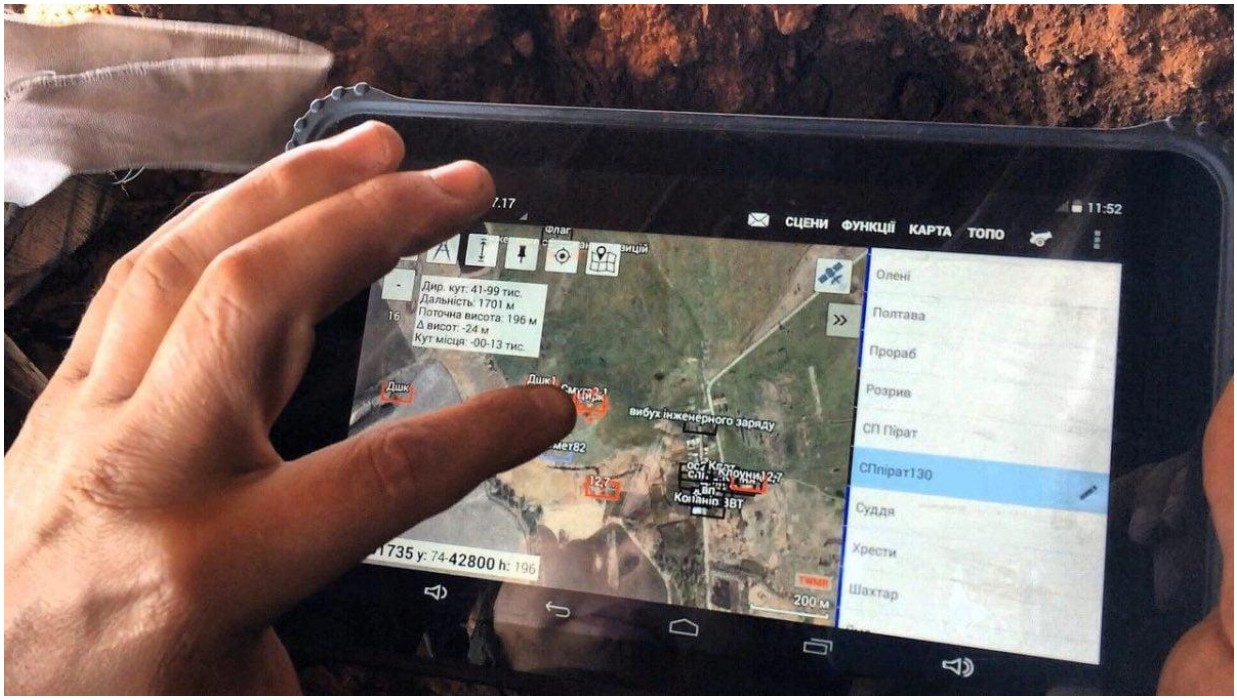
На противагу вузькоспеціалізованим рішенням, є такі системи, що охоплюють майже без винятку всі роди та види військ і типи підрозділів. Вони не мають якої-небудь чітко визначеної спеціалізації.

Наприклад, «Кропиву» нерідко називають «стандартним ПЗ, що є у всіх»[209]. Це система ТЛ, що є найбільше і найглибше інтегрованою у війська (станом на сьогодні, користувацька аудиторія налічує сотні тисяч). За оригінальним задумом, «Кропиву» було побудовано суто для артилерійського використання як балістичний калькулятор – тобто, первинно закладений функціонал чітко передбачав спеціалізацію. Проте, з часом вона «обросла» великою кількістю нових функцій, хоча так і не вийшла на оперативний рівень, залишившись глибоко інтегрованою на тактичному, де відсутні функції управління[210].

---

[205] Там само.
[206] «UkrspecSystems представила власний варіант сучасної ударно-розвідувальної системи», *Defense Express*: 20 вересня 2021. <https://defence-ua.com/news/ukrspecsystems_predstavila_vlasnij_variant_suchasnoji_udarno_rozviduvalnoji_sistemi-4813.html> [Переглянуто 2025 22 04].
[207] Михайло Ракушев, Віталій Зуйко, Роман Пантюшенко, «Аналіз використання інформаційно-телекомунікаційної системи «ТЕРМІНАЛ» в інтересах Сил оборони Києва». *Сучасні інформаційні технології у сфері безпеки та оборони*, 2022/Том 44 (№2), 55. <https://sit.nuou.org.ua/article/view/264158/261332> [Переглянуто 2025 21 04].
[208] Там само.
[209] З особистої розмови з розробником СПЗ «Вежа».
[210] З особистої розмови з фахівцем МОУ.

«Кропива» дозволяє наносити об'єкти на офлайнову мапу, також можлива проста комунікація: наприклад, з «Вежі» (або «DELTA») можна «залити» дані на «Кропиву»[211]. Обмін даними здійснюється напряму і швидко, але не з сусідніми батальйонами (тобто, відбувається сегментація передачі даних).[212]



Планшет з інформаційною мапою бойових дій у застосунку «Кропива». Джерело: АРМІЯ SOS.

Насамкінець, говорячи про **рівневість (c),** слід розуміти, що в контексті українського війська і війни, що триває, переважна більшість СПЗ використовується виключно на тактичному рівні. Деякі системи «роблять спроби виходу» на оперативний, проте стратегічний рівень наразі представляє собою майже абсолютний вакуум в плані того, що стосується впровадження і практичного застосування СПЗ.

Слід зауважити, що запропонована в цій частині роботи категоризація систем є умовним інструментом. З огляду на безперервність процесів розвитку технологій, тенденцію на впровадження технологій ШІ та МН, нарощення системами нових функцій, їхнє злиття і нашарування, – було би хибно стверджувати, що на тлі динамічного розвитку галузі в умовах активних бойових дій ця доволі примітивна категоризація могла би бути інклюзивною. Тож необхідно розуміти, що деякі системи не підпадають під жодну із запропонованих категорій.

[211] З особистої розмови з розробником СПЗ «Вежа».
[212] З особистої розмови з фахівцем МОУ.

***

Резюмуючи цей стислий опис, що мав на меті скласти нарис галузі в цілому, на даному етапі, слід зафіксувати деякі із загальних **тенденцій**, притаманних галузі СПЗ станом на сьогодні.

По-перше, **1) системи розвиваються переважно на тактичному рівні та у горизонтальному напрямку за рахунок охоплення все більшої кількості доменів** (БпЛА → наземний → артилерійський → морський) **і накопичення функцій**[213].

Наочним прикладом цього тренду може служити «Кропива», яка з балістичного калькулятора трансформувалась в один з найбільш популярних продуктів тактичного рівня, охоплюючи сьогодні безліч доменів і функцій[214]. В цьому випадку, розростання функцій було продиктовано попитом великої кількості користувачів (станом на зараз, це десятки тисяч). В певній мірі, цю тенденцію можна відстежити і на прикладі розвитку ІКС «DELTA», хоча слід зауважити, що протягом останніх років «DELTA» активно працює над інтеграцією модулів та інструментів екосистеми, функційно пов'язуючи їх між собою (див с. 85).

Втім, за словами фахівця МОУ, «[...] зайшовши у штаби оперативного рівня, не побачиш цифрових інструментів, адже там переважно використовуються паперові карти».[215] Частково, як пояснює він, відсутність вертикального росту систем можна пояснити тим, що оперативний рівень вже має гриф «Таємно», стратегічний – «Цілком таємно», а для впровадження АСУВ на оперативному рівні необхідно мати відповідний доступ.[216] (З іншого боку, «Дзвін-АС», система стратегічного рівня (див. с. 52), реалізувала обмін засекреченою інформацією. Проте, слід розуміти, що це вдалося зробити у протиправний спосіб.)

Відповідно, другий тренд, який можна виокремити, це **2) концентрація СПЗ на тактичному рівні.**

Можна стверджувати, що тактичний рівень сьогодні доволі щільно наповнений системами різного функціоналу та векторів спеціалізації. Натомість, на оперативному присутні деякі системи, чий функціонал дозволяє вирішувати задачі цього рівня. Водночас, стратегічний рівень фактично представляє собою вакуум.

[213] Там само.
[214] Там само.
[215] Там само.
[216] Там само.

Також, як слідує з опису та первинного аналізу галузі в цілому, можна зробити висновок, що **3) більшість СПЗ є спеціалізованими**, тобто, такими, чий інструментарій закладений в межах певної спеціалізації.

Наведені приклади включають, але не обмежуються системами, призначеними для автоматизації управління роботи ППО; інструментами аналітики; інструментами симуляції і планування місій; системами автоматизації взводів РЕР; рішеннями, базованими на OSINT підходах тощо.

Окремо слід звернути увагу на **4) активний розвиток СПЗ-інструментів аналітики на тлі широкомасштабної війни** як ще одну характерну тенденцію.

Як було аргументовано на конкретних прикладах (зокрема, системи «Avengers»), поточна війна продиктувала запит на впровадження технологій ШІ та МН, які застосовуються з метою збільшення рівня автоматизації операцій, що дозволяє значно скоротити кілчейн, і як наслідок, досягти вогневої переваги на полі бою.

Окрім цього, треба відзначити й те, що в поточних умовах **5) навчальні системи та симулятори набувають більшої актуальності.**

Активний розвиток рішень цієї категорії зумовлений потребою швидкого здобуття практичних навичок о/с, особливо у випадку відсутності досвіду бойових дій. Ці рішення часто базуються на технологіях AR/VR та включають елементи воргеймінгу.

II (і). Детальніший огляд деяких систем

COMBAT VISION[217]

«ComBat Vision» – це узагальнена назва групи програмних продуктів з розвідки і координації на полі бою, що налічує вже декілька поколінь софтверних рішень[218]. Команда розробляє продукти цієї категорії з 2012 р., прагнучи постійно покращувати їхні функціонал та інструментарій у відповідь на актуальні потреби і запити користувачів та зміни характеру війни.[219]

Наприклад, свого часу, «ComBat C2» широко використовували ССО ЗСУ та спец.підрозділи різних силових структур (з 2015 р.)[220]. Зокрема, на цій системі велася оборона Маріуполя полком «АЗОВ», а сьогодні її використовує штаб 3 ОШБ [з березня 2025 р. – Третій Армійський Корпус – ред.] для відображення власних сил (при цьому, основною системою планування на рівні корпуса є «DELTA»). Також, «ComBat Terminal», що є веб-плагіном до системи «ComBat C2», на початку війни використовували штаби секторів за підтримки «Аеророзвідки» для моніторингу лінії розмежування через охоронні камери вздовж лінії розмежування зони АТО та для дешифровки відео з БпЛА тих часів.[221]

До найсучаснішого покоління продуктів «ComBat» відносять «ComBat 4», розподілену геоінформаційну платформу ситуаційної обізнаності тактичного рівня, про яку і йтиметься надалі. Євген Максименко, розробник групи продуктів «ComBat Vision», який виступив респондентом, назвав «ComBat 4» результатом переосмислення попереднього 10-річного досвіду команди і бачення того, якою має бути професійна система керування боєм ТЛ, що побудована на стандартах НАТО і передових технологіях.[222]

Респондент звертає увагу на те, що «ComBat» в її нинішньому стані коректніше було би назвати **системою ситуаційної обізнаності з елементами управління боєм ТЛ**. Він пояснює, що до її становлення повноцінною системою управління боєм (див. с. 41) лишається впровадити деякі інструменти, що команда і планує зробити впродовж 2025 р. Водночас, фахівці дотримуються думки, що в українському контексті, «ComBat» є

[217] Інформація, наведена в цій частині дослідження, структурована автором на основі отриманих відповідей респондента – Євгена Максименка, розробника системи «CombatVision», під час проведеного з ним інтерв'ю. Джерела, використані додатково, позначені окремо.
[218] З інтерв'ю автора з Євгеном Максименком для Astero Analytics, грудень 2023 (особисті матеріали автора). <https://surl.gd/icgeuv> [Переглянуто 2025 05 05].
[219] Там само.
[220] Там само.
[221] Там само.
[222] Там само.

унікальним рішенням – адже в Україні наразі немає ані аналогів, ані конкурентів цій системі.[223] [Станом на сьогодні, серед усіх систем українського походження, «ComBat» є найближчою до категорії систем управління боєм. Порівняти її можна було би хіба що з системою «IcomWare», яка входить до складу «Hermes C2» – ред.].

Що стосується **функціоналу**, слід сказати, що «ComBat» – це система, яка створена для планування, розвідки і координації дій сухопутних підрозділів і призначена для застосування **в активних бойових діях**. **Інструментарій** «ComBat» розширюється з кожним оновленням системи, які команда проводить регулярно. [Наприклад, в листопаді 2024 р. Євген провів закриту лекцію для користувачів, представивши більш ніж 20 оновлень за півріччя[224] – ред.]. Сьогодні, система дозволяє здійснювати обмін тактичними даними штатними низькошвидкісними каналами зв'язку по безсерверній розподіленій архітектурі з можливістю виводу (перегляду) обстановки на трьохвимірних картах з доповненою реальністю (AR).

Сукупно, інструменти «ComBat» надають обізнаність про взаємне розташування дружніх сил (з метою уникнення дружнього вогню), уможливлюють швидкий вихід на позиції завдяки певним елементам навігації, дозволяють бійцям орієнтуватися під час активної фази бойових дій (в нападі або обороні).

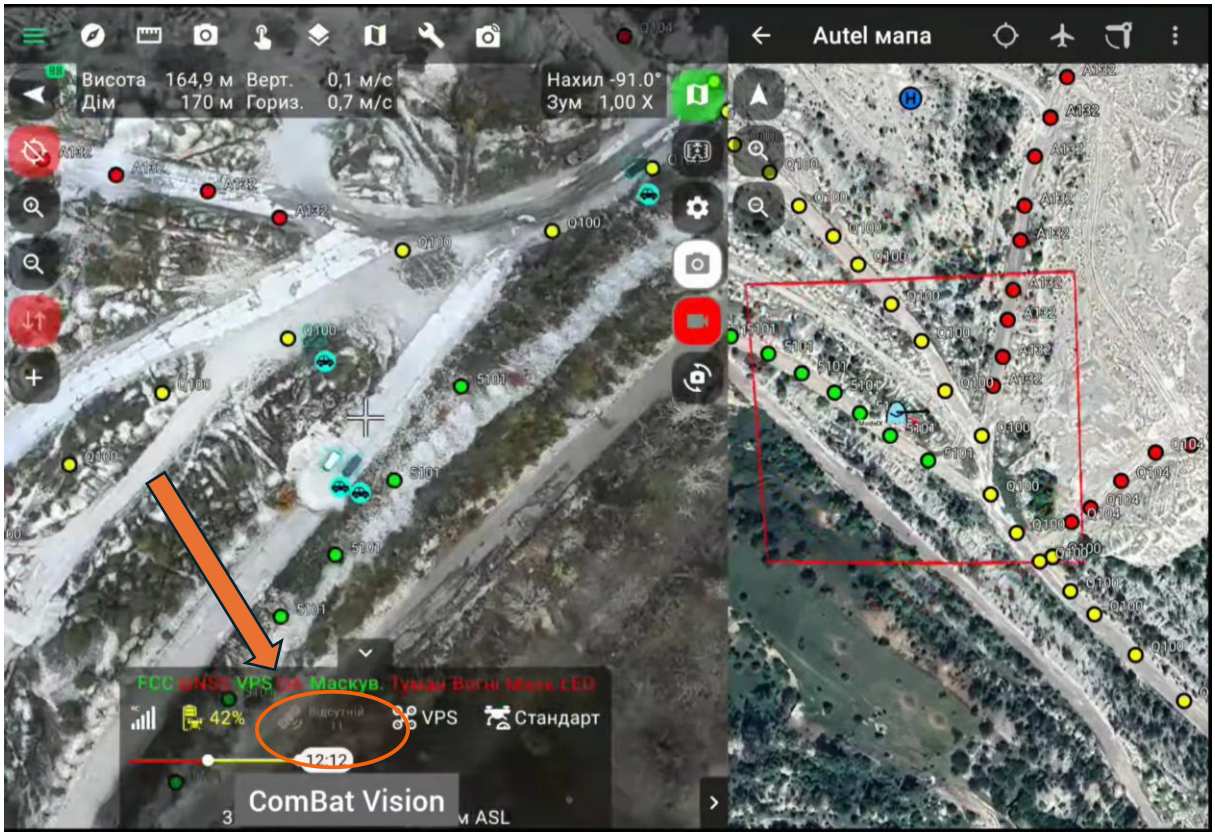
Як пояснює Євген, система здатна «покрити» роботу бійців у трьох фазах, а саме: 1) підготовчій («як діяти»), 2) виконавчій («як координувати та навігувати сухопотні підрозділи»), та 3) аналітичній (AAR). Наразі система реалізує повноцінне функціонування другої і третьої фаз, втім, перша ще потребує деякого доопрацювання. Зокрема, підготовча (фаза планування) включає в себе збір даних з інших систем про ситуацію та оперативне середовище, первинну розмітку території місцевості, прокладання маршруту, нанесення маршрутів руху дружніх підрозділів, планування власних дій та координацію дій підрозділів, а також складання подальших фаз.

У виконавчій фазі, пояснює Євген, система дозволяє бачити пересування бійців, знаходячись у штабі («[...] хто рухається, хто ні, а хто потребує допомоги»), а також навігувати підрозділ: наприклад, «попереду болото, не йдіть туди» або ж «там ворожий підрозділ». В режимі реального часу або часу, наближеного до реального, також можливо міняти план по ходу дії, наприклад, намалювавши новий маршрут просто в ріалтаймі і передавши його

[223] З особистої розмови з фахівцем МОУ та консультацій з військовими СОУ.
[224] З непублічної онлайн лекції (1).

всім залученим суб'єктам поля бою. Третя фаза представляє собою проведення аналізу бою та винесення висновків, що сукупно складає процес AAR (див. Глосарій).

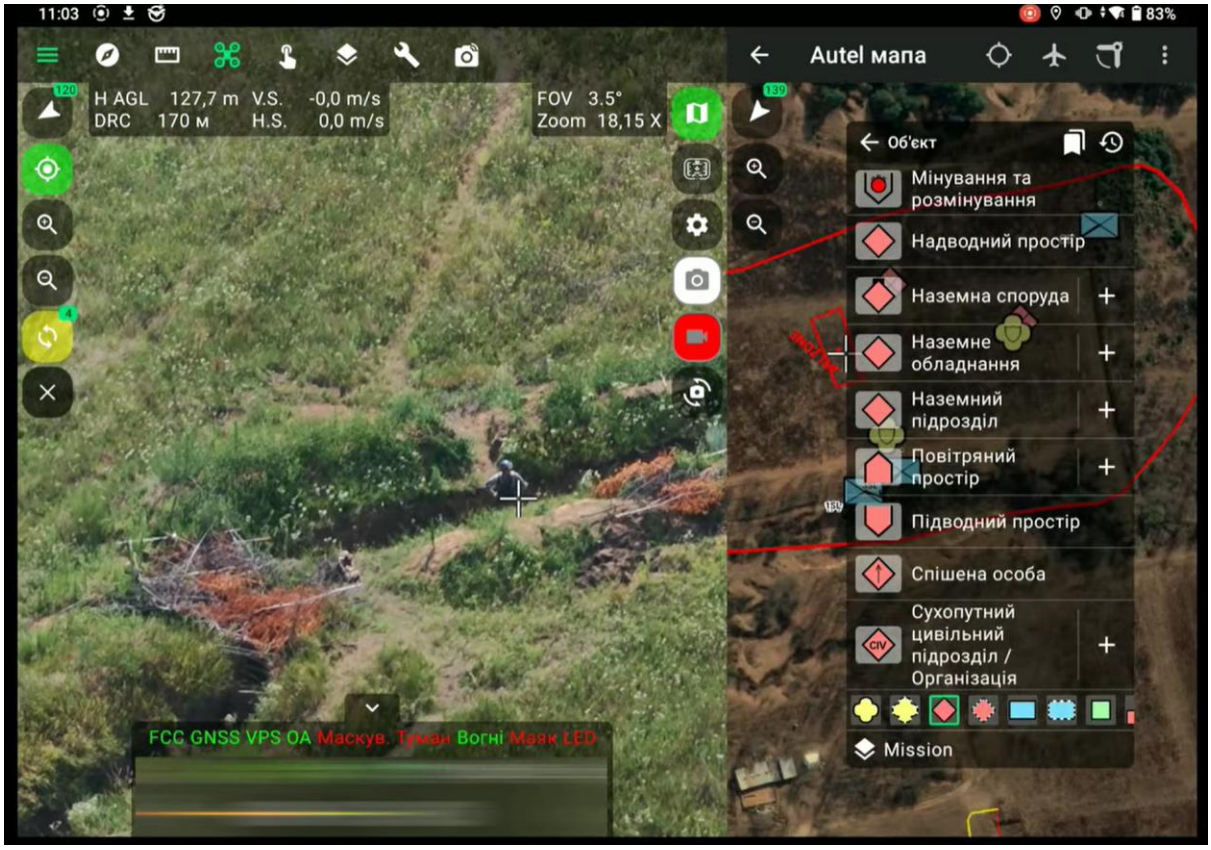
В цілому, це робить «ComBat» системою планування, підготовки та виконання сухопутних маневрених операцій з подальшим етапом AAR. Причому, зауважує Євген, слово «маневрених» тут є ключовим – адже система проявляє себе саме в активних бойових діях: «[ц]е система для рейдів на Курський напрямок, контрнаступальних дій на Херсонщині тощо».



Скріншот з відео. Приклад роботи «ComBat 4» на Autel 4T без GNSS. (Одне з оновлень системи за 2024 р.). Джерело: «ComBat Vision».

Євген також зазначає, що «ComBat» створена на основі принципу TLP, Troops Leading Procedure [– стандартизованій процедурі управління невеликими підрозділами, зокрема ланки «взвод» – ред.] (див. Глосарій), що є відмінним від принципу MDMP, Military decision making process (див. Глосарій). За його словами, призначення «ComBat» саме в тому, щоби «[…] на шматку фронту в 5 км здійснити операцію», і це, до слова, відрізняє систему від ІКС «DELTA», яка накопичує інформацію по всій лінії фронту. Тобто, окрім надання ситуаційної обізнаності, «ComBat» також допомагає координувати підрозділи в ріалтаймі, тримати під контролем ініціативу та виконання операції. [Примітка: в ІКС «DELTA», за словами Інни

Гончар, наразі доступна функція трекінгу, а навчання роботі в модулях екосистеми вже сьогодні відбувається за принципом TLP – ред.[225]]



Скріншот з відео (запис з пульта Autel). Нанесення тактичної інформації та передача її по радіозв'язку. Джерело: «ComBat Vision».

Технічно, «ComBat» підтримує всю номенклатуру **даних**. Втім, респондент зазначає, що можна виокремити 4 категорії «базових» даних, якими переважно оперує система. Перша категорія – це дані для підтримки функції Blue Force Tracking (див. Глосарій), що відповідає за позначення розташування дружніх сил. Друга – дані для позначення ворожих об'єктів – виконання компоненти Target Acquisition (TA). Третя – дані, що служать для розмітки території т.зв. «control features», тобто, різноманітними «контрольними властивостями», які описують «стаціонарні» явища. (Наприклад, географічні об'єкти та властивості рельєфу, як-то, «озеро», «пагорб», «висоти» і «низини», а також «мінні поля», «лінії заборони вогню», «атмосфера/метеорологія», «завдання операції» тощо. Всі ці «control features» є елементами оперативного середовища та/або важливими елементами місцевості.) До четвертої

[225] З консультації з Інною Гончар, керівницею напрямку «Управління знаннями» ГО «Аеророзвідка».

категорії можна віднести дані для створення маршрутів і навігації (дані про маршрути пересування).

Говорячи про **користувачів** та **рівні** застосування «Combat», слід зазначити, що це система тактичного рівня, призначена для керування «батальйоном і нижче». (Найвищим рівнем застосування системи є один батальйон – йдеться саме про дії всередині одного батальйону, а не між декількома.) «Це система для командира відділення, який йде в полі, і якому треба в телефоні подивитися, де знаходяться дружні підрозділи», – пояснює розробник. Зокрема, «ComBat» покликаний вирішувати проблему, притаманну маневреним операціям, а саме, «[...] відсутності координації дій між двома відділеннями, внаслідок чого люди заходять на ворожі блокпости, не бачать де свої, а де ворожі сили», – говорить Євген.

Враховуючи певні суб'єктивні обмеження, такі як нестача технологічного забезпечення, реально система є придатною до використання насамперед в спец.підрозділах силових структур та/або підрозділах із сильною технологічною складовою. Лінійні підрозділи (ТрО, Сухопутних військ та інших родів військ), як правило, не володіють належною технікою, необхідною для повноцінного користування інструментами та функціями «ComBat». Наразі основними користувачами системи є підрозділи ССО, ГУР МО та ДШВ.

Висловлюючись на тему **інтеграції** з іншими системами, респондент зазначає, що тут можна виокремити дві площини, а саме, 1) інтеграцію тактичними даними та 2) кешами карт. За словами Євгена, «ComBat» може бути інтегрований зі всіма картами різних систем, адже вона відкриває практично всі види офлайн кешів інших систем.

В цілому ж, важливо розуміти, що інтеграція як така здійснюється не з самими системами, а через стандарти, які підтримуються ними. Наприклад, «ComBat» може бути інтегрований із системою, яка підтримує NVG, NATO Vector Graphics. Серед українських систем або таких, що використовуються сьогодні в інтересах СОУ на полі бою, цей формат підтримує ІКС «DELTA» – отже, «ComBat» інтегрований з ІКС «DELTA» через NVG.

Аналогічно, інтеграція з американською системою «ATAK» (Android Tactical Assault Kit) [популярним інструментом серед військових в поточній війні – ред.] реалізована не напряму, а через CoT, Coursor-on-target, – формат, що лежить в основі «ATAK», а з «Кропивою» – через формат KML. Формати KML, KME, KMZ з розширеннями від «Кропиви»

дозволяють імпортувати та експортувати дані в «Кропиву», хоча і з певними обмеженнями, через які, власне, не вдається досягти 100% інтероперабельності з цією системою.

Респондент зазначає, що зі згаданими системами «ComBat» може здійснювати обмін даними, проте, йдеться не про онлайновий обмін. Формат GPX дозволяє імпорт та експорт маршрутів. Окрім цього, системою підтримується MIM (MIP[226] Information Model), стандарт НАТО з обміну інформацією.

Скріншот з відео демонстраційного показу, проведеного ComBat Vision разом із Himera Radios для СВ. Джерело: Himera Radios.

Проблема **інтероперабельності** українських систем, на думку респондента, сьогодні не є критичною. «Зараз ситуація набагато краща – принаймні, вже не треба вручну «переливати» дані», – говорить він, відзначаючи, однак, відсутність яких-небудь визначених стандартів для побудови СПЗ. «А такий стандарт має бути визначений, системи мають «розмовляти» однією мовою», – аргументує співрозмовник, «[...] наприклад, визначте певний формат і створюйте свої системи за цим форматом, а не за «DELTA» чи ще кимось».

Наразі ж, на його думку, на оперативному рівні відбувається т.зв. «лагідна дельтанізація» [від назви ІКС «DELTA» – ред.], а на тактичному рівні можна спостерігати намагання інших систем і команд «[...] навмання інтегруватися з «Кропивою»». Тобто, наразі

[226] MIP, Multilateral Interoperability Programme.

стандартизація на тактичному рівні не базується на якомусь-небудь визначеному стандарті: «[...] всі визнають, що «Кропива» є у всіх, і наосліп намагаються до цього факту пристосуватися».

Євген говорить, що система перебуває на **етапі** «вічного тестування», при цьому уточнюючи, що команда наразі і не ставить за мету проходження кодифікації. «Нам важливо вирішити проблеми користувачів, тому ми насамперед зайняті розробкою системи, яка допоможе це зробити», – говорить Євген. Він аргументує, що метою команди є не гонитва за кількістю користувачів як таких, а передусім – донесення до них значення командної роботи та важливості існування тактичної мережі. (Зокрема, Євген зазначає, що у разі відключенння Starlink, потреба в тактичному зв'язку, по якому можна було би вести бій, стане критичною.)

Він також пояснює, що система знаходиться в готовому для продуктової експлуатації стані, але не може бути введена в експлуатацію через ряд причин, що не залежать від команди. З одного боку, є готовий продукт, з іншого – немає користувача, який готовий був би його використовувати. «Тому, наразі про «ComBat» не можна сказати, що це повноцінний перевірений продукт», – говорить розробник, – адже він працює переважно в спец.підрозділах, наприклад, будучи у використанні служби РЕР 3 ОШБ [з березня 2025 р. – Третій Армійський Корпус – ред.] та деяких штабів, що застосовують систему для нанесення об'єктів на офлайнову мапу.

Однією з причин, що унеможливлюють повноцінне впровадження системи, Євген називає нестачу підготовки фахівців зв'язку в ЗСУ. На його думку, сьогодні це і є одним з **викликів** для галузі в цілому та реалізації ПЗ в окремих випадках. Ще одним блокером є те, що питання «цифровізації» бійця не є пріоритетним у війську на рівні десіжен-мейкерів. «Армія має еволюціонувати до того рівня, коли життя бійця буде важливим. Зараз воюють ротами, а координація всередині взводу лишається поза увагою», – аргументує респондент.

«Ніби всім зрозуміло, що бійцю треба дати планшет, а чим його живити протягом N годин бою – про це ніхто не подумав», – говорить Євген, пояснюючи, що гаджети потребують мобільного живлення, тобто, живлення безпосередньо на бійцеві. В Україні,

станом на сьогодні, немає ані виробників продукції, аналогічної до американського STAR-PAN виробництва Glenair[227], ані розвитку проектів в цьому напрямку.

Тому, дуже відчутний брак рішень, які би забезпечили постійну активність планшета і рації. «Немає інфраструктури зв'язку – за півдня планшет розряджається і перетворюється на «цеглу», яку приходиться носити з собою, а тому, планшет зараз – це штабна історія», – пояснює розробник: «[...] це все одно, що мати склад танків, не маючи від них ключів». Наприклад, проблема впровадження «ComBat Vision» в підрозділи ССО наразі полягає у банальній відсутності «шнурка» від Harris до Android.

У підсумку розмови, Євген виокремлює **дві ключові тези**. Перше, він акцентує на необхідності концентрації зусиль в практичній площині «цифровізації» піхотинця:

«Роботи замість людей будуть воювати за 10 років, тож до «війни роботами» ще треба дожити. А реальність є такою, що нам воювати треба вже, і воюємо ми все-таки людьми. Тому, треба посилювати спроможності звичайного піхотинця – вирішувати насамперед його проблеми. Це головне, а решта питань є другорядними».

Друге, що стосується характеру ведення війни на її нинішньому етапі, розробник звертає увагу на необхідність посилення маневреної складової, ефективність якої підвищують такі софтверні рішення, як системи управління боєм:

«Ми не переможемо, «перекидуючись» дронами. Нам треба навчитися ефективно пересуватися, тобто, ефективно маневрувати. Адже в цьому і є наша сила».

[227] STAR-PAN є системою підключення і підзарядки для бійців. Продукція представляє собою інтегрований багатопортовий USB хаб, системи розподілу живлення і тактичні з'єднання: «STAR-PAN™ Integrated Soldier Multiport USB Data Hub / Power Distribution Systems and Tactical Interconnects», Glenair. <https://www.glenair.com/star-pan/index.htm> [Переглянуто 25 22 04].

ГРК «Броня» («ARMOR»)[228]

Протягом останніх 11 років, що Україна перебуває у стані війни, команда «ARMOR» допомагає СОУ протистояти агресії шляхом розвитку і впровадження технологій. Про це говорить Олексій Гавриш, один з розробників системи, виступаючи у ролі респондента.

Починається розмова з озвученої Олексієм тези про зміну характеру бойових дій. Він зазначає, що характер війни 2015-го, 2016-го і 2019-го рр. значно відрізняється від характеру війни 2022-го, 2023-го, і 2024-го зокрема, номенклатурою озброєння. «ARMOR», також відому як ГРК «Броня», можна назвати однією із тих систем, що змогли адаптуватися до змін, лишаючись при цьому ефективним та результативним інструментом для планування та виконання завдань безпосередньо у зоні бойових дій.

«В якийсь момент, танкісти звернулись до нас із запитом допомогти в навігації. Тоді і з'явилась ідея створити інструмент для розрахунку стрільби для закритої вогневої позиції [надалі – закритої ВП – ред.]. Це і була перша версія застосунку, яка дозволила танку вражати цілі з закритої ВП. Все, що існувало до того, працювало лише з бусолі», – розповідає Олексій. [Закритою ВП називається така «[...] вогнева позиція, на якій гармати (міномети, бойові машини) під час ведення вогню закриті від наземного спостереження противника»[229] – ред.]

Першим кейзом для «ARMOR» був Т-64. «Зазначений танк здатний уразити ціль прямою наводкою на відстані максимум 3-3,5 км, а загалом, танкова гармата дозволяє здійснити постріл уламково-фугасним снарядом на відстань до 12,4 км. Впровадження «ARMOR» дозволило уражати цілі на відстані 10-12 км з цього виду озброєння (з гладкого ствола). Після відведення танків у 2016 р. команда вирішила зосередити зусилля на інтеграції та розширенні можливостей використанння групового піхотного озброєння, – йдеться про такі засоби як гранатомети, кулемети, БМП-1 та БМП-2.

Сьогодні «ARMOR» – це «система тактичного **рівня**, яка забезпечує розрахунки параметрів стрільби із закритих вогневих позицій для танків, БМП, БТР, ствольної артилерії, мінометів, РСЗВ, зенітної артилерії та групової піхотної зброї», – зазначають

[228] Інформація, наведена в цій частині дослідження, структурована автором на основі отриманих відповідей респондента – Олексія Гавриша, одного із розробників системи «ARMOR» (ГРК «Броня»), під час проведеного з ним інтерв'ю. Джерела, використані додатково, позначені окремо.
[229] «Керівництво з бойової роботи вогневих підрозділів артилерії». Міністерство оборони України, 2019, 1. <https://sprotyvg7.com.ua/wp-content/uploads/2022/06/%D0%9A%D0%91%D0%A0_2019.pdf> [Переглянуто 2025 22 04].

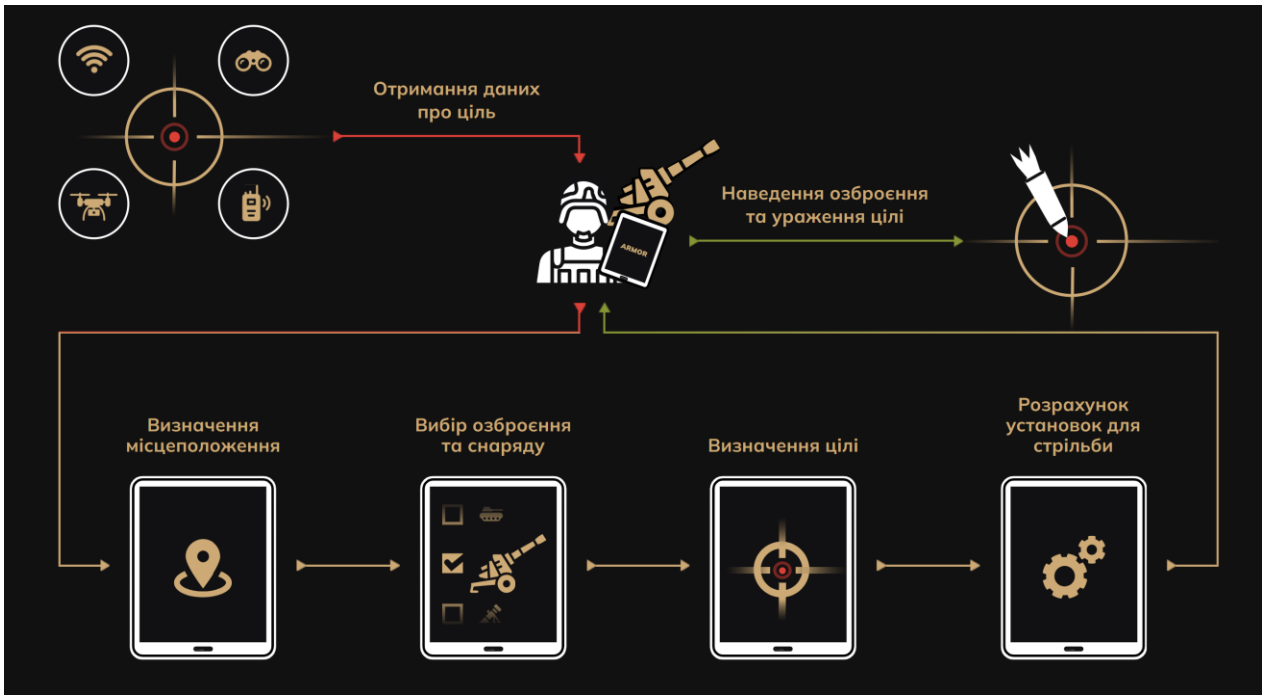
розробники[230]. Систему створено для артилерійських, механізованих підрозділів та підрозділів ППО,[231] які, завдяки її використанню можуть вести вогонь із закритих ВП, що підвищує їхню безпеку, та водночас, обмежує можливості противника вести вогонь у відповідь.[232] Окрім цього, система забезпечує «[...] високу точність ураження цілей у всіх діапазонах дальностей стрільби, навіть якщо вони приховані природними бар'єрами, рослинністю або рельєфом».[233] Сьогодні немає такої бригади, в якій не було б у використанні «ARMOR», як зазначає респондент. Серед **користувачів** – як підрозділи ЗСУ та НГУ, так і спеціальні сили.

Систему реалізовано у вигляді мобільного застосунку, основним призначенням якого є розрахунок параметрів ураження цілей із закритих ВП з широкого спектру озброєння (що можна вважати її основним **функціоналом**). Першочергово розробники зосередили зусилля на простоті засвоєння та застосування продукту в бойових умовах. Система включає широкий **діапазон інструментів**, який спрощує та прискорює планування і виконання завдань, та, зокрема, включає такі функції як цифрове картографування, навігацію, нанесення та моніторинг тактичної обстановки, формулювання завдань, оцінку можливості ураження цілі, координацію вогню тощо.[234] Вартує підкреслити, що ПЗ не є балістичним калькулятором у чистому вигляді, адже система також надає можливості оцінити ураження, провести координацію дій та корегувати вогонь, – пояснює Олексій.

Навчання з використання АГС-17 спільно з ГРК «Броня» (ARMOR) для ураження цілей із закритої ВП. Джерело: «ARMOR».

[230] З матеріалів, наданих Олексієм Гавришем, одним із розробників ГРК «Броня» (ARMOR).
[231] ARMOR. <https://armor.ua/ua/> [Переглянуто 2025 19 04].
[232] З матеріалів, наданих Олексієм Гавришем, одним із розробників ГРК «Броня» (ARMOR).
[233] Там само.
[234] Там само.

Система охоплює понад 60 різноманітних видів озброєння та більше 100 типів боєприпасів до нього[235]. Як це працює: ПЗ встановлюється на планшет і може бути використане у поєднанні з наявними вогневими засобами.[236] «Користувачу достатньо визначити власне місцеположення [місцеположення вогневого засобу – ред.], вибрати з переліку наявне у нього озброєння, зорієнтувати його на місцевості, визначити умови стрільби, визначити ціль та отримати параметри ураження для обраного вогневого засобу», – зазначають розробники[237]. Після цього лишається навести вогневий засіб (за отриманими розрахунковими параметрами) та виконати постріл[238].



Принцип функціонування «ARMOR» (ГРК «Броня»). Джерело: «ARMOR».

«ARMOR» дозволяє вражати ворожі цілі більш точно, швидко і безпечно та зі значною економією боєкомплекту, – пояснює респондент. При цьому, під «точністю» мається на увазі можливість проведення розрахунку таким чином, щоб уразити ціль з 1-3 пострілу. Говорячи про швидкість, йдеться про швидке отримання метеоданих для розрахунку установок[239] та більш швидке орієнтування вогневих засобів у порівнянні з типовими способами орієнтування. Загалом, час на ураження цілі скорочується з ~ 30 хв. до 5-7 хв. з

[235] Там само.
[236] Там само.
[237] Там само.
[238] Там само.
[239] ARMOR.

використанням застосунку.[240] Безпечність досягається за рахунок зменшення часу перебування у зоні вогню у відповідь[241], можливості не виходити в зону прямого ураження, зменшення самого часу ураження, а також меншого кількісного залучення о/с. Економії вдається досягти шляхом значного зменшення витрат боєприпасів (у 5-10 разів), що, як наслідок, також сприяє подовженню терміну служби озброєння.

Розрахунок ефективності ураження цілі (на прикладі 120мм міномету). Джерело: «ARMOR».

«Ми виконуємо індивідуальні установки для стрільби для ураження цілі з закритої ВП, враховуючи більше 10 різних параметрів, наприклад: перепад висот (щоб уникнути «перельоту» або «недольоту»), температуру, атмосферний тиск, силу вітра, напрям вітру, вологість тощо», – говорить Олексій.

За словами респондента, однією з ключових відмінностей системи є можливість орієнтування вогневого засобу без використання бусолі (орієнтування на основі

[240] Там само.
[241] З матеріалів, наданих Олексієм Гавришем, одним із розробників ГРК «Броня» (ARMOR).

вимірювання магнітного азимуту, найбільш неточний спосіб з існуючих, але найбільш поширений), віддаючи перевагу геодезичному способу, що є більш точним. В цілому, в програмі реалізовано три способи: астрономічний (за Сонцем), геодезичний та за допомогою магнітної стрілки бусолі. Найбільш часто використовується геодезичний, як більш простий і точний. За відгуками користувачів, це дозволяє з високою ефективністю застосовувати вогневі засоби в стані «кочуючих».[242]

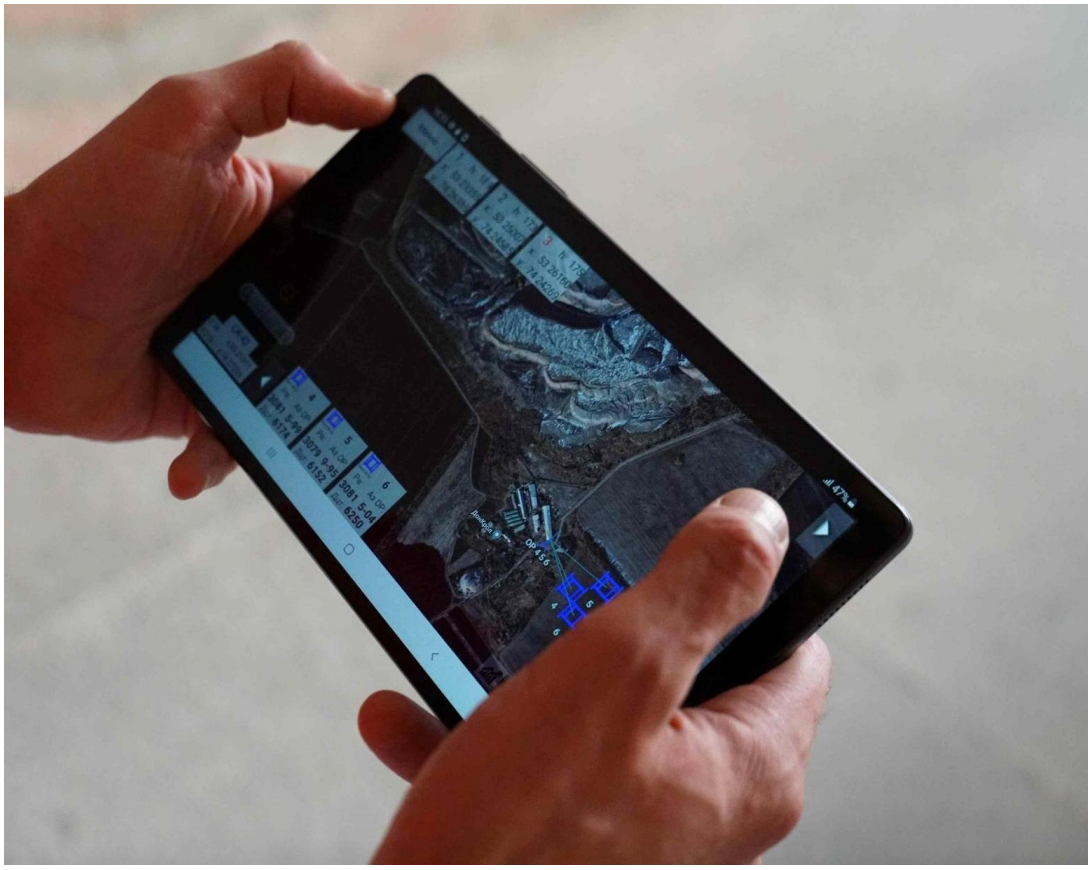
Співрозмовник також пояснює, що для визначення поправок дальності і напрямку програма дозволяє враховувати дані про відхилення (від табличних) напрямку і швидкості вітру, температуру повітря і заряду, атмосферного тиску, вагові знаки снаряду, втрату початкової швидкості снаряду, деривацію, а для систем виробництва країн-членів НАТО – також враховується густина повітря. Залежно від географічних умов, програма розраховує поправки на перевищення цілі та обертання Землі.

Програма може працювати як в онлайн, так і офлайн режимі. При цьому, доступне як автоматичне завантаження необхідних **даних**, так і ручне введення, що дозволяє використовувати продукт навіть в умовах відсутності зв'язку. Дані актуальні протягом обмеженого часового інтервалу, що також відстежується системою.

Команда постійно працює над покращенням якості вхідних даних від інших систем і провайдерів, які спеціалізуються на тих чи інших типах даних. «Для корегування використовуємо дані спостереження з КСП, аерофотозйомки. В якості топоснови (карти) може буде використаний ортофотоплан – супутникові знімки чи зображення, отримані з БпЛА», – говорить респондент. Окрім цього, є можливість використання даних, отриманих від інших систем, що передбачають надання ситуаційної обізнаності, наприклад, дані про ворожі цілі.

Олексій відзначає тенденцію зростання попиту на ПЗ: «[...] за перші пару місяців повномасштабної війни було активовано приблизно таку ж кількість планшетів, як і у період з 2015 до 2022 рр. сукупно», – говорить він, додаючи, що в місяць активується більше 200 планшетів, а всього, станом на сьогодні, було активовано понад 9000 планшетів «ARMOR». З них велику кількість (близько 55%) передано фонду «Повернись живим», з яким співпрацює команда. При цьому, у відкритому доступі ПЗ відсутнє – воно розповсюджується безпосередньо командою розробки і на поточний момент, надається військовим безкоштовно.

[242] ARMOR.



Застосунок «ARMOR» (ГРК «Броня») на планшеті. Джерело: надано Олексієм Гавришем.

Важливо відзначати, що команда «ARMOR» не лише створює продукт, але й навчає військових ним користуватися. Так, «Повернись живим» забезпечує навчання (у фонді є 4 інструктори з підготовки), а команда «ARMOR» надає безпосередньо свій продукт, встановлюючи ПЗ на планшети. «ARMOR» впроваджує підхід, в основі якого лежить концепція повного циклу «від ідеї → до розробки → до підготовки → до навченого бійця». Продукт орієнтовано на військовослужбовців з мінімальним досвідом, що дозволяє за 4-6 годин практичних занять з інструкторами «[…] підготувати військовослужбовця достатньо аби він міг самостійно виконувати бойові задачі та вражати цілі із закритої ВП», – говорить Олексій. Станом на сьогодні, кількість навчених військовослужбовців інструкторами фонду перевищує 15 000.

Вартує відзначити, що хоча «ARMOR» і «Кропива» покликані вирішувати схожі задачі, роблять вони це в різний спосіб. «Кропива» має ширший функціонал, проте «ARMOR» вирішує ефективніше основну задачу – точне ураження цілі. За словами респондента, «Кропива» надає ситуаційну обізнаність, має налагоджену систему зв’язку та обміну даними, а також безліч інструментів. Проте, «ARMOR» створений для того, аби точно і швидко вражати. Що стосується **інтеграції** з іншими системами, респондент відзначає

наміри команди інтегруватися з виробниками озброєння. Зокрема, вже є попередні домовленості з виробниками автоматизованих турелей та НРК.

Інтерфейс оновленої версії ГРК «Броня» («ARMOR») – наразі в роботі. Джерело: надано Олексієм Гавришем.

Говорячи про **виклики**, співрозмовник зазначає два найбільш актуальні: юридично-правовий і технічний. Перший – це відсутність чіткого роадмапу в контексті проходження процесу кодифікації: «З точки зору виробника ПЗ, не зрозуміло, які саме кроки потрібно зробити, і який алгоритм пройти. Немає чітко побудованого, зрозумілого процесу кодифікації ПЗ». [Слід, однак, зазначити внесення змін до Постанови КМУ № 234 від 31 січня цього року (див. с. 49) – ред.]

Другий виклик пов'язаний із тим, що після проходження кодифікації має бути сформована потреба (за ідеальних обставин), проте сьогодні такого механізму, який би гарантував виробнику наявність потреби, не існує. Тому, перед розробниками, зі слів Олексія, стоїть питання: «[я]ким чином залишитись корисним державі і вижити в умовах проекту, отримати фінансування та підтримувати розвиток продукту?». Найбільшою **потребою**, з його точки зору, сьогодні є чітко визначений алгоритм кодифікації та отримання замовлень: «[р]озробник має знати, що йому треба зібрати такий-то пакет документів і пройти такі-то процедури в такому-то порядку».

На завершення цієї розмови, Олексій формулює свою ключову **тезу**:

«Єдиний шанс для України встояти у війни – це, по-перше, впроваджувати асиметричні дії, а по-друге, – те, що називається «continuous innovations» [з англ. – безперервні інновації – ред.]. Бо коли ти щось винайшов, то мусиш це дуже швидко розвивати, адже ворог швидко пристосовується до твоєї інновації, знаходячи протидію, копіюючи ідею і швидко масштабуючи.

Тому, перша задача – це знайти цю інновацію, а друга – не зупиняючись її розвивати. І це можливо виключно за умов сталої підтримки зі сторони держави. Такою має бути стратегія».

GRISELDA[243]

У розмові про систему «Griselda» респондентом виступив співзасновник системи Дмитро Шамрай. Він розповідає, що команда розпочала створення системи на початку повномасштабної війни на базі Київської ВЦА, де був командний центр, допомагаючи з вирішенням задач, зокрема, обробкою повідомлень від громадян. Повідомлення, які тоді надходили, наприклад, через додаток «єВорог», «[...] були неструктурованими, було важко визначити їхню достовірність», – говорить Дмитро, – «[...] тому згодом, ми почали використовувати «більш аналітичні» інструменти».[244]

Сьогодні, серед користувачів система «Griselda» знана як автоматизована система нейронної обробки даних. Система працює на всіх **рівнях** і може бути використана як для десіжен-мейкерів, так і для цілевказання. Щодо **інструментарію**, то «Griselda» здатна обробляти будь-які дані – це і є її характерною властивістю, адже вона створювалась як агрегатор даних з метою подальшого їх перетворення на інформацію та передачі доступу, – пояснює Дмитро. Тобто, основний **функціонал** системи зосереджений в площині агрегації та обробки даних дуже широкого діапазону – і типів, і кількості.

«Тут важливо мати великий потік даних – поєднувати HUMINT з SIGINTом та знімками з космічної розвідки», – говорить Дмитро. (Наприклад, «DELTA» з цією метою віддала всі інформаційні потоки, зазначає співрозмовник.) Він пояснює, що в рамках такої роботи, дуже важливо поєднувати **дані** з різних джерел. Зокрема, команда «Griselda» працює з різними OSINT командами, які надають OSINT дані для подальшої обробки.

Слід зазначити, що команда представляє свою розробку як «систему систем» (англ. – System of systems, SoS, – див. Глосарій). Тож «Griselda» включає також внутрішні **інструменти**, наприклад, такі як «G-Radar» та «G-Sensors». Вони створені на основі ядра «Griselda» для агрегації даних з контрбатарейних радарів та передачі даних в ІКС «DELTA» та інші військові системи.

В цьому контексті, одна з проблем, за словами Дмитра, полягає в тому, що сьогодні приходиться мати справу з радарами «усіх часів та усіх країн», а вони є дуже

---

[243] Інформація, наведена в цій частині дослідження, структурована автором на основі отриманих відповідей респондента – Дмитра Шамрая, співзасновника системи «Griselda», під час проведеного з ним інтерв'ю. Джерела, використані додатково, позначені окремо.

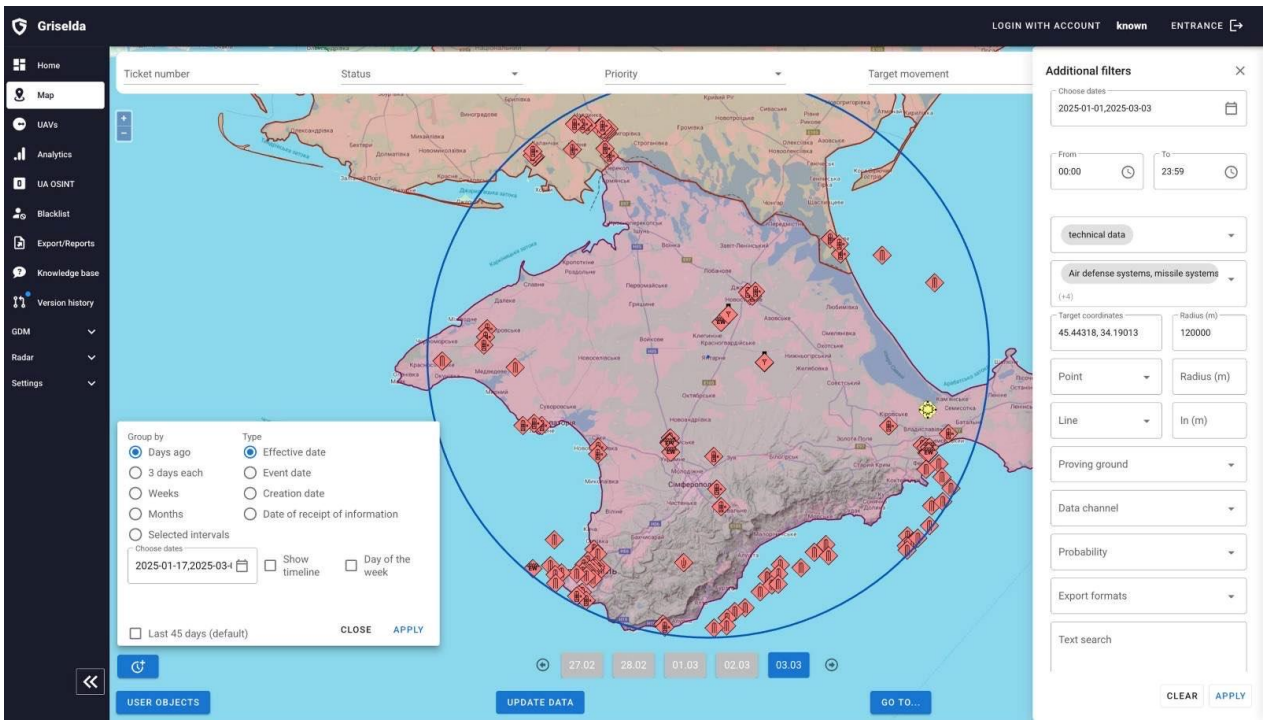
[244] Детальніше – в інтерв'ю Олексія Теплухіна, співзасновника системи «Griselda»: Богдан Машай, «Що таке Griselda. Як нова українська розробка змінює правила війни – велике інтерв'ю», *NV*, 5 листопада 2024. <https://nv.ua/ukr/ukraine/events/shtuchniy-intelekt-na-viyni-rozrobnik-sistemi-griselda-rozpoviv-yak-it-tehnologiji-zminyuyut-viynu-50463391.html> [Переглянуто 2025 21 04].

«різношерстними». Наприклад, систему «Karma» (розроблена на основі «Griselda», в експлуатації з січня 2024 р.) співрозмовник називає «чистим SIGINTом». Система зарекомендувала себе як надзвичайно ефективне рішення: за оцінкою розробників, вона дозволила підвищити кількість знищених ворожих артилерійських розрахунків втричі.

Окрім цього, командою створено закриті системи для різних підрозділів, які здатні обробляти потоки даних незалежно від команди розробників «Griselda». Тобто, в такому випадку, команда не має доступу до чутливої інформації, яка обробляється всередині підрозділу у закритому циклі, – пояснює Дмитро.

Респондент зазначає, що «Griselda» тісно співпрацює з іншими системами [на різних етапах роботи, зокрема на етапі використання даних – ред.]. Зокрема, «Griselda» **інтегрована** з ІКС «DELTA», а також «Кропивою», ГРК «ARMOR» та американською «ATAK».

Окрім розробки софтверної складової, команда також «інвестувала» у навчальну компоненту. Сьогодні «Griselda» вже розробила власну систему навчання та має власну школу. За словами респондента, користувачі відзначають, що цій системі характерний один з найкращих інтерфейсів. Загалом, це рішення можна назвати дуже «юзер-френдлі»: за 2 години можна навчитися оперувати системою.



Інтерфейс «Griselda». Зображено синтетичні, згенеровані події. Джерело: надано Дмитром Шамраєм.

Також необхідно підкреслити, що одна з концепцій «Griselda» – це можливість створювати рішення, які виконують певні задачі. Співрозмовник наводить один з прикладів: беручи участь у військових навчаннях в Польщі «FEX24», команда створила рішення за заданими параметрами всього за 3 дні, що є безпрецедентним результатом. «Серед конкурентів до цього навіть і близько ніхто не наблизився», – розповідає Дмитро.

Наразі, «Griselda» знаходиться **на шляху** до кодифікації. До слова, складність проходження процесу кодифікації респондент відзначає як один з найбільш релевантних **викликів** станом на сьогодні.

«Софтверні продукти важко кодифікувати, важко завести під державне замовлення – це ніби «порочне коло», де одне тягне за собою інше», – говорить Дмитро. Він пояснює, що кодифікація сьогодні відбувається за наявності програмно-апаратного комплексу – а це означає, що розробникам необхідно створити серверну складову, тобто поставляти «коробочну» компоненту. Відповідно, для цього потрібні значні кошти на закупку серверів, а в такому разі йдеться про «суми у мільярдах», за словами респондента. Водночас, необхідно розуміти, що маленькі команди (якою і є команда «Griselda») не мають лобізму, як не мають і великого майданчику для адміністрування роботи (на відміну від таких СПЗ, як скажімо, ІКС «DELTA»).

Також, респондент вказує на необхідність отримання грошового забезпечення – адже переважна більшість команд будувались як волонтерські. «Це все великий труд, і працювати необхідно виключно на фултаймі – очевидно, що робота на парттаймі зменшує ефективність команди», – аргументує співрозмовник. [В березні 2025 р., після опитування респондента, стало відомо про те, що команді «Griselda» вдалося залучити інвестиції та отримати грантове фінансування з допомогою фонду Double Tap Investments[245] – ред.]

В рамках питання **інтероперабельності** СПЗ в цілому, Дмитро вказує на проблему великої кількості систем, якими вимушений користуватися боєць одночасно: «[з]араз як? В одній руці у мене «DELTA», в іншій «Термінал», в правій кишені – «Очі», а в лівій – планшет з «Віражем»». Водночас, він наголошує на тому, що якраз-таки однією з місій команди «Griselda» і системи в цілому і є поєднання всіх систем в одну екосистему, тобто, інтеграція.

[245] Олександр Кузьменко, «Український розвідувальний ШІ-стартап Griselda з допомогою фонду Double Tap Investments залучив $600 000 інвестицій», *dev.ua*, 7 березня 2025. <https://dev.ua/news/600k-dlia-griselda-1741334724> [Переглянуто 2025 20 04].

До слова, говорячи про стан справ у партнерів (країн-членів НАТО) в розрізі інтероперабельності, респондент згадує доктрину JISR (див. с. 36), якою керуються країни-партнери, прагнучи вирішити проблему браку міжсистемної взаємодії. «Вони розуміють, що міждоменні системи не поєднані, і «відпадає» загальна картинка», – зазначає співрозмовник. Втім, говорячи про системи країн-членів НАТО, потрібно пам'ятати і про те, що всі вони створювались «в пісочниці», тобто, в лабораторних умовах, але не мали фактичного застосування у реальній війні.

На завершення розмови, Дмитро формулює свою основну **тезу** наступним чином:

«Держава має більш системно допомагати таким продуктам, хоча б у дослідному використанні. Не можна покладатися на одну систему, яка нібито може закрити всі проблеми. Завжди має бути варіант Б, мають бути інші, дублюючі системи. Покладатися на одну технологію – це занадто ризиковано».

ІКС «DELTA»[246]

Розмова з підполковником ЗСУ Артемом Мартиненком, архітектором ІКС «DELTA», починається з окреслення «великої картинки» та ролі ІКС «DELTA» в ній. «Війна – це складний комплексний процес, а «DELTA» є інструментом у цьому процесі», – говорить Артем. «Всі звикли до мапи, але «DELTA» – це давно вже не мапа, а екосистема продуктів, яка покликана забезпечити роботу різних напрямків», – пояснює співрозмовник.

Станом на сьогодні, це дійсно ціла **екосистема продуктів**, що об'єднує декілька модулів та інструментів, серед яких: модуль **Monitor** – система ситуаційної обізнаності за стандартами НАТО (також у версії мобільного застосунку Monitor Mobile); система **«Вежа»** (див. детальніший опис на с. 93-96) – модуль оперативної взаємодії, дешифрування трансляцій та статистики польотів БпАК (модуль **Tube**, стрімінговий інструмент для безпілотних систем та стаціонарних камер, функціонував до злиття із системою «Вежа»); **Mission Control** – матриця синхронізацій для планування польотних місій; захищений чат **Element** (також у версії мобільного застосунку); модуль **Target Hub**; хмарне сховище **Nextcloud** – аналог Google Drive.[247] [За генеральним задумом команди розробників, всі елементи екосистеми мають працювати у взаємодії – ред.]

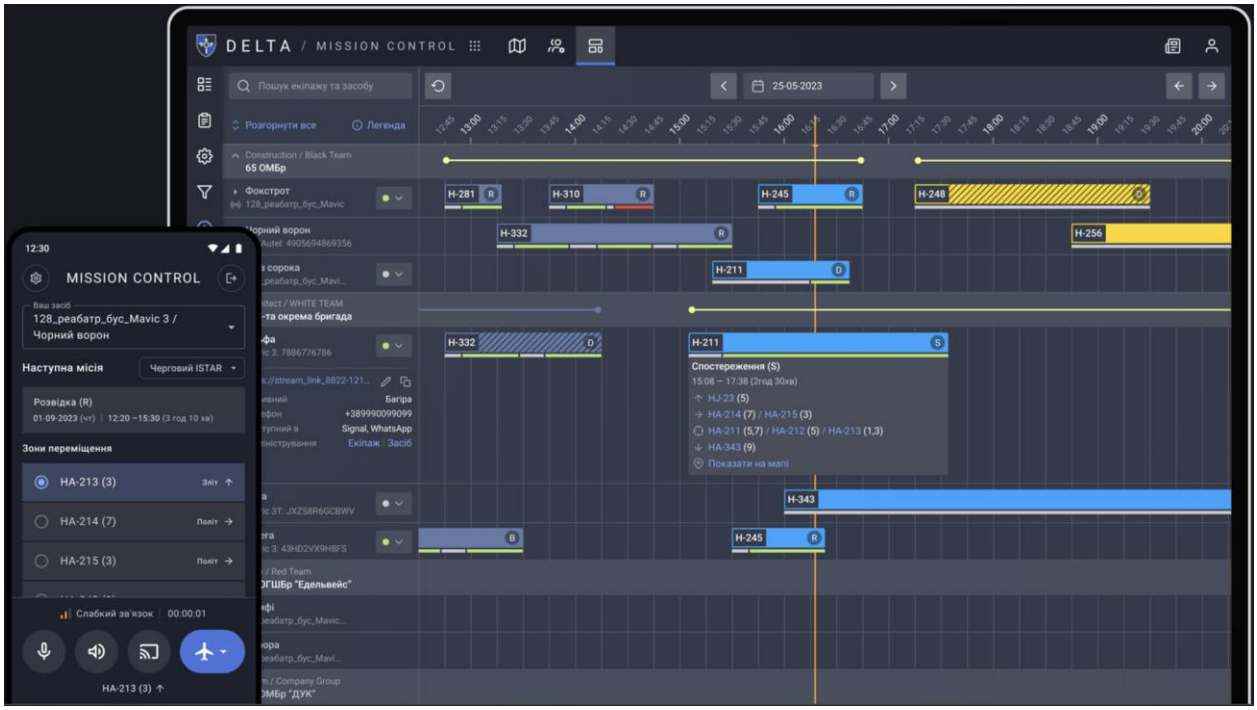
Можна стверджувати, що серед систем українського походження ІКС «DELTA» займає свого роду особливе місце, чому є декілька причин[248], одна з яких, безсумнівно, – підтвердження **взаємосумісності** з рядом ІТ-систем країн-членів НАТО, що за потреби дозволяє обмінюватись даними з партнерами в режимі реального часу[249].

Та насамперед, унікальність «DELTA» полягає в доведеній нею спроможності інтегрувати безпрецедентно велику кількість **даних**, що походять з різного роду джерел[250]. Підполковник Ярослав Гончар, голова ГО «Аеророзвідка», спільноти ти організації, яка свого часу виступила носієм ідеї та одним з ключових ініціаторів створення та

[246] Інформація, наведена в цій частині дослідження, структурована автором на основі отриманих відповідей респондента – Артема Мартиненка, архітектора ІКС «DELTA» під час проведеного з ним інтерв'ю. Джерела, використані додатково, позначені окремо.
[247] За відгуками користувача ІКС «DELTA», військового СОУ.
[248] Там само.
[249] «Що таке система DELTA і як вона задає тренди для країн НАТО?», Міністерство оборони України: 30 березня 2024. <https://mod.gov.ua/news/shho-take-sistema-delta-i-yak-vona-zadae-trendi> [Переглянуто 2025 24 04].
[250] За відгуками користувача ІКС «DELTA», військового СОУ.

впровадження системи «DELTA», називає її найбільшим, станом на сьогодні, джерелом знань для військового.[251]

Самих джерел даних також безліч. Респондент пояснює, що оскільки «DELTA» створювалась як інтеграційна платформа, її задачі першочергово включають забезпечення інтеграції, а також сприяння процесу прийняття рішень та мінімізацію людського фактору. Так, даними в роботі системи можуть служити як дані від БпЛА [в режимі реального часу – ред.], так і текстові файли, дані з супутникових джерел, радарів тощо [в тому числі, дані, отримані від інших систем – ред.].



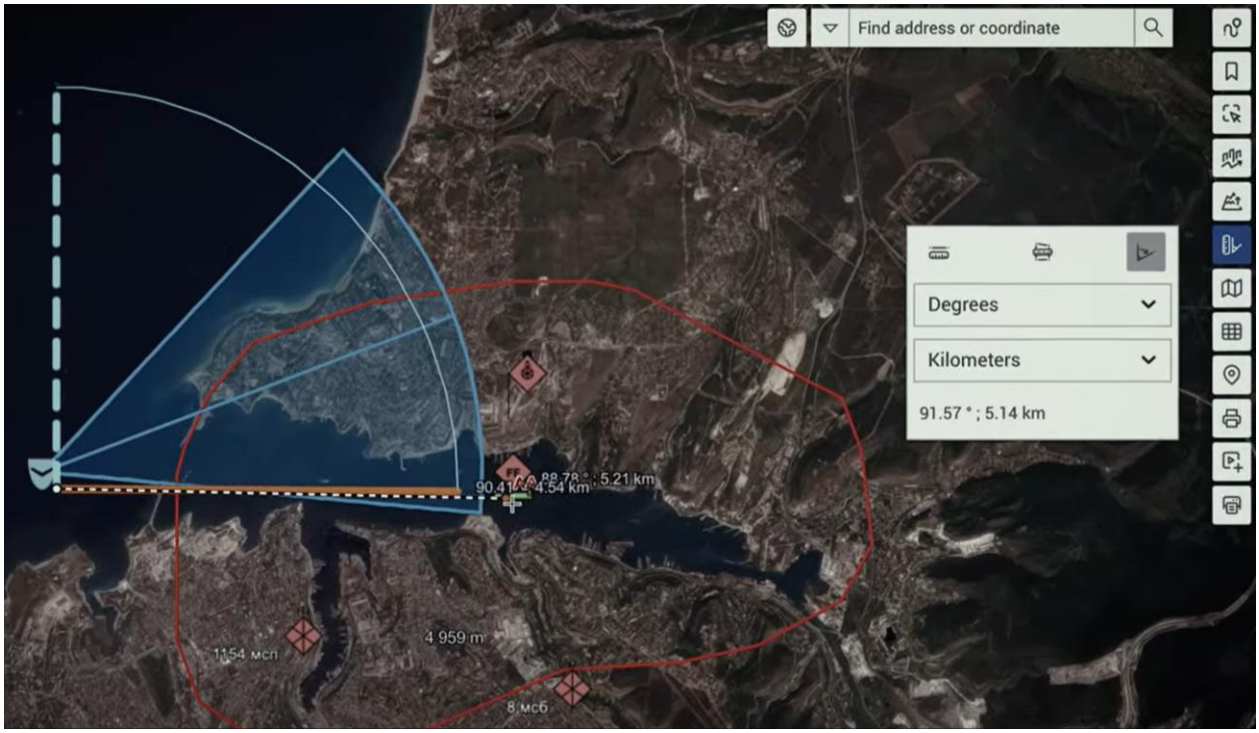
Інтерфейс Mission Control, одного з модулів ІКС «DELTA», що використовується для планування польотних місій. Джерело: DOU.

Як вже зазначалось, до **функціонала** ІКС «DELTA» сьогодні відносять не лише забезпечення ситуаційної обізнаності [основний, первинно закладений в неї функціонал – ред.], але й елементи управління військами [функції, що додались з часом у відповідь на запити війни – ред.]. (Еко)системою в цілому та окремими її модулями та/або інструментами активно користуються буквально в усіх **родах і видах військ** ЗСУ та інших формуваннях

[251] Тася Мельник, «Військовий софт Delta тепер офіційно у ЗСУ. Він допомагав у всіх великих операціях – від потоплення «Москви» до звільнення Зміїного. Чому з ним воювати швидше», *Forbes Ukraine*: 04 лютого 2023. <https://forbes.ua/innovations/twitter-dlya-zsu-viyskoviy-soft-delta-dopomagav-u-vsikh-velikikh-operatsiyakh-vid-potoplennya-moskvi-do-zvilnennya-zmiinogo-chomu-z-nim-zsu-voyuyut-shvidshe-07122022-10318> [Переглянуто 2025 24 04].

СОУ: найбільше – на тактичному та оперативному **рівнях** (скрізь і на щоденній основі), найменше – на стратегічному. Сьогодні ІКС «DELTA» налічує десятки тисяч користувачів.[252]

Респондент також додає, що з одного боку, можна було би назвати такі роди і види військ, які повністю побудували свою роботу на «DELTA». З іншого боку, є і такі, в яких «DELTA» «перекриває» лише деякі з функцій, наприклад, вогневу підтримку. «Чи є зараз у «DELTA» повний набір інструментів, який задовільняв би потреби всіх родів і видів військ? Наразі ні. Проте, основа є для всіх», – стверджує респондент.



Інтерфейс одного з модулів ІКС «DELTA». Джерело: Міністерство оборони України.

[Говорячи про **інструментарій**, який надає «DELTA», слід розуміти, що сьогодні він є значно розширеним в порівнянні навіть з версією ІКС до 2022 р., коли «DELTA» передусім сприймалася як цифрова мапа. Це спричинено нарощуванням функціоналу – великою кількістю та різноманітністю інтегрованих в ІКС модулів та інструментів. Зазвичай, говорячи про «DELTA», мають на увазі інформаційну платформу, що здатна акумулювати великі обсяги даних, відображаючи СОР (див. с. 27) і надаючи тим самим ситуаційну обізнаність (див. с. 29-30) всім залученим а́кторам тої чи іншої ділянки фронту. В цілому, для розуміння того, чим є ІКС «DELTA», достатньо знати, що вона є інструментом ISTAR (див. с. 34-40) – ред.].

[252] *Militarnyi*, 5 лютого 2023.

Зокрема, інструменти системи реалізують такий ланцюг взаємодії: підрозділи ISTAR збирають всі наявні первинні дані з усіх наявних джерел (повідомлення від інформаторів, дані з автоматизованих джерел (чат-ботів та інших інформаційних систем), супутникові знімки, дані аеророзвідки, радарів, дані з кіберпростору тощо) → надалі різні а́ктори сектору безпеки та оборони наносять інформацію в «DELTA», накладаючи її «шарами» на цифрову мапу, а інструменти системи приводять її до стандартизованого, придатного до «прочитання» вигляду, унеможливлюючи варіації трактувань цієї інформації (об'єкт на мапі, як-то, зразок ОВТ, є саме тим об'єктом, який було нанесено на мапу, і не може бути трактований ніяк інакше) → наявна інформація об'єктивно відображається на цифровій мапі в режимі наближеного до реального часу і є доступною для інших а́кторів, що потребують ситуаційної обізнаності на полі бою.[253]

Те, що етап збору інформації в цьому ланцюзі беруть на себе підрозділи ISTAR, дозволяє вивільнити час для аналітичної роботи розвідки та аналітиків, як пояснює Гончар.[254] [Під «аналітичною роботою» тут маються на увазі підпроцеси «обробка» та «використання» – див. Фігуру 7 на с. 36 – ред.].

Будучи практичним багатофункційним інструментом у веденні війни, що триває, «DELTA» **інтегрована** з багатьма СПЗ, серед яких «Віраж», «Кропива», «Графіт», а також американський «АТАК»[255]. За словами респондента, нещодавню інтеграцію з системою «Вежа» слід вважати некласичним прикладом інтеграції, адже «Вежа» стала «інтегрованою внутрішньо». Співрозмовник пояснює, що у цьому випадку, йдеться не про окремий продукт «ззовні», а елемент екосистеми всередині, що значно підсилює систему в цілому. Зазвичай, «класичний варіант» передбачає інтеграцію двох самостійних систем, що функціонують окремо.

За його словами, «Вежа» в процесі свого розвитку відштовхувалась від того, що стріми несуть в собі корисну інформацію, яка потребує обробки, а саме, логування даних та їх подальшого аналізу. Загалом, в цьому контексті, цікавий не стрімінг як такий, а дані, які можна отримати з нього. Власне, «Вежа» і є тою системою, що надає результати аналізу стрімінгу. «Те, що відбувається в ріалтаймі, і те, що дешифрує оператор, – ці всі дані відразу потрапляють на шари мап», – пояснює респондент, додаючи, що «DELTA» передбачає також інший модуль, який відповідає за застосування засобів. Окрім цього, функція

[253] Там само.
[254] Там само.
[255] За відгуками користувача ІКС «DELTA», військового СОУ.

оновлення статусів місії дозволяє зрозуміти, чи місія почалась, чи вже завершена – це було реалізовано завдяки можливості бачити дії оператора у модулі «Вежа».

Слід зазначити, що влітку 2024 р. для команди «DELTA», а також, експертної та користувацької спільнот в широкому сенсі відбулося декілька знакових подій.[256] По-перше, йдеться про отримання в липні 2024 р. **експертного висновку КСЗІ**, чому передував шлях тривалістю в декілька місяців, включно із роботою з аудиторами,[257] причому, сертифікацію було отримано за стандартами НАТО.[258] ІКС «DELTA» першою з українських систем проходила процес побудови КСЗІ за експериментальною процедурою, в основі якої – американський стандарт NIST 800-53[259].

Команда відзначає виконання Постанови КМУ № 139 як ще одну віхову подію у розвитку ІКС «DELTA», адже серед іншого, це означає зняття заборони з побудови ІКС з КСЗІ в хмарі за кордоном[260]– йдеться про розміщення системи на хмарних ресурсах та/або в центрах обробки даних (ЦОД), розташованих на території держав-членів НАТО[261].

По-друге, в серпні того ж року ЦІРОТ МОУ було визначено розпорядником, а ІКС «DELTA» введено в дослідну **експлуатацію**.[262] (Зокрема, відтепер ДСК інформацію може бути внесено в систему легально.)

[Серед інших оновлень також вартує згадати зусилля команди з впровадження підходу MDM, Mobile Device Management (див. Глосарій), що є важливим в контексті розвитку галузі в цілому – ред.]. MDM, який по суті своїй є захищеним середовищем на гаджеті військового, виконує функцію додаткового рівня безпеки, надаючи доступ до каталогу закритих військових застосунків: контролюється лише «військове» середовище користувача, а його особисте середовище лишається недоступним для будь-якого роду дій ззовні.[263] Зокрема,

---

[256] З непублічної онлайн лекції (2).
[257] Там само.
[258] «В Україні вперше перевірили кібербезпеку бойової системи за стандартами рівня НАТО», Міністерство оборони України: 17 липня 2024. <https://mod.gov.ua/news/v-ukrayini-vpershe-perevirili-kiberbezpeku-bojovoyi-sistemi-za-standartami-rivnya-nato> [Переглянуто 2025 24 04].
[259] Eleonora Burdina, ««Ми почали будувати захищену екосистему для всіх військових застосунків». Архітектор DELTA — про розвиток системи», *DOU*: 11 липня 2024. <https://dou.ua/lenta/interviews/delta-challenges-and-plans/?fbclid=IwZXh0bgNhZW0CMTAAAR3eDaW_UIFPnAOKu4qjNHw7ShMuN1478z_XOH3mMpyWgDindHie3C9878s_aem_6JTNM5d4JFoU59zXZq9tyg> [Переглянуто 2025 24 04].
[260] Там само.
[261] Постанова КМУ № 139 від 4 лютого 2023 «Деякі питання підвищення рівня цифровізації сил безпеки та сил оборони України у період воєнного стану». <https://zakon.rada.gov.ua/laws/show/139-2023-%D0%BF#Text> [Переглянуто 2025 24 04].
[262] З непублічної онлайн лекції (2).
[263] З непублічної онлайн лекції (2).

в разі втрати гаджету, адміністратором дистанційно може бути активовано видалення усього, «[…] що стосувалося військового захищеного контейнера».[264]

Станом на сьогодні, ІКС «DELTA» є однією з тих небагатьох СПЗ, що функціонують в інтересах СОУ, приносячи вагомі результати на полі бою та в стратегічному значенні ведення війни, маючи при цьому дуже розвинутий безпековий контур.[265] Команда постійно працює над вдосконаленням політики безпеки та захисту користувачів.[266] [В українському контексті, команду «DELTA» можна назвати численною. Наразі команда володіє необхідними ресурсами для імплементації задач з поліпшення безпеки – ред.]

Високий рівень безпеки гарантує декілька факторів, зокрема: a) розміщення в хмарному середовищі; b) використання FIDO2 – фізичного ключа безпеки (криптографічного токену) для багатофакторної автентифікації в системі, який вважається стійким до фішингових атак завдяки асиметричній криптографії, – за словами керівника напрямку ІТ ГО «Аеророзвідка» Руслана Прилипка[267]; c) наявність власної служби верифікації та підтримки; d) наявність власної команди безпеки (англ. – SOC, Security Operations Center), що включає програмний захист та перевірку на людський фактор); e) регулярне проведення PENTEST (тесту на проникнення) союзниками, що дозволяє виявити критичні вразливості ІКС під час тестування[268].

Говорячи про **виклики** – як галузі в цілому, так і ті, що є актуальними саме для команди, – співрозмовник пропонує розбити їх на 3 умовні групи. До першої він відносить виклики технологічні, тобто такі, що пов'язані із запитами користувачів та «[…] функційністю, про яку вони просять». Для команди «DELTA» викликом є власне оброблка цих запитів, адже велика кількість користувачів означає велику кількість їхніх запитів. Окрім цього, ще одним викликом респондент називає наявність певних відмінностей між вміннями користувачів, оскільки підрозділи володіють спроможностями різного рівня: хтось лише починає робити початкові кроки (у застосуванні системи), а комусь вже час «[…] давати в руки скальпель».

До другої групи респондент відносить виклики у правовому полі. За його словами, зараз існують ніби дві паралельні реальності, «[…] які доводиться мирити між собою». В одній, головною задачею є забезпечення роботи підрозділів «тут і зараз», а питання, які

[264] Burdina.
[265] За відгуками користувача ІКС «DELTA», військового СОУ.
[266] Там само.
[267] Ольга Карпенко, ««Аеророзвідка» роздасть безкоштовні ключі безпеки військовим-користувачам Delta», *AIN*: 24 березня, 2023. <https://ain.ua/2023/03/24/aerorozvidka-2/> [Переглянуто 2025 24 04].
[268] З непублічної онлайн лекції (2).

необхідно вирішувати – це «що робити зараз, щоб відповідати на виклики війни вчасно?». Водночас, в іншій реальності ключовою задачею вважається забезпечення правової сторони («забезпечення паперової безпеки»), і тут треба, аби все було, так би мовити, «згідно-відповідно». Наприклад, навіть в контексті побудови КСЗІ, за словами Артема, розробник має розуміти, що існує т.зв. «православне КСЗІ» і «людське КСЗІ», з якими прийдеться так чи інакше стикатися. [Мається на увазі, що перше поняття відповідає застарілій процедурі, створеній 20-30 років тому[269], чию актуальність по факту втрачено, але яка лишається офіційно затвердженою процедурою – ред.].

Як пояснює він, в цьому полі, виклик полягає у вмінні поєднувати дві реальності, ув'язуючи те, «[...] що відбувається насправді, із тим, як це описує вся наша «нормативка» і «регуляторка»». Втім, нинішню ситуацію респондент оцінює позитивно як результат вагомих позитивних змін.

Третя група – це виклики безпекові. На думку респондента, некоректно було би трактувати безпеку як стан. «Безпека – це процес постійний, це змагання», – говорить Артем, пояснюючи, що в цій площині виклики виникають постійно, отже, і побудова відповідей на ці виклики є безперервним тривалим процесом.

В рамках питання про **інтероперабельність** як характеристку стану галузі, респондент звертає увагу на те, що брак міжсистемної взаємодії є основною, але не єдиною проблемою на тлі утвореного т.зв. «зоопарку софтів». Іншим вагомим проблемним питанням, на яке респондент звертає особливу увагу, є безпека, актуальність якої знаходить прояв у таких питаннях, як, скажімо, зберігання військовими даних в приватній, а не державній системі: «[т]ут має вимальовуватися певна політика, і цим має займатися Міністерство оборони».

«Як такий «зоопарк софтів» є проблемою настільки, наскільки ми контролюємо ситуацію і розуміємо куди йдуть дані. У «ребівця» може бути своя система, у операторів БпЛА – своя, і це абсолютно прийнятно, без питань, спеціалізовані софти – це ОК [див. с. 57-61 – ред.]», – аргументує співрозмовник, додаючи, що при цьому, вкрай важливо, аби «[...] всі вони працювали в загальній екосистемі». Ситуація, в якій системи є ізольованими одна від одної, не можна назвати сприятливою у безпековому сенсі.

[269] Burdina.

На завершення розмови, респондент акцентує на двох основних, з його точки зору, викликах, на яких слід **зосередити увагу**, а саме:

перше - правовому регулюванні; друге – вирішенні питань взаємосумісності систем.

ВЕЖА[270]

В розмові про особливості системи «Вежа» респондентом виступив один з її розробників. Він розповів, що для команди «Вежа» робота почалась у 2022 р. з ідентифікації проблеми, що на той час вже «назріла» – а саме, необхідності облаштування системи обліку величезної кількості стрімів. Зокрема, така потреба була актуальною на рівні роботи батальйону БпЛА. Респондент пояснює, що на тому етапі, команда зробила спробу інтегруватися із системою «Очі», яка вже працювала на той час як стрімінгова платформа для корегування вогню, та інтеграція не відбулась, і команда «Вежа» почала втілювати у реальність свої задуми самостійно.

Система працює на фронті з лютого 2023 р., а з грудня того ж року «Вежа» вийшла у виробництво. Незабаром розпочався і процес інтеграції «Вежі» з ІКС «DELTA». [Інтеграцію було завершено у вересні 2024 р. – станом на сьогодні, «Вежа» є модулем відео аналізу поля бою – одним з декількох елементів екосистеми ІКС «DELTA» – ред.]. Наразі сигнали координації можуть «лягати» на певний шар в ІКС «DELTA» (див. також с. 88-89).

«Вежа» – це система стрімінгу і дешифрування відео, що здійснюються на основі **даних** з візуальних джерел (відеоспостереження). Зокрема, система дозволяє вирішувати питання взаємодії підрозділів під час розвідки та ураження. Окрім цього, вона має певні аналітичні інструменти, що дозволяє проводити AAR [і саме це відрізняє її від подібних систем даної категорії, що обмежуються однією лише стрімінговою функцією – ред.].

Що стосується **функціоналу** в цілому, то систему «Вежа» [до слова, як і ІКС «DELTA» – ред.] можна вважати такою, що є на межі систем ситуаційної обізнаності і систем управління військами.[271] **Інструментарій** «Вежі» дозволяє, по-перше, зробити зріз ситуації по різних ділянках фронту на основі зібраної та агрегованої інформації. По-друге, ці дані надалі можуть бути використані для прийняття рішень в рамках військового задуму.

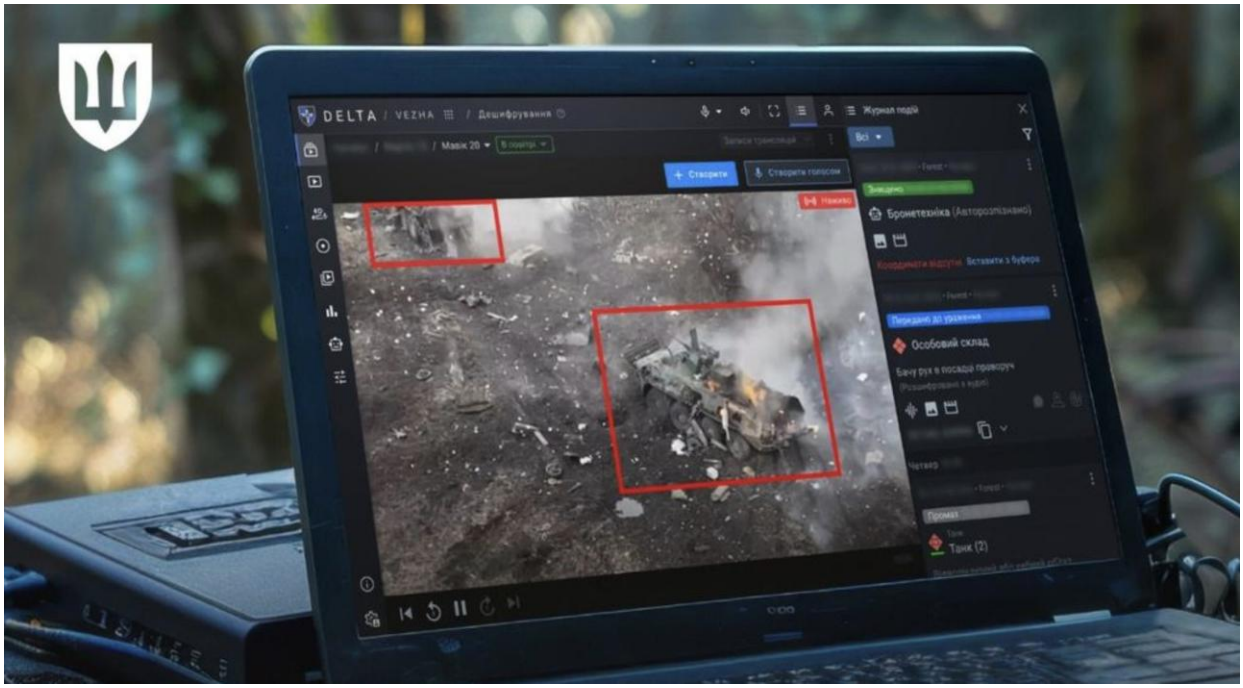
Говорячи про **рівні**, на яких система використовується, розробник зазначає, що в роботі «Вежі» один той самий стрім може виконувати різні функції на різних рівнях. Адже, на його думку, поняття тактичного та оперативного рівнів сьогодні є дещо розмитим. «Скажімо, на рівні бригади, це може бути елементом умовного контролю виконання

[270] Інформація, наведена в цій частині дослідження, структурована автором на основі отриманих відповідей респондента, одного із розробників системи «Вежа», під час проведеного з ним інтерв'ю. Джерела, використані додатково, позначені окремо.
[271] З особистої розмови з фахівцем МОУ.

операції – процесом, що також називається «командирським спостереженням»», – говорить співрозмовник.

На більш конкретному кейзі, це виглядає наступним чином. Під час бою, для отримання повноти інформації і прийняття рішень, командири мають бачити бій в режимі реального часу, тобто, «[...] бачити і лівий, і правий фланг, і центр, – по яких має вестися спостереження в ріалтаймі», – пояснює респондент. Тож фактично, «Вежа» не лише забезпечує поле бою елементами ситуаційної обізнаності, але й уможливлює процеси управління військами.

Стріми використовуються для розвідки, спостереження та рекогностування [що сукупно є процесом ISR, див. с. 34-40 – ред.]. Компонента Target Acquisition (TA) була закладена у функціонал системи згодом – це означає, що об'єкт можна позначити як «уражений», «обстріляний», «невлучений» тощо, таким чином визначивши його статус для цілевказання, як пояснює розробник. [Тобто, із впровадженням компоненти TA, «Вежа», як і «DELTA», стає інструментом процесу розвідки, або ж ISTAR (див. с. 34-40) – ред.]. В свою чергу, результат процесів розвідки за допомогою таких інструментів як «Вежа» та ІКС «DELTA» уможливлює інші процеси, такі як корегування вогню.



Інтерфейс платформи відеоаналізу поля бою «VEZHA», інтегрованої в ІКС «DELTA». Джерело: Міністерство оборони України.

Окрім цього, респондент розповідає, що «Вежа» також є **інструментом** оцінки ефективності формувань, таких як рота, батальйон, ОУВ, ОСУВ. Засоби системи дозволяють вивести дані на дашборди для подальшого аналізу роботи.

Що стосується **взаємосумісності та інтеграції** з іншими системами, то окрім вже завершеного процесу інтеграції з ІКС «DELTA», «Вежа» також інтегрована з системами «Неон» [див. с. 60-61 – ред.] та «Промінь» [див. с. 57 – ред.]. (Останню, за словами співрозмовника, можна з більшою вірогідністю віднести до систем стратегічного рівня.)

Зі слів розробника, сьогодні головне прагнення команди – це прийти до так званої «data-driven» армії. Тому, за стратегічний напрямок команда визначила рух у бік підвищення автоматизації процесів. Наразі, більшість процесів відбувається вручну через брак достатньої кількості кваліфікованих спеціалістів. Наприклад, зараз, на кожні 24 години відео вдається видати по 5 сигналів розвід.інформації.

Говорячи про **проблематику** галузі в цілому, респондент акцентує на питанні каналів і способів комунікації. Оскільки говорити по рації – небезпечно, доводиться залучати такі цивільні інструменти комунікації як Discord та Google Meet. (Як описує ситуацію співрозмовник, «[...] у нас війна зараз йде на Гуглміті».) Також, він розповідає, що в певний момент з'явилась необхідність створювати ситуаційні кімнати, в яких військові могли би дивитися кілька стрімів одночасно, а дешифрувальники паралельно виконувати свою роботу.

Окрім цього, архіважливим елементом, на думку респондента, є горизонтальна взаємодія, тобто, комунікація і взаємодія між безпосередніми сусідами. Це можуть бути різні підрозділи різних родів військ ЗСУ та спеціальних служб, які працюють поруч один з одним територіально. Ця ланка є ключовою, але, станом на сьогодні, злагоджена горизонтальна взаємодія лишається ціллю, якої треба прагнути.

Не менш вагомим питанням постає «легалізація» СПЗ, зокрема, таких систем як «Вежа». (Віховими подіями в т.зв. «легалізації» можна вважати отримання експертного висновку КСЗІ та постановку на озброєння.) Наразі «Вежа» знаходиться **на шляху** до отримання КСЗІ.

Що стосується найбільш актуальних **викликів**, респондент озвучив наступні два. Перший, на його думку, пов'язаний з рівнем підготовки о/с, зокрема у розвідці та артилерії. Він зазначає, що наразі офіцери не володіють практичними навичками користування подібними продуктами.

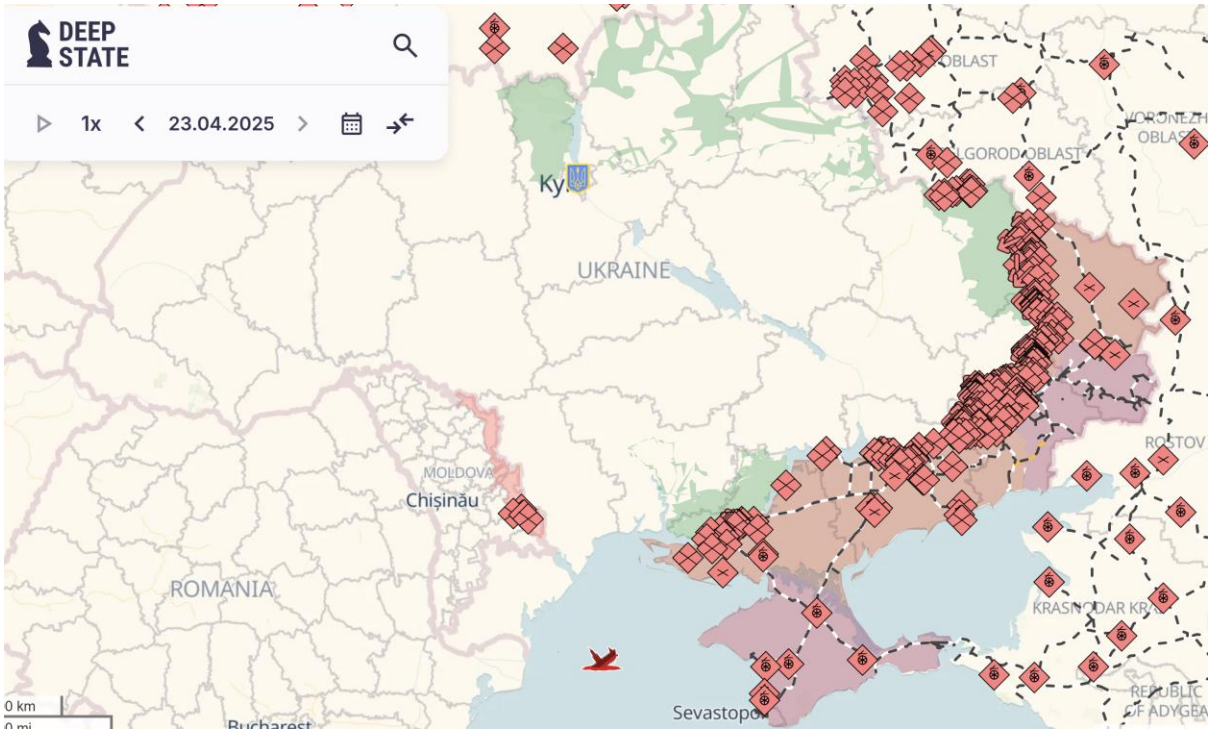
Другий виклик є більш глобальним: на його думку, сьогодні сама структура СОУ не відображає і не передбачає змін характеру війни, в якій аналітично-інформаційне забезпечення вже стало ключовим. Респондент пояснює, що в «ідеальному світі», мало би відбутися реформування системи, що забезпечило би появу повноцінних інформаційно-аналітичних підрозділів, з аналітиками і дешифрувальниками, яких не прийшлося би буквально «видирати» з інших посад, як це відбувається зараз.

«Інструмент ми створили, але ще не навчили армію ним користуватися»,

– цією **тезою** співрозмовник підсумовує розмову, акцентуючи на необхідності надання практичних навичок користування СПЗ у війську, в тому числі, такими як «Вежа».

KOLOSSAL[272]

Система «KOLOSSAL» ймовірно, не є такою відомою на загал, як її творці – команда DeepState, яка створила і на постійній основі веде оновлення в інтерактивній онлайн мапі бойових дій, що відображає зміни лінії фронту з найвищою у світі, станом на сьогодні, точністю. Розробники зазначають [273], що «KOLOSSAL», ще один проект команди, було створено як платформу, яка агрегуватиме та оброблятиме великі обсяги OSINT даних. Слід зазначити, що частково, «KOLOSSAL» вже зараз застосовується в цілях ведення інтерактивної мапи DeepStateMap.live[274].



Оновлення інтерактивної мапи станом на 23.04.2025. Джерело: DeepState.

Респондентом в цьому інтерв'ю виступив Руслан Микула, співзасновник проектів «DeepState» і «KOLOSSAL». Він розповідає, що по суті, «KOLOSSAL» є веб-додатком, який служить **інструментом** збору та обробки OSINT даних, які представляють певну цінність [та можуть бути перетворені на інформацію, в подальшому використану в інтересах СОУ – ред.].

[272] Інформація, наведена в цій частині дослідження, структурована автором на основі отриманих відповідей респондента – Руслана Микули, одного із розробників системи «KOLOSSAL» команди DeepState, під час проведеного з ним інтерв'ю. Джерела, використані додатково, позначені окремо.
[273] "Project "Kolossal", DeepState. <https://kolossal.deepstateua.tech/> [Переглянуто 2025 24 04].
[274] DeepState Map. <https://deepstatemap.live/#6/49.4383200/32.0526800> [Переглянуто 2025 24 04].

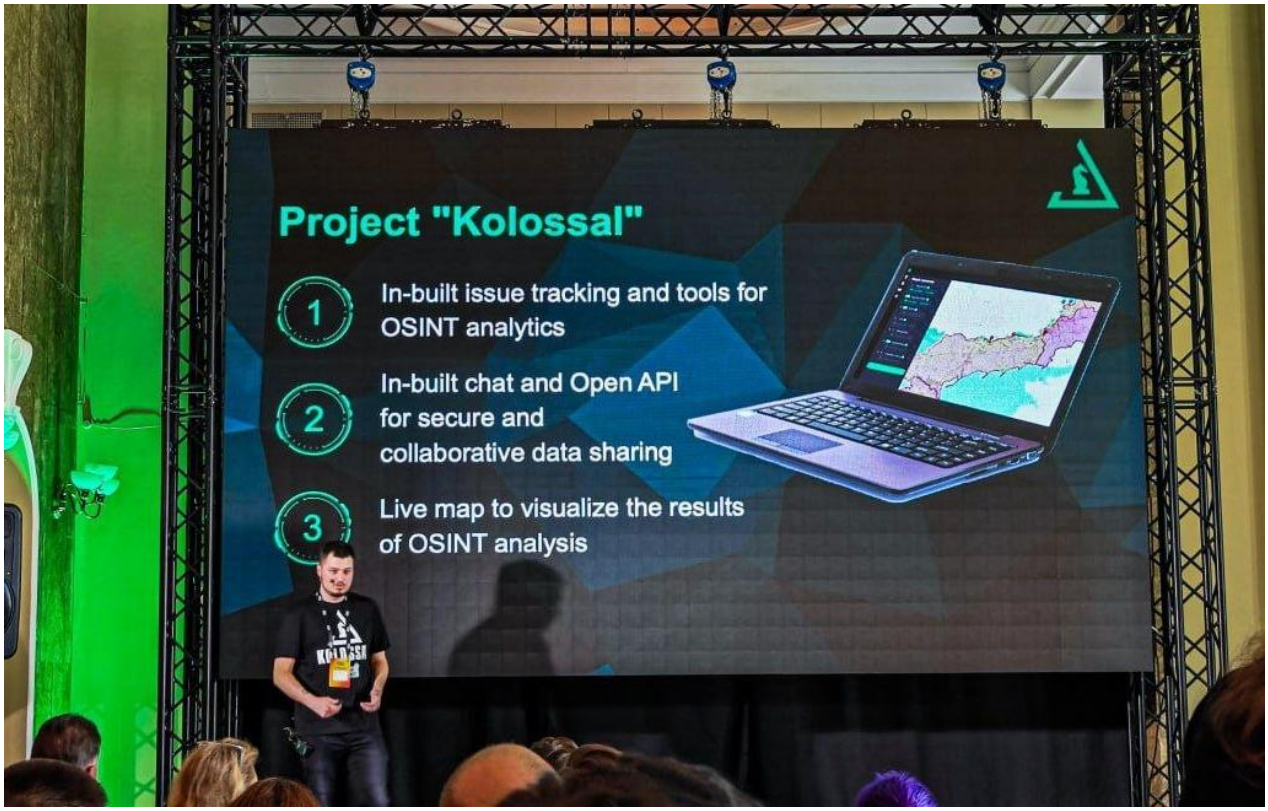
Зокрема, такими **даними** є інформація про розташування ворожих позицій та об'єктів, наприклад, інформація з соц.мереж (фото і відео), візуалізація ворожих чи дружніх уражень (фото і відео, зібрані з каналів, що налічують від декількох до мільйонів підписників), а також, загальнодоступні супутникові знімки, джерела з геоприв'язкою, дані з ворожих чатів тощо. Кінцевим результатом збору та обробки цих даних є надання ситуаційної обізнаності військовим, суб'єктам поля бою, що і можна вважати основною **функцією** додатку «KOLOSSAL». [Як відзначив розробник в одному з інтерв'ю для медіа, головною метою системи є створення пулу «[п]остійних користувачів (військових насамперед)», в якому можна було би бачити оновлення за будь-якої потреби[275] – ред.]

Руслан наводить приклад функціонування системи на одному з конкретних кейзів: «Скажімо, система збирає дані про ЛЕП та інженерно-фортифікаційні споруди. Часом буває так, що посадка вже по факту заросла, але ми встигли нанести лінії фортифікаційних споруд, і тому, військові бачать [завдяки системі – ред.], що вони там є, хоч зараз через зарості цього фактично і не видно». [Інший приклад, який можна навести, – це здійснення «гелокації подій»: військові звертаються із запитом на кшталт «по нам бив танк, скажіть звідки це було», – тоді команда «геолокує подію» та надає такі дані військовим[276] – ред.]

Окрім цього, платформа дозволяє військовим бачити, які підрозділи і як саме працюють, що є особливо актуальним для тих підрозділів, які тільки нещодавно зайшли на позиції. Руслан пояснює, що буває й так, що ворог фільмує штурм бою, демонструючи, як йому вдається штурмувати українські позиції. Подібні відео використовуються у навчальних цілях.

Станом на сьогодні, «KOLOSSAL» проходить **стадії** розробки і закрите тестування – це означає, що систему тестують військові. За словами респондента, окрім цього, військові залучені безпосередньо і до процесів розробки. Загалом, команда активно використовує свої досвід і експертизу в комунікаціях з військовими СОУ. Наразі «KOLOSSAL» готується до проходження процесів кодифікації. Стосовно **інтеграції** з іншими системами, Руслан зазначає, що станом на сьогодні, повноцінних інтеграцій ще немає, проте, в короткострокових планах передбачена інтеграція з ІКС «DELTA».

[275] Олексій Дзюба, ««ІТ може допомогти, але виграти війну за допомогою ІТ неможливо». Інтерв'ю з розробником найпопулярнішої в Україні карти бойових дій DeepState», *dev.ua*: 13 грудня 2023. <https://dev.ua/news/it-mozhe-dopomohty-ale-vyhraty-viinu-za-dopomohoiu-it-nemozhlyvo-interviu-iz-rozrobnykom-naipopuliarnishoi-v-ukraini-karty-boiovykh-dii-deepstate> [Переглянуто 2025 24 04].
[276] Там само.



Команда «Deep State» презентує систему «KOLOSSAL» на Lviv IT Arena у 2023 р. Джерело: @Deepstate_UA

Говорячи про **виклики**, з якими команда стикалась на особистому досвіді, респондент називає основні два. Перший – це втрата фахівців через недолугі систему мобілізації і впроваджені підходи. Другим викликом він зазначає бюрократію війська в цілому, як явище.

Щодо другого фактору, то Руслан пояснює детальніше: «[в] армії, на будь-якій з її ланок, від батальйону до рівня МОУ, завжди є такі «агресивно-консервативні» люди, які противляться будь-яким змінам, не сприймають діджиталізацію як таку». Він зазначає, що цей фактор має особливе значення в контексті змін характеру війни: «[с]таном на серпень 2022 р. йшлося про одні задачі, потім, на початку 2023 р. війна почала змінюватися, а зараз вже йде процес рефакторингу продукту – бо відтоді, як ми почали працювати, війна змінилась, а будь-якому продукту треба вміти бути гнучким в умовах війни».

Окрім цього, на питання про стан галузі в розрізі **інтероперабельності**, респондент відповідає, що за його оцінкою, так званий «зоопарк софтів» сьогодні дійсно існує. На його думку, маємо справу з дублюванням деяких стрімінгових систем: «[н]априклад, є «Очі» і є «Вежа» – хтось працює в одній, хтось в іншій системі, і це часом створює проблеми».

До того ж, співрозмовник вважає, що ситуацію ускладнюють і такі випадки, коли виробники хардверної оборонної продукції займаються розробкою окремого ПЗ «під себе». [Наприклад, компанія розробляє БпЛА типу «крило», а під нього створює своє софтверне рішення (mission planner) – ред.]. Як наслідок, збільшується кількість таких рішень-елементів екосистем, що не є інтегрованими, а часом, і сумісними з іншими рішеннями.

На завершення розмови, Руслан наводить **тезу**, яку хотів би донести до читачів:

«Автоматизація і діджиталізація у війську – це наші союзники. Люди, які протистоять цим процесам, є шкідниками, бо це те, що рятує життя. Це те, що наближає перемогу. Важливо, щоб ці люди, які чинять спротив, не впливали на ці процеси».

III. Частина третя. Актуальні проблеми і виклики.

Серед питань, обговорених в рамках інтерв'ю з респондентами, розробниками та засновниками систем, йшлося про поточні проблеми та виклики як галузі в цілому, так і в контексті окремих команд. Також, було зазначено ряд проблемних питань, які, не будучи «органічними» питаннями галузі, так чи інакше чинять прямий вплив на розвиток систем і команд, впровадження систем у війська та їхнє застосування тощо (як-то, питання щодо структури СОУ, ролі держави у розвитку галузі, освіти, політик врегулювання галузі тощо).

В *частині третій (III)* представлено результати аналізу найбільш релевантних проблем і викликів, озвучених респондентами під час інтерв'ю. Додатково, до аналізу було включено коментарі, зібрані в ході консультацій з фахівцями та іншими розробниками, а також дані з відкритих джерел. Зібрані дані було опрацьовано і згруповано у **13 груп проблемних питань/викликів**, кожну з яких представлено окремо в цій частині роботи. Наступна частина роботи (див. *Висновки та рекомендації*) надає рекомендації з огляду на виокремлені найбільш релевантні виклики та проблеми.

***

1. Виклики в правовій площині (архаїчність поточної нормативно-правової бази).

Найбільше уваги співрозмовники приділили висвітленню питань, що лежать в правовій площині. Аналіз зібраних в ході розмов даних дозволяє припустити, що питання цієї групи слід розцінювати як найбільш критичні станом на сьогодні.

Переважна більшість співрозмовників відзначили **складність проходження процесу кодифікації** (наприклад, див. с. 83). Зокрема, Гавриш звернув увагу на **відсутність чіткого роадмапу**, який давав би розуміння алгоритму дій (див. с. 79). Окрім цього, він пояснив, що викликом також є відсутність механізму, який надавав би розробнику гарантію того, що після кодифікування системи потребу буде сформовано, а слідом за нею – отримано держ.замовлення.

Однак, слід розуміти, що ці та інші виклики радше є наслідками більш глобальної і комплексної проблеми, коріння якої слід шукати у тому, що **вирішення поточних задач відбувається за умов дії чинної застарілої нормативно-правової бази**.

Зокрема, цю тему розкрив архітектор ІКС «DELTA», говорячи про те, що наразі одночасно доводиться працювати і над забезпеченням роботи СОУ «тут і зараз», і займатися «забезпеченням паперової безпеки» (див. с. 91). Наприклад, за його словами,

сьогодні вже існує напрацьований «людський» механізм побудови КСЗІ, що враховує реалії сьогодення (на базі експериментальної постанови КМУ № 139), проте, все-таки офіційно діючою лишається процедура, яку було затверджено пару десятиліть тому, і яка є ускладненою та громіздкою, особливо, в умовах повномасштабної війни. В цілому, як пояснив Мартиненко, для розробників бойових систем виклик полягає в тому, щоби весь час **балансувати між об'єктивною реальністю з її задачами та викликами поля бою,** – з одного боку, **та застарілою нормативно-правовою базою,** – з іншого.

На думку розробника системи «Неон», при поточному законодавстві, можна вважати, що українська галузь знаходиться у «напівкам'яній» добі в розрізі використання технологій[277]. Відзначивши певні зрушення у спрощенні роботи в площині ДСК інформації, він однак, зауважив, що наразі **Україна не може інтегруватися з партнерами** через «[...] поточну **архаїчність «нормативки» та взаємосумісності рівней класифікації (категорованості) систем**»[278].

Також, засновник системи «Comintify» (нині – частина системи «Стрибо») вказав на хибність самих **підходів до ведення розробок та введення систем в експлуатацію**[279]. Він пояснив, що сьогодні, «[в]есь світ розробляє софт по аджайлу», а це означає приблизно такий ланцюг подій: «[м]аємо ідею → треба провалідувати, чи гіпотеза працює → знайшли MVP[280] → знайшли користувачів, які кажуть, що саме треба покращити → таким чином проводимо сотні ітерацій, часто розвертаючись в процесі на 180 градусів».[281] В результаті, як пояснив він, часто кінцевий продукт може значно відрізнятися від оригінального задуму розробників, але при цьому, він є затребуваним та ефективним, адже здатен відповісти на запити користувачів.[282]

Натомість, за словами розробника, в Україні «легальний» спосіб введення системи в експлуатацію сьогодні виглядає наступним чином: «[д]ля того, щоби знайти замовника, треба прийти до командування (а це означає, умовно, до Командувача сухопутних військ) і сказати «будь моїм формальним замовником», потім складається ТТЗ, потім КСЗІ,... і в результаті, ти три роки займаєшся папірцями, потім закінчується війна, і зрештою виявляється, що твій софт нікому не потрібен. Таким шляхом, як це прописано в нашому законодавстві, ми витрачаємо багато років, а на виході отримуємо «Дзвін», який по факту,

[277] З особистої розмови з розробником системи «Неон».
[278] Там само.
[279] З особистої розмови із засновником системи «Comintify».
[280] Minimum viable product (мінімально життєздатний продукт).
[281] З особистої розмови із засновником системи «Comintify».
[282] Там само.

виявляється нікому не потрібним»[283]. Співрозмовник пояснив, що оптимальним варіантом був би такий алгоритм кроків, за яким виробник мав би звертатися безпосередньо до військової частини, а наступні свої кроки робив би з урахуванням запитів і потреб безпосередніх користувачів[284].

Тож парадокс наразі полягає в тому, що з одного боку, в Україні є провідні технології – а це унікальні рішення, створені українськими розробниками, які дають значущі результати на полі бою, – а з іншого боку, – нормативно-правова база, що ці рішення врегульовує, тягне за собою розвиток галузі на кілька десятиліть назад в минуле.

Комплексно поточну ситуацію в законодавчій площині роз'яснила Інна Гончар, керівниця напрямку «Управління знаннями» ГО «Аеророзвідка». Річ у тім, що історично, в Україні розробки велися у фреймворку т.зв. ДКР-ів, або дослідно-конструкторських робіт, які були покликані втілити задум створення ЄАСУ, Єдиної автоматизованої системи управління, [285] описаної в НДР «Акація» (прийнята ще в 2013 році). Всього, можна налічити понад 50 ДКР, які ведуться або велись в ЗСУ протягом останніх десяти років[286]. З них, абсолютна більшість зрештою виявилися вкрай низькоефективними, через що їх було призупинено на різних етапах виконання робіт.[287]

При цьому, важливо відзначити, що в межах концепту ЄАСУ було закладено поняття програмно-апаратного рішення – «[...] це коли ти про хмару навіть і не думаєш, на апараті здійснюєш обробку, а потім і розповсюдження інформації», – пояснила Гончар[288]. Відповідно, всі розробки, що велися в рамках ДКР («Дзвін», «Радник» тощо) лежать в площині програмно-апаратного рішення.[289] Тож станом на сьогодні, за словами Гончар, маємо ситуацію, в якій старі стандарти (ГОСТи) не скасовані, нові стандарти ще не введені, і водночас, архаїчний конструкт під назвою «НДДКР»[290] все ще має силу.[291]

---

[283] Там само.
[284] Там само.
[285] Детальніше: Олександр Пастухов, «АСУ Збройних сил», *Militarnyi*: 20 березня 2012. <https://mil.in.ua/uk/d0-b0-d1-81-d1-83-d0-b7-d0-b1-d1-80-d0-be-d0-b9-d0-bd-d0-b8-d1-85-d1-81-d0-b8-d0-bb/> [Переглянуто 2025 24 04].
[286] З особистої розмови з Інною Гончар, керівницею напрямку «Управління знаннями» ГО «Аеророзвідка».
[287] Пастухов.
[288] З особистої розмови з Інною Гончар.
[289] Там само.
[290] Див. Скорочення.
[291] З особистої розмови з Інною Гончар.

Більш того, необхідно розуміти, що свого часу, в основу існуючого процесу управління було закладено платформоцентричну концепцію застосування військ (сил)[292] (див. с. 31-34) і на ній же побудовано нормативну базу, яка є діючою і понині. Натомість, ведення війни сьогодні відбувається за мережецентричними підходами (див. с. 30-34). Тобто, **і управлінська модель, і законодавство передбачають платформоцентричність**, і як наслідок, – побудову СПЗ у фреймворку програмно-апаратних рішень, а **поточна війна диктує впровадження мережецентричних підходів**, в тому числі, – створення хмарних рішень. Фактично, в цьому дисонансі і полягає головний виклик.

За словами Гончар, це призвело до свого роду **«поляризації»**, адже можна стверджувати, що сьогодні «новий полюс» співіснує зі «старим», який чинить спротив новій системі та об'єктивній реальності[293].

«Новий полюс» формує навколо себе прийняття нових правових актів для унормування СПЗ – зокрема, йдеться про Закон про хмарні послуги[294], а також експериментальну Постанову КМУ від 04 лютого 2023 р. № 139,[295] що дала поштовх для побудови КСЗІ за іншою процедурою (американський стандарт NIST 800-53, який використовують західні партнери).[296] (Зокрема, таким шляхом експертний висновок КСЗІ отримала ІКС «DELTA» – див. с. 89). Тобто, йдеться про побудову нового юридичного поля згідно нових практик. Та допоки існуватимуть «подвійні нормативно-правові акти» у вигляді ГОСТів та постанов одночасно, галузь не зможе функціонувати належним чином, а ефективність найсучасніших передових технологій та бойових систем лишатиметься обмеженою.

Що стосується класифікації **СПЗ як складової ОВТ** на законодавчому рівні (див. с. 49), то можна стверджувати, що на момент написання цієї роботи, реальних значимих (позитивних) зрушень для розробників СПЗ у зв'язку зі змінами до Постанови КМУ № 234 не спостерігається.

2. Ригідність (негнучкість) структури СОУ.

В даному контексті, під «ригідністю» мається на увазі негнучкість і неспроможність системи впроваджувати необхідні зміни під впливом вагомих зовнішніх факторів, таких як

[292] «Щодо стану і перспектив розвитку розробок інформаційно-комунікаційних систем для потреб ЗСУ», складено експертами Громадської спілки «Фонд підтримки реформ в Україні» (непублічний звіт, надано Інною Гончар).
[293] З особистої розмови з Інною Гончар.
[294] Закон України «Про хмарні послуги», 2023. <https://zakon.rada.gov.ua/laws/show/2075-20#Text> [Переглянуто 2025 24 04].
[295] Постанова КМУ № 139.
[296] З особистої розмови з Інною Гончар.

ведення повномасштабної війни у фазі активних бойових дій. Як зазначили співрозмовники, ригідність властива як окремим інституціям СОУ, так і десіжен-мейкерам на різних рівнях. Також, йдеться про «заскорузлість» мислення на рівні вищого військового керівництва, що відображається на розвитку оборонного сектору в цілому, в тому числі, стану галузі СПЗ, і як наслідок, – результатах на полі бою.

Зокрема, одна з проблем полягає в тому, що оригінально закладена (в радянські часи) і нереформована належним чином **структура СОУ не включає і не передбачає постійних змін характеру війни** – фактору, що є ключовим в нинішній російсько-українській війні, яку можна вважати мережецентричною (див. с. 30-34). Як було аргументовано в *частині першій (I)*, мережецентричність, серед іншого, означає, що аналітично-інформаційне забезпечення сторін відіграє вирішальну роль. Тому, для зміщення балансу сил на користь України в розрізі володіння ситуаційною (інформаційною) перевагою, необхідним є перегляд ролі аналітично-інформаційної складової у веденні війни та впровадження оновлених підходів. Зокрема, розробник системи «Вежа» вказав на **необхідність інтеграції в структуру СОУ повноцінних інформаційно-аналітичних підрозділів** з офіційними посадами аналітиків і дешифрувальників з визначеними обов'язками (див. с. 96).

Цей аспект також було порушено в розмові з розробником системи «Неон»[297], який зазначив, що **аналітична робота у війську наразі відбувається здебільшого позаштатно**, адже аналітично-інформаційна елемента як така не передбачена в принципі. Окрім цього, він пояснив, що помітні зміни відбулись зі зміною військового командування[298]: «[м]и вимушені були розвернутися на 180 градусів, і сьогодні відбиваємося від поточної системи, а не від ворога»[299].

Розробник «KOLOSSAL» Микула зазначив фактор негативного впливу десіжен-мейкерів, що свідомо **перешкоджають процесам автоматизації і цифровізації** у війську (див. с. 99-100). Йдеться про **відторгнення** (навіть на ментальному рівні) **інновацій** як таких, що включають, серед іншого, інструменти автоматизації певних процесів з метою мінімізації людського фактору та збільшення ефективності опрацювання надвеликих обсягів даних. Як відзначив Микула, будь-якому продукту, який працює в інтересах СОУ,

[297] З особистої розмови з розробником системи «Неон».
[298] Мається на увазі зміна Головнокомандувача ЗСУ в лютому 2024 р. та інші, пов'язані з нею, призначення.
[299] З особистої розмови з розробником системи «Неон».

необхідно бути гнучким і здатним вчасно реагувати на зміни характеру війни. Так само, гнучкості і швидкості реагування потребує сама структура СОУ та окремі її елементи.

В цьому контексті, засновник системи «Comintify» також зазначив, що наразі, «[в]се що робиться – робиться всупереч, а не завдяки».[300] «Вся державна машина, і ЗСУ як структура, в першу чергу, дуже **ворожа до автоматизації**», – відзначив він. На думку розробника, за ідеальних умов, інноваціями мав би займатись приватний сектор – «[...] люди, які вмотивовані, які знають, як це робити»[301]. Втім, команди, які реалізують приватні ініціативи, часто стикаються з тим, що «[н]а ентузіазмі можуть зробити якусь першу версію, а далі їхній продукт підпадає під «парасольку» якогось генерала», а тоді вже розробка стає політичною історією», – пояснив співрозмовник.[302]

Спостереженнями поділився також співрозробник VR-фільму «Перший бій». З його досвіду (і точки зору військового), першим викликом є **прояв низової ініціативи**; другим він назвав донесення важливості **залучення людей різних дисциплін знань до роботи над розвитком інновацій у війську**[303]. Кирилів відзначив, що у війську зараз з'явилося «[...] дуже багато різних людей з різних сфер, зокрема, мобілізованих», – і тому, до командування необхідно донести розуміння того, що їхню цінність треба використати на повну».[304] Він підкреслив, що вкрай важливою є **міждисциплінарність** – адже для бачення «загальної картинки» необхідна координація експертів різних галузей, напрямків і рівнів, а натомість, на думку розробника, «[...] в армії зазвичай працює тунельне мислення, бачення «великої картинки» відсутнє»[305].

3. **Низький рівень військової освіти (підготовка фахівців; володіння необхідними навичками).**

Як зазначили декілька співрозмовників, сьогодні на практиці доводиться стикатися із тим, що **офіцери, не маючи достатнього рівня знань та навичок**, не можуть володіти у повній мірі інструментами, тобто, СПЗ. Розробник «ComBat Vision» відзначив **нестачу підготовлених фахівців зв'язку в ЗСУ**, що є викликом як для війська, так і для галузі в цілому, а у випадку «ComBat», – також і блокером широкому впровадженню системи у війська (див. с. 71). Розробник системи «Вежа» також звернув увагу на **недостатній рівень**

[300] З особистої розмови із засновником системи «Comintify».
[301] Там само.
[302] Там само.
[303] З особистої розмови з Віталієм Кирилівим, співрозробником VR-фільму «Перший бій».
[304] Там само.
[305] Там само.

підготовки офіцерів у розвідці та артилерії, що перешкоджає повноцінному користуванню продуктами, створеними для війська (див. с. 95).

Також, декілька співрозмовників вказали на **архаїчність самих навчальних закладів і освітніх** програм, що слід сприймати як вагомий виклик. При наявності в Україні цілих (спеціалізованих) інститутів, навчання в них відбувається за **давно застарілими програмами**, – за словами Інни Гончар, керівниці напрямку «Управління знаннями» ГО «Аеророзвідка».[306] Зокрема, досі навчають **на застарілій радянській зброї**, – зазначив Кирилів,[307] – незважаючи на той факт, що на полі бою вже давно інтегровані найсучасніші зразки західного озброєння, і навчання мало би включати опанування цих зразків ОВТ. На його думку, **змін потребують також навчальні центри і самі принципи та підходи до навчання**: «[т]реба навчати бізнес скілам, лідерству, проджект менеджменту, треба вводити бізнес спеціалістів у війська»[308].

Слід підкреслити, що ті навчальні програми і курси, які сьогодні надають бійцям практичні навички, зокрема в розрізі користування ПЗ, є приватними ініціативами, наприклад, «Victory Drones», школа «Боривітер», курси фонду «Повернись Живим», ГО «Аеророзвідка» тощо. (Виключенням можна вважати програми і курси, проведені за участі вищих військових навчальних закладів – як приклад, вперше в Україні проведений курс із застосування TLP та ІКС «DELTA» для викладачів військових закладів, що відбувся на базі Військової академії Одеси[309]).

4. Слабке технологічне забезпечення підрозділів СОУ.

В ході розмов було зазначено, що недостатнє (а часом і майже відсутнє) технологічне забезпечення підрозділів СОУ не дозволяє реалізувати повноцінне користування системами. Найбільше уваги цій темі, з усіх опитаних респондентів та співрозмовників, приділив розробник «ComBat Vision».

Одним з найбільш критичних питань Максименко назвав **ігнорування державою потреби в «цифровізації» піхотинця** (див. с. 71-72). Серед іншого, йдеться про потребу в мобільному живленні гаджетів (планшетів та рацій) для забезпечення їхньої постійної активності. Без можливості живити їх просто «в полі» і «на ходу», втрачає сенс не лише

[306] З особистої розмови з Інною Гончар.
[307] З особистої розмови з Віталієм Кирилівим.
[308] Там само.
[309] ГО «Аеророзвідка». <https://www.facebook.com/aerorozvidka/videos/997603335605070> [Переглянуто 2025 24 04].

наявність самих гаджетів, але й більшість створених систем (в тому числі, й ті, про які йдеться в даній роботі). Станом на сьогодні, розробок подібної продукції, яка би забезпечила постійну активність гаджетів, в Україні не ведеться. Цю проблему Максименко відносить до більш масштабної категорії викликів, яку називає **відсутністю інфраструктури зв'язку**, що значно ускладнює впровадження СПЗ у війська в цілому.

Також він пояснив, що підрозділи, які не мають належного технологічного забезпечення, – а такими, як правило, є лінійні підрозділи (ТрО, СВ, інші роди військ), – **лишаються поза користувацькою аудиторією** таких систем як «ComBat Vision». Як наслідок, деякі продукти сьогодні доступні лише для підрозділів СОУ, забезпечених необхідною технікою.

5. Фінансування.

В контексті фінансування команд, що уможливлює їхнє існування як таких, слід зауважити, що абсолютна більшість команд створювалась і понині функціонує суто як волонтерські ініціативи (деякі – впродовж 10-12 років). Зазвичай, йдеться про команду ентузіастів, об'єднаних ідеєю створення ефективних рішень для війська, яку розробники реалізують за рахунок власних ресурсів – часу та коштів. **Задачі із залучення зовнішніх фінансових ресурсів** у вигляді одноразових грантів, коштів донорів та/або інвестицій лягає на плечі самих розробників. За подібним принципом функціонує більшість українських команд розробників сьогодні. Виключення становлять одиниці.

Наразі, фінансова підтримка з боку держави таких проектів обмежується разовими (і невеликими в масштабах потреб) грантами за умов перемоги на тематичних хакатонах (наприклад, Brave 1, який є державною ініціативою Міністерства цифрової інформації). Втім, йдеться саме про гранти, а не системне фінансування. Адже гранти, надані державою у спосіб, реалізований Міністерством цифрової трансформації, не є сталою програмною реалізацією потреби ГШ ЗСУ та МОУ.

Зокрема, про **необхідність в більш системній фінансовій підтримці з боку держави** згадував Шамрай, один з розробників «Griselda», зокрема говорячи про підтримку у дослідному використанні (див. с. 83-84). Його колега, співзасновник системи «Griselda» Олексій Теплухін, в спілкуванні з медіа також зазначив, що команда не залучала фінансування від держави, і загалом, розвиток команди і самих продуктів відбувається паралельно з державою[310]. «Це неправильно, тому що неможливо будувати оборону

[310] Машай.

країни, якщо в тебе залежить якась ділянка твоєї оборони від волонтерської команди, яка тобі не підпорядковується, з якою в тебе немає стосунків»,[311] – аргументує Теплухін.

6. Інвестиційні виклики.

Окремо вартує висвітлити питання інвестицій в галузь СПЗ. Під час інтерв'ю та консультацій це питання було порушено лише побіжно. Втім, з додаткових джерел та попереднього спілкування з респондентами можна скласти уявлення про поточну ситуацію.

З інвестиційної точки зору, галузь СПЗ сьогодні не можна назвати такою, що є привабливою, особливо в порівнянні з іншими оборонними галузями. Цьому може бути декілька причин, з яких найбільш явними слід назвати наступні дві. По-перше, інвестори, як українські, так і іноземні, **радше інвестують в хард рішення** – адже умовний БпЛА приносить наочні, очевидні навіть для неекспертної аудиторії, результати на полі бою. В очах інвестора, софтверне рішення зазвичай не має цього ефекту, незважаючи на те, що зазвичай, саме воно уможливлює роботу роботизованих систем та реалізує процеси обробки і використання даних.

По-друге, іноземних інвесторів відштовхує **незрозумілий механізм «легалізації» СПЗ** в Україні: шлях від ідеї до введення системи в експлуатацію виглядає невизначеним і непрозорим (по суті, і будучи таким), особливо, враховуючи невелику кількість «історій успіху» в українському контексті. Невизначеності також додають багатошарові проблеми в правовій площині (див. п. 1).

Також, дивлячись на питання залучення інвестицій з точки зору розробника, слід сказати, що самих можливостей виходу на контакт з потенційними інвесторами загалом значно менше, ніж в галузях хардверної продукції.

7. Пасивність/відсутність держави в порядку денному галузі.

В цьому контексті, йдеться про брак залученості державних а́кторів у розвиток галузі в цілому або повну її відсутність у вирішенні питань, які потребують залученості. Здебільшого, **розвиток систем сьогодні відбувається ізольовано від держави**, що є абсурдним, адже стан фронту залежить у значній мірі від ефективності впровадження і застосування рішень на полі бою (див. п. 5).

[311] Там само.

Зокрема, Кирилів відзначив, що держава мала би створювати сприятливі умови для розробників, які демонструють реальні результати роботи у вигляді готових для експлуатації продуктів: **«[н]еобхідно працювати з розробниками, проводити «зріз» аналітики і дивитися, чий продукт працює краще** – звісно, за умов встановленого терміну».[312] Наразі, цього не відбувається, а проведення хакатонів, на його думку, є лише спробою залучити людей до технологій як таких загалом, що не є залученням до самої проблематики[313]. «Далі має бути долучення до бренд-продукту, до «купки» активних людей, які розробляють саме цей продукт, і дають на виході результат», – пояснив розробник[314]. Також, Кирилів зазначив, що на його думку, існує **потреба у створенні координаційного органу**, який об'єднав би потреби військових, цивільних розробників і державу[315].

Протилежною думкою щодо ролі держави в процесі розвитку галузі СПЗ поділився засновник системи «Comintify», зазначивши, що **найбільшою допомогою було би невтручання** – «[...] якби держава припинила вставляти палки в колеса», наприклад, спростивши шлях до офіційних застосувань системи.[316]

8. Безпекові виклики.

Тема безпекових викликів не отримала широкого висвітлення, зокрема, через об'єктивну сенсетивність питань. Проте, можна стверджувати, що всі без виключення команди розробників, з якими вдалося поспілкуватися в рамках дослідження, «інвестують» в безпекову складову своїх систем. Як сформулював визначення поняття безпеки Мартиненко, **безпеку слід усвідомлювати як постійний тривалий процес**, що є свого роду змаганням (див. с. 91). Також, він звернув увагу на **питання зберігання військовими даних** в приватних системах, а не єдиній державній системі (див. також п. 9). Архітектор ІКС «DELTA» пояснив, що в контексті інтероперабельності, **ізольованість систем** створює додаткові безпекові ризики (див с. 91).

Також, увагу на питання кіберскладової звернула Гончар, аргументуючи, що **посилення кіберзахисту** стає критичним в умовах розробки рішень в хмарному середовищі[317].

[312] З особистої розмови з Віталієм Кирилівим.
[313] Там само.
[314] Там само.
[315] Там само.
[316] З особистої розмови із засновником системи «Comintify».
[317] З особистої розмови з Інною Гончар.

9. Брак інтероперабельності систем.

Питання інтероперабельності (в рамках даної роботи відповідає значенню «міжсистемна взаємодія/взаємосумісність») було винесено окремим пунктом під час проведених інтерв'ю та консультацій. Надані відповіді дозволяють підсумувати, що в цілому, відзначаючи наявність такої проблеми, респонденти не вважають її критичною. Втім, слід зазначити деякі аспекти.

По-перше, Максименко відзначив **відсутність яких-небудь визначених стандартів для побудови СПЗ** (див. с. 70). Цей фактор слід розглядати як ключовий, говорячи про міжсистемну взаємодію та подальший розвиток галузі. Станом на сьогодні, впровадження таких стандартів, які би змушували системи «говорити однією мовою» за рахунок підтримки стандартів, форматів та уніфікацій, є першочерговою задачею в розрізі роботи над підвищенням рівня інтероперабельності.

Зокрема, брак інтероперабельності призводить до того, що сьогодні бійцям **доводиться користуватися доволі великою кількістю систем одночасно на різних пристроях,** а це створює доволі вагомі практичні незручності (наприклад, див. с. 83).

По-друге, як зазначив Мартиненко, проблему інтероперабельності слід розглядати в комплексі з іншою – **безпековою проблемою, що виникає на тлі т.зв. «зоопарку софтів»** – великої кількості розрізнених та різних за своїм призначенням систем (див. с. 91). Він пояснив, що «зоопарк софтів» і не був би проблемою за умов вирішення питання зберігання військовими даних та наявності контролю держави над ситуацією. В цьому контексті, важливим критерієм вбачається функціонування систем різної спеціалізації в одній загальній «екосистемі», що і вирішило би питання безпеки. Наразі ж, на думку респондента, вразливістю є те, що **держава не має контролю над джерелами зберігання даних, якими оперує велика кількість (розрізнених) приватних систем**.

Окрім цього, на цікавий аспект вказав Микула, член команди «Deep State». На його думку, **при створенні ПЗ «під себе»**, тобто, під хардверні продукти власної екосистеми, збільшується кількість дезінтегрованих рішень, що за своєю сутністю не покликані підтримувати сумісність з іншими системами поза межами екосистеми (див. с. 100).

10. Технічні виклики.

Серед викликів технічного характеру розробники систем озвучили деякі особливості своєї роботи та функціонування систем. Наприклад, Мартиненко вказав на **потребу опрацювання великої кількості запитів від великої кількості користувачів** (див с. 90).

(Сьогодні користувацька аудиторія ІКС «DELTA» налічує десятки тисяч.) У цьому випадку, такі запити (верифікація, відновлення профілю, додавання нових функцій тощо) здатні обробляти власні служби верифікації та підтримки, а також безпекова команда. Проте, так чи інакше, для вирішення всіх цих задач **потрібні люди, які здатні працювати в режимі 24/7**. Також, слід розуміти, що в менших командах, які складаються не з сотень, а, як правило, 5-10 працівників-волонтерів, питання обробки запитів є набагато актуальнішим.

Окрім цього, Мартиненко відзначив проблему **відмінностей між вміннями користувачів**, викликану тим, що різні підрозділи володіють різними спроможностями (див с. 90). Для одних, інструменти системи є надскладними, для інших – ті самі інструменти в якійсь мірі є пройденим етапом, і тому, виникає потреба в нарощенні більш просунутих функцій.

Ще одним проблемним питанням було зазначено **використання цивільних інструментів комунікації** (наприклад, Discord та Google Meet). Зокрема, про цей аспект згадував розробник «Вежі», пояснюючи, що такі канали зв'язку використовуються як альтернатива передачі інформації по рації (див. с. 95). Окрім цього, розробник «ComBat Vision» наголосив на **надмірній залежності від Starlink** та необхідності пошуку альтернативних рішень, які дозволили би реалізувати тактичний зв'язок для ведення бою (див. с. 71).

Важливий аспект висвітлив Кирилів, пояснивши, що для його команди самим викликом вже є той факт, що **команда складається з військовослужбовців ЗСУ**[318]. Він також звернув на увагу на те, що для багатьох розробників актуальними є **брак знання авторського права, питань інтелектуальної власності, базової «грамотності»,** необхідної для орієнтування в правових питаннях[319]. Наприклад, «[...] є такі інженери, які бояться про свої технології навіть говорити вголос», – зокрема через це, на думку Кирилова, виникає ефект «зоопарку софтів», бо «[...] кожен робить своє»[320].

11. Втрата фахіців через відсутність адекватної мобілізаційної політики.

Питання втрати фахівців через мобілізаційні заходи не було винесено на обговорення окремо, втім, його релевантність є безсумнівною, що підтверджено зворотним зв'язком від

[318] З особистої розмови з Віталієм Кирилівим.
[319] Там само.
[320] Там само.

інших розробників даної галузі. Зокрема, про втрату фахівців нагадав розробник проекту «KOLOSSAL» та член команди «Deep State» (див. с. 99).

Симулякр мобілізаційної системи, який функціонує сьогодні, передбачає широкий діапазон можливостей т.зв. «бронювання» від військової служби для військовозобов'язаних громадян цивільних, не пов'язаних з оборонним сектором професій. Втім, він **не визначає чіткого і легального фреймворку для повноцінної реалізації роботи розробників СПЗ**, які створюють інструменти для щоденної роботи війська.

12. Комплікованість (складність) систем.

В цьому контексті, йдеться про складність користування системами для непросунутого користувача. Можна стверджувати, що наразі вимальовується певний тренд: **системи стають «складними»** – навіть і ті, що колись мали геть простий функціонал, тепер «обросли» великою кількістю нових функцій та інструментів, які треба вміти застосовувати («Кропива» як приклад[321]).

«Хотілось би, щоб система була побудована як «людина Леонардо»[322] – дві руки, дві ноги, – а у нас натомість – багаторукий Шива»,[323] – пояснив фахівець МО. На його думку, в принципі, система може і має виконувати «мільярд функцій», що є прийнятним з точки зору розробника, проте, **з позиції користувача (військового) складність систем є недоліком**, адже «[...] військові люблять, щоб все було просто»[324].

13. Складність впровадження у війська «ексклюзивних» систем.

В цьому випадку, йдеться про складність впровадження деяких систем у війська через ряд об'єктивних та суб'єктивних факторів. Під «ексклюзивністю» мається на увазі наявність в системи комплексу певних характеристик, що роблять її свого роду унікальною, та разом з тим, унеможливлюють її «поголовне» використання військами. Як типовий приклад, в *частині другій II (і)* було наведено детальний опис системи «ComBat Vision» (див. с. 65-72). Фахівець МО також назвав це рішення прикладом «[...] системи з малою реалізацією, але дуже великим потенціалом».[325]

[321] З особистої розмови з фахівцем МОУ.
[322] Мається на увазі «Вітрувіанська людина» Леонардо да Вінчі.
[323] З особистої розмови з з фахівцем МОУ.
[324] Там само.
[325] Там само.

Розробник «ComBat Vision» пояснив, чому система, яка знаходиться в готовому для продуктової експлуатації стані, не може бути введена в експлуатацію, та які фактори перешкоджають цьому (див. с. 71-72). Серед іншого, він назвав: a) **нестачу технологічного забезпечення підрозділів** (див. п. 4), через що наразі користувацька аудиторія «ComBat» фактично зведена до спеціальних підрозділів силових структур та/або підрозділів із сильною технологічною складовою; b) **нестачу підготовки фахівців зв'язку у війську** (див. п. 3); c) **відсутність інфраструктури зв'язку** – зокрема відсутність рішень, які би забезпечили постійну активність планшета і рації бійця (див. п. 4).

Висновки та рекомендації

Для досягнення поставлених цілей цієї роботи, а саме, – 1) розкриття теми поточного стану галузі СПЗ, та 2) висвітлення проблематики та актуальних викликів з точки зору розробників, – було виконано дослідження на основі якісних даних. Спершу читачам було надано теоретичний базис для більш комплексного орієнтування в питаннях ведення модерної війни та розуміння ролі СПЗ в ній. Окремі поняття, концепти і теорії було структуровано у **теоретичні моделі** – див. *частину першу (I)*.

Стислий огляд галузі українського СПЗ, який представлено у *частині другій (II)*, структуровано, керуючись запропонованою категоризацією систем за **трьома принципами**: a) функціоналом; b) спеціалізацією та інструментарієм; c) рівнями застосування. Огляд дозволив виокремити деякі **тенденції**, характерні для розвитку систем сьогодні, а саме:

1. Системи розвиваються переважно на тактичному рівні та у горизонтальному напрямку за рахунок охоплення все більшої кількості доменів (БпЛА → наземний → артилерійський → морський) і накопичення функцій.
2. Системи, що функціонують у війську, сконцентровано на тактичному рівні. При цьому, оперативний рівень наповнений системами в меншій мірі, а стратегічний фактично представляє собою вакуум.
3. Більшість систем є спеціалізованими, тобто, їхній інструментарій закладено в межах певної спеціалізації.
4. Початок широкомасштабної війни сформував запит на розвиток СПЗ, що є інструментами аналітики. Впровадження технологій ШІ та МН викликано потребами поточної війни – а саме, необхідністю збільшення рівня автоматизації операцій, що дозволяє значно скоротити кілчейн, і як наслідок, досягти вогневої переваги на полі бою.
5. Навчальні системи та симулятори набувають більшої актуальності – насамперед, з огляду на потребу швидкого здобуття практичних навичок о/с, особливо у випадку відсутності досвіду бойових дій.

Надалі, було виконано ряд інтерв’ю з розробниками та співзасновниками систем (на основі техніки напівструктурованих інтерв'ю), результати яких склали основу для детального висвітлення **шести систем**, що слугують в інтересах СОУ (в порядку презентації):

- **«ComBat Vision»**, системи ситуаційної обізнаності з елементами управління боєм (тактичного рівня);
- **«ARMOR» («ГРК «Броня»)**, системи автоматизації розрахунків стрільби з закритої ВП (тактичного рівня);
- **«Griselda»**, автоматизованої системи нейронної обробки даних (функціонує на всіх рівнях);
- **ІКС «DELTA»**, екосистеми продуктів із забезпечення ситуаційної обізнаності з елементами управління військами (функціонує переважно на тактичному та оперативному рівнях);
- **«Вежа»,** системи стрімінгу і дешифрування відео з аналітичними інструментами на основі даних з візуальних джерел, одного з модулів ІКС «DELTA» (функціонує переважно на тактичному та оперативному рівнях);
- **«KOLOSSAL»**, системи збору та обробки OSINT даних (функціонує переважно на тактичному та оперативному рівнях).

Окрім цього, було проведено ряд консультацій з іншими розробниками, фахівцями та користувачами з метою збору додаткових даних. Сукупно, спираючись на дані, зібрані в ході інтерв'ю та консультацій, а також, дані з відкритих джерел, було складено загальний нарис галузі (**Ціль 1**) та проаналізовано найбільш актуальні виклики і проблеми (**Ціль 2**). В результаті аналізу вдалося виокремити **13 груп викликів/проблем**, серед яких – як «органічні» виклики галузі, так і ті, що походять з інших джерел, проте, чинять прямий вплив на розвиток галузі, впровадження систем у війська та їхнє застосування, – див. *частину третю (III)*.

В рамках цієї роботи, також надаються **рекомендації** (запропоновані зміни), які сформульовано тезово з огляду на виокремлені групи викликів/проблем (у тих випадках, де це дозволяє контекст) та адресовано відповідним структурним підрозділам МОУ та ГШ ЗСУ, а також іншим релевантним державним інституціям:

1. **Виклики в правовій площині (архаїчність поточної нормативно-правової бази).**

Департаменту юридичного забезпечення МОУ (далі – ДЮЗ МОУ); Центральному юридичному управлінню ГШ ЗСУ; Комітету ВРУ з питань національної безпеки, оборони та розвідки; Кабінету Міністрів України (далі – КМУ); Директорату цифрової трансформації у сфері оборони МОУ; Центральному науково-дослідному інституту ЗСУ (далі – ЦНДІ ЗСУ); Департаменту ОВТ (Головне управління оборонних інновацій); Центральному воєнно-науковому управлінню ГШ ЗСУ (далі – ЦВНУ ГШ ЗСУ).

- Оновити нормативно-правову базу з урахуванням: a) реалій повномасштабної війни – а саме, задач і викликів поля бою, що вимагають спрощеної та пришвидшеної процедури введення систем в експлуатацію; b) впровадження мережецентричних підходів у веденні війни – зокрема, створення і функціонування СПЗ на основі хмарних рішень; c) необхідності інтеграції з партнерами (країнами-членами НАТО).

- Для цього: 1) скасувати ГОСТи; 2) прийняти необхідні правові акти для унормування СПЗ (зокрема, що стосується роботи з інформацією під грифом «Таємно»); 3) запровадити нові стандарти (STANAGи); 4) створити зрозумілу офіційну систему класифікації СПЗ за визначеними критеріями;

- Створити юридичні засади для фаст-треку введення в експлуатацію СПЗ – за аналогією треку безпілотних систем (або будь-якого іншого виду ОВТ). За потреби, розробити та підготувати експериментальну постанову КМУ.

- Вжити заходів на законодавчому рівні задля створення і фактичного впровадження ЦОД.

2. Ригідність (негнучкість) структури СОУ.

Департаменту воєнної політики та стратегічного планування МОУ; Головному управлінню оборонного планування ГШ ЗСУ (J5); ДЮЗ МОУ; Центральному юридичному управлінню ГШ ЗСУ; Департаменту кадрової політики МОУ; Головному управлінню персоналу ГШ ЗСУ (J1); Директорату цифрової трансформації у сфері оборони МОУ; Управлінню розвитку автоматизації ГШ ЗСУ; ЦВНУ ГШ ЗСУ; Заступнику Головнокомандувача ЗСУ з напрямку інновацій; Заступнику міністра оборони України з напрямку оборонних інновацій.

Необхідні зміни:

- Створити механізми, які би передбачали постійні зміни характеру війни (на всіх рівнях) та дозволяли би як а) формувати реакцію на ці зміни, так і б) діяти проактивно, наперед прогнозуючи можливі зміни у характері та способах ведення війни, а за потреби – також ініціювати ці зміни, диктуючи оновлені «правила гри» противнику. (Успішним прикладом «нав'язування» змін характеру війни стала поява далекобійних дронів («діпстрайків») як окремого напрямку ведення війни на

стратегічному рівні, що достатньо швидко набув власної окресленої структури, механізмів та певної інституціоналізації.)

- В цілому, роль аналітично-інформаційної складової СОУ потребує перегляду, а питання бойових систем та їхньої ролі у веденні війни – виведення в пріоритетні задачі військово-політичного керівництва з посилення СОУ. (Необхідно розуміти, що в поточній війні із застосуванням мережецентричних підходів, переважає той, хто володіє абсолютною ситуаційною перевагою над противником.) Зокрема, системи, які надають ситуаційну обізнаність, мають стати щоденним і «буденним» інструментом в руках українського військового скрізь, в усіх родах і видах військ. До систем, що уможливлюють автоматизацію процесів управління, мають бути застосовані комплексні підходи з їхньої інтеграції в процеси управління військами. Системи, що реалізують агрегацію та оборобку даних, мають бути використані у повній мірі за своїм призначенням.

- За своєю структурою, СОУ мають стати інклюзивними в контексті інтеграції бойових систем у війська. Для цього необхідно створити механізми, в тому числі, правові, які би уможливили спрощений процес інтеграції та використання систем (див. п. 1).

- Інтегрувати в структуру СОУ повноцінні інформаційно-аналітичні підрозділи, які би включали офіційні посади аналітиків (розвідданих), дешифрувальників тощо з чітко визначеними посадовими обов'язками. (Припускається, що робота таких підрозділів підвищить ефективність виконання комплексних операцій підрозділами СОУ у всіх доменах ведення війни.)

- В оновленій корпусній структурі Збройних сил створити роти інноваційної підтримки, в яких інженери, розробники та винахідники зможуть розробляти та швидко впроваджувати інноваційні ідеї і технології та здійснювати обмін такими напрацюваннями із сусідніми підрозділами, створюючи єдину базу даних подібних напрацювань. (Припускається, що таким чином вдасться залучити людей різних дисциплін знань, в тому числі, серед мобілізованих, до роботи над розвитком інновацій у війську. Реалізація міждисциплінарності в такий спосіб уможливить бачення «великої картинки», використавши різні експертизи в інтересах СОУ.)

- Гнучкість мислення в умовах змін характеру війни, як того вимагає широкомасштабна війна у її нинішній фазі, має стати критичним фактором на рівні вищого військового командування та офіцерів середньої ланки. (Вміння мислити гнучко в умовах, що динамічно змінюються, насамперед впливає на швидкість управління.)

- Десіжен-мейкери (на рівні департаменту, управління, відділу, підрозділу тощо), які свідомо перешкоджають процесам автоматизації і цифровізації у війську, зокрема, впровадженню СПЗ у війська, не мають впливати на процеси прийняття рішень.

3. **Низький рівень військової освіти (підготовка фахівців; володіння необхідними навичками).**

Департаменту військової освіти і науки МОУ; Головній інспекції МОУ; Центральному управлінню військової освіти ГШ ЗСУ.

Необхідні зміни:

- В контексті впровадження СПЗ і користування ними на щоденній основі, критичним є посилення війська підготовленими та кваліфікованими фахівцями зв'язку, а також офіцерами у розвідці та артилерії. Навчальні програми Вищих військових навчальних закладів (ВВНЗ) МОУ, а також, Військових навчальних підрозділів закладів вищої освіти (ВНП ЗВО) та закладів фахової передвищої військової освіти (ЗФПВО) потребують оновлення відповідно до вимог модерної війни. Офіцери ЗСУ мають володіти такими знаннями і практичними навичками, які є затребуваними насамперед на полі бою та спираються на отриманий унікальний бойовий досвід українського війська на різних етапах російсько-української війни.

- Це включає, серед іншого, передачу досвіду бойових командирів, навчання за наявними відеоматеріалами боїв в обороні та наступі, впровадження інтерактивних підходів (навчання на симуляторах, застосування технік воргеймінгу тощо), навчання на прикладі сучасних зразків ОВТ, включаючи західні, що знаходяться в практичному використанні СОУ.

- Військова освіта має надавати практичні навички, необхідні для розуміння функціонування СПЗ на різних рівнях ведення війни (насамперед, тактичному та

оперативному), взаємозв'язків між суб'єктами поля бою у мережецентричній війні, а також, вчити баченню «великої картинки», в якій СПЗ є інструментами.

- В рамках навчання курсантів ЗФПВО, ВВНЗ та ВНП ЗВО – впровадити державні освітні курси, що надавали би практичні навички, необхідні для користування СПЗ, якими нині користуються у війську на тактичному та оперативному рівнях. Для військовослужбовців та мобілізованих – впровадити скорочені онлайн курси. (Станом на сьогодні, подібні навчальні програми та/або курси є приватними ініціативами. Першим, і на момент написання цієї роботи, єдиним виключенням є анонсована у березні 2025 р. навчальна програма для інструкторів ІКС «DELTA», розроблена ЦІРОТ МОУ та Командуванням підготовки Сухопутних військ ЗСУ[326]. Курс має проходити у навчальних центрах та ВВНЗ[327].)

- Окрім суто військових дисциплін, навчання може включати також оволодіння такими навичками як стратегування, критичне мислення, військове лідерство, бізнес-навички, проджект менеджмент тощо. (Передбачається залучення фахівців приватного сектору.)

4. Слабке технологічне забезпечення підрозділів СОУ.

Департаменту військово-технічної політики, розвитку озброєння та військової техніки МОУ (далі – ДВТП МОУ); Головній інспекції МОУ; Директорату економічного аналізу і планування МОУ; Департаменту політики закупівель МОУ (далі – ДПЗ МОУ); Головному управлінню зв'язку та кібербезпеки ГШ ЗСУ (J6); Центральному управлінню оборонних ресурсів ГШ ЗСУ (J8); Управлінню розвитку автоматизації ГШ ЗСУ; Директорату цифрової трансформації у сфері оборони МОУ; ЦВНУ ГШ ЗСУ.

Необхідні зміни:

- Гострою потребою вбачається розбудова інфраструктури зв'язку, яка є необхідною умовою для повноцінного використання бойових систем в ході виконання операцій. Під «інфраструктурою зв'язку» мається на увазі можливість функціонування СПЗ,

[326] «У ЗСУ стартує перша навчальна програма для інструкторів бойової системи DELTA», Міністерство оборони України: 17 березня 2025 <https://mod.gov.ua/news/u-zsu-startuye-persha-navchalna-programa-dlya-instruktoriv-bojovoyi-sistemi-delta?fbclid=IwY2xjawJEyzxleHRuA2FlbQIxMAABHeKi8llNWvVGOEtoNYTYNt9NnCAxeQ1o_HK3PStE2ccPMRLwi_sBcqTtAg_aem_eIxANbFPJGmYX9e9suT0KA> [Переглянуто 2025 24 04].
[327] Там само.

пристроїв та приладів зв'язку, «натільних» гаджетів бійця (зокрема засобів передачі даних), зарядних пристроїв, засобів для з'єднання пристроїв та приладів та іншої спеціальної техніки – усього переліченого в межах розгалуженої «екосистеми», яка би своєчасно надавала бійцеві доступ до необхідного йому діапазону «інструментів» та уможливила би їхню взаємодію та інтероперабельність.

- Зокрема, проблема відсутності розбудованої інфраструктури зв'язку в СОУ знаходить прояв в питанні «цифровізації» піхотинця. Насамперед, піхотинця необхідно забезпечити засобами мобільного живлення гаджетів (планшетів та рацій), які би гарантували їхню постійну активність – за потреби, протягом багатьох годин бою. Під «мобільним живленням гаджетів» мається на увазі можливість живлення безпосередньо на бійцеві. (Аналогом є американська розробка STAR-PAN виробництва компанії Glenair, яка перетворює самого бійця на мобільний «хаб підзарядки»[328].)

- Подібних розробок систем мобільного живлення в Україні наразі немає і навіть не ведеться. Необхідно створити механізми стимуляції розвитку технологій в цьому напрямку задля появи в Україні систем мобільного живлення (з можливістю живити пристрої та прилади «в полі» і «на ходу»). А саме – ініціювати виконання науково-дослідних і дослідно-конструкторських робіт (за потреби, із залученням фахівців приватного сектору).

- Забезпечити (посилити) лінійні підрозділи СОУ спеціальною технікою, приладами та пристроями (зокрема раціями, планшетами, зарядними станціями тощо), необхідними для повноцінного користування СПЗ. (Станом на сьогодні, через нестачу технологічного забезпечення, лінійні підрозділи часто лишаються поза користувацькою аудиторією СПЗ.)

5. Фінансування.

Комітету ВРУ з питань національної безпеки, оборони та розвідки; КМУ; Департаменту фінансів МОУ; Директорату цифрової трансформації у сфері оборони МОУ.

Необхідні зміни:

[328] Glenair.

- Команди розробників софтверних рішень потребують комплексної і системної фінансової підтримки з боку держави, яка би полегшила діяльність команд, зокрема, на етапі дослідного використання. (Разові гранти, в тому числі, реалізовані у фреймворку тематичних хакатонів за підтримки держави, не можуть покрити потреб команди в роботі над розробками протягом тривалого часу.)

- Створити програму державної фінансової підтримки команд розробників СПЗ на базі відповідних структурних підрозділів МОУ та ГШ ЗСУ. Для цього – відкрити необхідні бюджетні програми у ЦІРОТ МОУ, ГШ ЗСУ, ЦМТР ЗСУ, ЦВНУ ГШ. Напрацювати механізми, необхідні для функціонування програми.

- Визначити критерії, необхідні для отримання державної фінансової підтримки, а також, алгоритм дій для команд розробників для участі в програмі.

6. Інвестиційні виклики.

Директорату цифрової трансформації у сфері оборони МОУ; ДЮЗ МОУ.

Необхідні зміни:

- Уряд має створити умови для залучення інвестицій, зокрема, іноземних, в галузь СПЗ. Для цього, насамперед, необхідно спростити механізм «легалізації» СПЗ, зокрема, що стосується процедури отримання висновку КСЗІ (див. п. 1). Оновлення потребує нормативно-правова база в цілому – відповідно до вимог модерної війни, зокрема, з урахуванням мережецентричних підходів (див. п. 1). (Аргументується, що наразі, організація і проведення тематичних хакатонів, акселераційних програм та інших подібних заходів, орієнтованих на залучення інвестицій в дану галузь, не можна вважати ефективними інструментами, адже першочергово необхідно вирішити поточні проблеми, що перешкоджають повноцінному розвитку бойових систем та їхньому введенню в експлуатацію.)

- Створити алгоритм верифікації інвесторів (осіб, фондів тощо).

- Створити перелік технологій, визначених за критичністю відповідно до потреб СОУ та національних інтересів України в умовах експортного контролю та інвестиційної привабливості.

- Напрацювати механізми захисту іноземних інвестицій в Україні.

7. Пасивність/відсутність держави в порядку денному галузі.

Заступнику міністра оборони України з питань цифрового розвитку, цифрових трансформацій і цифровізації; Заступнику міністра оборони України з напрямку оборонних інновацій; Комітету ВРУ з питань національної безпеки, оборони та розвідки; Департаменту кібербезпеки СБУ.

Необхідні зміни:

- Створити «офіційний» трек ведення експериментальних розробок та введення систем в дослідну експериментальну експлуатацію, який передбачав би такий алгоритм кроків, за яким розробник мав би звертатися безпосередньо до потенційних користувачів (військової частини) для отримання конкретних запитів та розуміння їхніх потреб. Таким чином, подальші дії, необхідні для розвитку системи, розробник мав би виконувати з урахуванням цих запитів і потреб, що включає, зокрема, отримання та опрацювання фідбеку «напряму» (без прямого залучення вищого командування задля скорочення ланцюга у веденні розробок та введення їх в експлуатацію.)

- Створити політику, за якою a) отримання висновку КСЗІ не мало би бути обов'язковою умовою, та яка би водночас b) передбачала розміщення систем в певному безпековому контурі МОУ (за принципом AWS[329]). В ньому розробки мали би проходити дослідно-бойову експлуатацію з певним колом зазначених підрозділів, а після підтвердження характеристик, починали би процедуру КСЗІ (оновлену, за експериментальною Постановою №139) та проходили би решту алгоритму доступу до експлуатації.

- Створити чіткий і зрозумілий «роадмап» (алгоритм дій), який слугував би покроковою інструкцією для розробників у процесі кодифікування розробок (отримання експертного висновку КСЗІ).

[329] AWS – платформа хмарних сервісів.

- Визначити ТТЗ для бойових софтверних рішень – створити каталог бойових софтверних систем, що посилюють спроможності СОУ.

- Створити критерії оцінки систем: a) безпека, b) інтероперабельність, c) функційність, d) вартість розгортання і підтримки, e) інтуїтивно зрозумілий інтерфейс (запропоновані основні критерії).

- За визначеними критеріями відібрати пул систем та команд розробників.

- На регулярній основі проводити «зріз» аналітики серед команд, що демонструють результати роботи в рамках обумовленого таймлайну у вигляді готових до експлуатації продуктів (систем) з метою визначення перспективних розробок.

- Реактивувати «Продуктовий комітет» МОУ з метою координації трьох елементів: 1) потреб СОУ, 2) оцінки роботи продуктових команд та цивільних розробників за межами поля зору МОУ та СОУ, 3) роботи державних інституцій – відповідних структурних підрозділів МОУ та ГШ ЗСУ.

- Започаткувати створення та сприяти розвитку «військового магазину» електронних застосунків («військовий App Store»). Це надало би можливість військовому (після проходження авторизації) на уніфікованій платформі обрати необхідний йому софт, завантажити його та отримати доступ до функціоналу.

- Започаткувати створення та сприяти розвитку «військового GitHub[330]» – проекту військового простору для накопичення і поширення знань та репозиторіїв.

8. Безпекові виклики.

Директорату цифрової трансформації у сфері оборони МОУ; ДЮЗ МОУ; Головному управлінню зв'язку та кібербезпеки ГШ ЗСУ (J6); Управлінню розвитку автоматизації ГШ ЗСУ; Головному управлінню радіоелектронної та кіберборотьби ГШ ЗСУ; Державній

[330] GitHub – платформа для управління версіями коду та спільної роботи над проектами, що побудована на основі Git та предсталяє собою екосистему для програмістів, в якій можна створювати проекти, брати участь у відкритих розробках тощо. Детальніше: «Що таке GitHub і як з ним працювати», *go it*, 25.02.2025. <https://goit.global/ua/articles/shcho-take-github-i-iak-z-nym-pratsiuvaty/> [Переглянуто 2025 08 05].

Службі спеціального зв'язку та захисту інформації (ДССЗІ); Департаменту кібербезпеки СБУ.

Необхідні зміни:

- Ініціювати створення загального середовища (захищеного простору) для функціонування українських СПЗ різної спеціалізації в спільному безпековому контурі задля мінімізації безпекових ризиків.

- Надати контроль над джерелами зберігання даних уповноваженим інституціям – в межах структури МОУ та ГШ ЗСУ.

- Створити простір для розробки рішень (військовий аналог AWS, Github тощо – див. п. 7).

- Доопрацювати законодавчу базу для створення і фактичного впровадження ЦОД (див. п. 1). Сформувати бюджетні програми для розвитку ЦОД.

- За умов розробки рішень в хмарному середовищі – вжити заходів щодо посилення кіберзахисту.

9. Брак інтероперабельності систем.

Департаменту воєнної політики та стратегічного планування МОУ; Директорату цифрової трансформації у сфері оборони МОУ; Управлінню розвитку автоматизації ГШ ЗСУ.

Необхідні зміни:

- Впровадити «STANAG-и інтероперабельності», якими би керувалися розробники при розробці рішень. (Станом на сьогодні, в українському полі немає яких-небудь визначених стандартів для побудови СПЗ. Припускається, що за умов впровадження певних STANAG-ів, вдасться досягти вищого рівня міжсистемної взаємодії (інтероперабельності) за рахунок підтримки системами спільних стандартів, форматів, протоколів та уніфікацій.)

- Питання інтероперабельності систем слід розглядати в комплексі із безпековими питаннями (див. *частину III*, п.8 та запропоновані зміни до п.8).

10. Технічні виклики.

Директорату економічного аналізу і планування МОУ; Директорату цифрової трансформації у сфері оборони МОУ; ДВТП МОУ; ДПЗ МОУ; Головному управлінню зв'язку та кібербезпеки ГШ ЗСУ (J6); Центру масштабування технологічних рішень ЗСУ (ЦМТР ЗСУ); ЦІРОТ МОУ; Управлінню інноваційної діяльності ЗСУ; Управлінню інформаційних технологій МОУ (УІТ МОУ); ЦНДІ ЗСУ.

Необхідні зміни:

- У найкоротшій перспективі – напрацювати та впровадити рішення із забезпечення СОУ тактичним зв'язком для ведення операцій, що є альтернативою Starlink. (Станом на сьогодні, Starlink є основним способом реалізації тактичного зв'язку на всіх рівнях ведення війни, у всіх доменах та площинах, абсолютна залежність від якого створює вразливість для функціонування СОУ. У разі відключенння Starlink і відсутності вже впроваджених альтернативних рішень, потреба в тактичному зв'язку стане критичною, що негайно відобразиться на полі бою. Однією з альтернатив є продукція компанії Satcube, що виробляє термінали для супутникового зв'язку. Також, до уваги слід взяти приклад тактичного зв'язку, запровадженого в Курській обл. рф, що використовується СОУ для виконання операцій як експериментальний.)

11. Втрата фахіців через відсутність адекватної мобілізаційної політики.

Департаменту мобілізації МОУ; ДВТП МОУ; *Директорату цифрової трансформації у сфері оборони МОУ; Департаменту кадрової політики МОУ*.

Необхідні зміни:

- Надати можливість розробникам СПЗ отримати статус критично важливих та «забронювати» працівників.

- Для цього: створити критерії оцінки критичності розробок (оборонних ІТ-рішень) та R&D центрів (команд розробників); створити Цифровий реєстр розробників,

завдяки якому інженери, розробники, винахідники зможуть отримати відповідний статус.

12. Комплікованість (складність) систем.

(без рекомендацій)

13. Складність впровадження у війська «ексклюзивних» систем.

(без рекомендацій)

Appendix 1

Глосарій термінів і понять

за алфавітом

УКР **ENG**	**Значення УКР (стисло)**
A2/AD (Обмеження та заборона доступу та маневру) A2/AD (Anti-Access/Area Denial)	Спроможностями A2/AD називають механізми, які перешкоджають силам супротивника увійти до зони операції та/або розширити їхню діяльність від початкової точки розміщення сил.[331] Окремо, A2 (протидія доступу) означає будь-яку дію, активність або спроможність (зазвичай, дальної дії), створену для того, аби не допустити входу військових сил до оперативної зони. AD (забороною доступу) називають дію, активність або спроможність (зазвичай, ближнього радіусу дії), створену для того, аби обмежити свободу дій ворожих сил в оперативній зоні. Спроможності A2/AD зазвичай складаються з багатошарових та інтегрованих далекобійних високоточних систем, прибрежних протикорабельних спроможностей, засобів ППО, артилерійських та ракетних систем великої дальності. [332]
AAR/АПД (Аналіз післядії/Аналіз проведених дій) AAR (After Action Review)	Інструмент ретроспективного аналізу. Дозволяє аналізувати помилки під час виконання завдання, вивчати бойовий досвід, навчати особовий склад, згуртовувати людей, навчатися краще мислити і ухвалювати рішення. Процес AAR складається з чотирьох запитань/етапів: 1) що було заплановано? 2) що насправді відбулося? 3) чому щось

[331] MAJ Ben Jackman, “Understanding the Anti-Access and Area Denial Threat: An Army Perspective”, U.S. Army, 2015-01, 7. <https://apps.dtic.mil/sti/tr/pdf/AD1001466.pdf> [Переглянуто 2025 26 04].
[332] Congressional Research Service.

	відбулося саме в такий спосіб? (яких саме помилок було припущено?) 4) що треба зробити наступного разу, аби виправити помилки та покращити здобутки?[333]
AR (Доповнена реальність) AR (Augmented Reality)	Технологія, за допомогою якої цифровий контент накладається на живе зображення реального світу, яке сприймає користувач. Базується на GPS даних, супутникових зображеннях та ШІ.[334]
Blue force tracking (Ідентифікація дружніх сил «свій-чужий») Blue force tracking	Технологія, що уможливлює моніторинг розташування дружніх сил та засобів у певному районі ведення операції.[335]
BMC4I (Управління боєм, командування і управління, зв'язок, комп'ютери, розвідка) BMC4I (Battle Management, Command, Control, Communications, Computers, and Intelligence)	Тип інформаційно-керуючих систем управління боєм, що призначені для застосування системами ППО наземного базування (GBAD), системами протидії безпілотним літальним апаратам (C-UAS), а також, засобами C-RAM (виявлення та знищення цілей в повітрі).[336]

[333] «Як проводити Аналіз проведених дій (АПД, After action review – AAR)», Сили територіальної оборони ЗСУ: 03.05.2024. <https://tro.mil.gov.ua/yak-provodyty-analiz-provedenyh-dij-apd-after-action-review-aar/> [Переглянуто 2025 26 04].
[334] Robert Lawless and Hitoshi Nasu, "Augmented Reality Battlefield", Lieber Institute West Point, *Articles of War*: April 28, 2022. <https://lieber.westpoint.edu/augmented-reality-battlefield/> [Переглянуто 2025 26 04].
[335] "GPS Blue Force Tracking Systems Application Note", SAVER, U.S. Department of Homeland Security, Space and Naval Warfare Systems Center Atlantic: April 2014, 1. <https://www.dhs.gov/sites/default/files/publications/GPS-Blue-Force-AppN_0414-508_0.pdf> [Переглянуто 2025 26 04].
[336] Одним з прикладів спроможностей BCM4I є система SKYKEEPER: David Saw, "SKYKEEPER – Expanding Ground-Based Air Defence Possibilities in Britain", *European Security and Defence*: 15 November 2022. <https://euro-sd.com/2022/11/articles/26817/skykeeper-expanding-ground-based-air-defence-possibilities-in-britain/ > [Переглянуто 2025 26 04].

C2 (Командування і управління) C2 (Command and Control)	В широкому контексті: здійснення командиром повноважень і керівництва над виділеними наявними силами для належного виконання місії.[337] В контексті СПЗ (C2 як спроможності): системи C2 – це такі системи управління, в яких автоматизовані лише дві функції – командування і управління.[338]
C2IS (Інформаційні системи командування і управління) C2IS (Command and Control Information systems)	Діяльність, що націлена на інтеграцію бойових інформаційних систем в процес C2. Також, використовується в контексті спроможностей.
C4ISR (Командування і управління, зв'язок, комп'ютери (IT), розвідка, спостереження і рекогностування) C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance)	Стандарт військового управління. Також в значенні C4ISR як спроможностей: гнучка автоматизована система оперативного (бойового) управління, зв'язку, розвідки та спостереження, що діє за стандартами військового управління НАТО та дозволяє досягти інформаційної переваги над ворогом і трансформується в бойову могутність завдяки поєднанню роботи підрозділів й усіх розвідувальних спроможностей в єдиний цифровий дієвий простір.[339]
C5ISR (Командування і управління, зв'язок, комп'ютери (IT), кібер	Модифікація концепту C4ISR.

[337] JP 3-0, xiv.
[338] *Defense Express*, 31 травня 2020.
[339] Машталір та інш., 99.

спроможності, розвідка, спостереження і рекогностування) C5ISR (Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance)	
C6ISR (Командування і управління, зв'язок, комп'ютери (IT), кібербезпека, бойові системи, розвідка, спостереження і рекогностування) C6ISR (Command, Control, Communications, Computers, Cyber-Defense, Combat Systems, Intelligence, Surveillance, and Reconaissnace)	Модифікація концепту C4ISR.
C7ISR (Командування і управління, зв'язок, комп'ютери (IT), розвідка, спостереження, рекогностування, бойові системи, кібер	Найбільш просунута, станом на сьогодні, модифікація концепту C4ISR.

спроможності, співпраця (оперативна сумісність)) C7ISR (Command and Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance, Combat systems, Cyber, Collaboration)	
CJADC2 (Система комбінованого об'єднаного загальнодоменного командування і управління) CJADC2 (JADC2) (Combined Joint All-Domain Command and Control)	Система управління боєм на основі ШІ та МН, що покликана об'єднувати союзників та об'єднані сили в контексті ведення мультидоменних операцій задля створення переваги.[340] Також: механізм, що фокусується на стандартизації системних даних, міграції у хмару та дослідно-експериментальній діяльності на основі ПЗ.[341] (Метою конвергенції при цьому є надання бойовим системам автономії (див. Автономія) у взаємодії між розвідувальною, оперативною та вогневою функціями, що дозволяє зняти навантаження з командирів і штабів за рахунок технологій ШІ/МН, натомість даючи змогу зосередити зусилля на прискореному та оптимізованому процесі прийняття рішень.[342])
COMINT (Радіорозвідка, РР) COMINT	Одна з гілок радіоелектронної розвідки (SIGINT). Термін застосовують для позначення розвідки на основі сигналів, що включають текст або звукові повідомлення (текстові повідомлення, телефонні розмови, радіодзвінки та онлайн взаємодії).[343]

[340] Chief of Staff Paper #1, 30.
[341] Chief of Staff Paper #1, 8.
[342] Там само.
[343] Christopher Trick, "SIGINT vs. COMINT vs. ELINT: Key Differences and Must-Know Use Cases", *Blogs by Trenton Systems*, Trenton Systems, Oct 17 2022. <https://www.trentonsystems.com/en-us/resource-hub/blog/sigint-vs-comint-vs-elint> [Переглянуто 2025 26 04].

(Communications intelligence)	
COP (Загальна оперативна картина) COP (Common operating picture)	Єдине ідентичне відображення актуальної інформації, що є спільним більш ніж для одної групи військ (підрозділу), яке сприяє спільному плануванню та допомагає всім ешелонам досягти ситуаційної обізнаності.[344]
C-RAM (Протидія ракетам, артилерії та мінометам) C-RAM (Counter Rocket, Artillery and Mortar)	Спроможності ППО тактичної ланки, що застосовуються з метою виявлення та знищення цілей в повітрі (раннє попередження).
C-UAS (Протидія безпілотним літальним системам) C-UAS (Counter Unmanned Aerial Systems)	Спроможності, що застосовуються для виявлення та відстеження безпілотних літальних систем, виведення їх з ладу та/або знешкодження. До таких спроможностей відносять широкий спектр рішень, зокрема засоби РЕБ, системи озброєння середнього калібру, системи С2 тощо.[345]
CYBERINT (Кіберрозвідка/кібернетична розвідка) CYBERINT (Cyber intelligence)	Вид розвідки, в основі якої лежить процес знаходження інформації, наявної у кібернетичному просторі, моніторинг інформаційно-телекомунікаційних систем і процесів, які в них відбуваються під час їхнього функціонування. [346] Розподіляється на: розвідку телекомунікаційних систем та комп'ютерну розвідку.

[344] JP 3-0, GL-7.
[345] Наприклад, див.: "Defining Possible Against Unmanned Aerial Systems", Northrop Grumman. <https://www.northropgrumman.com/what-we-do/land/counter-unmanned-aerial-systems-c-uas> [Переглянуто 2025 26 04].
[346] Владислав Кива, Євген Судніков, Олександр Войтко, «Методи розвідки кіберпростіру». *Сучасні інформаційні технології у сфері безпеки та оборони*, 2018/Том 33 (№ 3), 45. <https://sit.nuou.org.ua/article/view/154348> [Переглянуто 2025 26 04].

Data driven decision Data driven decision	Принцип ухвалювання рішень на основі даних.
FM (Бойовий Статут Армії США) FM (Field Manual)	Одна з частин Доктрини Армії США. (Решта частин: Army Doctrine Publications (ADPs), Army Techniques Publications (ATP)). Ці публікації описують виконання операцій: планування місій, підготовку до них, виконання, оцінку на практиці.[347]
GBAD (Протиповітряна оборона наземного базування) GBAD (Ground-based Air Defense)	Засоби ППО наземного базування. В широкому сенсі, термін використовують для позначення категорії спроможностей, які покликані нейтралізовувати або зменшувати повітряну загрозу з боку авіаційних засобів, БпЛА, ракетних засобів тощо.[348]
GEOINT (Геопросторова розвідка) GEOINT (Geospatial intelligence)	Розвідувальні дані, отримані шляхом використання та аналізу геопросторової інформації, зображень (наприклад, супутникових знімків, карт) та інших даних для надання опису, оцінки або візуального зображення географічно прив'язаних дій та властивостей. Включає IMINT (візуальну розвідку) та вироблення або аналіз геопросторової інформації.[349]
HUMINT (Агентурна розвідка) HUMINT (Human intelligence)	Розвідувальні дані, отримані з інформації, яка була зібрана людьми та надана переважно людськими джерелами. Отримання даних досягається через спостереження або пряму комунікацію з людьми, що може включати такі методи як дебрифінг, роботу з джерелом, тактичне

[347] Matthew Tetreau, "A Beginner's Guide to Army Doctrine", *The Company Leader*: June 12, 2020. <https://companyleader.themilitaryleader.com/2020/06/12/on-doctrine/ > [Переглянуто 2025 27 04].
[348] "What is ground-based air defence?", SAAB. <https://www.saab.com/newsroom/stories/themes/what-is-ground-based-air-defence> [Переглянуто 2025 27 04].
[349] Joint Doctrine Publication 0-01.1 "UK Terminology Supplement to NATOTerm". UK Ministry of Defence (Edition A), March 2025, 23. <https://assets.publishing.service.gov.uk/media/651fcb7d79fc58000d63971c/20231004-JDP_0_01_1_2023_Edition_B_web.pdf> [Переглянуто 2025 27 04].

	опитування, допит, комунікацію з військовою розвідкою та приховане пасивне спостереження (усі методи здійснюються навченим персоналом). Передбачається, що HUMINT та контррозвідка мають співіснувати як комплементарні функції розвідки, що виключає їхню конкуренцію.[350] Термін також використовують для позначення виду розвідки (HUMINT як процес і діяльність).
I2CEWS (Розвідка, інформація, кібер спроможності, радіоелектронна боротьба та космічні спроможності) I2CEWS (Intelligence, Information, Cyber, Electronic Warfare, and Space)	Термін використовують у декількох значеннях. I2CEWS в значенні спроможностей служить назвою одній зі складових мультидоменних оперативних груп (MDTF). Вузол I2CEWS об'єднує засоби РЕБ, РЕР, кібер та космічні спроможності, декілька видів розвідок, інформаційні системи. Також, може означити підрозділ (батальйон) як структурну одиницю, яка оперує даними засобами.
IBCS (Інтегрована система бойового управління) IBCS (Integrated Battle Command System)	Технологія, що уможливлює координацію та ефективність роботи ППО та ПРО[351]. Об'єднуючи широкий спектр сенсорів, систем радарів і платформ озброєння в єдину мережу, IBCS покращує ситуаційну обізнаність і спроможності в процесі прийняття рішень, забезпечує швидке й точне розгортання необхідних засобів у відповідь на загрози[352].
IMINT	Вид розвідки, в основі якої лежить процес збору зображень, отриманих за допомогою візуальної фотографії,

[350] JDP 2-00 (2023, 4th ed.), 80.
[351] "Revolutionizing Command and Control", Northrop Grumman. <https://www.northropgrumman.com/what-we-do/land/integrated-battle-command-system-ibcs> [Переглянуто 2025 27 04].
[352] "Integrated Battle Command System (IBCS)", Missile Defense Advocacy Alliance, July 17, 2024. <https://missiledefenseadvocacy.org/integrated-battle-networks/integrated-battle-command-system-ibcs/ > [Переглянуто 2025 27 04].

(Видова/візуальна розвідка) IMINT (Imagery intelligence)	радіолокаційної апаратури, інфрачервоних сенсорів, лазерів та електрооптики.[353]
ISR (Розвідка, спостереження, рекогностування) ISR (Intelligence, surveillance, reconnaissance)	Процес та/або стандарт в системі бойового управління та/або спроможності, що уможливлюють цей процес/стандарт. В значенні ISR як процесу/стандарту: процес в системі бойового управління, що включає отримання оперативної задачі, надання напрямку спроможностям ISR, збір даних та інформації, перетворення їх на придатний для використання формат та передачу для подальшого використання десіжен-мейкерами, виконавцями та аналітиками розвідки. Складається з 5 покрокових етапів: 1) задачі, 2) збору, 3) обробки, 4) використання, 5) розповсюдження.[354]
ISTAR (Розвідка, спостереження, цілевказання, рекогностування) ISTAR (Intelligence, surveillance, target acquisition, reconnaissance)	Процес та/або стандарт в системі бойового управління та/або спроможності, що уможливлюють цей процес/стандарт. В значенні ISTAR як процесу/стандарту: процес і стандарт, що полягає у зборі, первинній обробці, співставленні, пріоритизації інформації та її швидкій передачі до зацікавлених споживачів – відповідних підрозділів та командирів.[355] Продуктом ISTAR є надання загальної оперативної картини (COP).
JEMSMO (Об'єднані операції з управління	Складаються з планування, координації та керування об'єднаним використанням електромагнітного спектру через здійснення операційних, інженерних та адміністративних процедур. Основна мета JEMSMO полягає

[353] "Intelligence Studies: Imagery/Geospatial Intelligence (IMINT/GEOINT)", U.S. Naval War College Library. <https://usnwc.libguides.com/c.php?g=494120&p=3381562> [Переглянуто 2025 27 04].
[354] JDP 2-00 (2023, 4th ed.), 86-87.
[355] «Напрям ISTAR», ГО «АЕРОРОЗВІДКА».

електромагнітним спектром) EMSMO (Joint electromagnetic spectrum management operations)	в тому, щоби уможливити виконання електронними системами своїх функцій в призначеному середовищі, не створюючи та не зазнаючи при цьому неприйнятного втручання.[356]
JEMSO (Об'єднані операції електромагнітного спектру) JEMSO (Joint electromagnetic spectrum operations)	Координовані зусилля РЕБ та JEMSMO з метою використання, здійснення атаки, захисту та управління електромагнітним оперативним середовищем.[357]
JISR (Об'єднані розвідка, спостереження, рекогностування, або Об'єднаний ISR) JISR (Joint intelleigence, surveillance, reconnaisence, or Joint ISR)	Інтегрований набір розвідувальних та оперативних спроможностей, який синхронізує та інтегрує планування та операції зі всіма спроможностями збору з обробкою, використанням та розповсюдженням отриманої інформації для прямої підтримки планування, підготовки та виконання операцій.[358]
LL (Засвоєні уроки) LL	В широкому контексті: процес навчання через здобуття досвіду для досягнення вищої ефективності. В контексті NATO LL:

[356] JP 3-13.1, I-10.
[357] JP 3-13.1, vii.
[358] NATO STANDARD AJP-2 "Allied Joint Doctrine for Intelligence, Counterintelligence and security", NATO, NATO Standardization Office (Edition A, Version 2): February 2016, 3-8. <https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP2.pdf> [Переглянуто 2025 28 04].

(Lessons Learned)	Метою процедури LL є ефективне навчання на основі отриманого досвіду та надання підтверджених обґрунтувань для внесення змін до існуючого способу виконання завдань, щоби покращити якість виконання операцій як під час їх проведення, так і в майбутньому.[359]
LSCO (Широкомасштабні бойові операції) LSCO (Large-scale Combat Operations)	Бойові операції за участю двох і більше ешелонів командування на рівні генерала або флагмана принаймні з одного боку, які маневрують своїм управлінням на підтримку кампанії проти ворога, що має аналогічні тактику та структуру сил.[360]
MASINT (Вимірювальна та сигнатурна розвідка) MASINT (Measurement and Signature intelligence)	Розвідувальні дані, отримані шляхом наукового та технічного аналізу даних, які, в свою чергу, були отримані з сенсорних пристроїв з метою ідентифікації яких-небудь відмінних ознак, пов'язаних з джерелом (випромінювачем або відправником) для полегшення вимірювання та ідентифікації цього джерела. Для цього використовують детальні вимірювання та сигнатури, а також порівняння певних явищ для виявлення, відстеження, ідентифікації та/або надання іншої характеристики зразку, об'єкту або події. Йдеться про геофізичні, електромагнітні або матеріальні властивості. Наприклад, такі розвід.дані можуть бути отримані в результаті вдосконаленої обробки акустичних або сейсмічних сигнатур тощо[361].
MDM	Захищене середовище («контейнер»), створене на мобільному гаджеті військового, що виконує функцію

[359] "The NATO Lessons Learned Handbook", NATO, Joint Analysis and Lessons Learned Centre (4th edition): June 2022, 9. <https://www.jallc.nato.int/application/files/4416/5781/2017/JALLC_LL_Handbook_Update_-_4th_Edition_FINAL_14072022.pdf> [Переглянуто 2025 28 04].

[360] MAJ John Dzwonczyk and MAJ Clayton Merkley, "Through a Glass Clearly: An Improved Definition of LSCO", *Military Review (Online Exclusive)*, November 2023, 4. <https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2023/Through-a-Glass-Clearly/Merkley-Through%20A%20Glass%20Clearly%20UA1.pdf> [Переглянуто 2025 28 04].

[361] JDP 2-00 (2023, 4th ed.), 78. Також, див. різновиди MASINT за класифікацією НАТО: Там само, 79.

MDM (Mobile Device Management)	додаткового рівня безпеки. Такий «контейнер» може вміщати закриті військові застосунки, зібрані у каталоги. При цьому, контроль здійснюється лише над цим «військовим» середовищем користувача, а його особисте середовище (інші застосунки, дані) лишається недоступним для будь-якого роду дій ззовні. В разі втрати гаджету, наприклад, адміністратором дистанційно може бути активовано видалення змісту всього військового «контейнера».
MDMP/ВППР (Військовий процес прийняття рішень) MDMP (Military Decision Making Process)	Тактичний процес керування плануванням. Також: модель планування, яка встановлює процедури аналізу завдання, розробку, аналіз та порівняння варіантів дій за визначеними критеріями, вибір оптимального варіанта дій та розробку плану або наказу. В порівнянні з процесом TLP (див. також TLP – інший тактичний процес), MDMP більш підходить для органу військового управління зі штабом. MDMP покликаний забезпечити логічну послідовність рішень та взаємодії між командиром та штабом для проведення оцінювання та розробки ефективних планів та наказів (розпоряджень); призначений для полегшення взаємодії командира, штабу та підлеглих штабів у процесі планування).* Складається з семи етапів: 1) Отримання завдання; 2) Аналіз завдання; 3) Розроблення варіантів дій; 4) Аналіз варіантів дій (воргеймінг); 5) Порівняння варіантів дій; 6) Затвердження варіантів дій; 7) Розроблення, видання та доведення наказу. Кожний з етапів MDMP має вхідні та вихідні дані.

	*У нижчих тактичних ешелонах командири не мають штабів – тому, командири на рівні роти та нижче використовують процедуру TLP для планування та підготовки до операції.[362]
NATO C3 Taxonomy NATO C3 Taxonomy	Інструмент управління компетенціями, що застосовується в управлінні операціями.
OSINT (Розвідка на основі відкритих джерел) OSINT (Open-source intelligence)	Розвідувальні дані, отримані із загальнодоступної інформації, а також іншої некласифікованої інформації, що має обмежене розповсюдження або доступ. Включає в себе процеси збору та обробки загальнодоступної інформації задля підтримки розвідувальних функцій, а також виготовлення OSINT продуктів.[363] Термін також використовують для позначення виду розвідки (OSINT як процес і діяльність).
SIGINT (Радіоелектронна розвідка/розвідка сигналів) SIGINT (Signals intelligence)	Вид розвідки, в основі якої лежить процес збору сигналів, що їх випромінюють системи зв'язку, радари, системи озброєння. Зібрані дані (наприклад, за допомогою радарів та БпАК, оснащеними інфрачервоними сенсорними камерами, наземними станціями, LIDAR тощо) потребують подальшої інтерпретації та аналізу, після чого дані перетворюються на придатну до роботи інформацію. Розрізняють дві гілки: COMINT та ELINT.[364]
SOCMINT (Розвідка з соціальних мереж) SOCMINT (Social Media Intelligence)	Вид розвідки (також відносять до галузей OSINT), в основі якої лежать процеси збору та обробки загальнодоступної інформації з соціальних мереж. Зокрема, розвідувальні дані можуть бути отримані через аналіз таких даних як вподобання користувачів, взаємодію з іншими користувачами та організаціями, місцезнаходження тощо.

[362] «Рекомендації з планування та організації бою за стандартами НАТО (частина 1)», Сили Територіальної оборони ЗСУ. <https://sprotyvg7.com.ua/lesson/rekomendacii-planuvanya-boyu-nato> [Переглянуто 2025 28 04].
[363] JDP 2-00 (2023, 4th ed.), 81.
[364] Trick.

TLP/ОБП (Організація бою підрозділів/процедура управління підрозділами) TLP (Troops Leading Procedures)	Стандартизована процедура управління невеликими підрозділами, розроблена для командирів ланки «взвод». Складається з восьми етапів, кількість та послідовність яких не є обов'язковими та залежить від обстановки та наявного часу на підготовку бою (дій), а окремі етапи можуть бути виконані паралельно з роботою старшого командира: 1) Аналіз отриманого завдання та оцінка обстановки; 2) Віддання попереднього бойового розпорядження (вказівок з підготовки бою (дій); 3) Вироблення замислу бою (дій); 4) Здійснення необхідних переміщень; 5) Проведення рекогносцировки; 6) Завершення формулювання рішення на бій (дії); 7) Підготовка та віддання бойового наказу; 8) Організаторська робота.[365] (Див. також MDMP – інший тактичний процес, що уможливлює керування плануванням.)
UMD UMD (Universal military dataset)	Військовий датасет, що представляє собою набір даних різних типів (зокрема візуальних, акустичних, гідро-акустичних, радіо-, теплових та РЛС-сигнатур), які детально анотовано («розмічено»), згруповано, каталогізовано для використання в навчанні систем МН (нейронних мереж).
VR (Віртуальна реальність) VR (Virtual Reality)	Технологія, яка допомагає користувачам зануритися в інтерактивне віртуальне середовище, яке імітує реальний світ. VR дозволяє взаємодіяти з об'єктами та персонажами в ньому, чути звуки, отримувати сенсорні відчуття тощо.[366]
Автономія Autonomy	Рівень незалежності, який люди надають системі для виконання певного завдання. Також: умова або якість (характеристика) системи у процесі самоуправління, що

[365] «Послідовність та зміст роботи командира з організації бою. (TLP)», Сили Територіальної оборони ЗСУ. <https://sprotyvg7.com.ua/lesson/poslidovnist-ta-zmist-roboti-komandira-z-organizacii-boyu-tlp> [Переглянуто 2025 28 04].

[366] Анастасія Шкальова, «Від авіасимуляторів до рекрутингу. Як AR/VR використовують у підготовці військових», *Vector*: 19 Травня 2023. <https://vctr.media/ua/vid-pidgotovki-pilotiv-do-rekrutingu-yak-ar-vr-vikoristovuyut-u-pidgotovczi-vijskovih-ta-stvorenni-zbroyi-183908/> [Переглянуто 2025 28 04].

	здійснюється задля досягнення поставленої задачі і базується на ситуаційній обізнаності, якою володіє система (сенсори, сприйняття та аналіз), а також, спроможності планування та прийнятті рішень.[367]
Асиметрична війна Assymetric warfare	Тип ведення війни, в якому сторони конфлікту володіють невідповідними військовими спроможностями або впроваджують невідповідні (по відношенню один до одного) методи ведення бою. В такому випадку, сторона, що має менш вигідне (у війському плані) положення, мусить у повному обсязі застосовувати свої особливі переваги або ефективно використовувати певні слабкості противника.[368]
АСКВ (Автоматизована система керування вогнем) AFCS (Automated Fire-control System)	Один з типів систем управління, що призначені для використання артилерійськими підрозділами. Можуть включати виконання таких задач як цілевказання, прийняття рішення на виконання вогневого завдання, виконання балістичних обчислень, оцінка результатів стрільби і впровадження необхідних поправок до вогневих засобів, обмін даних між елементами АСКВ, планування логістичної підтримки і місії в цілому, оцінка тактичної обстановки тощо.[369]
АСУВ (Автоматизована система управління військами) Automated Force Management System	Вид СПЗ. Взаємопов'язана сукупність засобів отримання та обробки інформації, передачі даних та зв'язку, яка забезпечує процеси збору, аналізу та оцінки обстановки, прийняття рішень, планування, доведення цих рішень до військ (сил) та контроль за ходом їх виконання шляхом зменшення безпосереднього втручання людини у відповідні процеси.[370]
БпАК	Система засобів і технологій, обов'язковими елементами якої є: безпілотний літальний апарат (БпЛА), наземна

[367] Rademaker and Mevissen, 5.
[368] 2001-2009 Archive for the U.S. Department of State. <https://2001-2009.state.gov/s/ct/info/c16718.htm> [Переглянуто 2025 28 04].
[369] За прикладом АСКВ «TOPAZ»: Заблоцький.
[370] Древницький.

(Безпілотний авіаційний комплекс)/БАС (Безпілотна авіаційна система) UAS (Unmanned Aerial System)	станція керування, канали передачі даних, по яких здійснюється зв'язок.
БСМ (Бездротові сенсорні мережі) WSN (Wireless Sensor Network)	Розподілені бездротові мережі, що складаються з маленьких вузлів (сенсорів), з інтегрованими функціями моніторингу навколишнього середовища, обробки і передачі даних.[371]
Ведення війни Warfare	Механізм, метод або ж модальність збройного конфлікту. Вказує на спосіб, в який сторони ведуть війну – відповідає на питання «як».[372]
Війна 4-го покоління 4GW (Fourth Generation warfare)	Узагальнений термін, що слугує описом одного з типів ведення війни, який відрізняється від війн 1-го, 2-го і 3-го поколінь, через певні властиві йому характеристики, такі як: неконвенційний/асиметричний характер дій; нанесення прямих ударів по культурних, політичних та цивільних цілях в обхід збройних сил противника; активне залучення децентралізованих недержавних áкторів. Втрата державою монополії на війну вважається ключовим чинником, що характеризує війни 4-го покоління (недержавні áктори воюють проти держав). (Війни 5-го та 6-го поколінь можна вважати версіями війни 4-го покоління. Втім, всі перелічені моделі є умовними теоретичними конструктами.)

[371] А.І. Міночкін, В.А. Романюк, О.В. Жук, «Перспективи розвитку тактичних сенсорних мереж», *Збірник наукових праць ВІТІ НТУУ «КПІ»,* 2007 (No 4), 112-119. <https://journal.viti.edu.ua/public/romanuk/2007/4_2007.pdf> [Переглянуто 2025 28 04].
[372] JP 1, I-4.

Військова розвідка Military intelligence	Знання, отримані шляхом збору, оцінки, аналізу, інтеграції та інтерпретації усієї наявної інформації щодо потенційного або фактичного противника та/або районів операції включно з погодою та місцевістю. Включає висновки (дедукції) про поточні та майбутні спроможності противника, вразливості та ймовірні напрямки його дій, які можуть вплинути на виконання місії. Ці знання використовуються як основа для всіх оперативних планів та попередніх оцінок. Військова розвідка також включає контррозвідку.[373] Зазвичай, використовується у значенні розвідки тактичного рівня. (Термін «військова розвідка» не є тотожним терміну «воєнна розвідка».)
Військовий інтернет речей Internet of military things (IoMT)	«Мілітаризована» розширена версія поняття «Інтернет речей» (the Internet of Things, IoT). Описує використання мережі пристроїв, підключених через Інтернет, та áкторів, що оперують в ньому.[374]
Вікно переваг Window of advantage	Стан, що досягається через конвергенцію (інтеграцію) спроможностей у часі та просторі в обраних доменах та середовищах з метою надання командирам можливості отримати локалізований контроль або фізичний, віртуальний та/або когнітивний вплив в межах визначеної території, щоб запобігти її використанню ворогом або створити умови, необхідні для виконання успішних дружніх операцій.[375]
Воргеймінг Wargaming	Інструмент планування та прогнозування збройних конфліктів, операцій, боїв.

[373] FM 30-5, Department of the Army Field Manual “Combat Intelligence”, February 1951. <https://ia802207.us.archive.org/30/items/KoreanWarFieldManuals/FM%2030-5%20%28%20Combat%20Intelligence%20%29.pdf> [Переглянуто 2025 28 04].
[374] Claire Withrington, “The Internet of Military Things”, *The Cove*: 24/08/2023. <https://cove.army.gov.au/article/internet-military-things> [Переглянуто 2025 28 04].
[375] TRADOC, 79.

	Передбачає програвання певних сценаріїв, які в сутності своїй є аналітичними іграми, що симулюють аспекти ведення війни на тактичному, оперативному або стратегічному рівнях. Ці ігри використовують з метою тестування концептів ведення війни, тренування та навчання командирів та аналітиків, вивчення сценаріїв, та надання оцінки того, як планування сил і вибір позиції впливають на результати кампанії.[376]
Дані Data	В контексті розвідки: Доступна для розуміння (трактування) репрезентація інформації у формалізований спосіб, придатний для комунікації, інтерпретації або обробки. Дані можуть оброблятися людьми або автоматично.[377]
Домен ведення війни Warfighting domain	Окреслене середовище, у яке гравці мають потрапити, маневрувати в ньому, домінувати або мати контроль задля досягнення військової цілі.[378]
Домінування в прийнятті рішень Decision dominance	Бажаний стан, в якому командири сприймають, усвідомлюють, вирішують, діють та оцінюють швидше та ефективніше за противника. Досягається за рахунок конвергенції.[379]
Електромагнітний спектр EMS (Electromagnetic Spectrum)	Повний діапазон частот електромагнітного випромінювання від нуля до нескінченності, що поділений на 26 смуг.[380]
Інтероперабельність Interoperability	В широкому сенсі: здатність діяти (на постійній основі) узгоджено, ефективно та результативно для досягнення тактичних, оперативних та стратегічних цілей.[381]

[376] “Wargaming”, RAND. <https://www.rand.org/topics/wargaming.html> [Переглянуто 2025 28 04].
[377] JDP 2-00 (2023, 4th ed.), 7.
[378] McManus.
[379] Chief of Staff Paper #1, 8.
[380] JP 3-13.1, GL-7.
[381] JP 6-0, GL-5.

	Також, в контексті міжсистемної взаємодії: стан, якого досягнуто між комунікаційно-електронними системами або елементами комунікаційно-електронного обладнання, при якому обмін інформацією або послугами може бути здійснено між ними та/або їхніми користувачами безпосередньо і задовільно.[382]
Інформація Information	В контексті розвідки: Дані, впорядковані для передачі значення.[383]
Кілчейн/ланцюг ураження цілі/F2T2EA (знайти, зафіксувати, відстежити, націлитись, уразити, оцінити) Kill chain/F2T2EA (Find, Fix, Track, Target, Engage, and Assess)	В контексті ведення війни: цикл вогневого ураження. Також, модель ураження цілі, що представляє собою ланцюг з декількох послідовних фаз, які необхідно виконати для того, аби a) завдати точного удару, та b) проаналізувати атаку та запобігти ураженню.
Комп'ютерний зір Computer Vision (CV)	Галузь ШІ, що фокусується на аналізі, класифікації і розпізнаванні зображень і відео. В основі систем комп'ютерного зору (CV-систем) зазвичай лежать алгоритми на базі МН, за допомогою яких ці системи «вчаться» відрізняти одні об'єкти від інших, розпізнавати патерни і закономірності.
Конвенційна війна Conventional warfare (CW)	Термін, що використовують для опису типу ведення війни, який передбачає залучення у конфлікт державних áкторів, «традиційні» методи ведення війни, конвенційні види озброєння, а також залученість конвенційних сил (військ). Конвенційними військами є такі, що складаються з регулярних збройних сил, розгортаються урядом, контролюються ним і підпорядковуються йому; оперують у

[382] Там само.
[383] JDP 2-00 (2023, 4th ed.), 7.

	бойових діях (відносно) високої інтенсивності, використовуючи конвенційні типи озброєння; в наступальних діях, переважно діють проти інших збройних груп, а не проти цивільного населення).[384]
Конвергенція Convergence	В широкому контексті: інтеграція спроможностей. Також: здатність бачити, сприймати, комунікувати, стріляти та рухатися зі швидкістю та у масштабі, поєднуючи всі необхідні сенсори з найкращим стрілком та необхідним вузлом С2. Завдяки конвергенції досягається домінування в прийнятті рішень.[385]
Контроль електромагнітного спектру EMSC (Electromagnetic Spectrum Control)	Координоване здійснення об'єднаних операцій електромагнітного спектру (JEMSO) з іншими летальними та нелетальними операціями, які уможливлюють свободу дій в електромагнітному оперативному середовищі.[386]
Крос-доменна взаємодія/міждоменна синергія Cross-domain Synergy	Використання двох або більше доменів для досягнення військової переваги. Часто передбачає застосування спроможностей одного домену в іншому задля покращення виконання операції та мінімізації непотрібних дублювань функцій в роботі об'єднаних сил. Досягається у випадку, коли інтегроване застосування спроможностей наземного, морського, повітряного, космічного та/або кібер домену дає комбінований результат, що є кращим за суму результатів, взятих окремо.[387]
ЛАСО (Летальна автономна система озброєння)	Категорія озброєння, яку відносять до роботизованих та автономних систем (див. РАС). До категорії ЛАСО входять такі системи озброєння, які без втручання людини

[384] Kateryna Kistol (Aniskina) "The ways to fight proxy war: Conventional vs. Unconventional warfare strategies. How is the warfare strategy related to conflict outcomes?", Dissertation, UCL, September 2020, 18. <https://surli.cc/lkmspi> [Переглянуто 2025 05 05].
[385] Chief of Staff Paper #1, 8.
[386] JP 3-13.1, GL-7.
[387] Odom and Hayes, 124.

також: АСО (автономна система озброєння) LAWS (Lethal Autonomous Weapon System) also: AWS (Autonomous Weapon System)	обирають та уражають цілі за певними, заздалегідь визначеними критеріями, слідуючи людському рішенню розгорнути озброєння, яке, в свою чергу, засновано на розумінні того, що атаку неможливо буде спинити втручанням людини після того, як її буде розпочато.[388]
МДО (Мультидоменні операції) MDO (Multi-domain operations)	Комбіноване (змішане) застосування сил об'єднаних та армійських спроможностей задля створення та використання відносних переваг, що дозволяють досягати цілей, перемагати сили супротивника та консолідувати здобутки за дорученням командирів об'єднаних сил.[389] Діючий операційний концепт Армії США (від 2022 р.)
Мережецентрична війна Net-centric/ Network-centric warfare (NCW)	Тип ведення війни, що базується на принципі отримання переваги над противником завдяки повній інформаційній (ситуаційній) обізнаності. Є концепцією операцій, яка реалізована завдяки інформаційній перевазі, і яка генерує зростання бойової сили через об'єднання в одну мережу «сенсорів», «десіжен-мейкерів» та «стрільців» задля досягнення спільної обізнаності, підвищення швидкості управління, вищого темпу операцій, вищої летальності (рівня втрат противника), вищої «живучості», а також вищого рівня самосинхронізації. Мережецентричний підхід полягає у перетворенні інформаційної переваги на бойову силу шляхом ефективного поєднання обізнаних суб'єктів на полі бою.[390]
МН (Машинне навчання)	Галузь ШІ, яка фокусується на розробці комп'ютерних алгоритмів, що мають здатність автоматично

[388] Rademaker and Mevissen, 5.
[389] FM 3-0, 1-2.
[390] Alberts et al., 2.

ML (Machine Learning)	покращуватися через набуття досвіду та використання даних. МН дозволяє комп'ютерам вчитися з наявних даних та приймати рішення або робити прогнози не потребуючи для цього явного програмування.[391]
Модель з нульовою довірою Zero Trust Security	Модель побудови інформаційних систем, що розглядає всіх користувачів як потенційну загрозу та запобігає доступу до даних і ресурсів, доки користувачів не буде належним чином автентифіковано та авторизовано. Архітектура надає користувачеві повний доступ, але лише до мінімуму, необхідного для виконання своєї роботи. В разі, якщо пристрій скомпрометовано (зламано), модель може гарантувати, що пошкодження буде локалізовано.[392]
Мультидоменний бій Multi-domain Battle (MDB)	Концепт, в основі якого – готовність битися у середовищі, в якому всі домени є оспорюваними (такими, за які ведеться боротьба).[393] Означає конвергенцію (інтеграцію) спроможностей для створення вікон переваг (часто тимчасових) у кількох доменах та оспорюваних територіях по всій глибині поля бою для захоплення, утримання та використання ініціативи, здолання противника та досягнення військових цілей.[394]
Мультидоменні оперативні групи MDTF (Multi-domain Task Force)	Підрозділи, створені для залучення у виконання мультидоменних операцій.
Неконвенційна війна	Термін, що використовують для опису типу ведення війни, який передбачає широкий спектр військових та парамілітарних операцій (як правило, довготривалих), які

[391] Matt Crabtree, "What is Machine Learning? Definition, Types, Tools & More", DataCamp, Nov 8, 2024. <https://www.datacamp.com/blog/what-is-machine-learning> [Переглянуто 2025 29 04].
[392] "Zero Trust Architecture", National Cybersecurity Center of Excellence. <https://web.archive.org/web/20210422024921/https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture> [Переглянуто 2025 28 04].
[393] Carafano, 27.
[394] TRADOC, 77.

Unconventional (irregular) warfare (UW)	проводяться переважно за сприяння місцевих або сурогатних сил, організованих, тренованих та екіпованих за підтримки зовнішнього джерела та керованих ним же. Включає, серед іншого, такі методи як партизанська війна, диверсії, саботаж, діяльність розвідки, а також дії, пов'язані з підготовкою сил опору силами спеціальних операцій.[395] Передбачає залучення неконвенційних військ (що є альтернативою регулярним військам).[396]
Об'єднані операції Joint Operations	Загальний термін, який описує військові дії, що проводяться об'єднаними силами або силами служб, задіяних під командуванням[397]. Означає форму застосування сил, залучених в інтегровані дії. Вказує на об'єднаний характер зусиль.
Об'єднані сили Joint Forces	Сили від двох і більше підрозділів, що діють під одним командуванням.[398]
Оперативне середовище, ОС Operational Environment (OE)	Сукупність умов, обставин та факторів, що впливають на використання спроможностей і застосування військ (сил) та рішень командира.[399]
Платформоцентрична війна Platform-centric warfare	Тип ведення війни, який передбачає, що певні платформи (бойові системи) володіють озброєнням, а озброєння має власні органічні «сенсори».[400] На практиці це означає, що деякі бойові групи мають «закріплене» за ними озброєння та доступ до «закріплених» за ними «сенсорів», що виключає можливість використання цього самого озброєння та інформації від цих самих «сенсорів» іншими суб'єктами поля

[395] Joint Publication 1-02 "Department of Defense Dictionary of Military and Associated Terms". Joint Chiefs of Staff, 12 April 2001 (As Amended Through 30 September 2010), 486. <https://irp.fas.org/doddir/dod/jp1_02.pdf> [Переглянуто 2025 29 04].
[396] Kistol (Aniskina), 19.
[397] JP 3-0, ix.
[398] "Military Command Structure", NATO. <https://shape.nato.int/military_command_structure> [Переглянуто 2025 29 04].
[399] «Планування вогневої підтримки на тактичному рівні (початок)».
[400] Alberts et al., 120.

	бою. Тобто, суб'єкти поля бою діють розрізнено (на відміну від мережецентричної війни, де всі суб'єкти поля бою об'єднані в «мережу».) По відношенню до підходів мережецентричної війни, платформоцентричні підходи вважаються традиційними. Їм притаманна слабкіша ситуаційна обізнаність, нижча швидкість управління та нижчий темп операцій, довший (громіздкий) кілчейн тощо, – в порівнянні з мережецентричними підходами.
РАС (Роботизовані та автономні системи) RAS (Robotic and Autonomous systems)	Термін, що використовують як фреймворк для опису систем із наявними двома компонентами: фізичною (роботизована компонента) та когнітивною (автономія).[401]
РЕБ (Радіоелектронна боротьба) EW (Electronic Warfare)	Військові дії, що включають використання електромагнітної та направленої енергій задля контролю над електромагнітним спектром або здійсненням атаки проти ворога.[402] Також: здатність використовувати електромагнітний спектр (такі сигнали як радіо, інфрачервоні сигнали та сигнали радарів) для сприйняття, захисту та зв'язку. Водночас, РЕБ може порушувати та погіршувати здатність супротивника використовувати ці сигнали та перешкоджати йому в цьому.[403]
Революція у військовій справі	В контексті теорії, що виникла на початку 1990-х рр., цей термін використовують для узагальнення ряду кардинальних технологічних змін у сенсорах, озброєнні,

[401] Rademaker and Mevissen, 5.
[402] JP 3-13.1, GL-8.
[403] "Electronic Warfare", Lockheed Martin. <https://www.lockheedmartin.com/en-us/capabilities/electronic-warfare.html> [Переглянуто 2025 28 04].

RMA (Revolution in military affairs)	платформах, що поєднують і те, і інше, та інформаційних технологіях, що мали змінити виконання військових операцій у XXI ст.[404] Термін RMA застосовують і в інших контекстах, що висвітлюють інші вагомі зміни та «революційні» зрушення в історії розвитку військової справи, зокрема в розрізі технологій.
РЕР (Радіоелектронна розвідка) ELINT (Electronic signals intelligence)	Технічні та геолокаційні розвідувальні дані, отримані зі сторонніх некомунікаційних електромагнітних випромінювань, що походять з джерел, відмінних від джерел ядерної детонації чи радіоактивних джерел.[405] Також, вважається однією з гілок SIGINT.
Робот Robot	Механізм, оснащений силовим агрегатом або елементом живлення, що здатен виконувати набір дій під прямим керуванням людини або комп'ютера або ж них обох, та який складається принаймні з платформи, ПЗ та джерела живлення[406].
Розвідка Intelligence	Термін використовується у декількох значеннях. Зокрема, говорячи про розвід.дані (англ. Intelligence), йдеться про продукт, отриманий в результаті спрямованого збору та обробки інформації про середовище, спроможності і наміри суб'єктів з метою визначення загроз та інших можливостей, що можуть бути використані десіжен-мейкерами.[407] Також, може означати процес і діяльність. (Див. також Військова розвідка.)
Система систем	Система, взаємодіючі елементи якої самі є системами. Така система володіє унікальними спроможностями, що їх не

[404] Davies, 2.
[405] JP 3-13.1, GL-8.
[406] Rademaker and Mevissen, 5.
[407] JDP 2-00 (2023, 4th ed.), 7.

SoS (System of systems)	можуть забезпечити складові системи, працюючи самостійно. Система систем може включати міжсистемну інфраструктуру, засоби та процеси, необхідні для інтеграції або взаємодії складових систем.[408]
Система ситуаційної обізнаності Situational Awareness System (SAS)	Вид СПЗ, що використовується переважно на тактичному та оперативному рівнях. Наділена функцією надання ситуаційної обізнаності, що дозволяє об'єднувати численні об'єкти поля бою і великі обсяги різних типів даних в єдину мережу. Застосовується для планування операцій, розвідки, координації сил під час виконання операції, а також на етапі аналізу проведеної операції.
Система управління боєм BMS (Battle Management System)	Вид СПЗ, що використовується на тактичному рівні в режимі активних бойових дій. Наділена функціями управління силами та засобами. Застосовується для планування операції, розвідки і координації сил під час виконання операції, а також на етапі аналізу проведеної операції.
Ситуаційна обізнаність Situational Awareness (SA)	Стан, що досягається через безперервну підтримку поінформованості про оперативне середовище в режимі реального часу або часу, наближеного до реального, у всіх доменах ведення війни та усіх вимірах. Також: комплексне розуміння поточної обстановки на полі бою, яке дозволяє командирам та військовим підрозділам ефективно приймати рішення та діяти.[409]
Спрямована енергія; Зброя спрямованої енергії DE	Спрямована енергія – це «парасольковий» термін для позначення технологій, що виробляють концентровану електромагнітну енергію та атомні або субатомні частинки.[410]

[408] Ron Ross, Mark Winstead and Michael McEvilley, "Engineering Trustworthy Secure Systems", National Institute of Standards and Technology, NIST Special Publication (SP) NIST SP 800-160v1r1, 2022, 8. <https://doi.org/10.6028/NIST.SP.800-160v1r1>. [Переглянуто 2025 29 04].
[409] «Напрям ISTAR», ГО «АЕРОРОЗВІДКА».
[410] JP 3-13.1, ix.

(Directed energy); Directed energy Weapon	Зброя спрямованої енергії – це система, що використовує спрямовану енергію головним чином як засіб для виведення з ладу, нанесення пошкоджень або знищення ворожого обладнання, об'єктів та/або персоналу.[411] Зокрема, прикладами є озброєння на основі мікрохвильового та лазерного випромінювання.
Театр війни/театр воєнних дій (ТВД) Theatre (of War)	Умовно окреслена географічна зона, що може включати наземний, повітряний та морський простори, в яких тривають бойові дії між сторонами збройного конфлікту.
Цілевказання TA (Target Acquisition)	В одному із значень – елемент концепту ISTAR. Включає: знаходження цілі, закріплення за нею та супроводження.[412]
Швидкість управління/швидкість командування Speed of Command	Час, необхідний для розпізнавання та розуміння ситуації (або зміни в ситуації), ідентифікації та оцінки варіантів, вибору відповідного курсу дій та перетворення його на дієві накази. Вважається базовим показником у вимірюванні ефективності підходу C2, організації та систем. Також: перетворення переважаючої інформаційної позиції на дію.[413]
ШІ (Штучний інтелект) AI (Artificial Intelligence)	Технологія, яка дозволяє комп'ютерам і машинам імітувати людське навчання, розуміння, вирішення проблем, прийняття рішень, прояви творчості та автономію у прийнятті рішень.[414]

[411] Там само.
[412] Davies, 2.
[413] Alberts et al., 88 and 163.
[414] Cole Stryker and Eda Kavlakoglu, "What is artificial intelligence (AI)", IBM: 9 August 2024. <https://www.ibm.com/topics/artificial-intelligence> [Переглянуто 2025 29 04].

Appendix 2

Перелік фігур

Бібліографія

1. 2001-2009 Archive for the U.S. Department of State. <https://2001-2009.state.gov/s/ct/info/c16718.htm> [Переглянуто 2025 28 04].
2. Alberts, David S., John J. Garstka and Frederick P. Stein, *Network Centric Warfare*, 2nd ed. (revised). DoD C4ISR Cooperative Research Program, Washington, D.C.: August 1999/Second printing February 2000. <http://www.dodccrp.org/files/Alberts_NCW.pdf> [Переглянуто 2025 19 04].
3. ARMOR. <https://armor.ua/ua/> [Переглянуто 2025 19 04].
4. Burdina, Eleonora, ««Ми почали будувати захищену екосистему для всіх військових застосунків». Архітектор DELTA — про розвиток системи», *DOU*: 11 липня 2024. <https://dou.ua/lenta/interviews/delta-challenges-and-plans/?fbclid=IwZXh0bgNhZW0CMTAAAR3eDaW_UIFPnAOKu4qjNHw7ShMuN1478z_XOH3mMpyWgDindHie3C9878s_aem_6JTNM5d4JFoU59zXZq9tyg> [Переглянуто 2025 24 04].
5. Carafano, James J., "America's Joint Force and the Domains of Warfare". 2018 Index of U.S. Military Strength, Dakota L. Wood (ed.), Davis Institute for National Security and Foreign Policy, The Heritage Foundation, 2018. <https://www.heritage.org/sites/default/files/2017-10/2018_IndexOfUSMilitaryStrength-2.pdf> [Переглянуто 2025 17 04].
6. Chernohorenko, Kateryna, 8 May 2025. <https://www.facebook.com/katheryn.chernohorenko/posts/pfbid0ck9fHauX8HbgQBZesMMnBhccMpv5AG7JJUxxkjiDNNLVPhuKe93Erk5PtbVWn8Skl > [Переглянуто 2025 08 05].
7. Chief of Staff Paper #1 "Army Multi-Domain Transformation", Unclassified Version, HQ, Department of the Army, 16 March 2021. <https://apps.dtic.mil/sti/pdfs/AD1143195.pdf> [Переглянуто 2025 19 04].
8. ComBat Vision, December 18, 2024. <https://www.facebook.com/watch/?v=3095915140567211> [Переглянуто 2025 29 04].
9. ComBat Vision, July 23, 2024. <https://www.facebook.com/watch/?v=3659430964386392 > [Переглянуто 2025 29 04].

10. Crabtree, Matt, “What is Machine Learning? Definition, Types, Tools & More”, DataCamp, Nov 8, 2024. <https://www.datacamp.com/blog/what-is-machine-learning> [Переглянуто 2025 29 04].
11. Daniel, Brett, “What Is Joint All-Domain Command and Control (JADC2)?”, Trenton Systems: Nov 9, 2020. <https://www.trentonsystems.com/en-us/resource-hub/blog/what-is-jadc2> [Переглянуто 2025 19 04].
12. Davies, Philip H.J., “ISR versus ISTAR: A Conceptual Crisis in British Military Intelligence”, draft paper (in press with *International Journal of Intelligence and Counterintelligence*, 2021/35 (1), 73-100). <https://bura.brunel.ac.uk/bitstream/2438/22272/3/FullText.pdf> [Переглянуто 2025 19 04].
13. Davis, Jr."Skip" Gordon B. and Lorenz Meier, “The Challenges Posed by 21st-Century Warfare and Autonomous Systems”, CEPA: October 25, 2023. <https://cepa.org/article/the-challenges-posed-by-21st-century-warfare-and-autonomous-systems/> [Переглянуто 2025 21 04].
14. DeepState Map. <https://deepstatemap.live/#6/49.4383200/32.0526800> [Переглянуто 2025 24 04].
15. DeepState UA, Oct 3, 2023. <https://x.com/Deepstate_UA/status/1709289488722108529> [Переглянуто 2025 24 04].
16. “Defining Possible Against Unmanned Aerial Systems”, Northrop Grumman. <https://www.northropgrumman.com/what-we-do/land/counter-unmanned-aerial-systems-c-uas> [Переглянуто 2025 26 04].
17. “DOD Dictionary of Military and Associated Terms”. Department of Defense, March 2017. <https://www.tradoc.army.mil/wp-content/uploads/2020/10/AD1029823-DOD-Dictionary-of-Military-and-Associated-Terms-2017.pdf> [Переглянуто 2025 04 16].
18. “Electronic Warfare”, Lockheed Martin. <https://www.lockheedmartin.com/en-us/capabilities/electronic-warfare.html> [Переглянуто 2025 28 04].
19. FM 3-0 “Operations”. HQ, Department of the Army, October 2022. <https://irp.fas.org/doddir/army/fm3-0.pdf> [Переглянуто 2025 17 04].
20. FM 30-5, Department of the Army Field Manual “Combat Intelligence”, February 1951. <https://ia802207.us.archive.org/30/items/KoreanWarFieldManuals/FM%2030-5%20%28%20Combat%20Intelligence%20%29.pdf> [Переглянуто 2025 28 04].

21. GEN Perkins, David G., “Multi-Domain Battle: Driving Change to Win in the Future”. *Military Review*, July-August 2017. <https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20170831_PERKINS_Multi-domain_Battle.pdf> [Переглянуто 2025 17 04].
22. “GPS Blue Force Tracking Systems Application Note”, SAVER, U.S. Department of Homeland Security, Space and Naval Warfare Systems Center Atlantic: April 2014. <https://www.dhs.gov/sites/default/files/publications/GPS-Blue-Force-AppN_0414-508_0.pdf> [Переглянуто 2025 26 04].
23. Harvey, Andrew S., “The Levels of War as Levels of Analysis”. *Military Review*, November-December 2021. <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2021/Harvey-Levels-of-War/> [Переглянуто 2025 29 04].
24. Himera Radios, March 21, 2025. <https://www.facebook.com/watch/?v=520682327658419> [Переглянуто 2025 29 04].
25. Horowitz, Michael and Paul Scharre, “An Introduction to Autonomy in Weapon Systems”, Center for a New American Security: February 13, 2015. <https://www.cnas.org/publications/reports/an-introduction-to-autonomy-in-weapon-systems > [Переглянуто 2025 21 04].
26. Horowitz, Michael and Paul Scharre, “Meaningful Human Control in Weapon Systems: A Primer”, Center for a New American Security: 16 March, 2015. <https://www.cnas.org/publications/reports/meaningful-human-control-in-weapon-systems-a-primer>. [Переглянуто 2025 21 04].
27. “Integrated Battle Command System (IBCS)”, Missile Defense Advocacy Alliance, July 17, 2024. <https://missiledefenseadvocacy.org/integrated-battle-networks/integrated-battle-command-system-ibcs/ > [Переглянуто 2025 27 04].
28. “Intelligence Studies: Imagery/Geospatial Intelligence (IMINT/GEOINT)”, U.S. Naval War College Library. <https://usnwc.libguides.com/c.php?g=494120&p=3381562> [Переглянуто 2025 27 04].
29. Joint Doctrine Publication 0-01.1 (JDP 0-01.1) “UK Terminology Supplement to NATOTerm”. UK Ministry of Defence (Edition A), March 2025. <https://assets.publishing.service.gov.uk/media/651fcb7d79fc58000d63971c/20231004-JDP_0_01_1_2023_Edition_B_web.pdf> [Переглянуто 2025 27 04].

30. Joint Doctrine Publication 2-00 (JDP 2-00) “Intelligence, Counter-intelligence and Security Support to Joint Operations”. UK Ministry of Defence, The Development, Concepts and Doctrine Centre, August 2023 (4th edition). <https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf> [Переглянуто 2025 19 04].
31. Joint Publication 1 (JP 1) “Doctrine for the Armed Forces of the United States”. Armed Forces of the United States, 25 March 2013, Incorporating Change 1, 12 July 2017. <https://irp.fas.org/doddir/dod/jp1.pdf> [Переглянуто 2025 16 04].
32. Joint Publication 1-02 (JP 1-02) “Department of Defense Dictionary of Military and Associated Terms”. Joint Chiefs of Staff, 12 April 2001 (As Amended Through 30 September 2010). <https://irp.fas.org/doddir/dod/jp1_02.pdf> [Переглянуто 2025 29 04].
33. Joint Publication 3-0 (JP 3-0) “Joint Operations”. Chairman of the Joint Chiefs of Staff, 11 August 2011. <https://irp.fas.org/doddir/dod/jp3_0.pdf> [Переглянуто 2025 19 04].
34. Joint Publication 3-13.1 (JP 3-13.1) “Electronic Warfare”. Chairman of the Joint Chiefs of Staff, 08 February 2012. <https://info.publicintelligence.net/JCS-EW.pdf> [Переглянуто 2025 19 04].
35. Joint Publication 6-0 (JP 6-0) “Joint Communications System”. Chairman of the Joint Chiefs of Staff, 10 June 2015, Incorporating Change 1, 04 October 2019. <https://irp.fas.org/doddir/dod/jp6_0.pdf> [Переглянуто 2025 19 04].
36. Judson, Jen, “US Army adopts new multidomain operations doctrine”. *DefenseNews*, 10 October 2022. <https://www.defensenews.com/land/2022/10/10/us-army-adopts-new-multidomain-operations-doctrine/ > [Переглянуто 2025 19 04].
37. Kistol (Aniskina), Kateryna, “The ways to fight proxy war: Conventional vs. Unconventional warfare strategies. How is the warfare strategy related to conflict outcomes?”, Dissertation, UCL, September 2020. <https://surli.cc/lkmspi> [Переглянуто 2025 05 05].
38. Lawless, Robert and Hitoshi Nasu, “Augmented Reality Battlefield”, Lieber Institute West Point, *Articles of War*: April 28, 2022. <https://lieber.westpoint.edu/augmented-reality-battlefield/> [Переглянуто 2025 26 04].
39. MAJ Dzwonczyk, John and MAJ Clayton Merkley, “Through a Glass Clearly: An Improved Definition of LSCO”, *Military Review (Online Exclusive)*, November 2023. <https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-

Exclusive/2023/Through-a-Glass-Clearly/Merkley-Through%20A%20Glass%20Clearly%20UA1.pdf> [Переглянуто 2025 28 04].

40. MAJ Granai, Cornelius, ““A Complex and Volatile Environment”: The Doctrinal Evolution from Full Spectrum Operations to Unified Land Operations”, U.S. Army, 2015-01. <https://apps.dtic.mil/sti/tr/pdf/AD1001386.pdf> [Переглянуто 2025 19 04].
41. MAJ Jackman, Ben, “Understanding the Anti-Access and Area Denial Threat: An Army Perspective”, U.S. Army, 2015-01. <https://apps.dtic.mil/sti/tr/pdf/AD1001466.pdf> [Переглянуто 2025 26 04].
42. McManus, Jeff, “Operating Successfully within the Bureaucracy Domain of Warfare: Part One”. *US Army War College Publications*, May 29, 2024. <https://publications.armywarcollege.edu/News/Display/Article/3789970/operating-successfully-within-the-bureaucracy-domain-of-warfare-part-one/> [Переглянуто 2025 16 04].
43. “Military Command Structure”, NATO. <https://shape.nato.int/military_command_structure> [Переглянуто 2025 29 04].
44. “Multi-Domain Battle: Evolution of Combined Arms for the 21st Century: 2025-2040”. TRADOC, December 2017, Version 1.0. <https://www.tradoc.army.mil/wp-content/uploads/2020/10/MDB_Evolutionfor21st.pdf> [Переглянуто 2025 17 04].
45. NATO STANDARD AJP-2 “Allied Joint Doctrine for Intelligence, Counterintelligence and security”, NATO, NATO Standardization Office (Edition A, Version 2): February 2016. <https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP2.pdf> [Переглянуто 2025 28 04].
46. NATO, Declassified. <https://www.nato.int/cps/en/natohq/declassified_138449.htm> [Переглянуто 2025 21 04].
47. Odom, William O. and Christopher D. Hayes, “Cross-Domain Synergy”. *Joint Force Quarterly*, 73, 2nd Quarter 2014. <https://ndupress.ndu.edu/portals/68/documents/jfq/jfq-73/jfq_123-128_odom-hayes.pdf> [Переглянуто 2025 19 04].
48. Pin, Clement, “Semi-structured Interviews”. *LIEPP Methods Brief*, Sciences Po, 2023 (№4). <https://sciencespo.hal.science/hal-04087970/document> [Переглянуто 2025 04 16].
49. “Project "Kolossal", DeepState. <https://kolossal.deepstateua.tech/> [Переглянуто 2025 24 04].

50. Rademaker, Michel and LtCol Sjoerd Mevissen, “Robotic and Autonomous Systems: From design to development and use in military operations” (ed. Alessandra Barrow), The Hague Centre for Strategic Studies: November 29, 2022. <https://hcss.nl/wp-content/uploads/2022/11/Robotic-and-Autonomous-Systems-From-design-to-development-and-use-in-military-operations-Final.pdf> [Переглянуто 2025 21 04].
51. “Revolutionizing Command and Control”, Northrop Grumman. <https://www.northropgrumman.com/what-we-do/land/integrated-battle-command-system-ibcs> [Переглянуто 2025 27 04].
52. Rosenberg, Barry, “How the Army is driving enterprise training across five warfighting domains and three dimensions”. *Breaking Defense*, May 23, 2024. <https://breakingdefense.com/2024/05/how-the-army-is-driving-enterprise-training-across-five-warfighting-domains-and-three-dimensions/> [Переглянуто 2025 19 04].
53. Ross, Ron, Mark Winstead and Michael McEvilley, “Engineering Trustworthy Secure Systems”, National Institute of Standards and Technology, NIST Special Publication (SP) NIST SP 800-160v1r1, 2022. <https://doi.org/10.6028/NIST.SP.800-160v1r1>. [Переглянуто 2025 29 04].
54. Saw, David, “SKYKEEPER – Expanding Ground-Based Air Defence Possibilities in Britain”, *European Security and Defence*: 15 November 2022. <https://euro-sd.com/2022/11/articles/26817/skykeeper-expanding-ground-based-air-defence-possibilities-in-britain/ > [Переглянуто 2025 26 04].
55. “Security within the North Atlantic Treaty Organization (NATO)”, NATO, Note by the Secretary General: 20 November 2020. <https://www.nbf.hu/docs/C-M%282002%2949-REV1.pdf> [Переглянуто 2025 21 04].
56. Seeback, Lesley, “Why the fifth domain is different”. *The Strategist*, 5 Sep 2019. <https://www.aspistrategist.org.au/why-the-fifth-domain-is-different/> [Переглянуто 2025 16 04].
57. “STAR-PAN™ Integrated Soldier Multiport USB Data Hub / Power Distribution Systems and Tactical Interconnects”, Glenair. <https://www.glenair.com/star-pan/index.htm> [Переглянуто 25 22 04].
58. Stenson, Randi, “US Army Training and Doctrine Command updates Army capstone doctrine, codifying shift to multidomain operations”. U.S. Army: October 10, 2022. <https://www.army.mil/article/260943/us_army_training_and_doctrine_command_updates_army_capstone_doctrine_codifying_shift_to_multidomain_operations> [Переглянуто 2025 19 04].

59. Strachan-Morris, David, “Knowledge gives strength to the arm: an agenda for studying combat intelligence as a discrete function within military Intelligence”. *Intelligence and National Security*, 2024 (vol.39), issue 7. <https://doi.org/10.1080/02684527.2024.2383011> [Переглянуто 2025 20 04].
60. Stryker, Cole and Eda Kavlakoglu, “What is artificial intelligence (AI)”, IBM: 9 August 2024. <https://www.ibm.com/topics/artificial-intelligence> [Переглянуто 2025 29 04].
61. Tetreau, Matthew, “A Beginner’s Guide to Army Doctrine”, *The Company Leader*: June 12, 2020. <https://companyleader.themilitaryleader.com/2020/06/12/on-doctrine/ > [Переглянуто 2025 27 04].
62. “The Army’s Multi-Domain Task Force (MDTF)”. Congressional Research Service, updated July 10, 2024. <https://sgp.fas.org/crs/natsec/IF11797.pdf> [Переглянуто 2025 19 04].
63. “The NATO Lessons Learned Handbook”, NATO, Joint Analysis and Lessons Learned Centre (4th edition): June 2022. <https://www.jallc.nato.int/application/files/4416/5781/2017/JALLC_LL_Handbook_Update_-_4th_Edition_FINAL_14072022.pdf> [Переглянуто 2025 28 04].
64. Trick, Christopher, “SIGINT vs. COMINT vs. ELINT: Key Differences and Must-Know Use Cases”, *Blogs by Trenton Systems*, Trenton Systems, Oct 17 2022. <https://www.trentonsystems.com/en-us/resource-hub/blog/sigint-vs-comint-vs-elint> [Переглянуто 2025 26 04].
65. “Wargaming”, RAND. <https://www.rand.org/topics/wargaming.html> [Переглянуто 2025 28 04].
66. “What is C4ISR”, ГО «АЕРОРОЗВІДКА», Sept 20, 2022. <http://surl.li/nlwnxd> [Переглянуто 2025 19 04].
67. “What is ground-based air defence?”, SAAB. <https://www.saab.com/newsroom/stories/themes/what-is-ground-based-air-defence> [Переглянуто 2025 27 04].
68. Withrington, Claire, “The Internet of Military Things”, *The Cove*: 24/08/2023. <https://cove.army.gov.au/article/internet-military-things> [Переглянуто 2025 28 04].
69. “Zero Trust Architecture”, National Cybersecurity Center of Excellence. <https://web.archive.org/web/20210422024921/https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture> [Переглянуто 2025 28 04].
70. «DELTA у трійці найпопулярніших бойових систем – Катерина Черногоренко про опитування в Армія+», Міністерство оборони України: 9 жовтня 2024.

<https://www.mil.gov.ua/news/2024/10/09/delta-u-trijczi-najpopulyarnishih-bojovih-sistem/> [Переглянуто 2025 21 04].

71. «UkrspecSystems представила власний варіант сучасної ударно-розвідувальної системи», *Defense Express*: 20 вересня 2021. <https://defence-ua.com/news/ukrspecsystems_predstavila_vlasnij_variant_suchasnoji_udarno_rozviduvalnoji_sistemi-4813.html> [Переглянуто 2025 22 04].
72. «Адміністративні домовленості щодо охорони інформації з обмеженим доступом між урядом України та організацією Північноатлантичного договору», 24.05.2017. <https://zakon.rada.gov.ua/laws/show/950_035-16#Text> [Переглянуто 2025 21 04].
73. «Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів», Збірник тез доповідей VIII Всеукраїнської науково-практичної конференції, Науково-дослідний центр службово-бойової діяльності Національної гвардії України, 31 жовтня 2019 року. <https://nangu.edu.ua/uploads/files/documenty/Naukova%20diyalnist/naukovu%20forumy/2019/9%20%20%20%20%20%2031.10.2019%20Zbirnyk%20tez%20NPK.pdf> [Переглянуто 2025 18 04].
74. «В Україні вперше перевірили кібербезпеку бойової системи за стандартами рівня НАТО», Міністерство оборони України: 17 липня 2024. <https://mod.gov.ua/news/v-ukrayini-vpershe-perevirili-kiberbezpeku-bojovoyi-sistemi-za-standartami-rivnya-nato> [Переглянуто 2025 24 04].
75. «Від C2 до C4ISR: що ховається за цими абревіатурами», *Defense Express:* 31 травня 2020. <https://defence-ua.com/weapon_and_tech/vid_s2_do_s4isr_scho_hovajetsja_za_tsimi_abreviaturami-872.html> [Переглянуто 2025 19 04].
76. ГО «Аеророзвідка». <https://www.facebook.com/aerorozvidka/videos/997603335605070> [Переглянуто 2025 24 04].
77. Дзюба, Олексій, ««IT може допомогти, але виграти війну за допомогою IT неможливо». Інтерв'ю з розробником найпопулярнішої в Україні карти бойових дій DeepState», *dev.ua*: 13 грудня 2023. <https://dev.ua/news/it-mozhe-dopomohty-ale-vyhraty-viinu-za-dopomohoiu-it-nemozhlyvo-interviu-iz-rozrobnykom-naipopuliarnishoi-v-ukraini-karty-boiovykh-dii-deepstate> [Переглянуто 2025 24 04].

78. Древницький, Данило, «Автоматизована система управління військами – зброя перемог». *Військовий кур'єр:* 3 грудня 2022. <https://mil.co.ua/avtomatyzovana-systema-upravlinnya-vijskamy-zbroya-peremogy/> [Переглянуто 2025 21 04].
79. Заблоцький, Володимир, «Чому "Топаз" - не "Оболонь"», *Defense Express*: 05 травня 2020. <https://defence-ua.com/weapon_and_tech/chomu_topaz_ne_obolon-645.html> [Переглянуто 2025 21 04].
80. «Завдяки системі DELTA знищено ворожої техніки на більше ніж 15 мільярдів доларів – Рустем Умєров», Міністерство оборони України: 26 серпня 2024. <https://mod.gov.ua/news/zavdyaki-sistemi-delta-znishheno-vorozhoi-tehniki-na-bilshe-nizh-15-milyardiv-dolariv> [Переглянуто 2025 21 04].
81. Закон України «Про хмарні послуги», 2023. <https://zakon.rada.gov.ua/laws/show/2075-20#Text> [Переглянуто 2025 24 04].
82. «ЗСУ отримали сучасні мобільні АСУ «Ореанда»», *Defense Express*: 23 грудня 2018. <https://old.defence-ua.com/index.php/home-page/6107-zsu-otrymaly-suchasni-mobilni-asu-oreanda> [Переглянуто 2025 21 04].
83. Інтерв'ю з Євгеном Максименком для Astero Analytics, грудень 2023 (особисті матеріали автора). <https://surl.gd/icgeuv> [Переглянуто 2025 05 05].
84. Інтерв'ю з респондентом Артемом Мартиненком, архітектором ІКС «DELTA».
85. Інтерв'ю з респондентом Дмитром Шамраєм, співзасновником системи «Griselda».
86. Інтерв'ю з респондентом Євгеном Максименком, розробником системи «CombatVision».
87. Інтерв'ю з респондентом Олексієм Гавришем, одним із розробників системи «ARMOR» (ГРК «Броня»).
88. Інтерв'ю з респондентом Русланом Микулою, одним із розробників системи «KOLOSSAL» команди DeepState.
89. Інтерв'ю з респондентом, одним із розробників системи «Вежа».
90. Карпенко, Ольга, ««Аеророзвідка» роздасть безкоштовні ключі безпеки військовим-користувачам Delta», *AIN*: 24 березня, 2023. <https://ain.ua/2023/03/24/aerorozvidka-2/> [Переглянуто 2025 24 04].
91. «Керівництво з бойової роботи вогневих підрозділів артилерії». Міністерство оборони України, 2019. <https://sprotyvg7.com.ua/wp-content/uploads/2022/06/%D0%9A%D0%91%D0%A0_2019.pdf> [Переглянуто 2025 22 04].

92. Кива, Владислав, Євген Судніков, Олександр Войтко, «Методи розвідки кіберпростіру». *Сучасні інформаційні технології у сфері безпеки та оборони*, 2018/Том 33 (№ 3). <https://sit.nuou.org.ua/article/view/154348> [Переглянуто 2025 26 04].
93. Консультації з військовими СОУ.
94. Консультація з військовим СОУ, користувачем ІКС «DELTA».
95. Консультація з Інною Гончар, керівницею напрямку «Управління знаннями» ГО «Аеророзвідка».
96. «Корупція в оборонці: викрито схему розкрадання коштів на систему «ДЗВІН» (ВІДЕО)», Національне Антикорупційне Бюро України: 19-02-2025. <https://nabu.gov.ua/news/koruptciia-v-oborontci-vykryto-skhemu-rozkradannia-koshtiv-na-systemu-dzvin/> [Переглянуто 2025 21 04].
97. Кузьменко, Олександр, «Український розвідувальний ШІ-стартап Griselda з допомогою фонду Double Tap Investments залучив $600 000 інвестицій», *dev.ua*, 7 березня 2025. <https://dev.ua/news/600k-dlia-griselda-1741334724> [Переглянуто 2025 20 04].
98. Матеріали, надані Дмитром Шамраєм, співзасновником системи «Griselda».
99. Матеріали, надані Олексієм Гавришем, одним із розробників ГРК «Броня» (ARMOR).
100. Матеріали, надані розробниками фільму «Перший бій»: <https://the-first-battle.minisite.ai/ua> [Переглянуто 2025 21 04].
101. Машай, Богдан, «Що таке Griselda. Як нова українська розробка змінює правила війни – велике інтерв'ю», *NV*, 5 листопада 2024. <https://nv.ua/ukr/ukraine/events/shtuchniy-intelekt-na-viyni-rozrobnik-sistemi-griselda-rozpoviv-yak-it-tehnologiji-zminyuyut-viynu-50463391.html> [Переглянуто 2025 21 04].
102. Машталір, Вадим, Олександр Жук, Людмила Міненко, Сергій Артюх, «Концептуальні підходи застосування бездротових сенсорних мереж арміями передових країн світу». *Сучасні інформаційні технології у сфері безпеки та оборони*. 2023/Том 47 (№ 2). <https://doi.org/10.33099/2311-7249/2023-47-2-96-112> [Переглянуто 2025 19 04].
103. Мельник, Тася, «Військовий софт Delta тепер офіційно у ЗСУ. Він допомагав у всіх великих операціях – від потоплення «Москви» до звільнення Зміїного. Чому з ним воювати швидше», *Forbes Ukraine*: 04 лютого 2023. <https://forbes.ua/innovations/twitter-dlya-zsu-viyskoviy-soft-delta-dopomagav-u-

vsikh-velikikh-operatsiyakh-vid-potoplennya-moskvi-do-zvilnennya-zmiinogo-chomu-z-nim-zsu-voyuyut-shvidshe-07122022-10318> [Переглянуто 2025 24 04].

104. «Методичні рекомендації використання спеціалізованого програмного забезпечення «Віраж-планшет» під час підготовки бойових обслуг підрозділів Зенітних ракетних військ Повітряних сил Збройних сил України», ВП 7-09(12).02, Центр оперативних стандартів і методики підготовки Збройнх сил України спільно з Командуванням Повітряних сил Збройних сил України, серпень 2019. <https://www.hups.mil.gov.ua/assets/uploads/library/nadhodzhennya/lypen-veresen-2020/pdf/30.pdf> [Переглянуто 2025 29 04].

105. Міністерство оборони України, August 26, 2024. <https://www.facebook.com/watch/?v=1194328181785172> [Переглянуто 2025 29 04].

106. «Міноборони представило інноваційні військові розробки на виставці NATO Edge 24», Міністерство оборони України, 12 грудня 2024. < https://mod.gov.ua/news/minoboroni-predstavilo-innovaczijni-vijskovi-rozrobki-na-vistavczi-nato-edge-24 > [Переглянуто 2025 08 05].

107. Міночкін, А.І., В.А. Романюк, О.В. Жук, «Перспективи розвитку тактичних сенсорних мереж», *Збірник наукових праць ВІТІ НТУУ «КПІ»,* 2007 (No 4). <https://journal.viti.edu.ua/public/romanuk/2007/4_2007.pdf> [Переглянуто 2025 28 04].

108. «Напрям ISTAR», ГО «АЕРОРОЗВІДКА». <https://aerorozvidka.ngo/direction/istar> [Переглянуто 2025 19 04].

109. «Не проти РФ: США розгорнуть наступний далекобійний Typhon з Tomahawk на Гаваях, а не у Європі», *Defense Express*: 18 березня 2025. <https://defence-ua.com/news/ne_proti_rf_ssha_rozgornut_nastupnij_dalekobijnij_typhon_z_tomahawk_na_gavajah_a_ne_u_jevropi-18291.html> [Переглянуто 2025 19 04].

110. Непублічна онлайн-лекція (1).

111. Непублічна онлайн-лекція (2).

112. «Обрій, Симулятор місій БПЛА». <https://www.obriy.airforce/> [Переглянуто 2025 21 04].

113. Особиста розмова з Віталієм Кирилівим, співрозробником VR-фільму «Перший бій».

114. Особиста розмова з Інною Гончар, керівницею напрямку «Управління знаннями» ГО «Аеророзвідка».

115. Особиста розмова з розробником системи «Неон».
116. Особиста розмова з розробником системи «Промінь».
117. Особиста розмова з розробником СПЗ «Вежа».
118. Особиста розмова з фахівцем МОУ.
119. Особиста розмова зі співрозмовником N.
120. Особиста розмова із засновником системи «Comintify».
121. Особисто отримана консультація з військовим СОУ, користувачем кількох систем.
122. Пастухов, Олександр, «АСУ Збройних сил», *Militarnyi*: 20 березня 2012. <https://mil.in.ua/uk/d0-b0-d1-81-d1-83-d0-b7-d0-b1-d1-80-d0-be-d0-b9-d0-bd-d0-b8-d1-85-d1-81-d0-b8-d0-bb/> [Переглянуто 2025 24 04].
123. «Планування вогневої підтримки на тактичному рівні (початок)», Сили територіальної оборони ЗСУ. <https://sprotyvg7.com.ua/lesson/planuvannya-vognevoi-pidtrimki-na-taktichnomu-rivni> [Переглянуто 2025 19 04].
124. «Платформа відеоаналізу поля бою Vezha тепер доступна в DELTA — Катерина Черногоренко», Міністерство оборони України, 14 жовтня 2024. <https://mod.gov.ua/news/platforma-videoanalizu-polya-boyu-vezha-teper-dostupna-v-delta-katerina-chernogorenko> [Переглянуто 2025 19 04].
125. «Послідовність та зміст роботи командира з організації бою. (TLP)», Сили Територіальної оборони ЗСУ. <https://sprotyvg7.com.ua/lesson/poslidovnist-ta-zmist-roboti-komandira-z-organizacii-boyu-tlp> [Переглянуто 2025 28 04].
126. Постанова КМУ № 139 від 4 лютого 2023 «Деякі питання підвищення рівня цифровізації сил безпеки та сил оборони України у період воєнного стану». <https://zakon.rada.gov.ua/laws/show/139-2023-%D0%BF#Text> [Переглянуто 2025 24 04].
127. Постанова КМУ № 234 від 3 березня 2021 р. «Про затвердження Порядку розроблення, освоєння та випуску нових видів товарів оборонного призначення, а також припинення випуску існуючих видів таких товарів». <https://zakon.rada.gov.ua/laws/show/234-2021-%D0%BF#Text> [Переглянуто 2025 21 04].
128. Пушкіна, Вікторія, «Поклик неба: Історія військового ЗСУ, який створив перший в Україні симулятор розвідки та коригування», *r_d media*. <https://robotdreams.cc/uk/blog/506-pershyy-v-ukrayini-symulyator-rozvidky-ta-koryhuvannya> [Переглянуто 2025 21 04].

129. Ракушев, Михайло, Віталій Зуйко, Роман Пантюшенко, «Аналіз використання інформаційно-телекомунікаційної системи «ТЕРМІНАЛ» в інтересах Сил оборони Києва». *Сучасні інформаційні технології у сфері безпеки та оборони*, 2022/Том 44 (№2). <https://sit.nuou.org.ua/article/view/264158/261332> [Переглянуто 2025 21 04].

130. «Рекомендації з планування та організації бою за стандартами НАТО (частина 1)», Сили Територіальної оборони ЗСУ. <https://sprotyvg7.com.ua/lesson/rekomendacii-planuvanya-boyu-nato> [Переглянуто 2025 28 04].

131. Сабадашина, Юлія, ««Коса смерті» для окупантів і захист для українських кулеметників. Розповідаємо про турель «ШаБля» та її розробників», *DOU*: 20 червня 2024. <https://dou.ua/lenta/articles/about-shablya-and-roboneers/> [Переглянуто 2025 21 04].

132. Сабадашина, Юлія, «Міноборони шукає фахівців з VR та AR, щоб створювати симулятори для навчання військових», *DOU*: 30 травня 2024. <https://dou.ua/lenta/news/vr-and-ar-in-the-army/> [Переглянуто 2025 21 04].

133. Сафронов, Тарас, «Система управління “Дзвін-АС” стала на озброєння України», *Militarnyi*: 8 грудня 2022. <https://mil.in.ua/uk/news/systema-upravlinnya-dzvin-as-stala-na-ozbroyennya-ukrayiny/> [Переглянуто 2025 21 04].

134. Стаття 1 Закону України «Про Державну таємницю». <https://zakon.rada.gov.ua/laws/show/3855-12#Text> [Переглянуто 2025 21 04].

135. «США розгортають п'ять Multi-Domain Task Forces для масштабної війни: коли гіперзвук об'єднують з хакерами», *Defense Express*: 29 лютого 2024. <https://defence-ua.com/army_and_war/ssha_rozgortajut_pjat_multi_domain_task_forces_dlja_masshtabnoji_vijni_koli_giperzvuk_objednujut_z_hakerami-14595.html> [Переглянуто 2025 19 04].

136. «Тренувальні системи», SKIFTECH. <https://ua.skif.cc/trenuvalni-sistemi/> [Переглянуто 2025 21 04].

137. «У ЗСУ стартує перша навчальна програма для інструкторів бойової системи DELTA», Міністерство оборони України: 17 березня 2025 <https://mod.gov.ua/news/u-zsu-startuye-persha-navchalna-programa-dlya-instruktoriv-bojovoyi-sistemi-delta?fbclid=IwY2xjawJEyzxleHRuA2FlbQIxMAABHeKi8llNWvVGOEtoNYTYNt9NnCAxeQ

1o_HK3PStE2ccPMRLwi_sBcqTtAg_aem_eIxANbFPJGmYX9e9suT0KA> [Переглянуто 2025 24 04].

138. «У кожному гаражі "Силіконова долина". Гончар про виробництво дронів в Україні», *Українське радіо*: 23.07.2024. <http://www.nrcu.gov.ua/news.html?newsID=104887> [Переглянуто 2025 19 04].

139. «Українські військові виявляють 12 тисяч цілей щотижня завдяки штучному інтелекту — Катерина Черногоренко», Міністерство оборони України, 23 вересня 2024. <https://mod.gov.ua/news/ukrayinski-vijskovi-viyavlyayut-12-tisyach-czilej-shhotizhnya-zavdyaki-shtuchnomu-intelektu-katerina-chernogorenko> [Переглянуто 2025 08 05].

140. Фотозвіти, АрміяSOS. <https://armysos.com.ua/uk/gallery-ua/> [Переглянуто 2025 29 04].

141. Чалий, Дмитро, «Уперше американську систему імітаційного моделювання JCATS випробували курсанти-зенітники», *АрміяInform*: 10 Квітня 2021. <https://armyinform.com.ua/2021/04/10/upershe-amerykansku-systemu-imitaczijnogo-modelyuvannya-jcats-vyprobuvaly-kursanty-zenitnyky/> [Переглянуто 2025 18 04].

142. Шкальова, Анастасія, «Від авіасимуляторів до рекрутингу. Як AR/VR використовують у підготовці військових», *Vector*: 19 Травня 2023. <https://vctr.media/ua/vid-pidgotovki-pilotiv-do-rekrutingu-yak-ar-vr-vikoristovuyut-u-pidgotovczi-vijskovih-ta-stvorenni-zbroyi-183908/> [Переглянуто 2025 28 04].

143. «Що таке GitHub і як з ним працювати», *go it*, 25.02.2025. <https://goit.global/ua/articles/shcho-take-github-i-iak-z-nym-pratsiuvaty/> [Переглянуто 2025 08 05].

144. «Що таке система DELTA і як вона задає тренди для країн НАТО?», Міністерство оборони України: 30 березня 2024. <https://mod.gov.ua/news/shho-take-sistema-delta-i-yak-vona-zadae-trendi> [Переглянуто 2025 24 04].

145. «Щодо стану і перспектив розвитку розробок інформаційно-комунікаційних систем для потреб ЗСУ», складено експертами Громадської спілки «Фонд підтримки реформ в Україні» (непублічний звіт, надано Інною Гончар).

146. «Як працює система управління військами Delta. Інтерв'ю зі співзасновником ГО "Аеророзвідка" Ярославом Гончаром», *Militarnyi*: 5 лютого 2023. <https://mil.in.ua/uk/articles/yak-pratsyuye-systema-upravlinnya-vijskamy-

delta-interv-yu-zi-spivzasnovnykom-go-aerorozvidka-yaroslavom-goncharom/> [Переглянуто 2025 21 04].

147. «Як проводити Аналіз проведених дій (АПД, After action review – AAR)», Сили територіальної оборони ЗСУ: 03.05.2024. <https://tro.mil.gov.ua/yak-provodyty-analiz-provedenyh-dij-apd-after-action-review-aar/> [Переглянуто 2025 26 04].

148. Ярова, Майя, ««Це – війна технологій». Як харків'яни створили тактичні симулятори SkifTech, які рятують життя військових», *AIN*: 17 лютого, 2023. <https://ain.ua/2023/02/17/yak-harkivski-trenuvalni-systemy-skiftech-ryatuyut-zhyttya-vijskovyh/> [Переглянуто 2025 21 04].