Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.34567/cal/215902

# Opportunities and threats of using artificial intelligence in multi-domain operations

# Szanse i zagrożenia wykorzystania sztucznej inteligencji w operacjach wielodomenowych

**Andrzej BOGDAŃSKI**
Akademia Sztuki Wojennej
ORCID: 0000-0002-3443-0741
E-mail: a.bogdański@akademia.mil.pl

## Abstract

In this article, the Author presents selected cybersecurity aspects related to the implementation of artificial intelligence (AI) in IT systems used in multi-domain operations. The main goal of the research was to analyze the determinants implying opportunities and threats related to the implementation and use of AI in the context of maintaining an appropriate level of security of processed information. The research goal of the article was to identify factors influencing the secure implementation of machine learning-based tools. The author formulated the main research problem as the following question: How should the implementation and operation of machine learning-based tools in the Polish Armed Forces be organized while ensuring the security of processed information?

## *Keywords*

*cybersecurity, multidomain operations, artificial intelligence*

## Streszczenie

W artykule Autor przedstawił wybrane aspekty dotyczące cyberbezpieczeństwa w zakresie implementacji sztucznej inteligencji (Artificial Intelligence, AI) w systemach teleinformatycznych wykorzystywanych w operacjach wielodomenowych. Celem głównym badań była analiza determinantów implikujących szanse i zagrożenia związane z wdrożeniem i wykorzystaniem sztucznej inteligencji w kontekście utrzymania odpowiedniego poziomu bezpieczeństwa przetwarzanych informacji. Celem poznawczym artykułu było wskazanie czynników wpływających na bezpieczną implementację narzędzi opartych o uczenie maszynowe. Główny problem badawczy autor sformułował w postaci pytania: W jaki sposób zorganizować wdrożenie i eksploatację w Siłach Zbrojnych Rzeczypospolitej Polskiej (SZRP) narzędzi opartych o uczenie maszynowe, zapewniając jednocześnie bezpieczeństwo przetwarzanych informacji?

***Słowa kluczowe***
*cyberbezpieczeństwo, operacje wielodomenowe, sztuczna inteligencja*

## Wstęp

Operacje wielodomenowe (Multidomain Operations, MDO) to obecnie jeden z kluczowych konceptów we współczesnej strategii wojskowej[1]. Istotą przedmiotowych operacji jest skoordynowanie, zintegrowanie i wykorzystanie zdolności sił zbrojnych państwa lub koalicji w celu uzyskania przewagi operacyjnej w różnych domenach. Jednocześnie należy podkreślić, że operacje w cyberprzestrzeni[2] odgrywają w MDO coraz większą rolę. Do niedawna mówiono o systemach klasy C4ISR. To akronim od Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance. Dość szybko pojawiło się piąte „C" oznaczają cyberprzestrzeń, a obecnie mowa jest o systemach klasy C6ISR które mają zawierać dodatkowo systemy walki, także w cyberprzestrzeni. Powodem determinującym pojawienie się domeny cyberprzestrzeni, był fakt powszechnej cyfryzacji życia społecznego i gospodarczego co determinuje rosnącą zależność państw od infrastruktury teleinformatycznej co z kolei implikuje pojawienie się nowych zagrożeń, a mianowicie cyberataków. W związku z agresywną polityką Rosji, a także niestabilną sytuacją w krajach Bliskiego Wschodu na 27 szczycie NATO w walijskim Newport zorganizowanym w dniach 4-5 września 2014 roku, podjęto decyzję o uruchomieniu „czterech sojuszniczych funduszy powierniczych dla Ukrainy o wartości 15 mln euro poświęconych: (…) m.in., wsparciu w zakresie dowodzenia, kontroli i łączności oraz wsparciu w budowie systemu obrony cybernetycznej"[3]. Cyberbezpieczeństwo[4] to także jeden z głównych celów określonych przez Szefów Państw i Rządów w deklaracji końcowej kolejnego szczytu NATO, który odbył się w Warszawie w dniach 8-9 lipca 2016 roku[5]. To właśnie na nim cyberprzestrzeń uznano za kolejną domenę walki. W związku z tym faktem na stałe weszło do użycia pojęcie C5ISR, gdzie kolejne „C" oznacza cyber[6] [według autora na tamtą chwilę walki w rozumieniu cyberobrony].

**Rys. 1.** Koncepcja C5ISR

[1] Operacje wielodomenowe – doświadczenia i persepktywy https://www.wojsko-polskie.pl/aszwoj/articles/aktualnosci-2/operacje-wielodomenowe-doswiadczenia-i-perspektywy [dostęp: 05.11.2025].
[2] Operacje w cyberprzestrzeni DD 3.20, 0203. Cyberprzestrzeń jako domena operacyjna, MON CDiSSZ szkol. 977/2020, s. 12.
[3] S. Koziej, P. Pietrzak, Szczyt NATO w Newport, "Bezpieczeństwo Narodowe" Biuro Bezpieczeństwa Narodowego" 2014, nr 31, s. 27.
[4] Cyberbezpieczeństwo - odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy definicja na podstawie Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560, t. j. Dz. U. z 2020 r. poz. 1369, s. 2).
[5] A. Bogdański, Cyberbezpieczeństwo uczelni wojskowej: aspekt prawny, [w:] M. Marczyk, M. Stolarz, B. Terebiński (red.), Działania hybrydowe a bezpieczeństwo sieci i systemów teleinformatycznych w SZ RP: wybrane aspekty, Warszawa 2021, s. 509-527.
[6] https://www.army.mil/article/157832/devcom_c5isr_center [dostęp: 05.11.2025].


**Źródło:** https://www.redcom.com/what-is-c5isr [dostęp: 05.11.2025].

Natomiast systemy klasy C6ISR mają zawierać dodatkowo systemy walki (Combat Systems)[7][8], także w cyberprzestrzeni[9] w rozumieniu działań proaktywnych. Systemy tej klasy umożliwiać mają zbieranie danych wywiadowczych, ciągłe monitorowanie przeciwnika w tym analizę przemieszczeń. Wykorzystanie sztucznej inteligencji w tych systemach umożliwiać ma generowanie przewagi informacyjnej oraz wspiera optymalizację procesów decyzyjnych na wszystkich szczeblach dowodzenia.

**Rys. 2** Koncepcja C6ISR


**Źródło:** https://peachcdus.com/index.php/services/c6isrew [dostęp: 05.11.2025].

Sztuczna inteligencja stanowi jeden z najbardziej dynamicznie rozwijających się obszarów współczesnych technologii wojskowych. Jej implementacja w siłach zbrojnych otwiera szerokie spektrum możliwości od

[7] M. Rahman Masum, C6ISR Training Workshop: Command, Control, Communications, Computers, Cyber-Defense, and Combat Systems, DOI: 10.13140/RG.2.2.24085.91368, s 2.
[8] https://peachcdus.com/index.php/services/c6isrew [dostęp: 05.11.2025].
[9] https://www.trentonsystems.com/en-us/resource-hub/blog/c2-c4isr-c5isr-c6isr-differences [dostęp: 05.11.2025].

usprawnienia procesów zarządzania i dowodzenia, poprzez automatyzację działań bojowych oraz logistycznych, aż po znaczące zwiększenie efektywności w zakresie rozpoznania, obrony cybernetycznej i bezpieczeństwa informacyjnego.

W kontekście operacji, zwłaszcza prowadzonych w cyberprzestrzeni, zastosowanie sztucznej inteligencji oferuje liczne korzyści dla systemów opartych na zaawansowanej infrastrukturze cyfrowej oraz rozwiązań wspierających działania na polu walki. Lawinowy przyrost danych determinował rozwój systemów oraz implementację nowych technologii. Zdolność do dowodzenia ma tym większą efektywność, im pewniej i szybciej będzie realizowana wymiana informacji. Zadaniem systemu łączności powinno być zapewnienie przekazywania informacji w sposób wiernej, skryty i terminowy[10].

Jednocześnie należy podkreślić, że wraz z dynamicznym wzrostem potencjału tej technologii, rośnie również skala i złożoność zagrożeń z nią związanych, zarówno w wymiarze technologicznym, jak i operacyjnym, co wymaga stałego monitorowania oraz rozwoju mechanizmów zabezpieczających. Ponadto ze względu na wysokie ryzyko technologiczne, działania te powinny być realizowane w ramach projektów badawczo-rozwojowych w obszarze bezpieczeństwa i obronności, z naciskiem na szybkie projektowanie, testowanie i wdrażanie rozwiązań.

Celem głównym badań była analiza determinantów implikujących szanse i zagrożenia związane z wdrożeniem i wykorzystaniem sztucznej inteligencji w kontekście utrzymania odpowiedniego poziomu bezpieczeństwa przetwarzanych informacji. Określenie celu głównego badań pozwolił autorowi na zdefiniowanie szczegółowych celów badań.

Jako cel praktyczny[11] autor przyjął scharakteryzowanie sposobu działania oraz metodę wdrożenia mechanizmów uczenia maszynowego.

Celem poznawczym[12] było wskazanie czynników wpływających na bezpieczną implementację narzędzi opartych o uczenie maszynowe.

Główny problem badawczy autor sformułował w postaci pytania: W jaki sposób zorganizować wdrożenie i eksploatację w SZRP narzędzi opartych o uczenie maszynowe, zapewniając jednocześnie bezpieczeństwo przetwarzanych danych?

Problem ten koncentruje się na zrównoważeniu dwóch kluczowych aspektów: innowacyjności technologicznej, a mianowicie na implementacji narzędzi wykorzystujących uczenie maszynowe w środowisku zautomatyzowanych systemów wsparcia dowodzenia, oraz bezpieczeństwa informacji, czyli konieczności ochrony ich przed nieautoryzowanym dostępem, modyfikacją lub utratą, zgodnie z obowiązującymi standardami. W oparciu o główny problem badawczy autor analizował aspekt bezpiecznej eksploatacji, który przedstawił w postaci pytania: W jaki sposób zapewnić bezpieczeństwo wdrażanych rozwiązań AI?

Autor założył następującą hipotezę badawczą: Siły Zbrojne są w stanie dokonać skutecznego wdrożenia oraz bezpiecznie eksploatować narzędzia oparte na uczeniu maszynowym w taki sposób, aby zapewnić wysoki poziom bezpieczeństwa przetwarzanych danych i minimalizować ryzyko naruszeń poufności, integralności oraz dostępności informacji. Według autora możliwe jest uzupełnienie eksploatowanych instancji systemów teleinformatycznych

[10] B. Terebiński, Teleinformatyka wojskowa, Warszawa, 2022, s. 63.
[11] M. Pelc, Elementy metodologii badań naukowych, Warszawa 2012, s. 15.
[12] Ibidem, s. 16.

eksploatowanych w SZRP o usługi oparte na uczeniu maszynowym. Ponadto możliwe jest zapewnienie bezpieczeństwa dostarczanych i przetwarzanych informacji niejawnych w oparciu o dedykowane urządzenia szyfrujące.

Przedstawione w artykule wyniki badań opierają się na wieloletnich obserwacjach oraz wywiadach przeprowadzonych z ekspertami. Materiał empiryczny został zgromadzony w trakcie największych ćwiczeń z udziałem wojskw latach 2015–2018. Proces obserwacji okazał się szczególnie przydatny w ocenie stopnia wykorzystania usług teleinformatycznych oraz w analizie potencjału wsparcia usług funkcjonalnych z zastosowaniem metod uczenia maszynowego. Zrealizowane obserwacje umożliwiły pozyskanie wartościowego materiału badawczego, stanowiącego podstawę dalszych analiz w ramach prowadzonych ćwiczeń pod kryptonimem: Dragon-15, Anakonda-16, Dragon-17, Anakonda-18. Natomiast wywiady z ekspertami autor przeprowadził w ramach ćwiczeń studyjnych organizowanych przez Akademię Sztuki Wojennej w latach 2022-2025. Mowa o ćwiczeniach pod kryptonimem: Brama Mazwowsza-22, Twierdza-23, Świder-23, Brama-23, Twierdza-24, Ryglowy Świder-24/II, Ryglowy Świder- 25/II.

Autor posługiwał się wywiadem niestandaryzowanym[13], zadającym jedno lub kilka pytań o charakterze niestrukturalnym, formułowanych spontanicznie, w zależności od przebiegu sytuacji badawczej. W swoich badaniach autor posługiwał się wywiadem niestandaryzowanym, swobodnym, który przyjmował formę luźnej rozmowy na określony temat. Dysponował ogólnym planem zagadnień oraz zestawem pytań, które modyfikował w zależności od przebiegu rozmowy i uzyskiwanych odpowiedzi. Takie podejście umożliwiło pogłębione poznanie opinii i doświadczeń respondentów oraz elastyczne dostosowanie kierunku wywiadu do kontekstu badanej sytuacji.

W trakcie badań autor wykorzystał wywiad narracyjny[14]. Metoda ta nie zakłada formułowania wstępnych hipotez, aby nie ukierunkowywać rozmowy i zachować jej naturalny charakter. Zastosowana tzw. zasada otwartości, polegała na tym, że to respondenci w dużej mierze określali ostateczne ramy przedmiotu badania. Autor dysponował jedynie listą zagadnień będących przedmiotem zainteresowania, natomiast przebieg rozmowy wynikał z narracji badanych, którzy opowiadali o swoich doświadczeniach zamiast odpowiadać na konkretne pytania.

W ramach badań dokonano również analizy dostępnej dokumentacji technicznej. Autor przeprowadził porównanie dokumentów planistycznych z wynikami uzyskanymi w toku obserwacji, co umożliwiło weryfikację zgodności założeń teoretycznych z praktycznym „przebiegiem analizowanych procesów.

## Zdolności SZRP w zakresie wdrożenia usług teleinformatycznych

Zdolności SZRP w przedmiotowym zakresie autor badał w oparciu o działania wdrożeniowe realizowane przez żołnierzy Centrum Wsparcia Systemów Dowodzenia Dowództwa Rodzajów Sił Zbrojnych[15]. Autor zwrócił

[13] Por. J. Lutyński, Metody badań społecznych. Wybrane zagadnienia. Analiza procesu otrzymywania informacji w badaniach z zastosowaniem wywiadu kwestionariuszowego, Łódź 2000, s.152-207.

[14] Zob. M. Prawda, Biograficzne odtwarzanie rzeczywistości, „Przegląd Socjologiczny” 1989, nr 4, s. 88-89.

[15] Zob. https://cwsdsz.wp.mil.pl, [dostęp: 05.11.2025].

uwagę, że resort planuje inwestycje w badania i rozwój przełomowych technologii sztucznej inteligencji, ukierunkowanych na budowanie długoterminowej przewagi operacyjnej. Jak wynika z badań, ze względu na wysoki poziom ryzyka technologicznego, działania te powinny realizowane w sposób scentralizowany, w ramach projektów badawczo-rozwojowych z zakresu bezpieczeństwa i obronności. Szczególny nacisk należy położyć na efektywne i skuteczne projektowanie, testowanie oraz wdrażanie innowacyjnych rozwiązań technologicznych. Według autora, bezpieczna eksploatacja usług AI jest możliwa w ramach istniejących instancji systemu teleinformatycznego Polish Mission Network, bazującego na idei Federated Mission Networking[16].

W oparciu o badania dotyczące wdrożeń usług podstawowych i dedykowanych realizowane w latach 2015-2018, przygotowanie do wdrożenia rozwiązań opartych na AI wymagać będzie zapewnienia odpowiedniego poziomu wiedzy teoretycznej, umiejętności praktycznych oraz wysokich kompetencji informatycznych żołnierzy i pracowników resortu obrony narodowej. Ponadto wdrożenie rozwiązań opartych na AI wymagać będzie modernizacji infrastruktury teleinformatycznej. Kluczowe może okazać się także zapewnienie dostępu do wiarygodnych i zweryfikowanych danych. Konieczne będzie również przeorganizowanie struktur organizacyjnych SZRP oraz dostosowanie obowiązujących przepisów prawnych i procedur operacyjnych. Wdrożenie sztucznej inteligencji w skali umożliwiającej jej szerokie zastosowanie opierać się powinno na zaufania do tej technologii, wspieraniu innowacyjności, rozwijaniu nowych koncepcji oraz doskonaleniu zdolności operacyjnych na potrzeby sił zbrojnych. Efektywne wdrożenie sztucznej inteligencji w skali umożliwiającej jej szerokie zastosowanie wymagać będzie intensywnego wspierania innowacyjności, rozwijania nowatorskich koncepcji oraz systematycznego doskonalenia zdolności operacyjnych sił zbrojnych. Istotnym elementem może okazać się nawiązywanie współpracy z kadrą naukową uczelni wojskowych: Akademią Sztuki Wojennej, Wojskową Akademią Techniczną, Akademią Wojsk Lądowych, Lotniczą Akademią Wojskową, czy Akademią Marynarki Wojennej oraz innymi placówkami naukowymi podlegającymi ministerstwu.

## Zagrożenia związane z big data

W obszarze ochrony zasobów autor przewiduje zabezpieczenie silników uczenia maszynowego w zakresie przeciwdziałania niekontrolowanemu rozprzestrzenianiu się niewiarygodnych wyników, a mianowicie monitorowanie i kontrolę „halucynacji" sztucznej inteligencji. W tym miejscu sięgnijmy do historii. Określenie big data w języku naukowym funkcjonuje od około lat dziewięćdziesiątych, a za jego twórcę uważa się Johna Macheya. Odnosi się ono do dużych zbiorów danych, których gromadzenie, przetwarzanie i analizowanie w sposób tradycyjny generuje wiele trudności. Zbiór ten poza dużym wolumenem powinien charakteryzować się różnorodnością, złożonością i zmiennością wynikającą z aktualizacji danych, a dane te powinny być dostarczane w sposób strumieniowy w czasie rzeczywistym[17]. Jak zauważył Dawid Orłowski, z biegiem

[16] Zob. A. Bogdański, Federated Mission Networking w ujęciu narodowych dokumentów doktrynalnych: aspekt bezpieczeństwa teleinformatycznego, [w:] M. Marczyk, M. Stolarz, B. Terebiński (red.), Bezpieczeństwo działań w cyberprzestrzeni: wybrane aspekty, t. 2, Techniczne aspekty cyberprzestrzeni, Warszawa 2022, s. 49-67.

[17] D. Orłowski, Wybrane aspekty zastosowania big data 2 w zarządzaniu zasobami ludzkimi w organizacji, [w:] R. Wolniak (red.), Management and Quality, Katowice 2022, s. 252, cyt. za A.

czasu, w wyniku pracy na big data uszczegółowiono jego kolejne właściwości. Przypisano cechę wiarygodności, która jest możliwa do zapewnienia poprzez odpowiednio dobraną weryfikację oraz świadomość pracy na niepewnych informacjach w przypadku źródeł internetowych (cechę tą przypisała firma IBM w 2015 r.). Ponadto dostrzeżono wymierną wartość płynącą z operacji gromadzenia i przetwarzania danych. Zauważono również zmienne tempo napływu i jakości danych, które wpływają na różne możliwości analityczne. Wykazano, że występuje zróżnicowany stopień poprawności i wzajemnego dopasowania danych. Określono konieczność zapewnienia bezpieczeństwa danych i konieczność ochrony już zgromadzonych z uwagi na występowanie danych wrażliwych lub danych stanowiących tajemnicę funkcjonowania organizacji. Z uwagi na wolumen danych cechujących się ulotnością, która dotyczy zasad archiwizowania i usuwania ich po określonym czasie[18].

Jak pokazują badania dotyczące wdrożenia usług podstawowych i dedykowanych, wdrożenie wymagać będzie przeprowadzenia licznych zmian organizacyjnych i technologicznych oraz dostosowania zasad funkcjonowania resortu obrony narodowej. Konieczne i kluczowe będą również inwestycje w redundantne systemy zasilania w energię elektryczną potrzebną do „nakarmienia" procesorów AI, a także w infrastrukturę teleinformatyczną, umożliwiająca przetwarzanie i przesyłanie ogromnych ilości danych.

## Szanse uczenie maszynowe wspierające działania bojowe

Pojęcie „uczenie maszynowe" autor przyjmuje jako część nauki o algorytmach komputerowych, które poprawiają się automatycznie wraz z doświadczeniem[19]. Istotą uczenia maszynowego jest samodzielne uczenie się na podstawie danych i doświadczenia, bez konieczności ręcznego programowania każdej reguły. Systemy te rozpoznają wzorce, dostosowują swoje działanie i podejmują decyzje, co pozwala na tworzenie inteligentnych aplikacji np. do rozpoznawania obrazów, mowy, czy systemów rekomendacji. Usługi oparte na sztucznej inteligencji mogą w przyszłości odgrywać kluczową rolę w działaniach bojowych na poziomie strategicznym, operacyjnym i taktycznym. Zastosowanie sztucznej inteligencji w SZRP może stanowić istotny element transformacji technologicznej Wojska Polskiego, umożliwiający zwiększenie efektywności działań operacyjnych, optymalizację procesów decyzyjnych oraz podniesienie poziomu bezpieczeństwa. Implementacja systemów sztucznej inteligencji obejmuje szereg strategicznych obszarów o fundamentalnym znaczeniu dla prowadzenia działań militarnych, a także dla efektywnego zarządzania i dowodzenia dostępnymi siłami oraz środkami.

Mechanizmy sztucznej inteligencji, dzięki zdolności szybkiego przetwarzania obszernego zasobu danych, mogą zwiększać świadomość sytuacyjną oraz usprawniać proces podejmowania decyzji na poziomie strategicznym, operacyjnym i taktycznym. Kluczową rolę odgrywa analiza danych wywiadowczych i rozpoznawczych umożliwiająca identyfikację wzorców oraz prognozowanie działań przeciwnika. Systemy oparte na algorytmach sztucznej inteligencji umożliwiają integrację i syntetyzowanie informacji pochodzących

Bahga, V. Madisetti, Big Data Science & Analytics: A Hands-On Approach, http://14.99.188.242:8080/ jspui/handle/123456789/12578, [dostęp: 28.10.2025].

[18] Ibidem.

[19] T. Mihchell, Machine Learning, Science, Engineering, Math 1997, s. 3, https://www.cs.cmu.edu /~tom/files/ MachineLearningTomMitchell.pdf, [dostęp: 28.10.2025].

z różnych źródeł, co przyspiesza ocenę sytuacji operacyjnej i wspiera planowanie działań bojowych

W obszarze bezpieczeństwa cybernetycznego systemy obrony cyberprzestrzeni wspierane przez sztuczną inteligencję odgrywają obecnie kluczową rolę w wykrywaniu i neutralizowaniu zagrożeń. Algorytmy oparte na sztucznej inteligencji potrafią w czasie rzeczywistym identyfikować podatności infrastruktury wojskowej, przeciwdziałać atakom oraz zwiększać odporność systemów informacyjnych na działania przeciwnika. Istotnym kierunkiem rozwoju zastosowań sztucznej inteligencji w siłach zbrojnych jest również tworzenie autonomicznych systemów bojowych, zdolnych do samodzielnego działania lub wspierania personelu wojskowego poprzez dostarczanie precyzyjnych analiz sytuacyjnych. Zaawansowane algorytmy umożliwiają realizację misji rozpoznawczych oraz prowadzenie operacji ofensywnych i defensywnych przy jednoczesnym ograniczeniu ryzyka dla żołnierzy. Sztuczna inteligencja może w istotny sposób usprawnić zarządzanie logistyką wojskową poprzez optymalizację wykorzystania zasobów, planowanie tras transportowych oraz prognozowanie potrzeb zaopatrzeniowych. Automatyzacja tych procesów przyczynia się do zwiększenia efektywności operacyjnej i umożliwia elastyczne reagowanie na dynamicznie zmieniające się warunki pola walki.

## Wsparcie systemu kształcenia i doskonalenia żołnierzy

Kształcenie i doskonalenie żołnierzy wykorzystujące sztuczną inteligencję odgrywają kluczową rolę w przygotowaniu żołnierzy do rzeczywistych działań bojowych. Zaawansowane systemy symulacyjne pozwalają na realistyczne odwzorowanie scenariuszy operacyjnych, co sprzyja testowaniu taktyki oraz doskonaleniu umiejętności personelu wojskowego w kontrolowanym środowisku. Symulacja wspierana AI generuje efekt synergii.

W procesie doskonalenia kompetencji żołnierzy szczególne znaczenie ma analiza danych szkoleniowych, która umożliwia projektowanie indywidualnych ścieżek rozwoju oraz podnoszenie jakości procesu kształcenia. Algorytmy sztucznej inteligencji pozwalają na rekomendowanie odpowiednich kursów i dostosowywanie materiałów dydaktycznych do poziomu wiedzy oraz postępów uczestników, co sprzyja skuteczniejszemu zarządzaniu talentami w siłach zbrojnych. Integracja sztucznej inteligencji w strukturach wojskowych stanowi nie tylko odpowiedź na wyzwania współczesnego pola walki, lecz także kluczowy czynnik determinujący przyszłą skuteczność sił zbrojnych. Rozwój i wdrażanie nowoczesnych technologii w obszarze obronności wymagają jednak precyzyjnie określonych strategii, efektywnego zarządzania ryzykiem oraz ścisłej współpracy na poziomie krajowym i międzynarodowym.

## Generatywna sztuczna inteligencja

Generatywna sztuczna inteligencja[20] (GenAI) to podkategoria sztucznej inteligencji, która w oparciu o dostarczone dane tworzy nowe i oryginalne treści,

[20] V. Alto, Practical Generative AI with ChatGPT. Unleash your prompt engineering potential with OpenAI technologies for productivity and creativity - Second Edition, Gliwice 2025, s. 386.

to nic innego jak technologia, która za pomocą poleceń, tzn. promptów[21], pozwala użytkownikom wygenerować nowe wcześniej nie znane rozwiązana lub po prostu treści. Algorytmy GenAI działają na podstawie danych dostarczonych zarówno podczas tworzenia narzędzia, jak i prowadzanych w trakcie jego użytkowania. Jakość generowanych treści zależy od jakości dostępnych danych, dlatego rezultaty pracy GenAI mogą nie być idealne.

Zanim skorzysta się z wybranego narzędzia GenAI, warto zapoznać się z poniższymi wskazówkami. Po pierwsze, należy pamiętać, że korzystając z GenAI, traci się kontrolę nad danymi, które się jej przekazuje. Nie mamy pewności, do czego mogą one zostać wykorzystane przez twórców systemu, ani w jaki sposób są przechowywane. Agencje rządowe zalecają, by do narzędzi GenAI nie wpisywać informacji, które:

- są niejawne lub zawierają dane wrażliwe;
- zawierają wewnętrzne informacje urzędowe, będące w fazie przygotowawczej, a tym samym nie przeznaczone do upublicznienia;
- zawierają dane osobowe, których ujawnienie narusza przepisy RODO[22].

Dodatkowo wśród rekomendacji działań koniecznych do podjęcia, przygotowanych przez MON, znalazły się:

- określenie potrzeb dotyczących zapewnienia wiedzy i kompetencji wymaganych do rozwoju i wykorzystania systemów AI w zakresie rekrutacji i szkolenia kadr;
- dokonanie przeglądu potrzeb i wymagań dotyczących implementacji AI w zdolnościach sił zbrojnych;
- określenie potrzeb w zakresie rewizji regulacji prawnych oraz obowiązujących w resorcie polityk, procesów i procedur;
- zdefiniowanie potrzeb w zakresie rozwoju resortowej infrastruktury cyfrowej;
- dokonanie analizy stanu prawnego, procedur i procesów w aspekcie wykorzystania systemów AI w zastosowaniach wojskowych;
- utworzenie dedykowanych dla obszaru sztucznej inteligencji struktur organizacyjnych[23].

Powyższe zalecenia podyktowane są faktem, iż generatywna sztuczna inteligencja wykorzystuje modele językowe LLM[24][25] (Large Language Models), czyli zaawansowane algorytmy uczenia maszynowego, które dzięki technikom głębokiego uczenia potrafią analizować wzorce językowe i generować spójny, logiczny tekst. Modele te są trenowane na ogromnych zbiorach danych tekstowych, co pozwala im rozumieć strukturę języka, zasady gramatyki, kontekst oraz fakty. Dzięki temu znajdują zastosowanie w wielu obszarach, takich jak: generowanie artykułów, raportów i wiadomości e-mail, tłumaczenia maszynowe, udzielanie odpowiedzi na pytania, analiza sentymentu, podsumowywanie dłuższych dokumentów, czy tworzenie chatbotów

[21] J. Phoenix, M. Taylor, Skuteczna inżynieria promptów. Przyszłościowe rozwiązania dla rzetelnych wyników generatywnej AI, Gliwice 2025, s. 376.
[22] Generatywna sztuczna inteligencja w służbie pracowników administracji publicznej https://ai.gov.pl/administracja-publiczna/generatywna-ai, [dostęp: 05.11.2025].
[23] N. Bochyńska, MON wziął się za AI. Wojsko jej użyje, ale są pewne warunki, https://cyberdefence24.pl/armia-i-sluzby/mon-wzial-sie-za-ai-wojsko-jej-uzyje-ale-sa-pewne-warunki, [dostęp: 05.11.2025].
[24] V. Alto, LLM w projektowaniu oprogramowania. Tworzenie inteligentnych aplikacji i agentów z wykorzystaniem dużych modeli językowych, Gliwice 2025, s. 344.
[25] L. Gazit, M, Ghaffari, Zaawansowane techniki przetwarzania języka naturalnego. Od podstaw do modeli LLM i zastosowań biznesowych w Pythonie, Gliwice 2025, s. 320.

umożliwiających naturalną interakcję z użytkownikami. LLM-y stanowią fundament współczesnych rozwiązań opartych na sztucznej inteligencji i przyczyniają się do dynamicznego rozwoju narzędzi wspierających komunikację oraz przetwarzanie języka naturalnego.

## Podsumowanie

Jeżeli wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji przechowywanych i przetwarzanych przez silniki uczenia maszynowego będą akceptowalne, to autor widzi możliwość uzupełnienia eksploatowanych instancji systemów teleinformatycznych SZRP o usługi AI. Implementacja narzędzi opartych na uczeniu maszynowym jest możliwe w ramach istniejących instancji systemu teleinformatycznego Polish Mission Network bazującego na idei Federated Mission Networking. Wykorzystanie instancji systemu teleinformatycznego przetwarzających informacje niejawne może zapewnić zachowanie odpowiedniego poziomu bezpieczeństwa zarówno baz danych uczących silnik, kierowanych zapytań, jak i wyników. Niemniej jednak podczas szacowania ryzyka należy przeprowadzić analizę i ocenę ryzyka, to znaczy określić, które rodzaje ryzyka są akceptowalne. Podczas analizy ryzyka należy przeprowadzić identyfikację i określić ich wielkość. Autor zwrócił uwagę na fakt, że resort obrony narodowej planuje inwestycje w badania i rozwój przełomowych technologii AI, ukierunkowanych na budowanie długofalowej przewagi operacyjnej. Jak określa przedmiotowy dokument, ze względu na wysokie ryzyko technologiczne, działania te będą prowadzone centralnie w ramach projektów badawczo-rozwojowych w obszarze bezpieczeństwa i obronności z naciskiem na szybkie, zdaniem autora, skuteczne i bezpieczne projektowanie, testowanie i wdrażanie rozwiązań. Ze względu na powyższe deklaracje autor przyjął hipotezę badawczą, że SZRP są w stanie zorganizować wdrożenie i eksploatację narzędzi opartych na uczeniu maszynowym przy zachowaniu poziomu bezpieczeństwa przetwarzanych danych. Z wyników badań przeprowadzonych przez autora można wysnuć wnioski, iż jest możliwe wdrożenie i eksploatacja w SZ RP narzędzi opartych na AI. Biorąc pod uwagę spełnienie wymagań dotyczących ryzyka, badania realizowane przez autora potwierdzają przyjętą hipotezę.

W części końcowej przedstawiono rekomendacje podkreślające, że skuteczne i odpowiedzialne wdrożenie rozwiązań opartych na AI w RON wymaga przyjęcia systemowego, spójnego podejścia do planowania i realizacji działań w tym obszarze. Ze względu na przełomowy charakter technologii AI oraz szeroki zakres jej potencjalnych zastosowań, niezbędne jest powołanie odpowiednich struktur zarządczych i wykonawczych odpowiedzialnych za koordynację, nadzór oraz realizację projektów i inicjatyw z zakresu AI. Działania te powinny być postrzegane jako kluczowy element szerszego procesu transformacji cyfrowej resortu. Ponadto mnogość usług informatycznych wymaga zwiększenia liczby i gruntownego przeszkolenia żołnierzy zarówno eksploatujących usługi AI, jak i zajmujących się ich administrowaniem. Zakres kompetencji i obowiązków personelu zarządzającego AI powinien być zdeterminowany zakresem usług eksploatowanych w obszarze wsparcia procesów. Żołnierze wsparcia zarządzający usługami AI powinni stanowić ściśle wyselekcjonowaną grupę specjalistów o odpowiedniej wiedzy teoretycznej i umiejętnościach praktycznych ukierunkowanych na właściwy obszar odpowiedzialności. Zalecana jest gruntowna reorganizacja systemu kształcenia i szkolenia w zakresie usług

teleinformatycznych, uzupełnienie treści o tematykę usług opartych na AI. Wymaga to wsparcia eksperckiego ze strony organizatora systemu informatycznego, w ramach którego usługi będą eksploatowane. Kształcenie kadr kierowniczych i szkolenie specjalistów wsparcia teleinformatycznego powinno być realizowane systemowo w odniesieniu do konkretnych usług AI. Istotnym czynnikiem jest system doboru kandydatów z dużym doświadczeniem zawodowym, jednocześnie zdeterminowanych do zdobywania nowej wiedzy i umiejętności w obszarze AI. Niezbędna jest również reorganizacja systemu wsparcia teleinformatycznego w obszarze sztucznej inteligencji w celu zwiększenia efektywności realizacji zadań. Proces ten ma charakter złożony i wymaga szczegółowego planowania. W celu zapewnienia efektywnego funkcjonowania i utrzymania usług opartych na sztucznej inteligencji proponuje się utworzenie dedykowanych komórek wsparcia użytkowników typu Help Desk AI, odpowiedzialnych za obsługę pierwszego poziomu i bieżące reagowanie na zgłaszane problemy. Takie rozwiązanie umożliwi ekspertom i specjalistom ds. utrzymania skoncentrowanie się na bezpośrednim wsparciu administratorów systemów AI oraz realizacji zadań o wyższym stopniu złożoności. Kluczowym elementem systemu powinno być także: dobór, szkolenie i zapewnienie odpowiedniej liczby specjalistów z zakresu sztucznej inteligencji na wszystkich szczeblach organizacyjnych, co pozwoli na utrzymanie nieprzerwanego wsparcia teleinformatycznego w trybie ciągłym (24/7/365). Dodatkowo proponuje się powołanie wyspecjalizowanej jednostki eksperckiej pełniącej funkcję ośrodka wsparcia trzeciego poziomu, dedykowanego administratorom i operatorom systemów wykorzystujących technologie sztucznej inteligencji.

Realizacja powyższych działań może przyczynić się do zwiększenia niezawodności infrastruktury teleinformatycznej, skrócenia czasu reakcji na incydenty oraz podniesienia ogólnego poziomu bezpieczeństwa i efektywności operacyjnej systemów wykorzystujących sztuczną inteligencję.

## Bibliografia

Alto V., LLM w projektowaniu oprogramowania. Tworzenie inteligentnych aplikacji i agentów z wykorzystaniem dużych modeli językowych, Gilwice 2025.

Alto V., Practical Generative AI with ChatGPT. Unleash your prompt engineering potential with OpenAI technologies for productivity and creativity - Second Edition, Gilwice 2025.

Bahga A., Madisetti V., Big Data Science & Analytics: A Hands-On Approach, https://openlibrary.telkomuniversity.ac.id/pustaka/229820/big-data-science-analytics-a-hands -on-approach.html.

Bogdański A., Federated Mission Networking w ujęciu narodowych dokumentów doktrynalnych: aspekt bezpieczeństwa teleinformatycznego, [w:] M. Marczyk, M. Stolarz, B. Terebiński (red.), Bezpieczeństwo działań w cyberprzestrzeni: wybrane aspekty, t. 2, Techniczne aspekty cyberprzestrzeni, Warszawa 2022.

Bochyńska N., MON wziął się za AI. Wojsko jej użyje, ale są pewne warunki, https://cyberdefence24.pl/armia-i-sluzby/mon-wzial-sie-za-ai-wojsko-jej-uzyje-ale-sa-pewne-warunki.

Gazit L., Ghaffari M., Zaawansowane techniki przetwarzania języka naturalnego. Od podstaw do modeli LLM i zastosowań biznesowych w Pythonie, Gilwice 2025.
Generatywna sztuczna inteligencja w służbie pracowników administracji publicznej, https://ai.gov.pl/administracja-publiczna/generatywna-ai.
Koziej S., Pietrzak P., Szczyt NATO w Newport, „Bezpieczeństwo Narodowe" 2014, nr 3.
Lutyński J., Metody badań społecznych. Wybrane zagadnienia. Analiza procesu otrzymywania informacji w badaniach z zastosowaniem wywiadu kwestionariuszowego, Łódź 2000.
Mihchell T., Machine Learning, Science, Engineering, Math 1997, https://www.cs.cmu.edu/~tom/files/MachineLearning TomMitchell.pdf.
Orłowski D., Wybrane aspekty zastosowania big data 2 w zarządzaniu zasobami ludzkimi w organizacji, [w:] Wolniak R. (red.), Management and Quality, Katowice 2022, http://14.99.188.242:8080/jspui/hadle/123456789/12578.
Pelc M., Elementy metodologii badań naukowych, Warszawa 2012.
Phoenix J., Taylor M., Skuteczna inżynieria promptów. Przyszłościowe rozwiązania dla rzetelnych wyników generatywnej AI, Gliwice 2025.
Prawda M., Biograficzne odtwarzanie rzeczywistości, „Przegląd Socjologiczny" 1989, nr 4.