

Tomasz Gergelewicz
Ministerstwo Obrony Narodowej
ORCID: 0000-0002-9145-5099
t.gergelewicz@wp.pl

Wykorzystanie potencjału sztucznej inteligencji w siłach zbrojnych – wywiad z Chatem GPT

Streszczenie

Wdrożenie systemów opartych na sztucznej inteligencji do obszarów funkcjonowania sił zbrojnych tworzy nowe zdolności, które w dużym stopniu odciążają dotychczas wykorzystywane mechanizmy. Wskazano szanse dla sił zbrojnych wynikające z użycie sztucznej inteligencji, jednocześnie podkreślono wyzwania, jakie tworzy użycie tej zaawansowanej technologii. Celem artykułu jest przedstawienie potencjału implementacji sztucznej inteligencji na potrzeby wojska i zestawienie go z treścią wygenerowaną podczas wywiadu przez Chat GPT, w odpowiedzi na pytania dotyczące różnych obszarów wykorzystania sztucznej inteligencji na potrzeby wojska.

Ponadto autor zaproponował skalę autonomii sztucznej inteligencji, a także zdefiniował trzy zasadnicze obszary, które należy opanować, żeby swobodnie posługiwać się sztuczną inteligencją bez obaw o ryzyko jej niepożądanego działania.

Wykorzystano metodę analityczną do wyodrębnienia obszarów zastosowania sztucznej inteligencji na potrzeby armii i wskazania potencjalnych kierunki jej wdrożenia. Zastosowano syntezę, żeby zaproponować skalę autonomiczności systemu względem decyzji człowieka. Posłużono się metodą wywiadu eksperckiego do zbadania jak sztuczna inteligencja ocenia własny potencjał do wykorzystania na potrzeby wojska.

We wnioskach wskazano, że treści generowane przez sztuczną inteligencję względem swojego własnego zastosowania w obszarze funkcjonowania wojska są zaawansowane, a Chat GPT może stanowić wartościowe narzędzie informacyjne, jako jedno z istotnych źródeł budowania świadomości sytuacyjnej.

Słowa kluczowe

Analiza przeprowadzona przez autora, a także wskazania samej sztucznej inteligencji świadczą o wielu korzyściach implementacji sztucznej inteligencji w siłach zbrojnych. Jednocześnie należy mieć świadomość wielu zagrożeń z tym związanych, ze względu na podatności, jakie to rozwiązanie obecnie tworzy.

sztuczna inteligencja, siły zbrojne, bezpieczeństwo, systemy autonomiczne, Chat GPT

Wstęp

Siły zbrojne jako wysoce wykwalifikowany instrument obrony państwa potrzebują nowoczesnych technologii, żeby sprostać coraz to nowym wyzwaniom i zagrożeniom. Sztuczna inteligencja jest technologicznym kołem napędowym naszych czasów, ale jej dwubiegowość skłania do głębszej refleksji nad jej dalszym rozwojem. Atrakcyjność wykorzystania sztucznej inteligencji jest ściśle związana z jej zdolnością do adaptacji i samouczenia się, możliwościami analitycznymi i predykcyjnymi, które umożliwiają tworzenie zaawansowanych i inteligentnych systemów. Jedną z najważniejszych zalet sztucznej inteligencji jest możliwość operowania ogromną ilością danych i podejmowanie na ich podstawie określonych działań: „Algorytmy stanowiące część AI mogą podejmować autonomiczne decyzje w oparciu o analizę dużych zbiorów danych, samodzielnie korygować błędy i podejmować decyzje w oparciu o wcześniejsze doświadczenie. Biorąc to pod uwagę, można je stosować tam, gdzie konieczna jest szybka analiza informacji i identyfikacja wzorców i współzależności. Pozwala to AI znaleźć optymalne rozwiązania danego problemu w nieporównywalnie krótszym czasie niż byłby potrzebny człowiekowi”¹. Świat sztucznej inteligencji doświadczył niezwyklej ewolucji, zwłaszcza w dziedzinie przetwarzania języka naturalnego. Duże modele językowe² takie,

- 1 K. Kaczmarek, M. Karpiuk, U. Soler, *The Potential Use of Artificial Intelligence in Crisis Management*, „Sicurezza, Terrorismo E Società” 2024, t. 20, nr 2, s. 142.
- 2 Large Language Models (LLM) – duże modele językowe. To modele głębokiego uczenia, które są wstępnie trenowane na ogromnych ilościach danych. Podstawowym elementem jest zestaw sieci neuronowych, które wyodrębniają znaczenia z sekwencji tekstu i rozumieją relacje między słowami i frazami. Zob. *What is LLM (Large Language Model)?*, <https://aws.amazon.com/what-is/large-language-model/> [dostęp: 20.12.2024].

jak: Chat GPT firmy OpenAI, Bard firmy Google czy Claude firmy Anthropic, są najlepszymi przykładami ewolucji tej nowoczesnej technologii. Modele te są katalizatorami interakcji pomiędzy ludźmi a platformami cyfrowymi³. Jednakże rozwiązania wykorzystujące sztuczną inteligencję nie są doskonałe, są bowiem obarczone niedoskonałością człowieka, który ją tworzy, oraz możliwościami ingerencji w jej działanie przez wrogich aktorów. Ponadto istnieje prawdopodobieństwo wytworzenia przez sztuczną inteligencję informacji nieprawdziwej, co z zastosowaniem śmiertelnej broni może okazać się tragiczne w skutkach.

Celem artykułu jest przedstawienie potencjału wykorzystania sztucznej inteligencji na potrzeby wojska i zestawienie go z treścią wygenerowaną przez Chat GPT⁴ w odpowiedzi na pytania dotyczące różnych obszarów wdrożenia sztucznej inteligencji na potrzeby armii. Autor wykorzystał metodę analityczną, żeby wyodrębnić obszary zastosowania sztucznej inteligencji na potrzeby sił zbrojnych, a także wnioskuje, żeby wskazać potencjalne kierunki jej implementacji. Wykorzystał także metodę wywiadu eksperckiego⁵ do przeprowadzenia wywiadu ze sztuczną inteligencją. Ponadto zastosował syntezę, żeby zaproponować skalę autonomii systemu względem człowieka, a także zdefiniował trzy podstawowe obszary, które należy opanować, żeby swobodnie posługiwać się sztuczną inteligencją bez obaw o ryzyko jej niepożądanego działania.

Autonomia a całkowita samodzielność sztucznej inteligencji

Jednym z głównych powodów wykorzystania sztucznej inteligencji w przypadku systemów uzbrojenia jest dążenie do samodzielności systemu w wykonaniu zadania. Docelowo ta samodzielność ma dotyczyć wszystkich etapów

- 3 *Comparative Analysis between OpenAI ChatGPT, Google Bard, Anthropic Claude, and Google Gemini*, <https://medium.com/@DigitalQuill.ai/comparative-analysis-between-chatgpt-bard-claude-and-gemini-ai-llms-30b7a4488c5d> [dostęp: 13.11.2024].
- 4 Chat GPT (Generative Pre-Trained Transformer) to program sztucznej inteligencji, który generuje naturalny dialog. Wykorzystuje algorytm uczenia maszynowego do przetwarzania i analizowania dużych ilości danych w celu opracowania odpowiedzi na zapytania użytkowników. Poprzez przetwarzanie języka jest w stanie zrozumieć język ludzki w jego naturalnym środowisku, tj. używany przez ludzi w sposób naturalny. Zob. *Chat GPT: What is it?*, <https://uca.edu/cetal/chat-gpt> [dostęp: 13.11.2024].
- 5 Autor 21 marca 2025 r. przeprowadził wywiad z darmową wersją Chat GPT-4-turbo dla system operacyjnego iOS.

realizacji misji, od zaplanowania operacji, zebrania i analizy danych, po podjęcie decyzji na polu walki. Dlatego należy wyjaśnić pojęcia „samodzielność” i „autonomiczność”. Według słownika języka polskiego autonomia to: „samodzielność i niezależność w decydowaniu o sobie [...] niezależność od norm etycznych zewnętrznych, innych niż własne sumienie”⁶. Portal polszczyzna.pl podaje, że „[...] w odniesieniu do człowieka autonomia to samodzielność i niezależność, która przejawia się swobodą działania i posiadaniem możliwości decydowania o sobie i rządzeniu się własnymi prawami, bez narzucania ich przez inne osoby”⁷. Według publikacji Komisji Europejskiej pt. „The Assessment List For Trustworthy Artificial Intelligence” autonomiczny system sztucznej inteligencji to system, który wykonuje zachowania lub zadania z dużym stopniem autonomii, czyli bez zewnętrznego wpływu (np. bez udziału człowieka)⁸. Autorzy encyklopedii zarządzania stwierdzają, że „[...] autonomia odnosi się do stopnia, w jakim pracownicy mają możliwość podejmowania decyzji i działania samodzielnie, bez nadzoru i kontroli ze strony przełożonych” i uszczegóławia, że „[...] ważne jest jednak zrozumienie, że autonomia nie oznacza całkowitego braku nadzoru. Chociaż autonomia daje pracownikom większą swobodę w podejmowaniu decyzji, nadal istnieje potrzeba monitorowania ich działań i zapewnienia, że decyzje podejmowane są zgodne z celami organizacji. W związku z tym, ważne jest ustalenie granic autonomii i jasne zdefiniowanie zakresu decyzji, które pracownicy mogą podejmować samodzielnie”⁹. Rafał Rejmانيak podkreśla, że autonomiczność systemów sztucznej inteligencji należy rozumieć jako „[...] zdolność do samodzielnego działania bez ingerencji człowieka”¹⁰. Autor uważa, że najbardziej trafna definicja została zaproponowana w encyklopedii zarządzania. Pomimo samodzielności ważny jest nadzór i monitorowanie osiągniętych celów.

6 *Autonomia*, <https://sjp.pwn.pl/sjp/autonomia;2551312.html> [dostęp: 20.03.2025].

7 *Autonomia – co to jest? Definicja, synonimy, przykłady użycia*, <https://polszczyzna.pl/autonomia-co-to-jest-definicja-synonimy-przyklady-uzycia> [dostęp: 20.03.2025].

8 *The Assessment List For Trustworthy Artificial Intelligence (ALTAI)*, Glossary, Independent High-Level Expert Group On Artificial Intelligence, Bruksela, 2020, <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment> [dostęp: 3.02.2025].

9 *Autonomia*, <https://mfiles.pl/pl/index.php/Autonomia> [dostęp: 20.03.2025].

10 R. Rejmانيak, *Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego*, „Rocznik Nauk Prawnych” 2021, t. 31, nr 3, s. 98.

Autor uważa, że cel sztucznej inteligencji z punktu widzenia jej autonomiczności może być wskazany bezpośrednio przed zadaniem lub pośrednio przy wprowadzaniu danych wejściowych¹¹.

Bezpośrednio polega na wskazaniu celu dla systemu, np. usunięcia przeszkody na drodze. System podejmuje decyzję, jakimi dostępnymi środkami wykona zadanie, a zadanie kończy się z chwilą usunięcia przeszkody. Można ogólnie stwierdzić, że system wykonał zadanie autonomicznie, tj. nie był sterowany przez człowieka i nie pytał człowieka o zgodę na wykorzystanie konkretnych środków, w tym sposobu ich użycia.

Pośrednio polega na wprowadzeniu poleceń na poziomie programowania i nasycania systemu danymi wejściowymi. Odnosząc się do wyżej zaproponowanego przykładu usunięcia przeszkody, polecenie wprowadzone podczas nasycenia danymi wejściowymi może dotyczyć usuwania wszystkich przeszkód, które np. uniemożliwiają kontynuowanie przemieszczania po wyznaczonej trasie. Jeżeli system napotka przeszkodę, to usuwa ją zgodnie z wcześniej określonymi celami. Można zatem ogólnie stwierdzić, że wykonał zadanie autonomicznie.

Autor obecnie nie dostrzega merytorycznych przesłanek do implementacji systemu całkowicie autonomicznego. Oznaczałoby to, że system inicjuje działanie, np. bojowe, bez żadnego udziału człowieka. Jeżeli nawet system będzie w stanie samodzielnie określić cele taktyczne lub operacyjne i sposób ich osiągnięcia, to nadrzędna struktura celów polityczno-strategicznych jest nadal definiowana przez człowieka. Autor twierdzi, że w momencie przekazania systemowi samodzielności nad określaniem celów polityczno-strategicznych lub nadania rzeczywistej i całkowitej autonomii systemowi opartemu na sztucznej inteligencji będzie to oznaczało wyparcie człowieka z cyklu decyzyjnego, jego marginalizację i alienację z funkcji kreatora środowiska własnego funkcjonowania.

11 Dane wejściowe – dane dostarczone do systemu AI lub bezpośrednio przez niego pozyskiwane, na podstawie których system generuje wynik. Zob. *Rozporządzenie 2024/1689 w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)*, Dz. Urz. UE 2024, L 1689, art. 3, pkt 33.

Autor proponuje skalę autonomii sztucznej inteligencji uwzględniającą poziom zaangażowania systemu i poziom zaangażowania człowieka w decyzyjność i sprawczość.

Tabela 1. Skala autonomii sztucznej inteligencji

Poziom autonomii sztucznej inteligencji	Charakterystyka zaangażowania systemu i człowieka	
	system	człowiek
Wykonawczy	brak autonomii; system wykonuje polecenia człowieka, wykorzystując swoje możliwości technologiczne	człowiek inicjuje działanie, decyduje o sposobie jego wykonania i zakończeniu; wspomaga się technologicznymi możliwościami systemu
Towarzyszący	wykonuje polecenia człowieka, wspomaga realizację zadań zgodnie ze swoimi możliwościami technologicznymi, wykazuje inicjatywę w ramach postawionych zadań, potrafi np. samodzielnie zaproponować różne warianty wykonania zadania czy samodzielnie zrealizować część misji zgodnie z postawionym celem	inicjuje działanie, decyduje o jego wykonaniu i zakończeniu, współpracuje z systemem z wykorzystaniem jego możliwości technologicznych, korzysta z inicjatywy systemu w sposobie realizacji zadań
Dominujący	otrzymuje od człowieka cel do osiągnięcia, sam dobiera sposób wykonania zadań i decyduje kiedy zostaną zakończone, a cel osiągnięty	stawia systemowi cel; cel może być określany bezpośrednio przed zadaniem lub w ramach danych wejściowych, na podstawie których system sam określi sposób wykonania; człowiek nie dobiera środków, a system sam decyduje, czy cel został osiągnięty

Źródło: Opracowanie własne.

Militarny potencjał sztucznej inteligencji

Sztuczna inteligencja jest technologią, w którą inwestuje coraz więcej armii, ponieważ przewaga w wyścigu technologicznym oznacza przewagę na polu walki. Jest wdrażana do rodzajów sił zbrojnych wielu państw, a jej zastosowanie wspomaga działanie armii na wielu płaszczyznach. Wykorzystanie sztucznej inteligencji może mieć zastosowanie w budowaniu świadomości operacyjnej,

logistyce i efektywności bojowej. Ahmed Banafa w publikacji pt. „Artificial Intelligence (AI) in Modern Military Applications” wymienia niektóre obszary i konkretne systemy, w których już zastosowano rozwiązania oparte na sztucznej inteligencji. Są to m.in. bezzałogowe platformy lądowe, które mogą wykonywać zadania rozpoznawcze, transportowe lub prowadzić działania bojowe z minimalnym udziałem człowieka. Jak wskazano na Platformie Przemysłu Przyszłości: „Pojazdy autonomiczne i bezzałogowe to systemy transportowe, które mogą poruszać się samodzielnie bez potrzeby bezpośredniego sterowania przez człowieka. Wykorzystują zaawansowane technologie, takie jak sztuczna inteligencja, czujniki i systemy nawigacyjne, aby samodzielnie analizować otoczenie, podejmować decyzje i przemieszczać się w środowisku. Tego rodzaju pojazdy mają szerokie zastosowanie w transporcie, logistyce, rolnictwie, wojsku i eksploracji”¹². Jednym z przykładów wykorzystania zaawansowanej technologii może być użycie robotycznego muła¹³, który w wojsku jest przeznaczony przede wszystkim do przenoszenia ciężkich ładunków, co z kolei odciąża żołnierzy wykonujących np. działania patrolowe¹⁴. Z kolei Firma BAE Systems Australia zaprezentowała autonomiczny opancerzony lekki system taktyczny ATLAS CCV (Autonomous Tactical Light Armour System Collaborative Combat Variant)¹⁵, sterujący pojazdem, który będzie pozwalał unikać przeszkód, planować trasę i podejmować decyzje taktyczne¹⁶. W logistyce warto podkreślić wykorzystanie sztucznej inteligencji w utrzymaniu predykcyjnym. Polega ono na zbieraniu danych o stanie maszyn i przebiegu procesów eksploatacyjnych. Na podstawie danych są tworzone modele pozwalające przewidywać wystąpienie awarii i określać stan urządzenia, np. stopień jego zużycia. Modele sztucznej inteligencji potrafią w czasie rzeczywistym określać ryzyko niesprawności i alarmować o możliwych problemach. Dzięki

12 *Pojazdy autonomiczne/bezzałogowe*, <https://przemyslprzyszlosci.gov.pl/technologie/cyfrowe/robotyzacja/pojazdy-autonomiczne-bezzałogowe> [dostęp: 3.03.2025].

13 *LS3: Legged Squad Support System*, <https://www.darpa.mil/research/programs/legged-squad-support-system> [dostęp: 3.03.2025].

14 *Testy LS3*, <https://www.youtube.com/watch?v=IIbtwn8jwwc&t=62s> [dostęp: 3.03.2025].

15 *Zob. Autonomous Tactical Light Armour System Collaborative Combat Variant (ATLAS CCV), Australia*, <https://www.army-technology.com/projects/atlas-ccv-australia> [dostęp: 3.03.2025].

16 *Bezzałogowy pojazd bojowy nowej generacji ATLAS CCV, 2024*, <https://tacgear.pl/2024/09/bezzałogowy-pojazd-bojowy-nowej-generacji-atlas-ccv> [dostęp: 23.02.2025].

wdrożeniu strategii utrzymania predykcyjnego można zmniejszyć koszty serwisu, ograniczyć czas przestojów, jednocześnie wydłużyć czas działania urządzeń i zwiększyć bezpieczeństwo¹⁷. Zastosowanie sztucznej inteligencji wspomaga także zdolności żołnierzy, dlatego że monitoruje dane dotyczące ich stanu zdrowia, żeby poprawiać proces szkolenia, a docelowo zwiększyć efektywność bojową. Jednym z elementów tego procesu może być *neurofeedback*, który jest nowym podejściem do przygotowania psychofizycznego żołnierzy i stanowi zaawansowaną metodę pozwalającą na świadomą regulację aktywności mózgowej¹⁸. Sztuczna inteligencja może także wesprzeć działania marynarki wojennej w prowadzeniu operacji morskich, np. poprzez realizację misji patrolowych, bojowych czy zbieranie danych wywiadowczych. Ponadto algorytmy sztucznej inteligencji przetwarzają dane z sonarów, żeby wykryć i śledzić pojazdy podwodne bardziej efektywnie niż człowiek. W przypadku sił powietrznych i kosmicznych sztuczna inteligencja może wspomagać zadania związane z wykorzystaniem dronów, wspierać pilotów czy monitorować ruch lotniczy. Dodatkowo algorytmy optymalizują pracę satelitów i mogą przewidywać potencjalną ich kolizję. W rzeczywistości cyberwojny sztuczna inteligencja jest narzędziem niezbędnym do wykrycia zagrożenia i reakcji na nie, a także ochrony sieci wojskowych przed atakami. Wykorzystanie sztucznej inteligencji pozwala prowadzić ofensywne operacje cybernetyczne poprzez identyfikację podatności wrogich systemów i automatyzację ataku¹⁹. W kwestii zagrożenia pociskami balistycznymi należy podkreślić, że z pomocą sztucznej inteligencji można wykryć nadlatujący pocisk balistyczny, próbować przewidzieć trajektorię jego lotu i w rezultacie spróbować zakłócić sygnał sterujący pociskiem lub przejąć na nim kontrolę. Przykładem niebojowego wykorzystania może być użycie oprogramowania do tłumaczenia i transkrypcji, które potrafi w czasie rzeczywistym wykonać tłumaczenie i transkrypcję wielu długich tekstów jednocześnie, na wiele języków. W obszarze szkolenia,

17 *Predictive Maintenance (Utrzymanie predykcyjne)*, <https://www.statsoft.pl/rozwiwania/zastosowania-technologiczne/predictive-maintenance> [dostęp: 23.02.2025].

18 A. Nowacka, *Zastosowanie neurofeedbacku w optymalizacji wydolności psychofizycznej żołnierzy*, <https://www.ezaf.pl/wpisy/zastosowanie-neurofeedbacku-w-optymalizacji-wydolnosc-psychofizycznej-zolnierzy,1842> [dostęp: 7.02.2025].

19 A. Banafa, *Artificial Intelligence (AI) in Modern Military Applications*, <https://www.linkedin.com/pulse/artificial-intelligence-ai-modern-military-prof-ahmed-banafa-e9sxc> [dostęp: 23.01.2025].

sztuczna inteligencja może być wykorzystana w symulatorach i тренаżerach, żeby jak najdokładniej odwzorować rzeczywiste pole walki. Szkolenie może być także prowadzone przez inteligentnego asystenta, np. chatbot, który w przeciwieństwie do podręczników będzie zawsze dysponował uaktualnianą bazą danych. Atutem użycia sztucznej inteligencji na potrzeby armii może być brak typowo ludzkich dylematów moralnych podczas podejmowania decyzji. Warto wspomnieć, że prowadzone są prace nad tym, żeby sztuczna inteligencja uczyła się samodzielnie, co ma ograniczyć udział człowieka i zmniejszyć koszty nasycania algorytmów danymi wejściowymi²⁰. Jak wskazano w projekcie Komisji Europejskiej „Horizon 2020”, żeby usprawnić proces uczenia się sztucznej inteligencji, zostało opracowanych kilka nowych technologii mogących prowadzić własne badania. Wskazano, że algorytmy „[...] mogą to robić automatycznie, konsultując się z zasobami internetowymi, na przykład bazami Google i Wikipedii, a także dzięki nowemu matematycznemu podejściu do uczenia się geometrii obiektów na podstawie obrazów i filmów bez konieczności korzystania z zewnętrznego źródła nadzoru”²¹. Kolejnym obszarem, w którym można wykorzystać sztuczną inteligencję, może być przeciwdziałanie wrogim operacjom informacyjnym, w tym procesowi dezinformacji. Autor wskazuje trzy filary dezinformacji, które są wykorzystywane do wprowadzenia w błąd użytkownika przestrzeni informacyjnej:

- manipulacja faktami,
- tworzenie fake-newsów,
- szum informacyjny²².

Sztuczna inteligencja jest w tym obszarze wykorzystywana do identyfikacji, analizy i monitorowania treści i tendencji w procesach dezinformacyjnych, daje np. możliwość przygotowania narracji informacyjnej w przypadku zaistnienia sytuacji kryzysowej lub możliwość określania kierunków komunikacji proaktywnej.

20 *Artificial Intelligence in Electronic Warfare*, <https://www.te.com/en/industries/defense-military/insights/ai-in-warfare-and-military-applications.html> [dostęp: 3.02.2025].

21 *Uczenie sztucznej inteligencji, jak ma się sama uczyć*, Europejska Rada ds. Badań Naukowych, <https://cordis.europa.eu/article/id/435616-teaching-ai-to-teach-itself/pl> [dostęp: 10.03.2025].

22 Zob. T. Gergelewicz, *Countering Disinformation Concept for building social resilience in times of cognitive warfare*, „Przegląd Nauk o Obronności. Defence Science Review” 2024, nr 20, s. 34.

Podsumowując, implementacja sztucznej inteligencji na potrzeby sił zbrojnych może bezpośrednio wpłynąć po poprawienie wydajności sił zbrojnych, a także na przyspieszenie procesów decyzyjnych. To z kolei może przejawiać się m.in. w takich obszarach, jak:

- podejmowanie decyzji – możliwość przetwarzania dużej ilości danych i dostarczanie dowódcom szybkich rekomendacji na podstawie konkretnych informacji. Ponadto warto zaznaczyć, że czas oszczędzony na wykonanie zadania wspartego sztuczną inteligencją to czas, który może być wykorzystany do opracowania bardziej kompletnych planów działania z większą liczbą wariantów²³,
- świadomość sytuacyjna – czujniki i narzędzia analityczne dają dokładniejszy obraz pola walki,
- ryzyko strat w ludziach – automatyczne systemy mogą wykonywać niebezpieczne zadania, potencjalnie ratować życie żołnierzy,
- wydajność zasobów – optymalizacja logistyki, utrzymanie i przemieszczanie zasobów, obniżanie kosztów i poprawa skuteczności realizacji zadań,
- czas reakcji – możliwość reagowania na zagrożenia w krótszym czasie niż operatorzy-żołnierze, potencjalnie zapewniać przewagę w krytycznych momentach,
- wydłużona gotowość do działania – możliwość działania nieprzerwanie bez zmęczenia, utrzymanie stałej gotowości,
- obliczenia kwantowe – potencjał dużej mocy przetwarzania danych i możliwości rozwiązywania złożonych problemów obliczeniowych,
- analiza predykcyjna wydarzeń geopolitycznych – prawdopodobieństwo przewidywania konfliktów²⁴.

Jak podkreślono w „Artificial Intelligence and National Security U.S.”, rozwój możliwości nowoczesnych technologii opartych na sztucznej inteligencji prawdopodobnie umożliwi przejście z misji bojowych załogowych na bezzałogowe i tym samym bardziej autonomiczne wsparcie żołnierzy przez roboty²⁵.

23 M. Zequeira, *U.S. Army, Artificial Intelligence as a Combat Multiplier, Using AI to Unburden Army Staffs*, Military Review Online Exclusive, 2024, <https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/AI-Combat-Multiplier> [dostęp: 18.01.2025].

24 A. Banafa, op. cit.

25 G. Allen, T. Chan, *Artificial Intelligence and National Security U.S. Intelligence Advanced Research Projects Activity (IARPA)*, Harvard Cennedy School – Belfer Center for Science and International Affairs, 2017, <https://www.belfercenter.org/sites/default/>

Rozwój sztucznej inteligencji na potrzeby wojska w ujęciu ogólnym zmierza w stronę samodzielnego nasycenia się danymi, możliwości autonomicznej analizy informacji i podjęcia suwerennej decyzji.

Militarny potencjał sztucznej inteligencji – wyzwania

Ciągły postęp w dziedzinie sztucznej inteligencji generuje coraz większe wyzwania dotyczące m.in. określenia podstaw prawnych i moralnych jej tworzenia oraz wykorzystywania. Wydaje się, że obecnie jednym z głównych problemów w tym zakresie jest zdefiniowanie zasad odpowiedzialności za potencjalne szkody, które mogą zostać wyrządzone w wyniku działania sztucznej inteligencji. Robert Weissman i Savannah Wooten w publikacji pt. „A.I. Joe: The Dangers of Artificial Intelligence and the U.S. Military” wyliczają wyzwania, z którymi należy się mierzyć podczas wdrażania sztucznej inteligencji na potrzeby wojska:

- etyka – użycie broni autonomicznej wywołuje pytania natury moralnej dotyczące roli człowieka w podejmowaniu decyzji na polu walki. Sztuczna inteligencja może mieć trudności w podejmowaniu decyzji, które wymagają empatii, zrozumienia kulturowego lub złożonych rozważań etycznych,

- rzetelność i nieprzewidywalność – systemy mogą działać w sposób nieprzewidywalny w złożonych, rzeczywistych scenariuszach, co może prowadzić do niezamierzonych rezultatów,

- podatność na wrogie przejęcie – systemy mogą zostać przejęte przez przeciwników, potencjalnie obracając broń przeciwko własnym operatorom.

Leonel Garciga²⁶ przestrzegął personel wojskowy i propagatorów sztucznej inteligencji, że „narzędzia sztucznej inteligencji zostały szeroko przyjęte ze względu na ich wysoką wydajność i łatwość użytkowania. Jednak stanowią one również wyjątkowe wyzwania pod względem prywatności danych,

files/2024-10/Artificial%20Intelligence%20and%20National%20Security.pdf [dostęp: 28.02.2025].

26 Szef ds. Informacji w Dowództwie Wojsk Lądowych Armii Stanów Zjednoczonych. Zob. Leonel Garciga on Army's Unified Network Operations Initiative, <https://executive.gov.com/2025/02/leonel-garciga-army-unified-network-operations-initiative> [dostęp: 2.02.2025].

bezpieczeństwa i kontroli nad generowaną treścią. Dlatego ich stosowanie powinno być starannie oceniane i monitorowane²⁷.

1. Zależność od danych. Do skutecznego działania systemy oparte na sztucznej inteligencji wymagają dużych ilości wysokiej jakości danych, które nie zawsze mogą być dostępne w sytuacjach bojowych.

Rozmieszczanie śmiertelnej broni opartej na sztucznej inteligencji w środowisku pola walki oznacza użytkowanie jej w warunkach, do których nie została zaprogramowana. Potencjalne problemy z wiarygodnymi danymi szkoleniowymi lub nieprawdziwymi danymi wywiadowczymi mogą skutkować błędną identyfikacją celów i niezamierzonym atakiem.

2. Ryzyko eskalacji. Efektywność działań bojowych z zastosowaniem sztucznej inteligencji może prowadzić do szybkiej eskalacji konfliktów, potencjalnie zwiększać ryzyko pełnoskalowej wojny. Ponadto dostęp do sztucznej inteligencji jest coraz bardziej powszechny, co zwiększa prawdopodobieństwo, że wpadnie w ręce aktorów niepaństwowych lub państw-agresorów.

3. Niejednoznaczność prawna. Wykorzystanie systemów autonomicznych powoduje pytania natury prawnej dotyczące odpowiedzialności i zgodności z prawem²⁸.

Kwestię odpowiedzialności prawnej za użycie sztucznej inteligencji podjął Rafał Rejmank w publikacji „Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego”. Zazaczył, że wraz ze wzrostem poziomu autonomiczności systemów sztucznej inteligencji rosną trudności ze wskazaniem odpowiedzialnego za ewentualne szkody w mieniu czy za narażenie zdrowia lub życia. Z reguły odpowiedzialność ponosi ten, który ostatecznie podejmuje decyzję o rozpoczęciu lub zaniechaniu działania. Natomiast jeżeli rola człowieka sprowadza się do nadzorującego system, to zarzutem nie jest to, że skutek wywołał, ale to, że mu nie zapobiegł, znając jego konsekwencje. Problemy ze wskazaniem odpowiedzialnego karnie za skutki powodowane przez systemy

27 Cyt. za: M. Easley, *Army implements generative AI platform to cArmy cloud environment*, 2024 <https://defensescoop.com/2024/09/10/army-generative-ai-capability-carmy-cloud> [dostęp: 2.02.2025].

28 R. Weissman, S. Wooten, *A.I. Joe: The Dangers of Artificial Intelligence and the U.S. Military*, 2024, s. 8–17, <https://www.citizen.org/article/ai-joe-report/> [dostęp: 13.01.2025].

w pełni autonomiczne wydają się wyzwaniem ze względu na brak związku pomiędzy wolą i świadomością człowieka a działaniem systemu²⁹.

Ponadto należy podkreślić, że przykładem nieprawidłowego działania sztucznej inteligencji mogą być tzw. halucynacje sztucznej inteligencji, które pojawiają się, gdy system regularnie generuje nieprawidłowe odpowiedzi i przedstawia je z dużą pewnością jako prawdziwe. Błędy te mogą być spowodowane m.in. przez niewystarczające dane szkoleniowe (na których sztuczna inteligencja się uczy), nieprawidłowe założenia przyjęte przez model lub błędy w danych wykorzystywanych do szkolenia³⁰.

Reasumując, autor definiuje trzy zasadnicze obszary, które należy opanować, żeby swobodnie posługiwać się sztuczną inteligencją bez obaw o ryzyko niepożądanego działania.

1. Awary – niedające się przewidzieć awary powodowane przez wadliwe elementy, co może prowadzić do zaniechania lub błędnego wykonania zadania.

2. Przejęcie – prawdopodobieństwo przejęcia systemów przez strony nieposiadające autoryzowanego dostępu, co mogłoby zostać wykorzystane do celów niezwiązanych z wolą i zamiarem właściwego operatora.

3. Autonomia – całkowita autonomia systemów opartych na sztucznej inteligencji, w perspektywie jej śmiertelności potencjału, może stanowić poważne zagrożenie w przypadku braku kontroli ze strony człowieka. Pełna decyzyjność po stronie systemu może być tragiczna w skutkach.

Wywiad z Chatem GPT

Prowadząc rozważania na temat wykorzystania sztucznej inteligencji na potrzeby sił zbrojnych, warto posłkować się głosem eksperckim. Autor zakłada, że eksperckie stanowisko może przedstawić sama sztuczna inteligencja, dlatego przeprowadził wywiad z tą technologią, która w tym przypadku jest reprezentowana przez Chat GPT.

²⁹ R. Rejmaniak, op. cit., s. 108.

³⁰ Na podstawie: T. Gergelewicz, *Bipolarity of Artificial Intelligence – Chances and Threats*, „Ius et Securitas” 2024, nr 2, s. 71–94.

1. Jakie obszary w wojsku są kluczowe do zastosowania sztucznej inteligencji?

„W wojsku sztuczna inteligencja (SI) może być zastosowana w wielu obszarach, a jej wdrożenie może znacząco zwiększyć efektywność operacji, poprawić bezpieczeństwo i zredukować ryzyko. Kluczowe obszary zastosowania SI w wojsku to:

1. Zautomatyzowane systemy rozpoznania i analizy danych: SI może analizować ogromne ilości danych z różnych źródeł (np. zdjęć satelitarnych, dronów, monitoringu) w celu wykrywania zagrożeń, identyfikowania celów lub monitorowania ruchów wroga.

2. Drony i roboty bojowe: Wykorzystanie SI do autonomicznych systemów bojowych (np. dronów, robotów naziemnych), które mogą prowadzić misje zwiadowcze, dostarczać zaopatrzenie, czy nawet przeprowadzać ataki precyzyjne.

3. Wspomaganie decyzji w dowodzeniu: Algorytmy SI mogą analizować dane strategiczne, prognozować możliwe scenariusze konfliktów i sugerować optymalne decyzje dowódcom, wspomagając procesy planowania i decyzyjne.

4. Cyberbezpieczeństwo i obrona przed atakami: SI jest kluczowym narzędziem w walce z cyberzagrożeniami, w tym w wykrywaniu ataków hakerskich, analizowaniu zachowań podejrzanych użytkowników i zabezpieczaniu systemów wojskowych.

5. Symulacje i treningi wojskowe: SI może służyć do tworzenia realistycznych symulacji, które pozwalają na doskonalenie umiejętności żołnierzy i sztabów wojskowych w bezpiecznym, wirtualnym środowisku.

6. Logistyka i zaopatrzenie: Optymalizacja procesów logistycznych za pomocą SI, w tym zarządzanie zaopatrzeniem, transportem, magazynowaniem i dystrybucją zasobów w trudnych warunkach wojennych.

7. Przewidywanie i zarządzanie zasobami: SI może pomóc w przewidywaniu potrzeb w zakresie personelu, sprzętu czy amunicji, umożliwiając bardziej efektywne planowanie zasobów i zmniejszając marnotrawstwo.

8. Medycyna wojskowa: Zastosowanie SI w diagnostyce medycznej, zdalnym monitorowaniu zdrowia żołnierzy oraz robotach medycznych do pomocy w terenie, zwłaszcza w sytuacjach wymagających natychmiastowej interwencji.

9. Zarządzanie komunikacją i koordynacją: SI może wspomagać systemy komunikacyjne, zapewniając szybkie, bezpieczne i efektywne przesyłanie

informacji w czasie rzeczywistym, co jest kluczowe w dynamicznych warunkach pola walki.

Implementacja sztucznej inteligencji w tych obszarach może poprawić szybkość, precyzję i bezpieczeństwo działań wojskowych, a także umożliwić lepsze wykorzystanie zasobów i wsparcie dla żołnierzy w trudnych warunkach”.

Chat trafnie wymienił i scharakteryzował większość zasadniczych obszarów wykorzystujących i potencjalnie wykorzystujących sztuczną inteligencję na potrzeby wojska. Należy zwrócić uwagę, że zadane pytanie nie zawierało oczekiwania uzasadnienia, ale Chat z własnej inicjatywy ogólnie scharakteryzował przedstawione obszary. Dodatkowo dokonał krótkiego podsumowania, w którym wskazał zalety wykorzystania sztucznej inteligencji na potrzeby wojska.

2. Które państwo obecnie może wykorzystać sztuczną inteligencję do prowadzenia działań agresywnych?

„Wykorzystanie sztucznej inteligencji (SI) do prowadzenia agresywnych działań wojskowych staje się coraz bardziej realne i jest rozwijane przez kilka państw. Wśród krajów, które inwestują i rozwijają technologie związane z SI w kontekście obronności i wojskowości, wyróżniają się przede wszystkim:

1. Stany Zjednoczone: USA są jednym z liderów w zastosowaniu SI w wojskowości. Amerykańska armia intensywnie inwestuje w rozwój autonomicznych systemów bojowych, dronów, cyberbezpieczeństwa oraz analityki danych opartej na SI. Dodatkowo, Stany Zjednoczone pracują nad rozwojem systemów wspierających decyzje dowódcze i automatycznych broni opartej na SI. Sztuczna inteligencja jest także wykorzystywana w cyberwojnie, co pozwala na ofensywne działania w sieci.

2. Chiny: Chiny są jednym z najbardziej zaawansowanych krajów w zakresie zastosowania sztucznej inteligencji w wojskowości. Chińska armia inwestuje w rozwój autonomicznych systemów takich, jak: drony bojowe, roboty czy technologie w zakresie wojny cybernetycznej. Chińska strategia wojskowa w dużym stopniu opiera się na »wojnie informacyjnej« i wykorzystaniu SI do przeprowadzania operacji wywiadowczych, analizie danych i atakach w cyberprzestrzeni.

3. Rosja: Rosja również rozwija technologie sztucznej inteligencji w kontekście działań wojskowych, szczególnie w zakresie dronów bojowych, autonomicznych systemów naziemnych i cyberbezpieczeństwa. Istnieją doniesienia

o wykorzystaniu SI w rosyjskich działaniach ofensywnych w cyberprzestrzeni, a także w analizie danych wywiadowczych oraz planowaniu operacji wojskowych.

4. Izrael: Izrael jest jednym z liderów w dziedzinie technologii obronnych, w tym sztucznej inteligencji. Kraj ten jest znany z zaawansowanych systemów obrony powietrznej, dronów oraz innych autonomicznych systemów, które mogą być wykorzystywane w ofensywnych operacjach wojskowych. Izrael również inwestuje w rozwój cyberwojny opartej na sztucznej inteligencji.

5. Zjednoczone Emiraty Arabskie: ZEA rozwijają autonomiczne systemy bojowe i inwestują w SI jako część swojej strategii obronnej. Drony i roboty bojowe są wykorzystywane zarówno w obronie, jak i do przeprowadzania ofensywnych działań.

6. Indie: Indie, choć na mniejszą skalę niż inne mocarstwa, również inwestują w sztuczną inteligencję w kontekście obronności, szczególnie w zakresie autonomicznych systemów, dronów, analityki danych oraz cyberbezpieczeństwa.

Sztuczna inteligencja w kontekście agresywnych działań wojskowych wiąże się z wieloma wyzwaniem etycznymi, prawnymi i technologicznymi. Wiele z tych państw bada kwestie związane z autonomią broni, analizą danych wywiadowczych oraz cyberatakami, co może mieć poważne konsekwencje w przypadku wykorzystania tych technologii w konfliktach zbrojnych. Oczekuje się, że w najbliższych latach konkurencja w tej dziedzinie będzie intensyfikować się, a rozwój SI będzie kluczowym elementem strategii obronnych w wielu państwach”.

Chat komplementarnie odpowiada na pytanie, rozwija swoją odpowiedź o szczegóły dotyczące konkretnych wskazanych państw. Na uwagę zasługuje obszar cyberwojny i cyberbezpieczeństwa. Jak wskazuje Chat:

- „Dodatkowo, Stany Zjednoczone pracują nad rozwojem systemów wspierających decyzje dowódcze i automatycznych broni opartej na SI. Sztuczna inteligencja jest także wykorzystywana w cyberwojnie, co pozwala na ofensywne działania w sieci”.

- „Chińska armia inwestuje w rozwój autonomicznych systemów, takich jak drony bojowe, roboty czy technologie w zakresie wojny cybernetycznej”.

- „Rosja: Istnieją doniesienia o wykorzystaniu SI w rosyjskich działaniach ofensywnych w cyberprzestrzeni”.

- „Izrael również inwestuje w rozwój cyberwojny opartej na sztucznej inteligencji”.

Należy zwrócić uwagę na charakterystykę Federacji Rosyjskiej. W przypadku np. Stanów Zjednoczonych Ameryki, Chin czy Izraela Chat jednoznacznie stwierdza wykorzystanie sztucznej inteligencji w obszarze cyberwojny. Jeżeli chodzi o Federację Rosyjską, to wskazuje jedynie na „doniesienia”. W rzeczywistości wielokrotnie dowiedziono, że Moskwa prowadzi działania ofensywne w cyberprzestrzeni, w tym z wykorzystaniem sztucznej inteligencji.

3. Czy obecny etap rozwoju sztucznej inteligencji w Polsce daje szanse na jej skuteczne zastosowanie na potrzeby wojska?

„W Polsce rozwój sztucznej inteligencji (SI) w kontekście wojskowym jest na wczesnym etapie, ale kraj podejmuje kroki w celu zbudowania podstaw do jej skutecznego zastosowania w obronności. Obecny etap rozwoju SI w Polsce daje pewne szanse na jej przyszłe zastosowanie w wojsku, ale także stawia wyzwania, które będą wymagały dalszych inwestycji, rozwoju technologii i współpracy międzynarodowej. Oto kilka kluczowych aspektów, które należy uwzględnić:

1. Inwestycje w rozwój technologii i infrastruktury. Polska stawia na rozwój sektora technologii, w tym sztucznej inteligencji, poprzez różne inicjatywy, takie jak Program Inteligentnego Rozwoju czy wsparcie dla start-upów technologicznych. Zostały również uruchomione projekty badawcze w dziedzinie sztucznej inteligencji, które mogą z czasem przyczynić się do rozwoju rozwiązań wojskowych, w szczególności współpraca między uczelniami, ośrodkami badawczo-rozwojowymi i przemysłem obronnym jest kluczowa, aby stworzyć technologie odpowiadające specyficznym wymaganiom sektora obronności.

2. Współpraca międzynarodowa. Polska jest członkiem NATO, a współpraca z sojusznikami, w szczególności z krajami takimi jak Stany Zjednoczone, Wielka Brytania czy Niemcy, może pomóc w przyspieszeniu wdrożenia SI w wojsku. Dzięki tej współpracy Polska może uzyskać dostęp do nowoczesnych technologii i wiedzy, a także uczestniczyć w międzynarodowych programach badawczo-rozwojowych.

3. Wykorzystanie sztucznej inteligencji w cyberbezpieczeństwie. Jednym z bardziej rozwiniętych obszarów w Polsce, w którym sztuczna inteligencja może mieć szybki i efektywny wpływ, jest cyberbezpieczeństwo. Siły zbrojne i agencje rządowe, takie jak Polska Agencja Kosmiczna czy Agencja Bezpieczeństwa Wewnętrznego, już pracują nad wdrożeniem SI do monitorowania

zagrożeń w cyberprzestrzeni. W tym zakresie Polska ma szansę na skuteczne wykorzystanie SI do ochrony infrastruktury krytycznej oraz obrony przed cyberatakami.

4. Autonomiczne systemy bojowe. Polska armia posiada już pewne autonomiczne technologie, jak bezzałogowe statki powietrzne (drony) wykorzystywane do celów zwiadowczych. Przyszłość w rozwoju autonomicznych systemów bojowych (np. drony bojowe, roboty naziemne) może również przynieść korzyści w zakresie zwiększenia efektywności działań wojskowych, a w Polsce trwają prace nad rozwojem takich systemów. Jednak pełne wdrożenie zaawansowanych autonomicznych systemów wymagających SI w Polsce wymagałoby znacznych inwestycji w badania, rozwój technologii oraz infrastrukturę.

5. Edukacja i rozwój kompetencji. Polska już teraz inwestuje w rozwój kompetencji w dziedzinie sztucznej inteligencji, co jest kluczowe dla dalszego rozwoju technologii obronnych. Wprowadzenie specjalistycznych kursów, szkoleń oraz współpraca z międzynarodowymi ośrodkami naukowymi może zbudować bazę wiedzy niezbędną do wdrożenia SI w wojsku.

6. Wyzwania związane z regulacjami i etyką. Sztuczna inteligencja w wojskowości wiąże się z licznymi wyzwaniami etycznymi i prawnymi, zwłaszcza w kontekście autonomicznych systemów bojowych. Polska, podobnie jak inne kraje, będzie musiała zmierzyć się z kwestiami regulacyjnymi dotyczącymi użycia SI w wojskowości, takimi jak odpowiedzialność za działania maszyn, a także przestrzeganie międzynarodowych norm prawnych dotyczących użycia broni.

7. Potrzebna jest większa integracja z przemysłem obronnym. Choć w Polsce istnieją firmy, które rozwijają technologie sztucznej inteligencji, ich integracja z przemysłem obronnym może być kluczowa dla skutecznego wdrożenia SI w wojsku. Wymaga to długofalowych inwestycji w badania, rozwój i współpracę z sektorem zbrojeniowym.

Podsumowanie: Obecny etap rozwoju sztucznej inteligencji w Polsce daje podstawy do przyszłego wykorzystania tej technologii w wojsku, szczególnie w zakresie cyberbezpieczeństwa, autonomicznych systemów bojowych oraz wsparcia w analizie danych. Jednak pełne wykorzystanie SI w obronności wymaga dalszych inwestycji w badania, rozwój, współpracę międzynarodową i budowanie odpowiedniej infrastruktury technologicznej. Polska ma szansę

na skuteczne zastosowanie sztucznej inteligencji w wojsku, ale potrzebne są dalsze wysiłki w tych obszarach”.

Chat trafnie, na dużym poziomie ogólności, opisuje zaawansowanie Polski w implementację sztucznej inteligencji na potrzeby wojska. Wymienia konkretne obszary wykorzystania oraz potencjalnego wykorzystania tej technologii, które w dużej mierze są spójne z obszarami wskazanymi w odpowiedzi na pytanie pierwsze. Niewskazywanym wcześniej elementem, a zarazem sugestią Chatu są obszary współpracy międzynarodowej i rozwoju przemysłu obronnego. Należy uznać te wskazania jako istotne, ponieważ *de facto* są to podstawowe obszary rozwoju zdolności sił zbrojnych.

Ponadto autor zwraca uwagę, że Chat nie wspomina, że 3 marca 2025 roku kierownictwo Ministerstwa Obrony Narodowej ogłosiło powstanie Centrum Implementacji Sztucznej Inteligencji w Wojskach Obrony Cyberprzestrzeni³¹, a 14 marca tegoż roku ogłoszono powstanie kolejnej instytucji związanej z tym obszarem, tj. fabryki sztucznej inteligencji w Poznaniu³².

4. Czy możliwe jest, że wojskowe systemy autonomiczne wykorzystywane w wojsku mogą działać przeciwko wojskom własnym?

„Tak, istnieje ryzyko, że wojskowe systemy autonomiczne mogą działać przeciwko własnym wojskom, jeśli nie będą odpowiednio zaprojektowane, kontrolowane i monitorowane. Takie scenariusze, choć wciąż rzadkie, są powodem do niepokoju i są brane pod uwagę przez ekspertów w dziedzinie sztucznej inteligencji, etyki wojskowej oraz prawa międzynarodowego. Potencjalne ryzyka:

- 31 Centrum Implementacji Sztucznej Inteligencji ma za zadanie wspieranie rozwoju Sił Zbrojnych RP m.in. poprzez wykorzystanie sztucznej inteligencji do analizy informacji wywiadowczo-rozpoznawczych, działania autonomicznych systemów bojowych czy wsparcia procesu decyzyjnego. Zob. *W Wojsku Polskim powstaje Centrum Implementacji Sztucznej Inteligencji*, <https://www.gov.pl/web/obrona-narodowa/w-wojsku-polskim-powstaje-centrum-implementacji-sztucznej-inteligencji> [dostęp: 1.03.2025].
- 32 Poznańska fabryka ma wspierać innowacje w takich sektorach, jak: zdrowie, cyberbezpieczeństwo, technologie kwantowe, robotyka i zrównoważony rozwój. Zob. *W Poznaniu powstanie fabryka sztucznej inteligencji*, <https://naukawpolsce.pl/aktualnosci/news%2C107049%2Cw-poznaniu-powstanie-fabryka-sztucznej-inteligencji.html> [dostęp: 23.03.2025].

1. Błędy w algorytmach: Autonomiczne systemy wojskowe, takie jak drony czy roboty bojowe, opierają się na algorytmach, które mogą popełniać błędy w analizie sytuacji na polu walki. Błędy w rozpoznawaniu celów (np. identyfikowanie własnych jednostek jako wroga) mogą prowadzić do ataków na siły własne. Nawet małe błędy w oprogramowaniu lub błędne interpretacje danych wywiadowczych mogą skutkować tragicznymi konsekwencjami.

2. Ataki cybernetyczne: Autonomiczne systemy wojskowe są podatne na ataki cybernetyczne. Złośliwe oprogramowanie lub hakowanie tych systemów może prowadzić do ich przejęcia przez wroga, co może skutkować ich skierowaniem do ataku na własne siły. Przykładem może być przejęcie kontroli nad dronem lub robotem bojowym i wykorzystanie go przeciwko własnym oddziałom.

3. Problemy z systemami rozpoznawania: Autonomiczne systemy wojskowe często korzystają z systemów rozpoznawania obrazu (np. kamery, sensory, lidar³³) do identyfikowania celów. Jeśli te systemy nie będą wystarczająco dokładne lub jeżeli wystąpią problemy z ich kalibracją, mogą błędnie rozpoznać własne jednostki jako wroga.

4. Brak elastyczności w podejmowaniu decyzji: Autonomiczne systemy mogą działać zgodnie z zaprogramowanymi procedurami, ale w sytuacjach niestandardowych, gdzie wymagana jest ocena kontekstu, mogą nie być w stanie podjąć właściwej decyzji. Na przykład, w trudnych warunkach konfliktu, gdzie wroga jednostkę można pomylić z własną, systemy autonomiczne mogą podjąć błędne decyzje, prowadzące do ataku na jednostki przyjazne.

5. Błąd ludzki w programowaniu i kontrolowaniu systemów: Nawet jeśli systemy autonomiczne są zaprojektowane tak, by unikać takich sytuacji, błędy popełnione przez programistów, techników czy dowódców mogą wpłynąć na ich działanie. Niewłaściwa konfiguracja, nieaktualne dane rozpoznawcze lub brak odpowiedniego nadzoru mogą prowadzić do błędów, które będą skutkować atakiem na własne wojska.

33 Dane pomiarowe LIDAR (ang. Light Detection and Ranging). Zob. *Dane pomiarowe LIDAR (LIDAR)*, <https://www.geoportal.gov.pl/pl/dane/dane-pomiarowe-lidar-lidar/> [dostęp: 23.03.2025].

Rozwiązania minimalizujące ryzyko

Aby zapobiec takim sytuacjom, należy wdrożyć szereg środków ochronnych i kontrolnych:

1. Testowanie i walidacja systemów autonomicznych: Systemy autonomiczne muszą przejść skomplikowane testy w różnych warunkach, aby upewnić się, że działają zgodnie z założeniami i nie będą stanowiły zagrożenia dla sił własnych.

2. Reguły angażowania systemów autonomicznych: Wiele armii pracuje nad stworzeniem zasad użycia systemów autonomicznych, które zapewnią, że będą one używane tylko w określonych, kontrolowanych warunkach i nie podejmą działań przeciwko własnym wojskom.

3. Mechanizmy awaryjne i nadzór ludzki: Nawet w przypadku autonomicznych systemów wojskowych, powinny istnieć mechanizmy awaryjne pozwalające na przejęcie kontroli przez człowieka w sytuacjach kryzysowych. Powinna istnieć możliwość zatrzymania systemu w przypadku wykrycia nieprawidłowego działania.

4. Szkolenia i procedury dla operatorów: Operatorzy systemów autonomicznych powinni być odpowiednio przeszkoleni i świadomi ryzyka, jakie niosą ze sobą błędy w działaniu takich systemów. Muszą wiedzieć, jak reagować w przypadku wykrycia problemów.

5. Zabezpieczenia przed atakami cybernetycznymi: Zabezpieczenie systemów autonomicznych przed cyberatakami jest kluczowe. Stosowanie zaawansowanych technik szyfrowania, systemów wykrywania intruzów i regularnych aktualizacji oprogramowania może zmniejszyć ryzyko przejęcia kontroli nad takimi systemami przez wroga.

Podsumowanie: Tak, istnieje ryzyko, że wojskowe systemy autonomiczne mogą działać przeciwko własnym wojskom, jeśli nie będą odpowiednio zaprojektowane, kontrolowane i monitorowane. Jednak poprzez odpowiednią kontrolę, testowanie, zabezpieczenia i nadzór ludzki, można minimalizować to ryzyko i zapewnić bezpieczne zastosowanie technologii autonomicznych w wojsku”.

Oprócz odpowiedzi na pytanie Chat wskazał „rozwiązania minimalizujące ryzyko”, które służą ograniczeniu możliwości zwrócenia się sztucznej inteligencji przeciwko wojskom własnym. Natomiast w odpowiedzi zawartej

w pkt 4 Chat rozszerza zawartą w pytaniu percepcję „wojsk własnych”, wzbogacając wypowiedzi o element wojsk przyjaznych:

„4. [...] Na przykład, w trudnych warunkach konfliktu, gdzie wroga jednostkę można pomylić z własną, systemy autonomiczne mogą podjąć błędne decyzje, prowadzące do ataku na jednostki przyjazne”.

Jako niecelowo zagrożonych aktorów działań zbrojnych Chat wskazuje nie tylko wojska własne, lecz także wojska sprzymierzone i strony neutralne.

5. Czy implementowanie sztucznej inteligencji to dobry kierunek inwestowania znacznych środków finansowych z budżetu na obronność?

„Implementowanie sztucznej inteligencji (SI) w obronności jest zdecydowanie jednym z najważniejszych i obiecujących kierunków inwestycyjnych na przyszłość, jednak wymaga dokładnej analizy i rozważenia zarówno korzyści, jak i wyzwań związanych z takim podejściem. Z perspektywy obronności, inwestowanie znacznych środków finansowych w SI ma wiele zalet, ale także wiąże się z pewnymi ryzykami, które należy wziąć pod uwagę. Korzyści z inwestowania w SI w obronności:

1. Zwiększenie efektywności operacyjnej:

- automatyzacja i autonomizacja: Wykorzystanie autonomicznych systemów bojowych, dronów czy robotów bojowych może zredukować konieczność angażowania ludzi w niebezpieczne operacje, jednocześnie zwiększając efektywność operacyjną i precyzję,

- zbieranie i analiza danych: SI może przetwarzać ogromne ilości danych w czasie rzeczywistym, co pozwala na lepsze monitorowanie sytuacji na polu walki, identyfikowanie zagrożeń oraz przewidywanie ruchów wroga. To daje przewagę strategiczną, a także przyspiesza podejmowanie decyzji.

2. Poprawa cyberbezpieczeństwa. Ochrona przed atakami: SI może pomóc w szybszym wykrywaniu i reagowaniu na cyberzagrożenia, chroniąc systemy obronne przed cyberatakami. W kontekście nowoczesnych konfliktów, gdzie wojna w cyberprzestrzeni staje się coraz bardziej istotna, inwestycje w SI mogą zapewnić przewagę w obronie przed cyberatakami.

3. Redukcja ryzyka i strat ludzkich. Zminimalizowanie zaangażowania żołnierzy w niebezpiecznych misjach: Drony, roboty bojowe i inne autonomiczne systemy mogą wykonywać misje zwiadowcze, transportowe, a nawet bojowe, zmniejszając ryzyko dla życia żołnierzy i umożliwiając wykonanie niebezpiecznych operacji z większą precyzją.

4. Długoterminowa przewaga technologiczna. Inwestycje w SI mogą zapewnić krajowi długoterminową przewagę technologiczno-wojskową. Z perspektywy rozwoju technologii, SI jest kluczowym elementem przyszłościowych systemów obronnych i może decydować o przewadze w konflikcie.

Wyzwania i ryzyka:

1. Koszty rozwoju i wdrożenia: Rozwój i implementacja sztucznej inteligencji wiąże się z wysokimi kosztami. Oprócz samego zakupu technologii, wymaga to również inwestycji w badania, rozwój, szkolenia oraz infrastrukturę technologiczną. Utrzymanie i aktualizacja tych systemów także wiąże się z długoterminowymi wydatkami.

2. Zależność od technologii: Zbyt duża zależność od autonomicznych systemów może stwarzać ryzyko w przypadku ich awarii, cyberataków czy błędów w działaniu. Istnieje ryzyko, że w sytuacji awarii systemów sztucznej inteligencji, armia może zostać narażona na poważne straty lub utratę kontroli nad działaniami.

3. Etyka i odpowiedzialność: Autonomiczne systemy bojowe, zwłaszcza te zdolne do podejmowania decyzji o użyciu siły, rodzą poważne pytania etyczne. Kwestie odpowiedzialności za decyzje podjęte przez maszyny w przypadku ofiar czy zniszczeń są nadal niejasne, a międzynarodowe prawo humanitarne w tej kwestii nie zostało jeszcze jednoznacznie opracowane.

4. Cyberzagrożenia: Autonomiczne systemy oparte na SI mogą być podatne na cyberataki. Przejęcie kontroli nad systemami obronnymi przez nieautoryzowane podmioty może mieć katastrofalne konsekwencje. Inwestycje w zabezpieczenia są więc niezbędne, co dodatkowo podnosi koszty.

5. Złożoność i trudności integracyjne: Wdrażanie sztucznej inteligencji w strukturach wojskowych, które już posiadają swoje ustalone procedury, może być trudne. Integracja nowych systemów z istniejącymi technologiami, infrastruktura i systemami operacyjnymi może być czasochłonna i kosztowna.

Podsumowanie: Inwestowanie w sztuczną inteligencję na potrzeby obronności jest zdecydowanie obiecującym kierunkiem, który może przynieść znaczące korzyści, takie, jak: zwiększenie efektywności, precyzji działań, ochrony cybernetycznej czy zmniejszenie ryzyka dla żołnierzy. Niemniej jednak wiąże się to także z wysokimi kosztami, ryzykami związanymi z bezpieczeństwem i etyką, a także z potrzebą zapewnienia odpowiednich mechanizmów kontroli i nadzoru. Decyzja o takim inwestowaniu powinna być dokładnie rozważona

i oparta na długoterminowej strategii obronnej, z uwzględnieniem zarówno korzyści, jak i ryzyk, jakie mogą wyniknąć z używania sztucznej inteligencji w wojsku. Inwestowanie w SI w obronności ma sens, ale musi być częścią kompleksowego planu modernizacji armii, uwzględniającego także inne aspekty technologiczne, edukacyjne i bezpieczeństwa”.

Chat wskazuje, że zasadne jest inwestowanie w implementację sztucznej inteligencji w obszarze obronności, nie wskazuje jednak jednoznacznie inwestowania „znaczących środków finansowych”. Warto zauważyć, że Chat wspomina o mechanizmie kontroli i nadzoru, które muszą być zapewnione przy wzbogacaniu obszaru obronności o możliwości oferowane przez sztuczną inteligencję. Wskazuje również, że jej wdrożenie powinno być sprzężone z modernizacją techniczną armii z uwzględnieniem innych ważnych aspektów dotyczących funkcjonowania wojska. Ponadto podkreśla zasadność funkcjonowania dotychczasowych systemów, nie dewaluując ich przydatności. Jednocześnie zaznacza potrzebę integracji i budowania interoperacyjności. Chat prezentuje podejście komplementarne, w którym wskazuje różnorodność czynników, jakie należy uwzględnić w ocenie wykonania zadania przez system oparty na sztucznej inteligencji.

Zakończenie

Analiza potencjału wdrożenia sztucznej inteligencji na potrzeby sił zbrojnych pokazuje duże możliwości, jakie daje jej zastosowanie. Wdrożenie tej nowoczesnej technologii tworzy nowe zdolności, które w dużym stopniu mogą usprawnić dotychczas wykorzystywane mechanizmy. Użycie sztucznej inteligencji na potrzeby armii należy rozpatrywać nie tylko z perspektywy misji bojowych i wsparcia, lecz także pod względem prowadzenia działań kinetycznych i niekinetycznych, co może w znacznym stopniu wpływać na operacje w wojnie hybrydowej. Rozwój zastosowania sztucznej inteligencji zmierza w kierunku jej całkowitej autonomii, która pozwoliłaby na samodzielne wskazywanie zadań i dobieranie środków do ich wykonania. Autor zaproponował „skalę autonomii sztucznej inteligencji” uwzględniającą poziom zaangażowania człowieka i systemu w decyzyjność i sprawczość.

Wydaje się, że państwa nie mają innej drogi jak inwestowanie w rozwój sztucznej inteligencji i jej wdrożenie na potrzeby wojska, gdyż pozostanie w tyle tego wyścigu zbrojeń sztucznej inteligencji nie daje szans na przetrwanie.

Należy zaznaczyć, że sztuczna inteligencja, z którą autor przeprowadził wywiad, trafnie rozpoznaje szanse i zagrożenia związane z wykorzystaniem jej potencjału w obszarze wojskowości. Treści generowane przez Chat GPT względem wykorzystania sztucznej inteligencji na potrzeby armii pokrywały się z analizą autora. Pomimo pojedynczych nieścisłości, należy uznać, że udzielone odpowiedzi mogą być cennym narzędziem wspomagającym świadomość sytuacyjną. Zdaniem autora zasadne jest, aby podobne narzędzia z zamkniętym systemem obiegu informacji (implikowanych pytań i generowanych treści) były powszechnie wykorzystywane w wojsku.

Komisja Europejska wskazuje, że wyzwaniem jest rozwój systemów opartych na sztucznej inteligencji, które będą wolne od wad i będzie można im ufać, gdyż „kluczowym wymogiem dla osiągnięcia godnych zaufania³⁴ systemów sztucznej inteligencji jest ich wiarygodność (zdolność do dostarczania usług, którym można zasadnie zaufać) i odporność (wiarygodność w obliczu zmian). Rzetelność techniczna wymaga, aby systemy sztucznej inteligencji były rozwijane z zapobiegawczym podejściem do ryzyka, żeby zachowywały się niezawodnie i zgodnie z przeznaczeniem, minimalizując niezamierzone i nieoczekiwane szkody, a także zapobiegając im, gdy jest to możliwe”³⁵. Jedynym z bardziej oczywistych rozwiązań wydaje się skuteczne prawodawstwo, które ograniczałoby rozwój tej technologii do bezpiecznego i akceptowalnego poziomu lub zakazywałoby rozwoju niektórych obszarów tej technologii, np. tworzenia całkowicie samodzielnych systemów bojowych. Komisja Europejska zatwierdziła rezolucję, w której wyrażono zaniepokojenie możliwymi negatywnymi konsekwencjami i wpływem autonomicznych systemów uzbrojenia na bezpieczeństwo globalne oraz stabilność regionalną i międzynarodową, w tym obawy o ryzyko pojawienia się wyścigu zbrojeń, obniżenia progu konfliktu i proliferacji, także w odniesieniu do podmiotów niepaństwowych³⁶. Jednocześnie jednym z podstawowych działań ograniczających potencjalną

34 „Godna zaufania sztuczna inteligencja” odnosi się do systemów sztucznej inteligencji, które są możliwe do wyjaśnienia, uczciwe, interpretowalne, solidne, przejrzyste, bezpieczne i pewne. Zob. *What is trustworthy AI?*, <https://www.ibm.com/think/topics/trustworthy-ai> [dostęp: 23.03.2025].

35 *The Assessment List for Trustworthy...*

36 Zgromadzenie Ogólne ONZ, *Siedemdziesiąta ósma sesja, 28. Spotkanie, GA/DIS/3731, 2023*, <https://docs.un.org/en/A/C.1/78/L.56> [dostęp: 23.02.2025].

agresywną autonomię sztucznej inteligencji i przestrzeni do jej wrogiego wykorzystania może być nadanie klauzuli niejawności grupom informacji dotyczących bezpieczeństwa. W związku z tym, że technologie oparte na sztucznej inteligencji potrzebują zasilania danymi, co stanowi o ich funkcjonalności, można ją ograniczyć poprzez hamowanie dostępu do treści wrażliwych i istotnych z punktu widzenia bezpieczeństwa państwa.

Żeby swobodnie posługiwać się sztuczną inteligencją bez obaw o ryzyko niepożądanego działania, autor definiuje trzy zasadnicze obszary, które należy opanować.

Według autora rozwój sztucznej inteligencji na potrzeby armii osiągnie poziom odstraszenia i potencjalnego czynnika rażenia porównywalnego ze skutkami z efektem nuklearnym. Powyższe należy rozumieć w kategorii możliwości oddziaływania na przeciwnika, niszczenia jego potencjału i ochrony potencjału własnego. Zanim aktorzy państwowi zrozumieją, że wyścig zbrojenia sztucznej inteligencji w rezultacie doprowadzi do tragicznych konsekwencji i zanim prawo skutecznie pozwoli usankcjonować wykorzystanie sztucznej inteligencji na potrzeby walki, część podmiotów będzie dysponowała potencjałem zdolnym do masowego autonomicznego rażenia.

Konieczne jest podjęcie otwartego i eksperckiego dyskursu na arenie międzynarodowej dotyczącego wdrożenia potencjału sztucznej inteligencji na potrzeby wojska w sposób, który zapewni jej bezawaryjność, odporność na manipulację i rzeczywisty nadzór człowieka nad jej działaniem.

Bibliografia

- Allen G., Chan T., *Artificial Intelligence and National Security U.S. Intelligence Advanced Research Projects Activity (IARPA)*, Harvard Cennedy School – Belfer Center for Science and International Affairs, 2017 <https://www.belfercenter.org/sites/default/files/2024-10/Artificial%20Intelligence%20and%20National%20Security.pdf> [dostęp: 28.02.2025].
- Artificial Intelligence in Electronic Warfare*, <https://www.te.com/en/industries/defense-military/insights/ai-in-warfare-and-military-applications.html> [dostęp: 3.02.2025].
- Assessment List For Trustworthy Artificial Intelligence (ALTAI)*, Glossary, Independent High-Level Expert Group On Artificial Intelligence, Bruksela, 2020, <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment> [dostęp: 3.02.2025].

- Autonomia*, <https://mfiles.pl/pl/index.php/Autonomia> [dostęp: 20.03.2025].
- Autonomia*, <https://sjp.pwn.pl/sjp/autonomia;2551312.html> [dostęp: 20.03.2025].
- Autonomia – co to jest? Definicja, synonimy, przykłady użycia*, <https://polszczyzna.pl/autonomia-co-to-jest-definicja-synonimy-przyklady-uzycia> [dostęp: 20.03.2025].
- Banafa A., *Artificial Intelligence (AI) in Modern Military Applications*, <https://www.linkedin.com/pulse/artificial-intelligence-ai-modern-military-prof-ahmed-banafa-e9sxc> [dostęp: 23.01.2025].
- Bezzałogowy pojazd bojowy nowej generacji ATLAS CCV*, 2024, <https://tacgear.pl/2024/09/bezzałogowy-pojazd-bojowy-nowej-generacji-atlas-ccv> [dostęp: 23.02.2025].
- Chat GPT: What is it?*, <https://uca.edu/cetal/chat-gpt> [dostęp: 13.11.2024].
- Comparative Analysis between OpenAI ChatGPT, Google Bard, Anthropic Claude, and Google Gemini*, <https://medium.com/@DigitalQuill.ai/comparative-analysis-between-chatgpt-bard-claude-and-gemini-ai-llms-30b7a4488c5d> [dostęp: 13.11.2024].
- Easley M., *Army implements generative AI platform to cArmy cloud environment*, 2024 <https://defensescoop.com/2024/09/10/army-generative-ai-capability-carmy-cloud> [dostęp: 2.02.2025].
- Gergelewicz T., *Bipolarity of Artificial Intelligence – Chances and Threats*, „Ius et Securitas” 2024, nr 2.
- Gergelewicz T., *Countering Disinformation Concept for building social resilience in times of cognitive warfare*, „Przegląd Nauk o Obronności. Defence Science Review” 2024, nr 20.
- Kaczmarek K., Karpiuk M., Soler U., *The Potential Use of Artificial Intelligence in Crisis Management*, „Sicurezza, Terrorismo E Societa” 2024, t. 20, nr 2.
- LS3: Legged Squad Support System*, <https://www.darpa.mil/research/programs/legged-squad-support-system> [dostęp: 3.03.2025].
- Nowacka A., *Zastosowanie neurofeedbacku w optymalizacji wydolności psychofizycznej żołnierzy*, <https://www.ezaf.pl/wpisy/zastosowanie-neurofeedbacku-w-optymalizacji-wydolnoscii-psychofizycznej-zolnierzy,1842> [dostęp: 7.02.2025].
- Pojazdy autonomiczne/bezzałogowe*, <https://przemyslprzyszlosci.gov.pl/technologie/cyfrowe/robotyzacja/pojazdy-autonomiczne-bezzałogowe> [dostęp: 3.03.2025].
- Rejmaniak R., *Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego*, „Rocznik Nauk Prawnych” 2021, t. 31, nr 3.
- Testy LS3*, <https://www.youtube.com/watch?v=Ilbtwn8jwwc&t=62s> [dostęp: 3.03.2025].
- Uczenie sztucznej inteligencji, jak ma się sama uczyć*, Europejska Rada ds. Badań Naukowych, <https://cordis.europa.eu/article/id/435616-teaching-ai-to-teach-itself/pl> [dostęp: 10.03.2025].
- Weissman R., Wooten S., *A.I. Joe: The Dangers of Artificial Intelligence and the U.S. Military*, 2024, <https://www.citizen.org/article/ai-joe-report/> [dostęp: 13.01.2025].
- What is LLM (Large Language Model)?*, <https://aws.amazon.com/what-is/large-language-model/> [dostęp: 20.12.2024].
- Zequeira M., *U.S. Army, Artificial Intelligence as a Combat Multiplier, Using AI to Unburden Army Staffs*, Military Review Online Exclusive, 2024, <https://www.>

armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/AI-Combat-Multiplier [dostęp: 18.01.2025].

The use of artificial intelligence potential in the armed forces – interview with Chat GPT

Abstract

The implementation of artificial intelligence-based systems into the armed forces creates new capabilities that significantly reduce the burden of previously used mechanisms. The opportunities for the armed forces are indicated, which result from the use of artificial intelligence. At the same time, the challenges posed by the use of this advanced technology are highlighted. The aim of the article is to present the potential of implementing artificial intelligence for military purposes and compare it with the content generated by Chat GPT during the interview, in response to questions about various areas of artificial intelligence absorption for military purposes.

In addition, the author proposed a scale of artificial intelligence autonomy and defined three fundamental areas, which have to be mastered in order to freely use artificial intelligence without worrying about the risk of undesirable action.

The analytical method was used to distinguish areas of application of artificial intelligence for the needs of the army and indicate potential directions of its implementation. Synthesis was employed to propose a scale of system autonomy in relation to human decisions. Expert interview method was applied to examine how artificial intelligence assesses its own potential for implementation for the needs of the army.

The analysis conducted by the author, as well as the indications of the artificial intelligence itself, point many benefits of implementing artificial intelligence into the armed forces. At the same time, one has to be aware of the many threats associated with the vulnerabilities this solution currently creates.

In conclusions it is indicated that the content generated by artificial intelligence during the interview, regarding its own use for the army, is advanced; and Chat GPT can be a valuable information tool, as one of the important sources in building situational awareness.

Keywords

artificial intelligence, armed forces, security, autonomous systems, Chat GPT