https://doi.org/10.31891/2307-5740-2026-356-20
УДК 355.4:004.8:623.4
JEL classification F52, H56, H83, K24, O33, O38

ГАВРИЛЕЧКО Юрій
ЗВО «Університет трансформації майбутнього»
https://orcid.org/0000-0003-1930-7638

ТРАНСФОРМАЦІЯ СУЧАСНОЇ ВІЙНИ: ЯК ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЗМІНЮЮТЬ МОДЕЛІ ПУБЛІЧНОГО УПРАВЛІННЯ

Статтю присвячено дослідженню якісної трансформації сучасної війни: від класичного збройного протистояння до парадигми, при якій головним полем бою стають інформаційно-обчислювальні системи на основі штучного інтелекту (ШІ), а людина поступово переходить у роль наглядача. Сучасна війна стає дедалі більше управлінсько-технологічною задачею, що вимагає високого рівня взаємодії між владою, освітою, бізнесом і військовими. Обґрунтовано чотири визначальні ознаки третьої епохи: когнітивна перевага через масову обробку даних і ШІ-інтеграцію OODA-циклу (Спостерігай – Орієнтуйся – Вирішуй – Дій); автономні системи зброї (АСЗ) як якісно новий клас акторів; державні датацентри як об'єкти стратегічного удару; структурна асиметрія етичних обмежень між демократіями і авторитарними режимами. На основі досвіду російсько-української війни показано, що театр бойових дій вже є лабораторією нової парадигми, що підтверджується зростанням частки FPV-дронів (First-Person View, дрони з відеопоглядом від першої особи) з елементами автономного наведення і стратегічною роллю інтеграції ШІ в оперативні процеси. Додатково аналізується вплив трансформації на систему публічного управління: необхідність інституційної адаптації, формування системи інформаційної безпеки, нормативно-правового регулювання роботи державних службовців з ШІ та цілеспрямованої підготовки фахових операторів ШІ для Міноборони і держслужби. Визначено умови збереження людського нагляду за АСЗ як ключової умови невідчуження відповідальності.

Ключові слова: штучний інтелект, автономні системи зброї, цифрова війна, державне управління, інформаційна безпека, петля Бойда, система Палантир, когнітивна перевага, кіберстратегія, державна кібербезпека.

GAVRYLECHKO Yuriy
Higher Educational Institution "University of Future Transformation"

TRANSFORMING MODERN WARFARE: HOW INFORMATION TECHNOLOGY IS CHANGING PUBLIC ADMINISTRATION MODELS

The article investigates the qualitative transformation of modern warfare: from classical armed confrontation to a paradigm in which information-computational systems based on artificial intelligence (AI) become the principal actors on the battlefield, while the human progressively shifts to the role of overseer. Modern war is increasingly a managerial and technological task requiring high-level cooperation between government, education, business and the military – a thesis confirmed by the empirical evidence of the Russo-Ukrainian conflict. Three stages of the evolution of armed conflict are substantiated and four defining features of the third epoch are identified: cognitive advantage through mass data processing and AI-mediated compression of the OODA (Observe–Orient–Decide–Act) decision cycle; the emergence of autonomous weapons systems (AWS) as a qualitatively new class of actors; state data centres as primary strategic strike targets; and the structural asymmetry of ethical constraints between democracies and authoritarian regimes in the development of military AI. Drawing on the experience of the Russo-Ukrainian war, the article demonstrates that the theatre of military operations has already become a laboratory of the new paradigm, confirmed by the growing share of AI-enabled FPV drones with autonomous targeting elements and the strategic role of AI integration in operational processes. The implications for public administration are analysed: the need for institutional adaptation, the formation of a state information security system, normative-legal regulation of civil servants' use of AI, and the training of qualified AI operators for the Ministry of Defence and the civil service. Conditions for preserving meaningful human oversight of AWS as a key safeguard of legal and moral accountability are identified and policy recommendations formulated.

Keywords: artificial intelligence, autonomous weapons systems, digital warfare, public administration, information security, Boyd's loop, Palantir system, cognitive advantage, cyber strategy, public cybersecurity.

Стаття надійшла до редакції / Received 27.06.2026
Прийнята до друку / Accepted 20.07.2026
Опубліковано / Published 27.08.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Протягом тисячоліть війна залишалася процесом, який фундаментально залежав від людських якостей: хоробрості, стратегічного генія, фізичної витривалості. Навіть поява індустріальної зброї – танків, літаків, ракет – не змінила цієї логіки: машина посилювала людину, але хтось все одно тримав штурвал. Сьогодні ця парадигма зазнає принципової зміни: на поле бою виходять алгоритми, а людина поступово перетворюється з актора на наглядача.

Сучасна війна стає дедалі більше управлінсько-технологічною задачею. Це означає, що перемога визначається вже не лише мужністю солдата чи досвідом командира, а здатністю держави організувати системну взаємодію між владою, освітою, бізнесом і збройними силами. Відсутність такої взаємодії – одна з

ключових причин технологічного відставання демократій у гонці озброєнь з авторитарними режимами, що не мають інституційних обмежень для мілітаризації технологій.

Червоними свідченнями цього переходу надають російсько-українська війна, війна в Газі (2023–2024), зіткнення з автономними підводними човнами або системами ПРО на основі навчання з підкріпленням (RL – Reinforcement Learning, навчання з підкріпленням). Експоненційне зростання інформаційних потоків у сучасному бойовому просторі – дрони, супутники, радіоперехоплення, сенсори IoT (Інтернет речей) – створює середовище, обробка якого виходить за межі людських когнітивних можливостей без ШІ. [1; 2]

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблематика використання ШІ у військовій сфері досліджується як у західній, так і у вітчизняній науці. Перший систематичний аналіз наслідків роботизації збройних сил здійснив Singer P.W. у монографії «Wired for War». [1] Спираючись на інтерв'ю з сотнями вчених, військових і правозахисників, він доводить, що технологія змінює не лише спосіб ведення бойових дій, але й саму природу рішення про застосування сили. Принциповим є його спостереження про зниження психологічного бар'єру до початку війни в умовах дистанційного управління зброєю: *«Коли літаки можна відправити в бій з офісу за 10 000 миль... досвід війни і сам образ воїна змінюються докорінно»* [1]. Singer також ставить питання, яке залишається відкритим і нині: «Чи дозволимо ми собі, через те що все це звучить як наукова фантастика, заперечувати реальність поля бою?» [1] Ця риторична конструкція точно описує інституційне відставання – держави реагують на загрозу тоді, коли вона вже стала буденністю. У свою чергу, Scharre P. у фундаментальній праці «Army of None» [3] запропонував класифікацію, яка стала стандартом у дискусії про автономність: «людина в петлі» (напівавтономні системи), «людина на петлі» (системи під наглядом) і «людина поза петлею» (повна автономність). Дослівно автор визначає ці рівні так: *«У напівавтономних системах машина виконує завдання, а потім чекає на дію оператора перед продовженням. [...] У системах під наглядом людина перебуває «на петлі». [...] Повністю автономні системи сприймають, вирішують і діють цілком без участі людини»* [3, ч. I].

Цінною є і нормативна позиція Scharre щодо темпу гонки автономних озброєнь: «невпорядкована гонка за автономністю, без розуміння того, куди вона нас веде, не вигідна нікому» [3, ч. VI]. Дослідник закликає до стримування, а не до заборони, вказуючи, що держави мають «об'єднатися для вироблення розуміння того, які застосування автономності є прийнятними, а які заходять надто далеко і відмовляються від людського судження там, де воно необхідне у війні» [3, ч. VI].

Kissinger H., Schmidt E., Huttenlocher D. у колективній монографії «The Age of AI» [4] розглядають трансформацію не лише через воєнну, але й через цивілізаційну призму. Їхня ключова теза: «Жодного разу від часів Доби Розуму ми не змінювали того, як ставимося до безпеки, економіки, порядку і навіть до самого знання». Вони фіксують принципово нову якість ШІ-рішень: «Отже, ШІ приймає рішення про те, що важливо, і дедалі частіше про те, що є правдою» («AI, then, is making decisions about what is important – and, increasingly, about what is true») [4]. Це безпосередньо стосується збройних систем: непрозорість алгоритмічних рішень руйнує епістемологічну основу людської відповідальності за наслідки бою.

Karp A. у публіцистичному маніфесті в NYT [5] формулює дилему, яку він називає «Oppenheimer Moment»: демократія, що не будує технологічної зброї, програє тим, хто будує її без моральних гальм. Allen G. і Chan T. [2] запропонували рамку для аналізу воєнного і розвідувального застосування ШІ для захисту національної безпеки США, визначивши три пріоритети: збереження технологічного лідерства, підтримка мирного використання і пом'якшення катастрофічних ризиків.

У вітчизняній науковій традиції значний внесок зробили дослідження CSIS (Bondar K. [6]), Lieber Institute West Point (Bendett S., Kirichenko D. [7]), та KSE Institute [8]. Ці роботи документують конкретний досвід України щодо впровадження ШІ в бойові системи і формують емпіричну базу для теоретичних узагальнень. RAND Corporation [9] і Belfer Center [2] розробили аналітичні рамки для оцінки стратегічних ризиків і заходів зміцнення стабільності в умовах гонки ШІ-озброєнь. Огляд засвідчує, що попри значний масив праць, питання інституційної адаптації публічного управління до умов цифрової війни залишається малодослідженим як в українській, так і в зарубіжній науці.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Мета статті – на основі моделі трьох епох збройного протистояння проаналізувати структурні зміни природи війни в умовах інтеграції штучного інтелекту в бойові системи; визначити нові вразливості держав на рівні критичної інфраструктури та когнітивного домінування; розкрити структурну асиметрію етичних і регуляторних обмежень між демократичними та авторитарними системами у розвитку воєнного ШІ; а також запропонувати інституційні умови збереження людського нагляду за автономними системами зброї в контексті адаптації системи публічного управління до викликів цифрової війни.

Завдання дослідження. Для досягнення зазначеної мети визначено такі дослідницькі завдання:

1) Обґрунтувати модель трьох епох збройного протистояння (доіндустріальної, індустріальної, інформаційної) та визначити ключові ознаки переходу до третьої, інформаційної епохи;

2) Розкрити механізм формування когнітивної переваги через ШІ-інтеграцію OODA-циклу (петлі Бойда) на прикладі конкретних платформ (Palantir Gotham) і практик застосування (HIMARS, FPV-дрони з елементами автономного наведення);

3) Виявити нові об'єкти стратегічної вразливості держав в умовах цифрової війни – державні датацентри, енергетичну та телекомунікаційну інфраструктуру, комерційні хмарні платформи;

4) Проаналізувати структурну асиметрію етичних і регуляторних обмежень між демократичними і авторитарними режимами у розробці воєнного ШІ (на прикладі Project Maven і політики військово-цивільного злиття КНР);

5) Визначити рівні та умови збереження «осмисленого людського контролю» (meaningful human control) над автономними системами зброї відповідно до темпу загрози й наявної міжнародно-правової рамки (EU AI Act, ініціативи ООН);

6) Обґрунтувати напрями інституційної адаптації системи публічного управління до умов цифрової війни: формування системи інформаційної безпеки держави, нормативно-правове регулювання роботи державних службовців з ШІ, підготовку фахових операторів ШІ, перехід від реактивної до антиципаційної моделі держави.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Для опису трансформації, що відбувається, запропоновується модель трьох епох збройного протистояння, що відрізняються за домінуючим суб'єктом бою, ключовою перевагою і природою вразливостей (табл. 1).

Таблиця 1.

Три епохи збройного протистояння

Епоха	Домінуючий суб'єкт	Ключова перевага	Вразливість
I. Доіндустріальна	Людина (солдат, офіцер)	Фізична витривалість, досвід, хоробрість	Стомлення, паніка, обмеженість кута огляду
II. Індустріальна	Людина + машина (танк, літак, ракета)	Вогнева міць, мобільність, дальність ураження	Логістика, паливо, промислова база
III. Інформаційна (поточна)	Датацентр + модель ШІ	Швидкість обробки даних, когнітивна перевага	Кіберзахист, енергетична інфраструктура, якість даних

Джерело: розроблено автором на основі [3; 4; 11].

Перша, доіндустріальна епоха характеризується прямою залежністю результату від індивідуальних якостей воїна. Стратегічна перевага формується на рівні полководницького таланту (Олександр Македонський, Наполеон, Суворов) і здатності до тактичної ініціативи в умовах «туману війни» (clausewitzівська концепція). Ключова вразливість – людські обмеження: стомлення, паніка, обмежений кут огляду, неможливість одночасно обробляти інформацію з великої кількості точок.

Друга, індустріальна епоха підносить машину в ранг рівноправного актора, але не замінює людину – вона підсилює її. Танк дозволяє швидше атакувати, літак бачити далі, ракета уражати без наближення. Проте командувач все одно тримає штурвал у голові: він визначає напрям удару, оцінює ризик, видає наказ. Ключова вразливість зміщується від людського фактору до промислово-логістичного: хто швидше виробить і доставить більше ресурсів – той переможе. Обидві світові війни є підручниковими ілюстраціями цієї логіки.

Третя, інформаційна епоха, у якій ми перебуваємо, є принципово іншою. Найкоректніша аналогія переходу до неї – керівник безпілотного літака: людина встановлює місію, система визначає оптимальний маршрут, а міра людського контролю визначається темпом бою, допустимою невизначеністю та ієрархією цінностей, що закладається в систему. [3]

Перехід між епохами не є лінійним і не означає повного виключення попередніх акторів. Більш точна аналогія – шарова архітектура: кожна наступна епоха додає нові рівні взаємодії, не скасовуючи попередніх. Солдат Третьої епохи не зникає – він стає оператором, аналітиком і наглядачем систем, що діють автономно на нижчих рівнях рішення. Принципова новизна полягає в тому, що певний клас рішень «вбивати чи ні» вже де-факто делегований машині не через злий умисел, а через фізику швидкості бою.

Важливо підкреслити: модель трьох епох є аналітичним інструментом, а не телеологічною схемою прогресу. Кожна епоха несе власні ризики і власні вразливості. Третя епоха не є «кращою» за попередні – вона є принципово складнішою для управління, насамперед тому, що розриває усталені ланцюжки відповідальності. [4]

Ключовим концептом для розуміння трансформації залишається OODA-петля (або петля Бойда), введена полковником ПС США Boyd J.R. [11]: Спостерігай (Observe) – Орієнтуйся (Orient) – Вирішуй (Decide) – Дій (Act). Конкурентна перевага досягається через проходження циклу швидше за ворога. Військова доктрина США з 1980-х років будується навколо ідеї «влізти в петлю ворога» – діяти настільки швидко, щоб ворог не встигав відреагувати. ШІ радикально прискорює фази визначення (ідентифікація цілі за даними з десятків джерел одночасно) і орієнтації, роблячи цикл у рази коротшим.

Конкретним прикладом платформи, що реалізує ШІ-інтеграцію OODA-циклу на практиці, є Palantir Gotham. [5] Система інтегрує дані з гетерогенних джерел: супутники радарного зондування (ICEYE, Capella Space), радіоперехоплення, сигнали мобільних мереж і дані соціальних мереж. Це дозволяє відтворювати оперативну картину бою в режимі реального часу з рівнем деталізації, недосяжним для будь-якого людського штабу. Конкретні переваги: виявлення патернів переміщення в масиві даних розміром у терабайти; прогнозування місця концентрації ворожих сил за 12–48 годин до атаки; автоматичне формування пріоритетного списку цілей для ударних систем.

Емпіричним доказом стиснення циклу ураження слугують операції з використанням HIMARS (High Mobility Artillery Rocket System, висококобільна ракетна артилерійська система) в Україні, де інтеграція зовнішніх розвідувальних даних зменшила час на підготовку цільової задачі з декількох годин до хвилин. Зростання частки FPV-дронів (First-Person View) з елементами автономного наведення підтверджує парадигмальний зсув війни. [6; 7; 8]

Boyd J.R. зазначав, що перевага в OODA-циклі є не кількісною, а якісною: «перемога дістається не тому, хто має перевагу в силі, а тому, хто може найшвидше перейти з одного стану в інший». [11] ШІ-системи за визначенням мають перевагу в швидкості переходу між станами – а це означає, що сторона без ШІ-асистованого OODA-циклу програє структурно, а не тактично. Навіть нечисленний, але технологічно оснащений противник здатен нейтралізувати кількісну перевагу ворога просто тому, що він «бачить» поле бою раніше і реагує швидше.

Показовим прикладом є також використання ізраїльської системи «Господар системи» (система управління цілями з елементами ШІ) у війні в Газі (2023–2024), де, за даними розслідувань ЗМІ, алгоритм генерував списки цілей, які люди-оператори затверджували в прискореному режимі. Це є практичною реалізацією того, що Scharre [3] називає «людина на петлі» з фактичним ризиком перетворення на «людину поза петлею»: формально людина підтверджує рішення, але за умов сотень цілей на добу це підтвердження стає ритуалом, а не аналізом.

Традиційна логіка знищення командного пункту набуває у Третій епосі нового виміру: знищення датацентру або переривання кабельної інфраструктури еквівалентне знищенню оперативного штабу. Атакуєш вже не штаб, а сервер. Не генерала, а GPU-кластер (GPU – Graphic Processing Unit, графічний процесор, ключовий обчислювальний елемент ШІ-систем).

Ця логіка вже реалізована практично: російська війна включає масивні удари по цивільній інфраструктурі – енергетиці і телекомунікаційним системам. Ізраїль у Starlink (супутникова комунікаційна мережа SpaceX) побачив не лише комунікаційний сервіс, але й дані для наведення. [12] Microsoft Azure і Amazon AWS надають хмарні послуги оборонним відомствам ряду країн, фактично перетворюючись на елементи військової інфраструктури. [13]

Lin H. і Zegart A. [14] у збірнику «Bytes, Bombs, and Spies» детально аналізують стратегічний вимір кібератак: вони можуть бути не менш деструктивними, ніж фізичне знищення об'єктів. Кібератака на інфраструктуру ШІ-системи є стратегічним ударом, не меншим за знищення командного пункту. Це означає, що кіберзахист, надійність хмарної інфраструктури і резервування обчислювальних потужностей набувають статусу питань національної безпеки першого рівня.

Окремого виміру набуває поняття «цифрової суверенності»: залежність оборонних систем від комерційних хмарних платформ іноземних провайдерів (навіть союзних) створює структурну вразливість. Рішення корпорації – не держави – може в будь-який момент змінити умови доступу. Саме тому питання про розміщення критичних оборонних даних і алгоритмів виключно на власній або союзній захищеній інфраструктурі є не технічним, а суверенним рішенням [9; 14].

Watling J. і Reynolds N. [12] у звіті RUSI фіксують: російська тактика масованих ударів по інфраструктурі в Україні (2022–2023) демонструє усвідомлення цього принципу – знищення енергетики і зв'язку послаблює не лише цивільне життя, але й обороноздатність в умовах, коли бойові системи залежать від стабільного живлення і з'єднання.

Одним з найменш обговорюваних аспектів є структурна асиметрія між демократіями і авторитарними режимами щодо технологічного розвитку в збройній сфері. Демократичні суспільства мають вбудовані гальмівні механізми: етичні дискусії, парламентський контроль, незалежні ЗМІ, громадські активісти. Це добре в мирний час. Але в технологічній гонці ця характеристика перетворюється на структурну вразливість.

Конкретним проявом цієї асиметрії була ситуація з Project Maven (Google): у 2018 р. понад чотири тисячі співробітників Google підписали петицію проти участі компанії у розробці військових технологій, і Google вийшов з проєкту. [15] Аналогічної дискусії в Пекіні чи Москві не відбувалося і не могло відбутися. Китайський закон про військово-цивільне злиття (PLA – People's Liberation Army, Народно-визвольна армія Китаю) [16] зобов'язує технологічні компанії співпрацювати з PLA без додаткових дискусій.

Allen G. [10] у доповіді CNAS (Center for a New American Security, Центр нової американської безпеки) зазначає: Китай активно реалізує стратегію «воєнно-цивільного злиття», спрямовану на системну інтеграцію комерційних технологій у воєнні розробки. Це дозволяє китайській оборонній промисловості використовувати найкращі технологічні рішення комерційного сектору без правових та етичних бар'єрів, характерних для демократичних систем.

Це не означає, що демократії мають відмовитися від дискусій. Це означає, що вони мають вирішити, яка ціна цих дискусій і чи є у них час на них у поточному вікні розвитку. Karp A. [5] ставить дилему гостро: «якщо ви не дасте алгоритмам право приймати рішення, ви програєте тим, хто це право вже дав». Пасивна відмова від розвитку бойових ШІ-систем не є нейтральною позицією – вона є позицією вразливості.

Український досвід демонструє альтернативну модель: відповідальність без відмови від інституційного контролю. Державна програма Delta і розробки у сфері FPV-дронів із елементами автономного наведення здійснюються за участю державних інституцій із збереженням правової рамки і прозорості. [9] Це може стати прикладом для інших демократій – не «або принципи, або технологія», а «принципи через технологію».

Гіперзвукові платформи фізично виключають можливість повноцінного людського аналізу в петлі вирішення. Саме це обумовило автоматичний режим систем Aegis (US Navy – Військово-морський флот США) і Iron Dome, [3] де людина залишається у ролі формального затвердження. Комітет ООН з питань роззброєння з 2014 р. обговорює проблему АСЗ, [17] але практика випереджає дипломатію.

Scharre P. [3] пропонує вимірюваний стандарт: людина має зберігати «meaningful control» (осмислений контроль) над силою, яку застосовує механізм, навіть якщо це означає сповільнення швидкості. Це принципово важливо: відповідальність без розуміння процесу є юридичною фікцією, а не реальною гарантією. Якщо оператор підтверджує список з тисячі цілей за хвилини – він не здійснює «осмислений контроль», а виконує ритуальну функцію.

Практичне питання полягає не в тому, «чи потрібен людський нагляд» (відповідь очевидна – так), а в тому, «де саме у процесі прийняття рішень він є реальним, а де – лише видимістю». Scharre пропонує розрізняти три рівні:

1) визначення цілей і правил бою – виключно людина;
2) ідентифікація і класифікація цілей – людина з ШІ-асистенцією;
3) безпосереднє ураження – залежно від темпу загрози і наявності часу на підтвердження.

Eu AI Act (Regulation (EU) 2024/1689) [18] встановлює принцип «людина в петлі» для систем ШІ «високого ризику», до яких відносяться системи, що впливають на безпеку. Проте бойові АСЗ виведені з-під дії Регламенту (виняток для оборонних застосувань). Це означає, що міжнародно-правова рамка для регулювання бойових ШІ-систем фактично відсутня, а практика – вже далеко попереду.

NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence, Кооперативний центр передового досвіду з кіберзахисту) [19] ідентифікує три критичні виміри поєднання ШІ і кібербезпеки: (1) ШІ як інструмент кібератак; (2) ШІ як мішень кібератак; (3) ШІ як інструмент захисту. В усіх трьох вимірах людський нагляд є необхідним, але в кожному – різної природи. Особливо критичним є другий вимір: атака на ШІ-систему оборони через підміну тренувальних даних (data poisoning) або маніпуляцію вхідними сигналами (adversarial inputs) може нейтралізувати систему без жодного фізичного удару.

Трансформація збройного протистояння вимагає не лише технологічної, а й структурної відповіді з боку системи публічного управління. [18]

Формування системи інформаційної безпеки держави. Цифрова війна розмиває межі між оборонною і цивільною сферами. Ураження на датацентр державної влади, на енергетичну або транспортну інфраструктуру є еквівалентним військовому акту, коли ці системи забезпечують функціонування ШІ-систем оборонного призначення. Тому комплексна державна стратегія інформаційної безпеки має охоплювати: захист датацентрів і кабельної інфраструктури; кіберостійкість державних ІС; протоколи обміну даними між відомствами та резервування обчислювальних потужностей для критичних функцій в умовах бойових дій. [14]

Регламентація роботи державних службовців з ШІ. Інтеграція ШІ в адміністративні процеси без належної правової рамки створює системні ризики для державного управління. Досвід європейської регуляції (Regulation (EU) 2024/1689, AI Act – закон ЄС про алгоритмічний інтелект) [18] свідчить: без чіткої норми про допустимі межі використання ШІ держслужбовцями, вимог прозорості й алгоритмічної підзвітності, заборон на прийняття рішень без участі людини в критичних сферах – все це прямо стосується держслужби. Для України необхідна розробка спеціального нормативно-правового регулювання використання ШІ в державному секторі з чітким розмежуванням відповідальності за помилки ШІ.

Підготовка фахових операторів ШІ для Міноборони і держслужби. Досвід показує, що найбільш критичною ланкою в ШІ-інтегрованих системах є не технологія, а людина. Оператор, який не розуміє принципів роботи штучно-інтелектуальної системи, є джерелом небезпеки на рівні валідності результатів: хибні дані розвідки, помилкова ідентифікація цілей, некоректна інтерпретація оперативної картини можуть мати незворотні наслідки. [3; 19]

Необхідна дворівнева система підготовки операторів. Перший рівень – оперативний: військовослужбовці, що працюють з Palantir, Delta, системами наведення, потребують спеціалізованої технічно-тактичної підготовки з розумінням архітектури моделей, інтерпретації виведень та меж автономії. Другий рівень – управлінський: аналітики для Міноборони і держслужбовці, що забезпечують штучно-інтелектуальні функції, потребують навичок критичного оцінювання виведень ШІ у предметній галузі. [18; 19]

Інституційна адаптація: від реактивної до антиципаційної держави. OECD (Організація економічного співробітництва і розвитку, Organisation for Economic Co-operation and Development) [20] фіксує ключовий розрив між державами, що вже розробили комплексні алгоритмічні стратегії оборони, і тими, що все ще відстають від досягнення регуляторної зрілості. Для України в умовах активної фази війни немає розкоші на відкладене врегулювання. Необхідна антиципаційна держава – та, яка не лише реагує на цифрові загрози, але здатна їх прогнозувати, формувати власні операційні потужності і запобігати алгоритмічній вразливості.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Російсько-українська війна підтвердила: технологічна і організаційна неготовність держави до епохи цифрової війни виявляється не лише в технологічній, але й в стратегічній, організаційній і правовій площинах. Війна стає міждисциплінарною задачею влади, освіти, бізнесу і збройних сил. Проведений аналіз дозволяє сформулювати чотири ключових висновки.

1. Сучасна війна входить у третю епоху збройного протистояння, де домінуючим суб'єктом стають інформаційно-обчислювальні системи на основі ШІ, а людина поступово переходить у роль наглядача або наглядача. Цьому сприяє когнітивна перевага через ШІ-інтеграцію OODA-циклу і принципова зміна в логіці ведення війни.
2. Датацентри державної влади, енергетична і телекомунікаційна інфраструктура перетворюються на об'єкти стратегічного удару нової епохи: атака на сервер стратегічно еквівалентна знищенню командного пункту. Це вимагає системного захисту інфраструктури як складової державної оборонної стратегії.
3. Асиметрія етичних обмежень між демократіями і авторитарними режимами є структурною загрозою. Демократії не можуть дозволити собі односторонньо відмовитися від розробки військового ШІ і одночасно зберегти свої цінності – розв'язання цього парадоксу вимагає розробки власної етичної рамки.
4. Інституціоналізація людського нагляду за АСЗ, нормативно-правове регулювання роботи з ШІ і цілеспрямована підготовка фахових операторів ШІ є невід'ємними умовами збереження юридичної і моральної відповідальності в умовах, коли швидкість прийняття рішень виходить за межі людського реагування.

Таким чином, війна в епоху ШІ перестає бути виключно військовим завданням – вона перетворюється на комплексну міждисциплінарну задачу державного управління, освіти, бізнесу і збройних сил. Україна, яка першою серед демократій зіткнулась із цією парадигмою на полі бою, має виняткову можливість перетворити воєнний досвід на стратегічну перевагу у повоєнному світі – за умови системної реалізації чотирьох описаних пріоритетів.

Література

1. Singer P.W. Wired for War: The Robotics Revolution and Conflict in the 21st Century. New York: Penguin Press, 2009. 499 p. ISBN: 978-1-594-20229-2. URL: https://www.penguinrandomhouse.com/books/303774/wired-for-war-by-p-w-singer/
2. Allen G., Chan T. Artificial Intelligence and National Security. Belfer Center for Science and International Affairs. Harvard Kennedy School. 2017. 132 p. URL: https://www.belfercenter.org/publication/artificial-intelligence-and-national-security. PDF: https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/AI%20NatSec%20-%20final.pdf
3. Scharre P. Army of None: Autonomous Weapons and the Future of War. New York: W. W. Norton & Company, 2018. 448 p. ISBN: 978-0-393-35658-8. URL: https://wwnorton.com/books/Army-of-None/
4. Kissinger H., Schmidt E., Huttenlocher D. The Age of AI: And Our Human Future. New York: Little, Brown and Company, 2021. 272 p. ISBN: 978-0-316-27380-0. URL: https://www.hachettebookgroup.com/titles/henry-a-kissinger/the-age-of-ai/9780316274104/
5. Karp A. Our Oppenheimer Moment: The Creation of A.I. Weapons. The New York Times. 2023. July 25. URL: https://www.nytimes.com/2023/07/25/opinion/karp-palantir-artificial-intelligence.html
6. Bondar K. Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare. Center for Strategic and International Studies (CSIS). 2025. URL: https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare
7. Bendett S., Kirichenko D. The Continuing Autonomous Arms Race. Lieber Institute for Law and Land Warfare, West Point. 2025. URL: https://lieber.westpoint.edu/continuing-autonomous-arms-race/
8. KSE Institute. Harnessing Ukraine's Drone Innovations to Advance Autonomous Systems. Kyiv School of Economics. 2025. URL: https://kse.ua/wp-content/uploads/2025/11/KSE_Institute_Report_Harnessing_Ukraines_Drone_Innovations_to_Advance.pdf
9. Cummings M. et al. AI and International Stability: Risks and Confidence-Building Measures. RAND Corporation. 2023. Report RR-A1764-1. URL: https://www.rand.org/pubs/research_reports/RRA1764-1.html

10. Allen G. Understanding China's AI Strategy. Center for New American Security (CNAS). 2019. URL: https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy
11. Boyd J.R. Patterns of Conflict. Unpublished briefing (December 1986). In: A Discourse on Winning and Losing. Maxwell AFB: Air University Press, 2018. URL: https://www.coljohnboyd.com/static/documents/1986-12__Boyd_John_R__Patterns_of_Conflict__PPT-PDF.pdf
12. Watling J., Reynolds N. Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. RUSI Special Report. May 2023. URL: https://www.rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine PDF: https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf
13. Microsoft. Supporting Ukraine. Microsoft On the Issues. 2022–2024. URL: https://blogs.microsoft.com/on-the-issues/tag/ukraine/
14. Lin H., Zegart A. (eds.) Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations. Washington, DC: Brookings Institution Press, 2019. 367 p. ISBN: 978-0-815-73718-3. URL: https://www.brookings.edu/books/bytes-bombs-and-spies/
15. Oremus W. et al. Inside the Google worker revolt over Project Maven. Washington Post. 2022. URL: https://www.washingtonpost.com/technology/2022/04/16/google-workers-protest-ai/
16. Kania E. China's Military-Civil Fusion Strategy. CNAS Report. 2019. URL: https://www.cnas.org/publications/reports/chinas-military-civil-fusion-strategy
17. UN Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS). Report. Geneva: UNODA, 2023. URL: https://www.un.org/disarmament/the-conference-on-disarmament/lethal-autonomous-weapons
18. European Parliament and Council of the EU. Regulation (EU) 2024/1689 (AI Act – Regulation on Artificial Intelligence). Official Journal of the EU. L 2024/1689. 12.07.2024. ELI: http://data.europa.eu/eli/reg/2024/1689/oj. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
19. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). AI and Cyber: Use of AI in Cyber Operations. Tallinn, 2023. URL: https://ccdcoe.org/research/
20. OECD. OECD Framework for the Classification of AI Systems. OECD Digital Economy Papers No. 323. Paris: OECD Publishing, 2022. DOI: 10.1787/cb6d9eca-en. URL: https://doi.org/10.1787/cb6d9eca-en

References

1. Singer, P.W. (2009). Wired for War: The Robotics Revolution and Conflict in the 21st Century. Penguin Press. ISBN: 978-1-594-20229-2. URL: https://www.penguinrandomhouse.com/books/303774/wired-for-war-by-p-w-singer/
2. Allen, G., & Chan, T. (2017). Artificial Intelligence and National Security. Belfer Center, Harvard Kennedy School. URL: https://www.belfercenter.org/publication/artificial-intelligence-and-national-security
3. Scharre, P. (2018). Army of None: Autonomous Weapons and the Future of War. W. W. Norton & Company. ISBN: 978-0-393-35658-8. URL: https://wwnorton.com/books/Army-of-None/
4. Kissinger, H., Schmidt, E., & Huttenlocher, D. (2021). The Age of AI: And Our Human Future. Little, Brown and Company. ISBN: 978-0-316-27380-0. URL: https://www.hachettebookgroup.com/titles/henry-a-kissinger/the-age-of-ai/9780316274104/
5. Karp, A. (2023, July 25). Our Oppenheimer Moment. The New York Times. URL: https://www.nytimes.com/2023/07/25/opinion/karp-palantir-artificial-intelligence.html
6. Bondar, K. (2025). Ukraine's Future Vision for AI-Enabled Autonomous Warfare. CSIS. URL: https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare
7. Bendett, S., & Kirichenko, D. (2025). The Continuing Autonomous Arms Race. Lieber Institute, West Point. URL: https://lieber.westpoint.edu/continuing-autonomous-arms-race/
8. KSE Institute. (2025). Harnessing Ukraine's Drone Innovations. Kyiv School of Economics. URL: https://kse.ua/wp-content/uploads/2025/11/KSE_Institute_Report_Harnessing_Ukraines_Drone_Innovations_to_Advance.pdf
9. Cummings, M. et al. (2023). AI and International Stability. RAND Corporation. RR-A1764-1.
10. Allen, G. (2019). Understanding China's AI Strategy. CNAS.
11. Boyd, J.R. (1986). Patterns of Conflict. In: A Discourse on Winning and Losing. Air University Press, 2018. URL: https://www.coljohnboyd.com/static/documents/1986-12__Boyd_John_R__Patterns_of_Conflict__PPT-PDF.pdf
12. Watling, J., & Reynolds, N. (2023). Meatgrinder: Russian Tactics. RUSI Special Report. URL: https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf
13. Microsoft. (2022–2024). Supporting Ukraine. Microsoft On the Issues.
14. Lin, H., & Zegart, A. (eds.) (2019). Bytes, Bombs, and Spies. Brookings Institution Press. URL: https://www.brookings.edu/books/bytes-bombs-and-spies/
15. Oremus, W. et al. (2022). Google worker revolt over Project Maven. Washington Post.
16. Kania, E. (2019). China's Military-Civil Fusion Strategy. CNAS.
17. UN GGE on LAWS. (2023). Report. UNODA, Geneva.
18. European Parliament and Council of the EU. (2024). Regulation (EU) 2024/1689 (AI Act). OJ L 2024/1689. ELI: http://data.europa.eu/eli/reg/2024/1689/oj
19. NATO CCDCOE. (2023). AI and Cyber: Use of AI in Cyber Operations. Tallinn.
20. OECD. (2022). OECD Framework for the Classification of AI Systems. OECD Digital Economy Papers, No. 323. https://doi.org/10.1787/cb6d9eca-en