ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ВІЙСЬКОВИХ ЦІЛЯХ

ГОНЧАРУК Дмитро Романович - аспірант ДТЕУ, 1 курс, Міжнародне право
DOI: https://doi.org/10.32782/LAW.UA.2024.1.29

Стаття аналізує застосування технологій штучного інтелекту (ШІ) у військовій сфері, з акцентом на сучасний стан регулювання відповідно до правил ведення війни задля виконання військових цілей. Дослідження охоплює використання ШІ для автоматизації розвідки, навігації автономних літальних апаратів, системи виявлення та відстеження цілей та розробку стратегій ведення бойових дій. Методологія статті базується на основі прикладів застосування штучного інтелекту, реакції міжнародної спільноти, та технологічних ініціативах, що забезпечують перевагу на полі бою. Саме тому стаття акцентує увагу на становленні міжнародних вимог і правил, етичних викликах та потенційних ризиках, пов'язаних із застосуванням ШІ у військовій сфері.

Розвиток технологій створює нові умови для трансформацій ідей, концепцій та природу ведення війни. Системи атаки та захисту отримують усе нові інструменти. Спільним новітнім інструментом виступає штучний інтелект (далі – ШІ). Головною особливістю ШІ є швидка еволюція від концепції до технологій, що функціонують у реальних ситуаціях.

ШІ виступає технологією змін, що прогресивно впливає на навколишній світ, у цивільному та військовому житті людини. Ця прогресивна технологія фактично розвиває середовище для створення нових загроз та викликів.

Однією з найбільших загроз є здібності до швидкого аналізу величезних масивів даних. Дані, що аналізуються, можуть бути як виокремлені в групи чи кластери для виокремлення особливостей та надання аналізу поставленої задачі. Якщо застосувати цю технологію в період військової необхідності, то ШІ може бути використаний для створення нових видів зброї, які є: точними, потужними та автономними, та бути тригером до зростання ризику глобального конфлікту та масового знищення. Якщо застосувати ШІ до інформаційних джерел та засобів масової інформації, то швидкий аналіз даних ШІ можна застосувати для створення нових методів пропаганди та дезінформації, та підриву демократичних інститутів. Чи підвищить це ризик зростання авторитаризму та тоталітаризму?

У зв'язку з вищезазначеним, дослідження видів та загроз застосування ШІ у військових цілях заслуговує уваги. Оскільки кожен з нас має усвідомлювати майбутні перспективи, ризики, загрози, фактори і способи убезпечення себе під час використанням ШІ у військовій сфері.

Метою дослідження пропонується вважати аналіз застосування ШІ у військових цілях.

Гіпотеза зосереджена на тому, що просунуті системи штучного інтелекту, що не мають адекватного контролю та регуляцій, можуть створювати значні безпекові ризики, включаючи непередбачуване використання у військових та цивільних сферах. І тільки ефективні стратегії, що включають розробку міжнародних стандартів та

директив з безпеки ШІ, етичні рамки для розробки та застосування ШІ, та активне співробітництво між державними регуляторами, науковими колами та промисловістю – мінімізують ці ризики.

Завдання дослідження полягає у вирішенні наступних питань:

- Проаналізувати сучасний стан розробки та застосування ШІ у військовій сфері;
- Охарактеризувати основні загрози, пов'язані з використанням ШІ у військових цілях;
- Запропонувати заходи для мінімізації потенційних ризиків, пов'язаних з використанням ШІ у військовій сфері.

Станом на сьогодні, військові експерти навчилась адаптуватись до майже будь-яких ситуацій. На жаль, воєнні конфлікти дають дорогі уроки для людства. І саме тому технологічні експерти почали застосовувати штучний інтелект для уникнення технологічної відсталості та здобуття переваги на полі бою. Прикладами можна вважати розвиток: систем управління, зброї, оборонної інфраструктури і т.д. Особливий вплив помітний у створенні нових типів боєприпасів, вибухонебезпечних речовин, керування військовою технікою і т.д. З точки зору ведення війни прогнозується, що саме штучний інтелект має всі можливості стати «гейм ченджером», тобто радикальною силою змінити хід розвитку військової справи для тих, хто нею володіє. [1]

Розробка нових технологій ШІ не стоїть на місці. Однією з провідних компаній, у цьому напрямку є Palantir Technologies. Це американська компанія, розробник програмного забезпечення з аналізу даних. У травні 2023 року Palantir Technologies та Міністерство цифрової трансформації України оголосило про партнерство, яке має на меті використання технологій компанії для підтримки оборони України у війні проти Росії. Особливе значення у партнерстві грає інтеграція систем на основі штучного інтелекту, щоб посилити потенціал країни у сферах від розвідки до військової логістики.

Ефективне впровадження передових технологічних рішень має важливе значення для зменшення або нівелювання феномену "туману війни", який характеризується невизначеністю та мінливістю інформації, що маскує об'єктивний стан справ на полі бою. Одним із таких рішень є застосування засобів штучного інтелекту (ШІ), зокрема, технологій, розроблених компанією Palantir Technologies, для аналізу даних. Ці технології дозволяють визначити місцезнаходження союзних та ворожих сил, а також вибрати оптимальні типи озброєння для конкретних бойових умов. Крім того, коректне застосування OSINT-методів у поєднанні з ШІ сприяє виявленню військових злочинів. [10]

У контексті розвитку ШІ в Україні слід також згадати компанію Clearview AI, яка спеціалізується на ідентифікації осіб. Clearview AI використовує базу даних, що містить понад 10 мільярдів фотографій з соціальних мереж, для ідентифікації загиблих солдатів. Ця технологія первісно застосовувалася правоохоронними органами США для виявлення злочинців, але за даними BuzzFeed News, з 2020 року компанія планувала розширити свою присутність на 22 міжнародних ринках, у тому числі і в Україні. [11]

Значну дискусію сьогодні викликає автономна зброя, яка може самостійно, на власний «розсуд» виявляти, ідентифікувати, вражати ціль, використовуючи при цьому відповідні датчики і штучний інтелект (наприклад, бойові автономні роботизовані системи, смертоносні автономні засоби, робототехнічні комплекси) [2]

Одним із науковців, який досліджує загрози, пов'язані з ШІ у військовій сфері, є Роберт Олтман, професор факультету штучного інтелекту Університету Карнегі-Меллона. Олтман є автором книги "Штучний інтелект війни: технології, стратегії та етика" (2020), у якій він розглядає потенційні загрози, пов'язані з використанням ШІ у військовій сфері. Олтман вважає, що ШІ має потенціал для створення нових видів зброї, які є більш точними, ефективними та небезпечними, ніж будь-яка зброя, яка існувала раніше. Він також вважає, що ШІ може бути використаний для створення нових методів пропаганди та дезін-

формації, які можуть бути використані для підриву демократичних інститутів. Олтман закликає до міжнародного співробітництва для розробки заходів, які допоможуть мінімізувати потенційні ризики, пов'язані з використанням ШІ у військовій сфері. Він вважає, що такі заходи повинні включати в себе розробку міжнародних норм та правил, які регулюють використання ШІ у військовій сфері, а також розвиток нових технологій, які допоможуть захиститися від зброї, що використовує ШІ.[3]

Проте, хіба технологічний прорив лякає людину? Чи можливо потенціал та непередбачуваність подальшого застосування нової технології? Вважаємо, що безпрецедентне застосування таких технологічних можливостей несе ще і безпрецедентну невідомість впливу ШІ на майбутнє. Саме тому хотілось би підкреслити необхідність дослідження застосування та регулювання ШІ у сферах, що впливають на життя, безпеку та здоров'я людини. Важливо досліджувати: мілітаризацію штучного інтелекту, виклики розвитку військового штучного інтелекту для міжнародного гуманітарного права, міжнародну конкуренцію в дослідженнях ШІ, аналіз здобутків та ризиків штучного інтелекту і т.д.

Людство знає достатньо прикладів технологічних змін у військовій справі, що радикально впливали на конфлікти, такі як винахід: сокири, пороху, вогнепальної зброї, танків, військових літаків, ядерної зброї. Кожен з цих винаходів був під контролем людини. І тільки ШІ, як нова технологія, що застосовується у військовій сфері не підконтрольна людині повністю. Оскільки, наприклад, автономні летальні апарати чи масована дезінформація в інтернеті – не є підконтрольним.

Глобальна гонка технологій на полі штучного інтелекту не тільки призводить до стрімкого розвитку цієї галузі, але й створює потенційні конфлікти, які можуть мати серйозні етичні та правові наслідки. Вважаємо, що Україні та міжнародному співтовариству потрібна стратегія розвитку та застосування штучного інтелекту, яка окреслюватиме не лише шляхи уникнення технологічної залежності від штучного інтелекту, а й визначається як фактор сприяння економічному, технологічному та політичному розвитку. Загрози, пов'язані із досягненням поставлених завдань, полягають у потенційній втраті контролю над системами штучного інтелекту, що може порушити принципи конфіденційності та законного використання ШІ. Міжнародне конкурентне протистояння може послужити стимулом для виникнення нових етичних, правових чи військових конфліктів. Важливо відзначити, що громадяни країни, яка прагне мати технологічну перевагу, можуть стати жертвами цього процесу. Здебільшого, лише міжнародне гуманітарне право (МГП) може вплинути на ситуацію до того моменту, коли буде розроблено всеохоплююче регулювання у галузі штучного інтелекту.

Принципи відповідальності, розрізнення та пропорційності МГП повинні бути впроваджені у процесі інтеграції автономних систем наведення в системи управління та військової інфраструктури. Іншими словами, автономні системи наведення не повинні застосовуватися за принципом «один підходить всім», а розробники військових технологій повинні дотримуватися принципів МГП. Автономні системи наведення, які використовуються військовими, повинні дотримуватися принципів, уникаючи стандартизації та враховуючи контекст конкретного конфлікту. Це сприятиме створенню етичного та відповідального підходу до застосування штучного інтелекту в сфері безпеки та оборони. Завдяки цьому можна буде забезпечити не лише захист національних інтересів, але й уникнути потенційних негативних наслідків в глобальному масштабі.

Переходячи від теорії до практики, можемо зазначити, що вже сьогодні загрозу становлять розробки технологій безпілотних літальних апаратів та систем протиповітряної оборони що містять технології штучного інтелекту. Технологічний інтерфейс, який, дозволяє виділити наступні типи взаємозв'язку: «людина як частина циклу», «людина в середині циклу», та «людина поза циклом» роботи зі штучним інтелектом. І як наслідок існує – напівавтоном-

на, контрольовано автономна та автономна летальна зброя.

Аналізуючи потенціальні переваги та ризики застосування штучного інтелекту у військових цілях, потрібно сказати про явну зміну парадигми у військовій діяльності. Штучний інтелект змінює процес проєктування зброї, командування та управління, матеріально технічне забезпечення та процес прийняття рішень. На стратегічному рівні штучний інтелект може використовуватись для створення та розповсюдження величезних обсягів неправдивої інформації для захисту чи атаці на супротивника. На тактичному рівні може допомогти операторам для керування безпілотними системами та надавати швидкого аналізу вхідних даних [8].

Синергетичні впливи штучного інтелекту (ШІ) та автономії у сфері оборони породжують ряд проблем, пов'язаних із використанням автономних систем озброєнь, що базуються на ШІ. Незважаючи на те, що такі системи можуть виявитися ефективнішими, ніж традиційні системи озброєнь, їх використання може призвести до серйозних небезпек, оскільки вони можуть функціонувати без людського контролю.

Ці проблеми викликають загрози, які викликають серйозне занепокоєння не лише серед експертів НАТО, але й у всьому світі. Зокрема, реальні ризики появи летальних автономних систем зі штучним інтелектом на полі бою та їхні можливі наслідки для цивільного населення вимагали перегляду пріоритетів в діяльності Управління Організації Об'єднаних Націй (ООН) з роззброєння (UNODA). Відповідно, зміст діяльності Інституту ООН з дослідження проблем роззброєння (UNIDIR) було адаптовано, а також створено спеціальну Групу урядових експертів з питань летальних автономних систем (GGE LAWS) у межах UNODA.

Штучний інтелект є передовою технологією, яка може радикально змінити сучасний світ, але водночас має потенціал створення нових загроз, зокрема у сфері безпеки. Однією з основних загроз, пов'язаних з ШІ, є його руйнівна потужність, здатність створювати нові види зброї, які є точнішими, потужнішими та автономними, ніж будь-яка раніше існуюча зброя. Це може призвести до збільшення ризику глобальних конфліктів та масового знищення. Для протидії цій загрозі необхідно розробляти відповідні системи ШІ для протидії високоінтелектуальній зброї противника, проводити дослідження з безпеки ШІ та розробляти ефективні заходи протидії цим загрозам. З цією метою важливо створити науково-дослідні організації та впровадити відповідні нормативно-правові документи, які регулюють використання ШІ подвійного призначення.

Сьогодні сильні геополітичні гравці, такі як – США, Китай, та Росія ведуть активну роботу над геополітичною перевагою. Особлива робота спрямована на переоснащення військових систем зброєю синхронізованою зі штучним інтелектом. З цього приводу президент Росії В.Путін заявив у 2017р: «Хто стане лідером у розробці штучного інтелекту – стане правителем світу» [4].

У 2017 році Китай оприлюднив свою національну стратегію штучного інтелекту, заявивши, що штучний інтелект є стратегічною можливістю і що Китай прагне домінувати у світі в технологіях ШІ. [5]

21 жовтня 2021 року міністри оборони країн НАТО узгодили першу Стратегію НАТО у сфері штучного інтелекту. У документі описано, як ШІ може бути застосований у сфері оборони та безпеки захищеним і етичним способом. Стратегія встановлює стандарти відповідального використання технологій ШІ відповідно до міжнародного права та цінностей НАТО. У ній також розглядаються загрози, що створюються шляхом використанням ШІ противниками, та способи встановлення надійної співпраці з інноваційною спільнотою в сфері ШІ [9].

30 жовтня 2023 року Білий Дім опублікував інформаційний бюлетень з указом президента Байдена про безпечний, захищений і надійний штучний інтелект. Згідно з цим указом встановлюються нові стандарти безпеки задля конфіденційності, інноваціям та лідерства США у сфері штучного інтелекту у світі [6].

Тому, як ми бачимо, робота з питання регулювання ведеться. На сьогодні актори міжнародного права розробляють юридичний «фреймворк» для застосування ШІ локально та більш глобально. Щоб сприяти глобальному інклюзивному підходу, у жовтні 2023 року Генеральний секретар ООН Антоніо Гутеріш зробив важливий крок у регулюванні штучного інтелекту, а саме: скликав Консультативний орган високого рівня з питань штучного інтелекту за участю багатьох зацікавлених сторін для проведення аналізу та надання рекомендацій щодо міжнародного управління. Отже, і ООН не залишається осторонь та розуміє рівень загроз, пов'язаних із ШІ, тому зміцнення взаємовідносин та довіра виступає на противагу конкуренції з питань штучного інтелекту. [7]

Щодо найширших узгоджених документів з регулювання ШІ сьогодні, є Декларація Блетчлі про безпеку штучного інтелекту. У ній 28 країн світу, включаючи Африку, Близький Схід і Азію, а також ЄС, погоджуються з нагальною потребою розуміти потенційні ризики та колективно керувати ними за допомогою нових спільних глобальних зусиль із забезпечення штучного інтелекту. Тому ми можемо висловити надію, що людство має всі шанси уникнути або хоча б радикально зменшити потенційні ризики від застосування штучного інтелекту у військових цілях.

Підводячи підсумки, мусимо сказати, що штучний інтелект є потужним інструментом, який може бути використаний як на благо, так і на шкоду людству. Для того, щоб мінімізувати потенційні ризики, пов'язані з ШІ, необхідно вжити відповідних заходів, зокрема:

- Розробити нові системи ШІ для протидії високоінтелектуальній зброї противника.
- Провести дослідження з безпеки ШІ.
- Розробити нормативно-правові документи, які регулюють використання ШІ подвійного призначення.

Також необхідно усвідомлювати потенційні ризики, пов'язані з синергетичними ефектами ШІ та автономії у військовій сфері, і вжити заходів для їх мінімізації. Оскільки ШІ та супутні технології можуть бути використані для створення нових загроз. Тому на противагу мають бути технології, які є більш ефективними та складними для захисту. Варто тверезо та відповідально аналізувати роботу над розвитком штучного інтелекту. Та сприяти тому, щоб загрози, пов'язані зі штучним інтелектом, були нівельовані.

Література

1. Forrest Morgan and others, 'Military Applications Of Artificial Intelligence: Ethical Concerns In An Uncertain World' (RAND Corporation 2021)<https://www.rand.org/pubs/research_reports/RR3139- 1.html>

2. Боевые работы: угрозы учтенные или непредвиденные? Индекс безопасности. No 3–4 (118–199). Т. 22. URL: http://pircenter.org/media/content/files/13/14875332590.pdf

3. Altman, R. (2020). Artificial Intelligence in War: Technologies, Strategies, and Ethics. Oxford University Press.

4. Vadim Kozyulin, 'Militarization Of AI' [2019] Russian Center for Policy Research <https://stanleycenter.org/wp-content/uploads/2020/05/MilitarizationofAI-Russia.pdf> accessed 20 February 2021 Citing President Vladimir Putin (2017)

5. Gregory Allen, 'Understanding China's AI Strategy: Clues To Chinese Strategic Thinking On Artificial Intelligence And National Security. Washington, D.C.: Center For A New American Security February 2019' (2019) 3 SIRIUS citing Maj. Gen. Ding Xiangrong at the Beijing Xiangshan [2018]

6. House, W. (2023, October 30). FACT SHEET: President Biden issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

7. High-Level Advisory Body on Artificial Intelligence | Office of the Secretary-General's Envoy on Technology. (n.d.). https://www.un.org/techenvoy/ai-advisory-body

8. Getting To Grips With Military Robotics' (The Economist, 2021) <https://www.economist.com/special-report/2018/01/25/getting-to-grips-with-military-robotics> accessed 5 March 2021.

9. Nato. (n.d.). Summary of the NATO Artificial intelligence Strategy. NATO. https://www.nato.int/cps/en/natohq/official_texts_187617.htm

10. Мельник, Т. (2024, January 27). «Ядерна зброя в IT». Американський Palantir має контракти з ЦРУ, а з травня допомагає Україні. Наскільки є вирішальною роль штучного інтелекту на війні. https://forbes.ua/innovations/yaderna-zbroya-v-it-amerikanskiy-palantir-mae-kontrakti-z-tsru-a-z-travnya-dopomagae-ukraini-naskilki-virishalna-rol-shtuchnogo-intelektu-na-viyni-10032023-12280

11. Clearview AI's Facial Recognition Platform Achieves Superior Accuracy and Reliability Across All Demographics in NIST Testing. (2021, November 1). www.businesswire.com. https://www.businesswire.com/news/home/20211101005283/en/Clearview-AI%E2%80%99s-Facial-Recognition-Platform-Achieves-Superior-Accuracy-and-Reliability-Across-All-Demographics-in-NIST-Testing

SUMMARY

The article analyses the application of artificial intelligence (AI) technologies in the military sphere, with a focus on the current state of regulation in accordance with the rules of warfare to achieve military objectives. The study covers the use of AI for intelligence automation, navigation of autonomous aerial vehicles, target detection and tracking systems, and the development of warfare strategies. The article's methodology is based on examples of AI applications, the international community's reaction, and technological initiatives that provide an advantage on the battlefield. That is why the article focuses on the development of international requirements and rules, ethical challenges and potential risks associated with the use of AI in the military sphere.