Ministerstwo Obrony Narodowej

Resortowa strategia sztucznej inteligencji do roku 2039

Warszawa

sierpień 2024

Spis treści

Wstęp

Resort obrony narodowej (dalej: RON lub Resort) musi przygotować się na funkcjonowanie w warunkach globalnej konkurencji technologicznej charakteryzującej się gwałtownymi zmianami w środowisku bezpieczeństwa. *Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020*[1] zwraca uwagę na ogromny potencjał tej technologii jako katalizatora wzrostu gospodarczego mającego wpływ na niemal wszystkie dziedziny codziennego życia. Rozwój, wdrażanie i wykorzystanie systemów sztucznej inteligencji (AI[2]) mają kluczowe znaczenie dla sprostania wymogom ogólnoświatowej transformacji cyfrowej.

Zapewnienie szerokiego dostępu do informacji i gwałtowny postęp technologiczny zmieniają charakter działań militarnych. Chcąc sprostać współczesnym i przyszłym wyzwaniom w zakresie bezpieczeństwa, resort obrony narodowej musi nadać priorytet badaniom naukowym, pracom rozwojowym oraz eksperymentowaniu, zapewniając warunki do uzyskania przewagi strategicznej nad potencjalnymi adwersarzami poprzez wykorzystywanie innowacyjnych koncepcji i najnowocześniejszych osiągnięć technologicznych, w szczególności opartych na sztucznej inteligencji.

Konflikty, w całym spektrum operacji wojskowych, stają się coraz bardziej złożone i dynamiczne. Zwiększenie tempa i natężenia działań militarnych prowadzonych w wielodomenowym środowisku operacyjnym skutkuje znaczącym skróceniem czasu na wypracowanie opartej o analizę danych decyzji w zakresie skutecznej odpowiedzi. Ilość dostępnych danych stanowi wyraźne wyzwanie dla ludzkiej percepcji i zdolności do reagowania. Powodzenie w rozstrzyganiu przyszłych konfliktów będzie silnie uzależnione od możliwości szybkiej analizy dużych wolumenów danych i podejmowania na tej podstawie świadomych decyzji o zastosowaniu środków odpowiedzi. Efektywność przyjętych rozwiązań będzie w coraz większym stopniu zależeć od zdolności wykorzystania najnowszych rozwiązań technologicznych, w tym zaawansowanych systemów sztucznej inteligencji.

Celem implementacji Strategii[3] jest stworzenie warunków do odpowiedzialnego rozwoju, wdrożenia i wykorzystania AI, co będzie wymagać szeregu zmian w kulturze organizacyjnej i zasadach funkcjonowania RON, zbudowania i utrzymania wymaganych kompetencji, dokonania niezbędnych inwestycji w infrastrukturę teleinformatyczną oraz stymulacji prac badawczych, rozwojowych i wdrożeniowych w tym zakresie. Aby zapewnić systemowe podejście do implementacji sztucznej inteligencji, w tym sprawne kierowanie, zarządzanie i koordynowanie procesem rozwoju AI oraz wdrażanie i wykorzystanie nowych rozwiązań, niezbędne jest utworzenie specjalnych struktur organizacyjnych przeznaczonych do: (1) kierowania i koordynacji całokształtu działań w przedmiotowym obszarze, (2) realizacji projektów z partnerami, eksperymentowania i wdrażania wybranych rozwiązań oraz (3) utrzymywania i zapewniania wykorzystania wdrożonych rozwiązań AI.

[1] Załącznik do uchwały nr 196 Rady Ministrów z dnia 28 grudnia 2020 r. (poz. 23).

[2] *Artificial Intelligence*.

[3] Niniejszy dokument nie stanowi strategii rozwoju w myśl *Ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju*, tudzież *Uchwały nr 162/2018 Rady Ministrów z dnia 29 października 2018* r. *w sprawie przyjęcia „Systemu zarządzania rozwojem Polski"*, jednak jego nazwa podkreśla strategiczny wymiar zawartych treści dla działań w ramach resortu obrony narodowej.

Mając na względzie globalne trendy technologiczne oraz potencjalne korzyści wynikające z wdrożenia i wykorzystania sztucznej inteligencji, należy wskazać implementację systemów AI jako jeden z głównych priorytetów w planowaniu rozwoju Sił Zbrojnych RP. Możliwość szerokiego zastosowania AI w rozwiązaniach wojskowych należy rozpatrywać zarówno w perspektywie zwiększania własnych zdolności, jak i wyzwań związanych z wykorzystaniem tej technologii przez adwersarzy.

Resort będzie stymulować i wspierać krajowy ekosystem AI podczas realizacji projektów z potencjałem wykorzystania w obszarach bezpieczeństwa i obronności, tworząc dynamiczne partnerstwo z przemysłem oraz środowiskami akademickim i naukowym. Wzmacniając powiązania z sektorem cywilnym, będzie zachęcać do inwestowania w badania i rozwój technologii podwójnego zastosowania oraz wprowadzi uproszczone zasady uzyskania dostępu do swoich danych i zasobów niezbędnych do prowadzenia przedmiotowych prac. Resort podejmie również działania w kwestii usprawnienia systemu pozyskiwania sprzętu i usług, aby zwiększyć jego elastyczność oraz przyśpieszyć procesy rozwijania i wprowadzania wymaganych zdolności operacyjnych. Ponadto zostaną podjęte kroki w kierunku stworzenia nowych możliwości współpracy z małymi i średnimi przedsiębiorstwami oraz maksymalizacji wykorzystania i komercjalizacji własności intelektualnej związanej ze sztuczną inteligencją.

Resort będzie podnosił swoją efektywność i wydajność poprzez rozwijanie i wdrażanie dostępnych rozwiązań AI obejmujących *Data Science*, uczenie maszynowe i zaawansowane techniki statystyki obliczeniowej. Równolegle, wraz z partnerami, będzie realizował prace badawczo-rozwojowe nad nowymi przyszłościowymi systemami AI i ich zastosowaniem. Wykorzystując współpracę z sojusznikami i partnerami, Resort będzie dążyć do opracowania innowacyjnych rozwiązań odpowiadających wspólnym wyzwaniom, co przyczyni się do optymalizacji kosztów utrzymania niszowych zdolności do rozwoju i testowania sztucznej inteligencji, w tym wykrywania anomalii i nieautoryzowanych ingerencji w zasady jej funkcjonowania.

Wszystkie działania będą realizowane w sposób odpowiedzialny i bezpieczny, z pełnym poszanowaniem norm etycznych, moralnych i obowiązującego prawa[4].

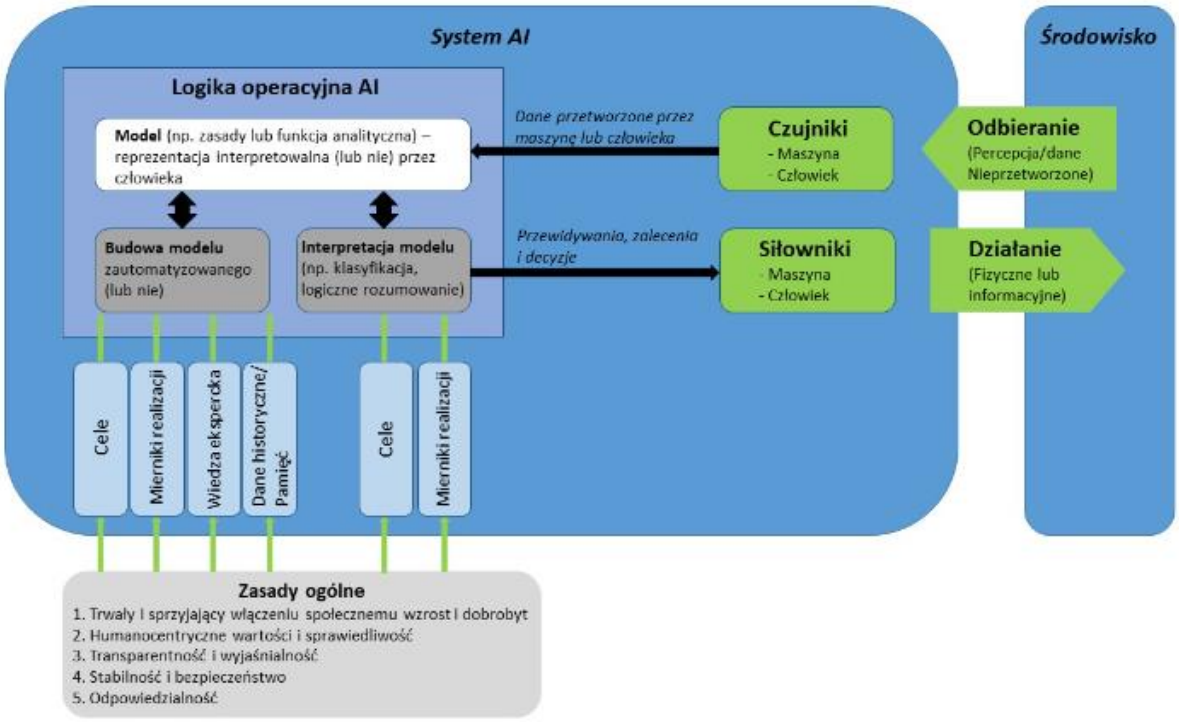
[4] M.in. zgodnie z PO(2021)0350, *Annex 1 – NATO's Artificial Intelligence Strategy* oraz *EU Artificial Intelligence Act.*

Pojęcia podstawowe

Sztuczna Inteligencja (AI) – w kontekście niniejszej Strategii za sztuczną inteligencję uważana jest zdolność maszyny do wykonywania zadań, które są zwykle kojarzone z ludzkimi zdolnościami poznawczymi, takimi jak rozpoznawanie wzorców, uczenie się na podstawie doświadczeń, przewidywanie zdarzeń i wyciąganie wniosków oraz rekomendowanie i podejmowanie działań w przestrzeni cyfrowej lub świecie rzeczywistym z wykorzystaniem systemów autonomicznych.

Rozpatrując AI, należy dostrzec jej transformacyjny charakter ze względu na zasięg możliwego zastosowania oraz rolę katalizatora rozwoju innych technologii, takich jak: analiza danych (*Big Data*), systemy autonomiczne, biotechnologia czy technologie materiałowe.

System AI – w kontekście niniejszej Strategii będzie rozumiany jako system oparty na koncepcji maszyny, który został zaprojektowany do działania z różnym poziomem autonomii, i który może wykazywać zdolność adaptacji po jego wdrożeniu, posiadający potencjał wpływania na środowisko (rzeczywiste lub wirtualne) poprzez tworzenie zaleceń, przewidywanie (predykcję), podejmowanie decyzji na temat określonych celów na podstawie danych wejściowych (pochodzących od maszyn lub ludzi). AI wykorzystuje dane wejściowe do: postrzegania środowiska, tworzenia i interpretowania jego modeli (ręcznych lub automatycznych) oraz formułowania wniosków na tej podstawie. Systemy AI składają się z trzech głównych elementów: czujników (sensorów), logiki operacyjnej (modeli algorytmów) oraz aparatu wykonawczego.



Rys. 1. System AI[5]

[5] Źródło: Portal sztucznej inteligencji, https://www.gov.pl/web/ai

Krajowy **ekosystem AI**[6] – stanowi horyzontalne środowisko przeznaczone do inicjowania i wspierania działań podejmowanych przez szerokie grono interesariuszy na rzecz rozwoju polskiej innowacyjności w obszarze AI i pozycjonowania polskiej własności intelektualnej na możliwie wysokich poziomach globalnego łańcucha wartości związanego z przetwarzaniem danych, a także w celu zminimalizowania ewentualnych ryzyk związanych z trwającą na świecie rywalizacją w obszarze sztucznej inteligencji i dokonującą się transformacją gospodarki i społeczeństwa.

Działania podejmowane w ramach ekosystemu AI mają:

- wspierać powstawanie polskich podmiotów gospodarczych budujących rozwiązania AI;
- promować wykorzystywanie rozwiązań AI w całej polskiej gospodarce;
- wspierać eksport polskich firm branży AI;
- sprzyjać kształceniu, zdobywaniu kwalifikacji oraz rozwijaniu kompetencji i umiejętności w obszarze AI;
- wspierać badania, w szczególności interdyscyplinarne, w obszarze AI;
- promować udział polskich naukowców i przedsiębiorców w gremiach międzynarodowych dyskutujących o AI i jej rozwoju.

Rys. 2. Krajowy ekosystem AI

[6] Zgodnie z załącznikiem do uchwały nr 196 Rady Ministrów z dnia 28 grudnia 2020 r. (poz. 23): Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020.

Kontekst strategiczny

Rozwój technologiczny jest płaszczyzną narastającej i coraz zacieklejszej konkurencji między państwami dążącymi do poprawy dobrobytu oraz zapewnienia sobie bezpieczeństwa. Poszczególne kraje, chcąc uzyskać przewagę strategiczną na wypadek zaistnienia konfliktu, angażują znaczne siły i środki w rozwój nowych oraz przełomowych technologii. Należy przyjąć, że przyszłe bezpieczeństwo, odporność na zagrożenia, pozycja międzynarodowa, a także dobrobyt będą uzależnione od zdolności rozumienia oraz wykorzystania szybkich zmian technologicznych i dostosowania się do nich.

W kontekście intensywnego rozwoju technologicznego pojawiają się nowe wyzwania, które wymagają skoordynowanych działań na poziomie międzynarodowym. Kluczowe jest tutaj zrozumienie, że technologie, które dziś są innowacyjne, jutro mogą stać się standardem. Dlatego też państwa powinny współpracować ze sobą, aby stworzyć wspólne normy i dobre praktyki, które będą chronić przed nadużyciami, wspierając jednocześnie działania na rzecz rozwoju technologicznego.

Wykorzystanie sztucznej inteligencji w zastosowaniach wojskowych jest rozważane zarówno w aspekcie możliwych do uzyskania korzyści, jak i potencjalnych związanych z tym ryzyk. Inwestycje w rozwiązania wykorzystujące AI mogą znacząco zwiększyć zdolności operacyjne sił zbrojnych, ale jednocześnie wymagają starannego zarządzania ryzykiem, przestrzegania norm etycznych i międzynarodowych regulacji, aby zapobiec potencjalnym negatywnym konsekwencjom. Stąd podejmowane są kolejne inicjatywy mające na celu ustanowienie ogólnie przyjętych standardów rozwoju oraz wykorzystania nowych i przełomowych technologii, w tym sztucznej inteligencji[7].

Dokonujący się postęp technologiczny pozwala na zwiększenie posiadanych lub uzyskanie nowych zdolności poprzez wprowadzenie innowacyjnych rozwiązań do techniki wojskowej. Doświadczenia ze współczesnych wojen i konfliktów zbrojnych potwierdzają, że nowe technologie zmieniają współczesne pole walki. Systemy wspierane sztuczną inteligencją są w szybkim tempie wprowadzone do użycia w różnych kontekstach operacyjnych. Przykłady zastosowań dotyczą m.in. zwiększenia zdolności do szybkiej analizy dużych wolumenów informacji i danych celem wsparcia procesów decyzyjnych, w tym targetingu, poprawienia cyberbezpieczeństwa, wsparcia działalności wywiadowczo-rozpoznawczej, zarządzania rojami platform (obiektów) autonomicznych czy zwiększenia poziomu autonomii wykorzystywanych systemów uzbrojenia. Na uwagę zasługuje również wykorzystanie sztucznej inteligencji do prowadzenia działań w przestrzeni informacyjnej z zastosowaniem dostępnych narzędzi, m.in. do szerzenia dezinformacji.

Nie bez znaczenia jest zwiększenie dostępności zaawansowanych narzędzi bazujących na AI dla aktorów niepaństwowych, w tym grup terrorystycznych. Perspektywa wykorzystania nowych narzędzi może wpłynąć na zmianę sposobów działania tych grup, m.in. w zakresie prowadzenia działań propagandowych czy akcji rekrutacyjnych ukierunkowanych na konkretne osoby. Istnieje również ryzyko wykorzystania nowych narzędzi do przyśpieszenia

[7] M.in.: *Responsible Artificial Intelligence in the Military Domain*; *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*; *EU Artificial Intelligence Act*; *UN resolution 78/241 "Lethal autonomous weapon systems"*.

badań i rozwoju technologii produkcji broni masowego rażenia (jądrowej, chemicznej, biologicznej lub radiologicznej).

Rozwój sztucznej inteligencji pozwala potencjalnym adwersarzom na łatwiejsze i szybsze wytwarzanie znacznych ilości nieprawdziwych informacji, które mogą służyć manipulowaniu nastrojami użytkowników mediów społecznościowych lub przeciążaniu zdolności poznawczych człowieka, podważając wiarygodność dostępnych informacji, a tym samym zmniejszając zaufanie i odporność społeczeństwa na działania hybrydowe.

Diagnoza gotowości resortu obrony narodowej na wdrożenie sztucznej inteligencji

Resort obrony narodowej musi podjąć szereg działań w kierunku osiągnięcia gotowości do skalowalnego wdrożenia rozwiązań i wykorzystania potencjału AI.

Pomimo zaangażowania polskich przedstawicieli w prace nad przygotowaniem sojuszniczych dokumentów dotyczących transformacji cyfrowej, wykorzystania danych czy właśnie sztucznej inteligencji nie opracowano dotychczas resortowych dokumentów kierunkowych w tym zakresie. Brak jednoznacznego wskazania poziomu ambicji, celów czy opracowania strategii działania w zakresie implementacji nowych i przełomowych technologii stanowi przeszkodę dla obrania spójnego kierunku i zapewnienia skoordynowanego podejścia.

Brak nadrzędnego planu, który pozwoliłby Resortowi skutecznie zapewnić koordynację i odpowiednie zarządzanie inwestycjami lub rozwinąć odpowiednie postawy, umiejętności i zdolności w celu skutecznego, bezpiecznego i odpowiedzialnego wdrożenia sztucznej inteligencji, nie pozwala na efektywne wykorzystanie posiadanych zasobów.

Na uwagę zasługuje również brak jednoznacznego wskazania odpowiedzialnego za zarządzanie i nadzorowanie prac prowadzonych w obszarze sztucznej inteligencji w ujęciu holistycznym. Skutkuje to rozproszeniem odpowiedzialności, a w konsekwencji utrudnia realizację współpracy w ujęciu krajowym (przemysł, środowiska naukowe), międzyresortowym i międzynarodowym.

Strategicznymi czynnikami budowania potencjału w obszarze sztucznej inteligencji są: (1) zapewnienie dostępu do zweryfikowanych danych wysokiej jakości, (2) posiadanie wiedzy, kompetencji, umiejętności i kwalifikacji, (3) dostosowanie prawa, jak również ustalenie adekwatnych procesów i procedur, (4) inwestowanie w rozwój technologii i infrastrukturę cyfrową, (5) rozwój ekosystemu innowacji, szczególnie w obszarach priorytetowych.

Rozpatrując powyższe, należy wskazać na potrzebę podjęcia zdecydowanych działań celem:

- odejścia od silosów danych oraz zmiany w trybie zarządzania dostępem do wyspecjalizowanych zasobów zawierających ustandaryzowane i zweryfikowane dane wysokiej jakości;
- zapewnienia koordynacji wysiłków podejmowanych w obszarze AI w wymiarze krajowym;
- zapewnienia wymaganej wiedzy i kompetencji poprzez skuteczną rekrutację talentów oraz podnoszenie kwalifikacji technicznych zatrudnionych kadr poprzez realizację dedykowanych kursów i szkoleń;
- dostosowania przepisów prawa umożliwiających wykorzystanie potencjału sztucznej inteligencji, jak również ustalenie procedur i procesów zgodnych z zasadami etyki, prawami człowieka oraz międzynarodowym prawem humanitarnym konfliktów zbrojnych służących skutecznemu zarządzaniu tym obszarem;
- zapewnienia, adekwatnego do poziomu ambicji, finansowania i ukierunkowania inwestycji na rozwój technologii, jak również budowę infrastruktury teleinformatycznej wymaganej do jej wdrożenia;
- stymulowania rozwoju oraz wykorzystania potencjału krajowego i globalnego ekosystemu sztucznej inteligencji do wzmocnienia zdolności w obszarze bezpieczeństwa i obronności,

– rozwijania współpracy z sojusznikami oraz organizacjami międzynarodowymi w zakresie wymiany wiedzy nt. technologii AI, aby uzyskać znaczący postęp we wdrożeniu systemów AI poprzez korzystanie z najlepszych praktyk i najnowszych osiągnięć technologicznych.

Wizja strategiczna 2039

Do roku 2039 wykorzystanie nowoczesnych technologii, w tym sztucznej inteligencji, będzie warunkiem posiadania zdolności do efektywnej realizacji odstraszania i obrony przez Siły Zbrojne RP. Systemy sztucznej inteligencji będą odgrywać znaczącą rolę w działaniach militarnych, co zrewolucjonizuje sposób zarządzania i prowadzenia operacji wojskowych w przyszłym zdigitalizowanym środowisku walki. Jej wszechstronne zastosowania będą wpływać nie tylko na zwiększenie tempa operacyjnego i efektywności wykorzystania zaangażowanych sił, ale także kreować nowe wyzwania etyczne i prawne.

Wykorzystanie systemów sztucznej inteligencji w działaniach militarnych będzie dotyczyć m.in.:

- autonomicznych systemów bojowych, które będą mogły prowadzić operacje bez bezpośredniego zaangażowania człowieka lub wspierać jego działania, przedstawiając stosowne rekomendacje; dzięki zaawansowanym algorytmom AI i zdolności do samodzielnego podejmowania decyzji systemy będą mogły przeprowadzać misje rozpoznawcze (oraz inne ofensywne i defensywne) z większą precyzją i bez narażania ludzkiego personelu;
- analizy informacji rozpoznawczo-wywiadowczych pozyskiwanych z różnych źródeł ze względu na możliwość przetwarzania ogromnych ilości danych; pozwoli to identyfikować pewne wzorce i trendy, szybciej oraz skuteczniej przewidywać i oceniać działania przeciwnika, a także usprawnić procesy planowania, prowadzenia i oceny operacji;
- optymalizacji logistyki, co umożliwi efektywniejsze zarządzanie zasobami, redukcję czasu prac serwisowych i naprawczych, planowanie tras transportowych i przewidywanie potrzeb zaopatrzeniowych; efektywniejsza logistyka oznacza szybsze reagowanie na zmieniające się warunki i lepsze wsparcie dla jednostek realizujących zadania bojowe;
- systemów obrony cyberprzestrzeni, wspierając obronę przed cyberatakami; algorytmy AI mogą zdecydowanie szybciej niż człowiek identyfikować i neutralizować zagrożenia, zapewniając bezpieczeństwo infrastruktury wojskowej i informacji, jak również mogą wykrywać podatne zasoby wymagające bezzwłocznych działań;
- symulacji i szkolenia, do tworzenia materiałów szkoleniowych stosowanych w szkoleniu oraz realistycznych symulacji bojowych, które pomogą w szkoleniu żołnierzy i testowaniu strategii; wirtualne środowiska treningowe umożliwią bezpieczne i efektywne przygotowanie do rzeczywistych operacji;
- wsparcia decydentów/dowódców w podejmowaniu decyzji, poprzez analizowanie różnych scenariuszy rozwoju sytuacji i sugerowanie optymalnych rozwiązań zwiększając świadomość sytuacyjną oraz szybkość wypracowywania decyzji; możliwość szybkiego przetwarzania dużych ilości danych i przedstawiania bazujących na nich rekomendacji usprawni proces dowodzenia oraz zwiększy trafność podejmowanych decyzji;
- analizy danych szkoleniowych (e-learning), która umożliwi projektowanie spersonalizowanych ścieżek rozwoju poprzez właściwą rekomendację niezbędnych kursów czy szkoleń oraz dostosowywanie poziomu materiałów szkoleniowych w zależności od posiadanej wiedzy, czynionych postępów oraz indywidualnych potrzeb. Analiza danych szkoleniowych zapewnia właściwe warunki do identyfikacji oraz procesu zarządzania talentami.

Systemy sztucznej inteligencji w zastosowaniach militarnych – szanse i zagrożenia

Sztuczna inteligencja stała się siłą transformacyjną w różnych sektorach, a domena wojskowa nie pozostaje tutaj wyjątkiem. Dzięki możliwości przetwarzania ogromnych ilości danych, analizowania złożonych wzorców i podejmowania natychmiastowych decyzji sztuczna inteligencja rewolucjonizuje technologię wojskową. Niezależnie od tego, czy ułatwia rozwój platform autonomicznych, czy odgrywa kluczową rolę w cyberbezpieczeństwie, w ostatnich latach AI przyczyniła się do osiągnięcia znaczących postępów w obszarze rozwoju zdolności obronnych. Zastosowania sztucznej inteligencji w technice wojskowej mogą dotyczyć, chociaż nie ograniczają się wyłącznie do:

1. Autonomicznych systemów uzbrojenia i transportu. Jednym z najistotniejszych sposobów wykorzystania sztucznej inteligencji w siłach zbrojnych jest rozwój autonomicznych systemów uzbrojenia. Bezzałogowe statki powietrzne, pojazdy naziemne i nawodne oraz podwodne wyposażone w systemy sztucznej inteligencji mają zastosowanie w rozpoznaniu, targetingu i misjach uderzeniowych, a w przyszłości przewiduje się radykalne zwiększenie ich roli. Powszechne wdrożenie systemów autonomicznych wpłynie na sposób postrzegania konfliktów zbrojnych, oddalając ludzi od pola walki. Ochrona siły żywej stanowi priorytet dla wielu sił zbrojnych, stąd obserwowane są znaczące inwestycje w rozwój systemów autonomicznych.
2. Inteligentnych systemów decyzyjnych. Sztuczna inteligencja wspiera systemy dowodzenia i kierowania, umożliwiając analizę danych w czasie rzeczywistym oraz budowanie na tej podstawie świadomości sytuacyjnej i podejmowanie decyzji. Systemy oparte na sztucznej inteligencji umożliwiają prowadzenie analiz dużych wolumenów danych znacznie wydajniej i szybciej niż w przypadku pracy zespołów analityków. Systemy sztucznej inteligencji mogą usprawnić proces decyzyjny, dostarczając informacje i wskazówki potrzebne do podejmowania świadomych decyzji na wszystkich poziomach kierowania i dowodzenia. Narzędzia wykorzystujące AI przyczynią się do optymalizacji planowania misji, alokacji zasobów i realizacji działań militarnych.
3. Wsparcia działań logistycznych. Współczesne działania bojowe zależą od coraz bardziej złożonych i współzależnych sieci logistycznych, które wymagają sprawnego zarządzania. Choć siły zbrojne przez lata udoskonalały te sieci, nadal są one podatne na błędy ludzkie i wymagają optymalizacji. Wykorzystanie technologii opartych na sztucznej inteligencji pomaga obniżyć ogólne koszty, zminimalizować potrzebę udziału człowieka oraz zoptymalizować dystrybucję i transport. Wraz z rozwojem internetu rzeczy (IoT[8]) i wzrostem dostępności danych wejściowych zdolność sztucznej inteligencji do skutecznej automatyzacji dużych części procesu logistycznego będzie rosła wykładniczo. Dzięki temu powstaną bardziej wydajne i responsywne systemy logistyczne, które dostosują się do zmieniających się warunków, aby zapewnić najlepsze możliwe wyniki.
4. Bezpieczeństwa w cyberprzestrzeni. Sektor obronny jest w coraz większym stopniu zależny od wzajemnie połączonych systemów i sieci cyfrowych. Zapewnia to wiele korzyści, a jednocześnie stanowi potencjalną słabość. Jeśli adwersarz naruszy bezpieczeństwo tych systemów, konsekwencje mogą być niezwykle poważne. Sztuczna inteligencja może odegrać kluczową rolę w wykrywaniu zagrożeń w cyberprzestrzeni oraz

[8] *Internet of Things.*

łagodzeniu skutków prowadzonych ataków. Algorytmy uczenia maszynowego analizują ruch sieciowy, identyfikują potencjalne luki i reagują na cyberataki w czasie rzeczywistym. Pomaga to zabezpieczyć sieci przed atakami. Takie systemy również uczą się na podstawie poprzednich incydentów i stale ewoluują, tworząc sprawną oraz responsywną infrastrukturę cyberbezpieczeństwa.

5. Systemów rozpoznawczo-wywiadowczych. Sztuczna inteligencja rewolucjonizuje wykorzystanie gromadzonych danych rozpoznawczo-wywiadowczych. Zaawansowane techniki widzenia komputerowego umożliwiają analizę ogromnych ilości obrazów i danych wideo, pomagając w identyfikacji, śledzeniu i rozpoznawaniu obiektów. Algorytmy sztucznej inteligencji potrafią analizować ogromne ilości danych z różnych źródeł, w tym z mediów społecznościowych, w celu wydobycia odpowiednich informacji i zwiększenia świadomości sytuacyjnej. Przyjęcie i wdrożenie zaawansowanych rozwiązań wykorzystujących sztuczną inteligencję pozwoli również analizować duże ilości danych heterogenicznych, co wcześniej było praktycznie niewykonalne.
6. Symulacyjnych systemów szkolenia. Symulacje i środowiska wirtualne oparte na sztucznej inteligencji stanowią znaczące wsparcie służące realizacji szkolenia w realistycznych scenariuszach. Inteligentni, wirtualni przeciwnicy mogą dostosowywać swoje zachowanie, uczyć się na podstawie interakcji i zapewniać realistyczne doświadczenia treningowe. Mogą również dostosować swoje reakcje i bodźce treningowe do konkretnych osób. Pozwala to na stworzenie indywidualnych programów szkoleniowych dostosowanych do potrzeb i możliwości szkolonych. Systemy symulacyjne oparte na sztucznej inteligencji wspierają rozwijanie zdolności podejmowania decyzji oraz reagowania w złożonych i dynamicznych warunkach operacyjnych. Symulacje pozwalają realizować szkolenia i treningi na różnych poziomach od taktycznego do polityczno-strategicznego bez narażenia szkolonych na niebezpieczeństwo, zapewniając jednocześnie wysoką efektywność kosztową.
7. Realizacji szkoleń. Sztuczna inteligencja posiada ogromny potencjał w zakresie zrewolucjonizowania szkolenia, w tym szkolenia na odległość, które może skutkować wieloma korzyściami zarówno dla szkolących/nauczycieli, jak i szkolonych/uczniów. Wśród nich występuje możliwość personalizacji treści szkoleniowych, a co za tym idzie ich dostosowania do aktualnych potrzeb szkolonych i ich możliwości w zakresie przyswajania wiedzy. Sztuczna inteligencja pozwoli także na zautomatyzowanie procesów analizy wyników i postępów w realizacji szkolenia (automatyczna ocena zadań i testów, a także analiza danych dotyczących postępów szkolonych w celu zapewnienia wartościowych informacji na ten temat). Sztuczna inteligencja może również zapewnić interaktywne narzędzia do nauki, tworzyć moduły szkoleniowe, gry edukacyjne i symulacje, które angażują szkolonych i przyczyniają się do utrwalenia przyswajanej wiedzy. Narzędzia sztucznej inteligencji mogą także stanowić nieodzowne wsparcie dla szkolących/nauczycieli w dostosowywaniu programów nauczania do bieżących wymagań i potrzeb szkoleniowych, analizowaniu efektywności metod nauczania oraz tworzeniu multimedialnych materiałów szkoleniowych. Ponadto sztuczna inteligencja może znaleźć zastosowanie w automatycznym tłumaczeniu tekstu i mowy na różne języki, a także wspierać komunikację między szkolonymi/uczniami a szkolącymi/nauczycielami poprzez przetwarzanie języka mówionego.

Należy przy tym zaznaczyć, że uniwersalność i zasięg wykorzystania sztucznej inteligencji w działaniach wojskowych oraz związane z nimi szanse i zagrożenia są przedmiotem ożywionej debaty na różnych forach międzynarodowych (NATO, UE, ONZ). Bezsprzeczną kwestią wydaje się być brak możliwości zignorowania trwającej rywalizacji w zakresie rozwoju systemów sztucznej inteligencji, które w przypadku konfrontacji mogą zapewnić strategiczną przewagę dla jednej ze stron konfliktu w wybranej lub wielu domenach operacyjnych.

Szanse związane z wykorzystaniem AI w działaniach wojskowych

Wykorzystanie sztucznej inteligencji w działaniach wojskowych może zwiększyć zdolności bojowe oraz efektywność wykorzystania posiadanych zasobów. Rozpatrując możliwe do osiągnięcia korzyści, należy zwrócić uwagę m.in. na:

- zwiększenie efektywności operacyjnej wojsk dzięki poprawieniu koordynacji prowadzonych działań i optymalizacji wykorzystania zasobów w oparciu o zdolności AI do przetwarzania dużych ilości danych w krótkim czasie, a także możliwości odciążenia personelu poprzez delegowanie rutynowych, powtarzalnych zadań do kontrolowanych przez AI systemów automatycznych;
- poprawę szybkości i skuteczności podejmowania decyzji, zapewniając możliwość szybkiego analizowania dużych zbiorów danych i przekazywania użytecznych informacji podnoszących świadomość sytuacyjną wraz z rekomendacjami dotyczącymi możliwych kierunków działania opartymi również na danych historycznych;
- wzmocnienie zdolności rozpoznawczo-wywiadowczych poprzez wykorzystanie potencjału AI do analizy dużych zbiorów danych heterogenicznych celem identyfikacji wzorców i anomalii mogących wskazywać na potencjalne zagrożenia, jak również wsparcie automatycznych systemów monitorowania, dowodzenia i kierowania, co usprawni procesy wykrywania i identyfikacji określonych obiektów;
- poprawę precyzji i skuteczności systemów uderzeniowych, wspierając działanie bezzałogowych systemów uzbrojenia (drony, roboty) w zakresie nawigacji i wyboru celów;
- wsparcie operacji logistycznych poprzez optymalizację planowania dostaw i zarządzanie zapasami, jak również umożliwienie predykcyjnej realizacji obsługiwania i remontów wykorzystywanego sprzętu;
- wsparcie cyberobrony dzięki wykorzystaniu algorytmów AI do monitorowania anomalii i ataków w sieciach komputerowych umożliwiających reakcję na zagrożenia w czasie rzeczywistym;
- wsparcie szkolenia i treningów poprzez wykorzystanie AI do tworzenia materiałów szkoleniowych oraz realistycznych scenariuszy treningowych i symulacji dostosowujących poziom trudności indywidualnie do szkolonych celem zwiększenia efektywności szkolenia;
- wsparcie operacji w środowisku informacyjnym z użyciem AI do organizowania, przetwarzania i analizowania dostępnych danych, co zapewni lepsze rozumienie sytuacji taktycznej, operacyjnej i strategicznej, jak również wykrywanie i przeciwdziałanie operacjom kognitywnym, w tym budowaniu odporności kognitywnej;
- wsparcie podsystemu medycznego poprzez wykorzystanie AI do prowadzenia analiz wyników badań i stawiania diagnoz, a w przyszłości do wspomagania lekarzy w czasie zabiegów chirurgicznych.

Zagrożenia wynikające z wdrożenia AI w działaniach wojskowych

Wykorzystanie sztucznej inteligencji w działaniach wojskowych niesie ze sobą również poważne zagrożenia, które mogą mieć daleko idące konsekwencje. Główne z nich mogą być związane m.in. z:

- wykorzystaniem autonomicznych systemów uzbrojenia, w stosunku do których występuje ryzyko utraty kontroli człowieka i ich nieprzewidywanego zachowania, np. w przypadku wystąpienia zakłóceń lub prób wrogiego przejęcia; osobno rozważane są kwestie prawne i etyczne dotyczące przekazania AI uprawnień do podjęcia decyzji o oddziaływaniu kinetycznym na wybrane cele;
- atakami hakerskimi na systemy sztucznej inteligencji wykorzystującymi ich podatność na manipulację danymi, co może skutkować przejęciem kontroli, zakłóceniami działania lub podejmowaniem błędnych decyzji i działań;
- ryzykiem eskalacji wyścigu zbrojeń będącego konsekwencją zwiększenia ryzyka konfliktu w dynamicznie zmieniającym się środowisku bezpieczeństwa oraz zaistnienia dysproporcji sił wynikających z posiadania bardziej zaawansowanych technologicznie systemów uzbrojenia;
- zawodnością technologii skutkującą możliwymi błędami i awariami prowadzącymi do nieprzewidzianych działań, a z drugiej strony nadmiernego zaufania i polegania na skuteczności maszyny, co może prowadzić do zaniedbywania rozwoju kreatywności i ograniczenia zdolności decyzyjnych człowieka;
- brakiem lub zbyt późnym w stosunku do postępu technologicznego wprowadzaniem regulacji prawnych powodującym powstawanie luk prawnych w kwestiach odpowiedzialności człowieka i zarządzania ryzykiem; osobną kwestią pozostaje ustalenie mechanizmów pozwalających na egzekwowanie porozumień międzynarodowych;
- możliwą dehumanizacją wojny poprzez delegowanie szerokich uprawnień do systemów uzbrojenia kierowanych algorytmami sztucznej inteligencji, które nie są zdolne do moralnego osądu podejmowanych działań;
- podejmowaniem błędnych decyzji na podstawie rekomendacji będących efektem halucynacji AI;
- wykorzystaniem sztucznej inteligencji opracowanej na potrzeby zastosowań wojskowych do zwiększonej kontroli i inwigilacji społeczeństwa.

Rozpatrując wykorzystanie AI w działaniach wojskowych, szczególną uwagę należy zwrócić na odpowiednie zarządzanie ryzykiem oraz uwzględnianie kwestii etycznych i prawnych, aby zapewnić bezpieczne i odpowiedzialne stosowanie tej technologii. Aby zminimalizować zagrożenia, kluczową kwestią jest opracowanie regulacji, zasad oraz mechanizmów kontroli, które zapewnią odpowiedzialne i bezpieczne wykorzystanie sztucznej inteligencji.

Cele i kierunki interwencji dotyczące obszaru sztucznej inteligencji

Celem skalowalnego wprowadzenia systemów sztucznej inteligencji do użycia w resorcie obrony narodowej jest zapewnienie przewagi technologicznej nad potencjalnymi adwersarzami, co wzmocni zdolności do odstraszania i obrony. Odpowiedzialny rozwój i implementacja systemów sztucznej inteligencji przyczyni się do:

- **usprawnienia procesów decyzyjnych,**
- **zwiększenia efektywności operacyjnej,**
- **zwiększenia bezpieczeństwa.**

Aby stworzyć warunki do odpowiedzialnego, skalowalnego wprowadzenia do użycia systemów sztucznej inteligencji w Resorcie, niezbędne jest przeprowadzenie szeregu prac przygotowawczych dotyczących przygotowania danych, uzyskania wiedzy i kompetencji, dostosowania prawa oraz obowiązujących procesów i procedur, rozwoju technologii i infrastruktury teleinformatycznej oraz wzmocnienia ekosystemu AI.

Siły Zbrojne RP zapewnią, aby wykorzystanie systemów sztucznej inteligencji w działaniach wojskowych każdorazowo było zgodne z przepisami prawa krajowego i międzynarodowego, w tym z postanowieniami międzynarodowego Prawa Humanitarnego Konfliktów Zbrojnych. Podczas podejmowania decyzji o użyciu systemów AI przeprowadzone zostaną rozważania obejmujące kwestie przyjęcia odpowiedzialności za potencjalne skutki działania systemów AI oraz zapewnienia poszanowania przepisów prawa i ogólnie przyjętych norm etycznych. Celem odpowiedzialnego wykorzystania AI przez Siły Zbrojne RP stworzone zostaną warunki do zapewnienia:

- rozliczalności decyzji oraz realizacji zadań w ramach łańcucha dowodzenia i kierowania,
- zbalansowania ryzyka z możliwymi do osiągnięcia korzyściami przy określonym, akceptowalnym jego poziomie,
- minimalizacji ryzyka związanego ze stronniczym działaniem lub nieprzewidywalnym zachowaniem wykorzystywanych systemów AI.

Siły Zbrojne RP podejmą wymagane kroki, aby zapewnić odpowiedzialny rozwój, wdrażanie i użycie systemów uzbrojenia wykorzystującego AI[9]. W związku z powyższym w cyklu całego życia systemów uzbrojenia wykorzystujących AI zostaną wdrożone odpowiednie środki kontroli.

[9] Uwzględniając m.in. zasady określone w przyjętej w dniu 11 grudnia 2023 r. *Deklaracji Politycznej w sprawie AI* (*Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*).

Cel operacyjny nr 1: przygotowanie do implementacji sztucznej inteligencji w Resorcie

Kierunek interwencji: zapewnienie wymaganej wiedzy i kompetencji

Pomimo korzyści wynikających z wykorzystania AI do usprawniania lub wsparcia realizacji zadań wykonywanych przez człowieka pojawiające się wyzwania niezmiennie będą wymagać ludzkiej kreatywności i myślenia kontekstowego. Prowadzenie działań militarnych wymaga zapewnienia ludzkiego osądu i wzięcia odpowiedzialności za ich skutki. Niemniej jednak implementacja sztucznej inteligencji zmieni potrzeby w zakresie zaangażowania człowieka, redefiniując jego zakres działania. Resort zapewni wsparcie pracownikom dotkniętym skutkami wdrażania sztucznej inteligencji, pomagając w uzyskaniu wymaganych kwalifikacji i znalezieniu nowych stanowisk pracy.

Jako domyślne podejście do wdrażania sztucznej inteligencji w Resorcie przyjmie się tworzenie i wykorzystanie zespołów człowiek-maszyna (HMT[10]) celem zwielokrotnienia posiadanego potencjału, łącząc możliwości poznawcze i kreatywność człowieka ze zdolnościami analitycznymi i szybkością maszyn.

Dostępność wykwalifikowanych kadr ma decydujące znaczenie dla przygotowania Resortu do wdrożenia sztucznej inteligencji. Globalny rynek pracy cechuje wysokie zapotrzebowanie na ekspertów z dziedziny AI, dlatego Resort może doświadczyć poważnego deficytu kompetencji.

Perspektywiczne spojrzenie na potrzeby RON w zakresie zapewnienia wymaganej wiedzy i kompetencji w obszarze AI wymaga przeprowadzenia analizy i odpowiedniego dostosowania programów kształcenia i szkolenia w Resorcie oraz zwrócenia uwagi na szczególne uwarunkowania związane z rozwijaniem i wykorzystywaniem systemów AI w działaniach wojskowych.

Aby zachęcić najlepszych specjalistów do podjęcia pracy w Resorcie, musi być ona postrzegana jako atrakcyjny wybór. Za najbardziej korzystny sposób zapewnienia wymaganych kadr należy uznać zwiększanie kompetencji osób już zatrudnionych poprzez stworzenie ścieżek kariery wymagających odbycia obowiązkowych szkoleń. Ważne jest identyfikowanie i rozwijanie kompetencji osób z określonymi predyspozycjami i motywacją do rozwijania kariery w obszarze AI.

Szerokie wykorzystanie systemów AI w Resorcie będzie skutkowało wymogiem zapewnienia operatorom posiadania niezbędnej wiedzy specjalistycznej w zakresie ich odpowiedzialnego i efektywnego wykorzystania.

Niezwykle istotną kwestią dla odpowiedzialnego rozwoju i wykorzystania systemów AI jest zbudowanie niezbędnej wiedzy wśród kadry kierowniczej. Brak zrozumienia możliwych do osiągnięcia korzyści, jak również zagrożeń związanych z wykorzystaniem AI, w tym aspektów prawnych, etycznych i społecznych, nie może stanowić przeszkody w efektywnym wykorzystaniu zdobyczy technologicznych.

[10] *Human-Machine Teaming*.

Mając powyższe na uwadze, podjęte zostaną działania:

1) w zakresie kształcenia i szkolenia nowych kadr:

   – analiza i dostosowanie programów kształcenia i szkolenia w Resorcie celem podniesienia wiedzy i kompetencji związanych z różnymi aspektami (etycznymi, prawnymi, technicznymi i operacyjnymi) użycia systemów sztucznej inteligencji w zastosowaniach wojskowych;

2) w zakresie planowania pozyskania i utrzymania kadr:

   – opracowanie wykazu pożądanych kompetencji w obszarze AI,
   – przygotowanie oferty i standardów rekrutacji oraz strategii utrzymywania wykwalifikowanych pracowników;
   – identyfikacja i usuwanie potencjalnych przeszkód w procesie rekrutacji specjalistów;
   – opracowanie systemu zachęt do podjęcia i kontynuowania pracy w Resorcie oraz podnoszenia kwalifikacji;
   – wykształcenie przyszłych kadr i uzyskanie pożądanych kwalifikacji w oparciu o szkolnictwo wojskowe;

3) w zakresie rekrutacji specjalistów:

   – opracowanie ścieżek rozwoju kariery dla specjalistów z obszaru AI;
   – wprowadzenie mechanizmów rozwijania kompetencji AI, m.in. badanie uzdolnień, zapewnienie możliwości elastycznego wejścia do nowego obszaru kompetencyjnego, wdrożenie programów motywacyjnych zachęcających do korzystania z zaawansowanych kursów technicznych;
   – zapewnienie warunków zatrudnienia na podobnych zasadach jak dla personelu z obszaru cyberbezpieczeństwa;
   – wzmocnienie partnerstwa ze środowiskami akademickimi i naukowymi, w ramach którego będą realizowane programy wsparcia (programy stypendialne, studia doktoranckie, studia magisterskie i podyplomowe czy kursy konwersji zawodowej) oferujące możliwość realizacji projektów na rzecz obronności;
   – wykorzystanie potencjału żołnierzy dobrowolnej zasadniczej służby wojskowej i żołnierzy rezerwy posiadających kwalifikacje z obszaru AI, dostosowując programy ćwiczeń wojskowych w sposób umożliwiający efektywne wykorzystanie ich doświadczenia i wiedzy;

4) w zakresie weryfikacji i rozwoju kompetencji operatorów systemów AI:

   – ustanowienie transparentnych i podlegających kontroli procesów licencjonowania i certyfikacji wojskowych operatorów systemów AI;
   – włączenie aspektów wykorzystania AI i realizacji zadań w ramach HMT do programów szkoleniowych i ćwiczeń wojskowych;

5) w zakresie zapewnienia wymaganej wiedzy wśród kadry kierowniczej:

   – przygotowanie szkoleń dla kadry kierowniczej na wszystkich poziomach decyzyjnych obejmujących prezentacje możliwych do uzyskania korzyści i zagrożeń wynikających z wdrożenia i wykorzystania AI,
   – stworzenie systemu przeznaczonego do wymiany doświadczeń i najlepszych praktyk,

- dostosowanie obowiązujących procedur i procesów podejmowania decyzji celem zapewnienia kierownictwu uprawnień wymaganych do wykorzystywania potencjału sztucznej inteligencji.

Kierunek interwencji: dostosowanie infrastruktury teleinformatycznej

Zapewnienie skalowalnej mocy obliczeniowej oraz wydajnej i bezpiecznej infrastruktury sieciowej ma kluczowe znaczenie dla efektywnego wykorzystania AI, ponieważ umożliwia niezakłócony przepływ danych między sensorami, systemami, decydentami i efektorami. Hosting w chmurze jest niezbędny do zapewnienia skalowalnej mocy obliczeniowej potrzebnej modelom sztucznej inteligencji. Z uwagi na to, że operacyjne wykorzystanie AI będzie się często opierać na danych wrażliwych, konieczne jest ustanowienie skutecznej metody przesyłania danych o różnej klasyfikacji.

Wykorzystanie zaawansowanych sensorów, rozwiązań sprzętowych nowej generacji i nowatorskie podejście do przetwarzania brzegowego będą miały kluczowe znaczenie dla zastosowania sztucznej inteligencji w działaniach obronnych, w tym zapewnienia możliwości prowadzenia działań w trudnych warunkach braku komunikacji lub jej zakłócenia. Uzasadnia to inwestycje w prace badawczo-rozwojowe oraz rozwijanie partnerstw i współpracy między podmiotami rządowymi, środowiskami naukowymi i przemysłem podczas opracowywania i wdrażania sprzętu nowej generacji.

Resort planuje zapewnienie szerszego dostępu do posiadanych niszowych zdolności, w tym infrastruktury testowej, dla partnerów ze środowisk akademickich i naukowych oraz przemysłu, korzystając z doświadczeń podobnych inicjatyw rządowych.

Mając powyższe na uwadze, podjęte zostaną m.in. następujące działania:

- analiza potrzeb w zakresie dostosowania infrastruktury teleinformatycznej celem spełnienia niezbędnych standardów dla implementacji sztucznej inteligencji;
- wykorzystanie sojuszniczych doświadczeń w zakresie transformacji cyfrowej;
- opracowanie zasad bezpieczeństwa w zakresie przetwarzania danych w środowiskach chmurowych/rozproszonych;
- zapewnienie odpowiednich zasobów, w tym finansowych, celem modernizacji infrastruktury teleinformatycznej zgodnie z przyjętymi dokumentami kierunkowymi;
- zapewnienie niezbędnej mocy obliczeniowej oraz implementacja rozwiązań chmurowych.

Kierunek interwencji: zapewnienie dostępu do zaufanych i zweryfikowanych danych

Pomimo że w dobie transformacji cyfrowej dane uznaje się za zasób o strategicznym znaczeniu, bywają one często niewłaściwie zarządzane, niedoceniane lub nawet odrzucane. Dlatego Resort przeprowadzi przegląd polityk, procedur i posiadanych zdolności w zakresie przetwarzania danych. Transformacja Resortu w organizację opartą na danych zakłada rezygnację z izolowanych magazynów danych oraz ustanowienie wspólnej architektury, standardów, etykietowania i platform ich wykorzystania. Wymagane jest również zapewnianie stosownego dostępu do zintegrowanych, wyselekcjonowanych i zweryfikowanych danych w Resorcie.

W ramach zacieśniania współpracy z deweloperami AI (przemysłem i nauką) zostaną zbadane możliwości udostępnienia im wybranych zbiorów danych. Zapewnienie dostępu do wyselekcjonowanych zasobów o wysokiej jakości, wymaganych do trenowania i dostrajania

algorytmów AI, będzie jednym z kluczowych elementów współpracy Resortu z partnerami krajowymi w obszarze sztucznej inteligencji. Należy przy tym uwzględnić fakt, że część posiadanych unikalnych, wielkoskalowych zbiorów danych obejmuje informacje pozbawione pożądanego kontekstu operacyjnego. Mogą być one również niewłaściwie zorganizowane lub posiadać wysokie klauzule niejawności, co ogranicza możliwość ich wykorzystania do trenowania algorytmów oraz opracowywania innowacyjnych aplikacji. W przypadku danych wrażliwych rozwiązaniem może być zastosowanie technik anonimizacji dla zwiększenia ich ochrony. Dlatego Resort przeprowadzi analizę możliwości opracowania i udostępniania reprezentatywnych, syntetycznych zestawów danych w ramach współpracy z partnerami z przemysłu oraz środowisk akademickich i naukowych.

Mając powyższe na uwadze, podjęte zostaną m.in. następujące działania:

- opracowanie strategii wykorzystania danych poprzez identyfikację zasobów o kluczowym znaczeniu dla uzyskania przewagi lub zwiększenia efektywności użycia sił i określenie sposobu ich pozyskania;
- analiza możliwości udostępnienia wybranych danych w ramach Resortu celem eksperymentowania i zapewnienia interoperacyjności;
- określenie procesów i sposobów pracy z danymi (w tym szablonów, formatów i standardów) w celu wygenerowania ustrukturyzowanych rejestrów danych, które można skutecznie wykorzystać na dalszych etapach przetwarzania;
- wprowadzenie protokołów zapewnienia wiarygodności i integralności zbiorów danych, w tym uzyskanych z zewnętrznych źródeł (również otwartych), co ograniczy ryzyko ich zafałszowania;
- przegląd porozumień w zakresie udostępniania danych dla sojuszników, przemysłu oraz środowisk akademickich i naukowych, a także analiza możliwości usprawnienia obowiązujących w tym zakresie procedur oraz wprowadzenia środków zapewniających Resortowi dostęp do danych znajdujących się w posiadaniu partnerów lub przez nich generowanych;
- opracowanie protokołów bezpieczeństwa celem skuteczniejszej ochrony zasobów przed atakami i manipulacjami, w tym poprzez odpowiednie mechanizmy odtajniania i wydawania pozwoleń, które będą sprzyjać udostępnianiu danych dla deweloperów AI realizujących projekty na rzecz obronności.

Kierunek interwencji: dostosowanie przepisów prawa i procedur operacyjnych

Resort dostrzega znaczenie perspektywicznego podejścia do kształtowania prawa, procedur i procesów, aby stworzyć odpowiednie warunki do wdrożenia i wykorzystania pojawiających się zdolności AI w wymaganym czasie. Przykładem potrzeby wprowadzenia odpowiednich rozwiązań może być kwestia delegowania uprawnień do realizacji funkcji C2[11] do systemu AI. Właściwe merytorycznie komórki Resortu przeanalizują obowiązujące regulacje w zakresie prawa, procedur i procesów w aspekcie wykorzystania zdolności AI do zastosowań obronnych oraz podejmą proaktywne kroki celem ich dostosowania.

[11] *Command and Control*.

Mając powyższe na uwadze, podjęte zostaną m.in. następujące działania:

- ustanowienie multidyscyplinarnej grupy zadaniowej do spraw wykorzystania AI w operacjach w celu identyfikacji i przygotowania propozycji odpowiedzi na wyzwania związane z jej użyciem w krajowych lub koalicyjnych operacjach wojskowych,
- nawiązanie współpracy międzyresortowej celem identyfikacji i rozwiązania problematycznych kwestii doktrynalnych i prawnych.

Kierunek interwencji: dostosowanie struktur organizacyjnych

Do zapewnienia odpowiedzialnej i efektywnej implementacji oraz wykorzystania sztucznej inteligencji wymagane jest posiadanie odpowiednich struktur organizacyjnych odpowiedzialnych zarówno za określenie strategicznych ram polityki dotyczącej rozwoju, wdrażania i wykorzystania sztucznej inteligencji, jak i wykonawczych, realizujących zadania w zakresie wspierania rozwoju i wykorzystywania AI w Resorcie, tworzenia warunków do szybkiego rozwoju, dostarczania i skalowania projektów AI i ich koordynacji, a także zapewniania dostępu do danych i usług cyfrowych oraz wiedzy eksperckiej.

Realizowana centralnie i obejmująca cały Resort koordynacja polityki i zarządzanie procesem implementacji AI ma kluczowe znaczenie dla zapewnienia spójności podejmowanych działań oraz interoperacyjności wdrażanych rozwiązań. Ponadto wszystkie jednostki organizacyjne powinny we własnym zakresie podejmować działania w kierunku integracji rozwiązań AI w ramach istniejących struktur i procesów. Podejście polegające na odgórnym ustalaniu polityki i zarządzaniu działalnością oraz oddolnym wprowadzaniem innowacji pozwoli na dostosowanie rozwiązań AI do konkretnych scenariuszy wykorzystania oraz potrzeb jednostek organizacyjnych.

Mając powyższe na uwadze, podjęte zostaną m.in. następujące działania:

- utworzenie w strukturze Ministerstwa Obrony Narodowej, w tym w Sztabie Generalnym WP, dedykowanych komórek wewnętrznych, w odpowiedzialności których będzie znajdowało się definiowanie i nadzór nad przestrzeganiem strategicznych ram polityki w zakresie rozwijania, wdrażania i wykorzystania sztucznej inteligencji, realizacja współpracy międzyresortowej i międzynarodowej oraz zapewnianie ogólnej spójności realizowanych inicjatyw i projektów;
- utworzenie Centrum Implementacji Sztucznej Inteligencji, które będzie pełniło rolę ośrodka kompetencyjnego odpowiedzialnego za realizację prac B+R oraz rozstrzyganie kwestii merytorycznych i technicznych z obszaru AI; do zakresu działania Centrum należeć będzie: (1) wspieranie rozwoju i wykorzystania sztucznej inteligencji w sektorze obronnym, (2) umożliwianie i koordynowanie szybkiego rozwoju, dostarczania i skalowania projektów AI zapewniających osiągnięcie przewagi strategicznej, (3) zapewnienie dostępu do podstawowych usług cyfrowych/danych i źródeł wiedzy specjalistycznej, (4) realizacja współpracy z przemysłem i środowiskami akademickim i naukowym celem zapewnienia synergii podejmowanych wysiłków oraz umożliwienia dwukierunkowego przepływu talentów oraz (5) weryfikowanie przydatności pojawiających się na rynku rozwiązań komercyjnych dla zastosowań wojskowych. Centrum opracuje zestaw niezbędnych dokumentów ukierunkowujących prace związane z implementacją AI w RON, w tym koncepcję implementacji AI, wskazując m.in.: (1) standardy i akceptowalne ryzyka dla różnych kontekstów operacyjnych, (2) metody testowania, oceny, weryfikacji i walidacji

opracowywanych rozwiązań oraz (3) środki ochrony technologii; ponadto będzie kierować tworzeniem nowoczesnego cyfrowego środowiska DevSecOps[12], wspólnych usług i narzędzi oraz zaufanych źródeł danych niezbędnych do budowania prototypów rozwiązań, ich testowania i certyfikacji, a następnie wdrażania w wymaganej skali i czasie;

- utworzenie w jednostkach i komórkach organizacyjnych Resortu, adekwatnie do potrzeb, zespołów zadaniowych AI odpowiedzialnych za określanie potrzeb i kontekstów operacyjnych wykorzystania rozwiązań AI oraz nadzór nad wdrażaniem i eksploatacją systemów AI w całym ich cyklu życia;
- ze względu na specyficzne wymagania dotyczące zapewnienia standardów bezpieczeństwa dla AI w zastosowaniach obronnych – poddanie analizie kwestii utworzenia ośrodka przeznaczonego do testowania i certyfikowania opracowywanych rozwiązań AI oraz HMT dysponującego możliwościami ich sprawdzania zarówno w środowisku fizycznym, jak i środowisku wirtualnym (symulowanym).

[12] *Development Security Operations*.

Cel operacyjny nr 2: skalowalne wdrożenie sztucznej inteligencji

Resort będzie dążyć do odpowiedzialnego, skalowalnego wykorzystania sztucznej inteligencji w obszarze bezpieczeństwa i obronności. Realizując działania na rzecz ustalenia systemowego, skoordynowanego podejścia do wdrożenia systemów sztucznej inteligencji w wymaganej skali i czasie, niezbędne jest ustalenie strategicznych ram polityki dotyczących sztucznej inteligencji w Resorcie, określenie odpowiedzialności podmiotów za nadzorowanie i koordynowanie działań, zapewnienie strategicznej i operacyjnej integracji zdolności w obszarze wszystkich domen operacyjnych, zapewnienie wymaganej infrastruktury teleinformatycznej, środowisk i narzędzi informatycznych oraz proaktywne poszukiwanie rozwiązań odpowiadających potrzebom poszczególnych rodzajów wojsk.

Kierunek interwencji: zbudowanie zaufania do technologii

Zbudowanie zaufania do rozwiązań wykorzystujących AI jest podstawowym warunkiem dla wykorzystania tej technologii na dużą skalę. Aby to osiągnąć, należy dążyć do sytuacji, w której: (1) ludzie dysponują odpowiednim przeszkoleniem, wiedzą i doświadczeniem, (2) rozwój technologii następuje w sposób odpowiedzialny i zgodnie z przyjętymi zasadami i normami[13], (3) rozwiązania wykorzystujące AI są właściwie przetestowane i dopuszczone do wykorzystania oraz stale monitorowane w całym cyklu ich życia.

W porównaniu z tradycyjnymi rozwiązaniami systemy AI stwarzają odmienne wyzwania w zakresie testowania i zapewniania bezpieczeństwa. Wynika to między innymi z faktu, że wyjaśnienie podstaw decyzji podejmowanych przez system AI może być trudne technicznie. Dlatego należy dążyć do równoważenia ryzyk i możliwych do osiągnięcia korzyści, dostarczając bezpieczne, efektywne i odporne na cyberataki zdolności AI w czasie odpowiadającym potrzebom Resortu.

Mając powyższe na uwadze, podjęte zostaną m.in. następujące działania:

- we współpracy z partnerami – opracowanie innowacyjnego podejścia do testowania, weryfikacji i walidacji systemów AI poprzez rozwijanie bezpiecznych i wiarygodnych zdolności do realizacji testów w środowisku rzeczywistym i wirtualnym (w tym w oparciu o modele cyfrowe i symulacje);
- ustalenie kompleksowych ram testowania, zabezpieczania i certyfikacji systemów AI w odniesieniu do ludzkich i technicznych komponentów HMT; metody zarządzania ryzykiem związanym ze sztuczną inteligencją będą oparte na zasadach i mechanizmach przyjętych dla systemów o krytycznym znaczeniu dla bezpieczeństwa; obejmie to realizację testów i sprawdzeń w całym okresie eksploatacji systemów z uwzględnieniem faktu, że AI będzie się nadal uczyć i dostosowywać swoje działanie do zmieniających się okoliczności i warunków również po wdrożeniu do użycia;
- podjęcie współpracy z innymi resortami, organami legislacyjnymi i standaryzacyjnymi, przemysłem, środowiskami akademickimi i partnerami międzynarodowymi celem wprowadzenia elastycznych, a jednocześnie zapewniających bezpieczeństwo

[13] Zgodnie z prawem krajowym i międzynarodowym oraz dokumentami kierunkowymi takimi jak: *NATO's Artifical Intellicence Strategy, Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy* czy *EU Artificial Intelligence Act*.

standardów technicznych, zasad i przepisów dotyczących projektowania, rozwoju, eksploatacji i wycofywania systemów sztucznej inteligencji.

Kierunek interwencji: promowanie innowacyjności, rozwoju koncepcji i eksperymentowania

Promowanie kultury innowacyjności oraz rozwoju koncepcji i eksperymentowania jest istotne, aby umożliwić wdrożenie nowych technologii, w tym sztucznej inteligencji, w wymaganym czasie. Należy przy tym przyjąć, że integracja AI z systemami fizycznymi lub cyfrowymi jest procesem równie skomplikowanym i wymagającym jak rozwijanie samej technologii. Co istotne, przy opracowywaniu nowych zdolności należy odejść od rozwijania technologii w izolacji i uwzględnić szerszy kontekst środowiskowy (operacyjny).

W związku z powyższym podjęte zostaną m.in. następujące działania:

- wspieranie budowania wiedzy przez eksperymentowanie z wykorzystaniem stosunkowo nieskomplikowanych projektów AI celem zapewnienia szybkich korzyści na zasadzie ewolucji dostępnych rozwiązań;
- wdrażanie kultury systematycznego rozwoju koncepcji i eksperymentowania oraz testowania zdolności, opracowywania dokumentów standaryzacji operacyjnej, jak również zwiększania zdolności do wprowadzania innowacji w wymaganym czasie;
- opracowywanie systemów AI przy zaangażowaniu zespołów składających się z użytkowników operacyjnych, programistów oraz zamawiających podczas całego procesu projektowania i rozwoju rozwiązania;
- zapewnienie realizacji badań i rozwoju technologii oraz programów pozyskiwania rozwiązań zgodnie z przyjętymi strategiami uwzględniającymi również późniejsze potrzeby w zakresie pozyskiwania sprzętu i usług oraz prowadzenia działań operacyjnych;
- stosowanie nowatorskich zdolności modelowania i symulacji (np. cyfrowy bliźniak) oraz podejścia DevSecOps celem przyśpieszenia realizacji rozwoju i dostarczania nowych algorytmów i zdolności wykorzystujących AI;
- zapewnianie odpowiedzialnego podejścia do rozwoju algorytmów i systemów AI z dbałością o bezpieczeństwo i niezawodność rozwiązań oraz respektowanie norm etycznych w działalności innowacyjnej;
- uruchamianie konkursów skierowanych do przedstawicieli świata nauki i przemysłu propagujących prace nad rozwiązaniami podwójnego zastosowania.

Kierunek interwencji: wdrażanie zdolności AI

Wiele korzyści dotyczących zwiększenia efektywności i produktywności Resortu może zostać osiągniętych dzięki systematycznemu rozwijaniu oraz wdrażaniu aktualnie dostępnych, dojrzałych rozwiązań technologicznych. Możliwości w tym obszarze dotyczą wykorzystania analizy danych, uczenia maszynowego i zaawansowanych technik statystyki obliczeniowej do wsparcia działalności administracyjnej, usprawnienia procesów logistycznych i działalności rozpoznawczo-wywiadowczej.

Mając powyższe na uwadze, podjęte zostaną m.in. następujące działania:

- identyfikowanie przez jednostki organizacyjne i zarządzających systemami funkcjonalnymi nowych projektów badawczo-rozwojowych spełniających ich potrzeby;

- nadanie priorytetu dla wdrażania sprawdzonych w sektorze prywatnym metod postępowania, współpracy partnerskiej w celu zbierania doświadczeń i przejmowania najlepszych praktyk oraz wykorzystywania technologii COTS[14], zapewniając ścisłą współpracę w ramach krajowego ekosystemu sztucznej inteligencji;
- zapewnienie ogólnej spójności programowej realizowanych działań na szczeblu centralnym;
- powierzenie identyfikacji produktów i rozwiązań potrzebnych do osiągnięcia pożądanych celów strategicznych lokalnym zespołom zadaniowym.

Dodatkowo Resort będzie inwestować w przygotowanie rozwiązań przyszłościowych, tj. badania i rozwój przełomowych rozwiązań AI stanowiących odpowiedź na wyzwania długofalowe, dążąc do uzyskania przewagi podczas prowadzenia operacji wojskowych. Uwzględniając podwyższone ryzyko (techniczne i polityczne) związane z dostarczaniem przełomowych zdolności operacyjnych, działania te będą realizowane centralnie, w ramach resortowych projektów badawczo-rozwojowych z obszarów bezpieczeństwa i obronności. Ważnym elementem tej działalności pozostaje zapewnienie zdolności do szybkiego opracowywania, testowania, integrowania i wdrażania powstałych systemów.

Celem przyśpieszenia wdrożenia przyszłościowych technologii AI podjęte zostaną m.in. następujące działania:

- monitorowanie programów badawczo-rozwojowych oraz prowadzenie oceny i weryfikacji technologii i zagrożeń w odniesieniu do projektów realizowanych w środowisku akademickim oraz przez kluczowych deweloperów;
- zapewnienie ścisłej współpracy między zarządzającymi obszarami funkcjonalnymi a podmiotami prowadzącymi prace badawczo-rozwojowe;
- angażowanie się w ambitne projekty badawcze, co wpłynie stymulująco na inwestycje w badania i rozwój oraz narzuci tempo wdrażania nowych zdolności i koncepcji do Sił Zbrojnych RP;
- realizacja przeglądu wymagań sprzętowych uwzględniająca możliwości implementacji rozwiązań AI w platformach uzbrojenia, sensorach i efektorach.

W celu właściwego ukierunkowania badań i rozwoju systemów AI należy identyfikować scenariusze wymagające nadania priorytetu, takie jak wsparcie procesu decyzyjnego, mobilność wojskowa, wsparcie logistyczne, wsparcie działalności rozpoznawczo-wywiadowczej czy przygotowanie odpowiedzi na działania poniżej progu wojny.

Kierunek interwencji: budowanie wzajemnego zaufania pomiędzy Resortem a partnerami

Podstawą budowania właściwych relacji biznesowych Resortu ze środowiskiem cywilnym, w tym z przemysłem oraz środowiskami akademickimi i naukowymi, jest wzajemne zaufanie. Ważne jest uświadomienie partnerom, że Resort przyjmie bezpieczne i odpowiedzialne podejście do wykorzystania sztucznej inteligencji w odniesieniu do wszystkich rozwiązań opracowywanych oraz wdrażanych w sektorze obronnym.

[14] *Commercial of the Shelf.*

W związku z powyższym podjęte zostaną m.in. następujące działania:

- zapewnienie transparentności w zakresie wykorzystania rozwiązań AI zgodnie z najwyższymi standardami etycznymi i moralnymi oraz obowiązującym prawem;
- zapewnienie deweloperom możliwości zgłaszania uwag i wątpliwości w zakresie wykorzystania opracowanych przez nich rozwiązań oraz uzyskiwania kontekstowych informacji na ich temat;
- informowanie o mechanizmach zapewniających wykorzystywanie rozwiązań AI w sposób odpowiedzialny i bezpieczny (np. dotyczących ich testowania, oceny, weryfikacji i walidacji).

Kierunek interwencji: rozwijanie współpracy w ramach ekosystemu AI

Rozwijanie współpracy w ramach krajowego ekosystemu AI wymaga wszechstronnego zrozumienia wyjątkowego kontekstu i wyzwań związanych z opracowywaniem rozwiązań dla sektora obronnego oraz specyficznych oczekiwań w zakresie odpowiedzialnych innowacji. Dla przykładu wymagania sprzętowe dotyczące zastosowań wojskowych mogą zakładać mniejszą tolerancję ryzyka niż w warunkach komercyjnych, środowiska programistyczne i testowe powinny być bardziej restrykcyjne, a procesy testowania, oceny, weryfikacji i walidacji mogą wymagać uwzględnienia dodatkowych zakłóceń, niewłaściwego użycia lub wrogiej ingerencji.

W związku z powyższym podjęte zostaną m.in. następujące działania:

- ustanowienie szerszej współpracy z interesariuszami z instytucji rządowych, tworząc platformę wymiany informacji na temat wymagań i najlepszych praktyk w kontaktach z przemysłem i środowiskiem akademickim;
- identyfikowanie wspólnych wyzwań stojących przed różnymi sektorami gospodarki i przygotowywanie wspólnych rozwiązań możliwych do wykorzystania w obszarze bezpieczeństwa i obronności;
- zaangażowanie w rozwój technologii podwójnego zastosowania, uzyskując dostęp do rozwiązań komercyjnych;
- badanie możliwości usprawnienia procesów pozyskiwania zdolności, informując jednocześnie potencjalnych dostawców o istniejących ograniczeniach i wymaganiach specjalnych;
- opracowywanie zasad kreowania innowacyjnych rozwiązań w odpowiedzialny sposób we współpracy z ośrodkami akademickimi, naukowymi i przemysłowymi.

Kierunek interwencji: usuwanie barier we współpracy z przemysłem oraz środowiskami akademickimi i naukowymi

Aby umożliwić skuteczne wspieranie krajowego ekosystemu AI, wymagane jest usunięcie barier we współpracy z podmiotami naukowymi i przemysłem, a tym samym pogłębienie partnerstwa we wszystkich aspektach działalności ekosystemu na wszystkich poziomach gotowości technologicznej i w odniesieniu do wszystkich powiązanych technologii. Dotyczy to zwiększenia transparentności w zakresie przedstawiania długoterminowych priorytetów, wczesnego angażowania przemysłu w poszukiwanie rozwiązań dla wymaganych zdolności, zmniejszania barier dla małych i średnich przedsiębiorstw oraz zwiększenia współpracy z partnerami celem przekonania firm do inwestowania w rozwój nowych technologii. Dotyczy to również rozwinięcia współpracy z partnerami z innych resortów, dostawcami oraz

partnerami międzynarodowymi przy jednoczesnym zapewnieniu ochrony własnych zdolności AI o krytycznym znaczeniu oraz własności intelektualnej.

Mając powyższe na uwadze, podjęte zostaną m.in. następujące działania:

- poszukiwanie metod realizacji szybszego pozyskiwania najnowocześniejszych technologii w ramach istniejącego kompleksowego systemu pozyskiwania;
- identyfikowanie wyzwań stojących przed mniejszymi dostawcami celem usunięcia przeszkód uniemożliwiających firmom eksperckim wejście do resortowego łańcucha dostaw;
- stworzenie mechanizmów szybkiego uruchamiania testów wybranych rozwiązań AI w Resorcie, usprawnienie procesu podejmowania decyzji o ich wdrożeniu w przypadku powodzenia testów oraz ustanowienie programów finansowania dalszego rozwoju.

Kierunek interwencji: rozwijanie współpracy z krajowymi instytucjami rządowymi

Sztuczna inteligencja zmieni krajobraz gospodarczy Polski, co będzie wymagało wysiłku całego społeczeństwa i rządu. Rząd określił swoje cele dotyczące sztucznej inteligencji w różnych perspektywach czasowych w *Polityce dla rozwoju sztucznej inteligencji w Polsce od roku 2020*. Dokument ten nie obejmuje działań państwa w obszarze bezpieczeństwa i obrony narodowej, jednak zakłada współpracę sektora cywilnego z wojskowym w obszarach użytecznych dla potrzeb obronności państwa zgodnie z priorytetami określonymi w *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*. Współpraca Resortu z partnerami rządowymi będzie dotyczyć zwiększenia spójności i wykorzystania synergii w krajowym ekosystemie sztucznej inteligencji oraz maksymalizacji potencjalnych zysków z inwestycji w sektorze obronnym, a także identyfikowania możliwości ich wykorzystania do zastosowań wojskowych i cywilnych.

W związku z powyższym podjęte zostaną m.in. następujące działania:

- identyfikowanie możliwości dzielenia się obciążeniami i realizacji współpracy z innymi ministerstwami w celu opracowywania oraz wykorzystywania nowych rozwiązań AI, w tym poprzez określenie wspólnych priorytetów w zakresie rozwoju zdolności;
- rozwijanie współpracy w zakresie wspólnego tworzenia i udoskonalania rozwiązań AI z partnerami z innych resortów, przemysłu oraz nauki, celem stopniowego budowania zdolności;
- wspieranie inicjatyw międzyresortowych zmierzających do wzmocnienia ochrony technologii i kształtowania globalnych systemów regulacyjnych oraz przeciwdziałania proliferacji niebezpiecznych technologii.

Kierunek interwencji: rozwijanie współpracy międzynarodowej

Współpraca z sojusznikami i partnerami międzynarodowymi umożliwia szybkie rozwinięcie technologii AI. Stąd istotne jest zapewnienie na forach międzynarodowych: (1) wymiany informacji, doświadczeń i najlepszych praktyk, (2) wspieranie wymiany talentów, (3) realizacja wspólnych projektów w odpowiedzi na powszechne wyzwania oraz (4) współdzielenie obciążeń utrzymania niszowych, ale niezbędnych zdolności do rozwoju i testowania sztucznej inteligencji. Należy przy tym zadbać o kwestie interoperacyjności, aby umożliwić wykorzystanie i współpracę systemów opartych na AI w ramach koalicyjnych operacji wojskowych oraz zapewnić komplementarność procesów i wymagany poziom zaufania.

NATO pozostaje najważniejszym sojuszem strategicznym i będzie kluczowym forum do konsultacji z krajami członkowskimi w sprawie sztucznej inteligencji i innych pojawiających się technologii. Strategia NATO w zakresie sztucznej inteligencji (2024) określa, w jaki sposób Sojusz będzie podchodzić do kluczowych kwestii związanych z AI, takich jak przyjęcie wspólnych standardów i zasad wykorzystania zdolności czy zapewniania interoperacyjności. Obejmuje to rozwój kompetencji i programów stypendialnych oraz ustanowienie sieci centrów testowania sztucznej inteligencji (wspólnych ośrodków, w których instytucje NATO i państwa członkowskie mogą współpracować w celu wspólnego opracowywania i testowania odpowiednich zastosowań sztucznej inteligencji wraz z partnerami z sektora prywatnego i akademickiego).

W stosunkach bilateralnych należy dążyć do jak najszerszej współpracy ze Stanami Zjednoczonymi Ameryki jako liderem w zakresie prac nad sztuczną inteligencją i naszym najważniejszym partnerem zagranicznym. Stanowić to będzie najwyższy priorytet w zakresie współpracy badawczo-rozwojowej i budowania zdolności w obszarze sztucznej inteligencji. Dodatkowo, dostrzegając potencjał do uzyskania wzajemnych korzyści z realizacji zbieżnych celów, prowadzone będą rozmowy i współpraca z partnerami europejskimi. Priorytetowo w tym zakresie będą traktowane kontakty z Wielką Brytanią, Francją i Niemcami, które ogłosiły ambitne plany przekształcenia się w światowych liderów w zakresie sztucznej inteligencji.

Utworzenie w Resorcie jednostek/komórek organizacyjnych przeznaczonych do prac w obszarze sztucznej inteligencji pozwoli na efektywniejsze prowadzenie współpracy międzynarodowej, w tym z amerykańskim Chief Digital and AI Office (CDAO[15]) oraz brytyjskimi Defence AI and Autonomy Unit (DAU[16]) i Defence AI Centre (DAIC[17]), przygotowując odpowiedzi na wspólne wyzwania dotyczące rozwoju zdolności.

[15] CDAO – biuro odpowiedzialne za przyśpieszenie prac Departamentu Obrony USA w zakresie wykorzystania danych, analityki i sztucznej inteligencji do stworzenia przewagi decyzyjnej na każdym poziomie prowadzenia działań

[16] DAU – jednostka odpowiedzialna za ustanowienie strategiczne ramy polityki regulującej rozwój, wdrażanie i wykorzystanie sztucznej inteligencji.

[17] DIAC – stanowi centralny punkt zajmujący się badaniami i rozwojem sztucznej inteligencji oraz kwestiami technicznymi.

Cel operacyjny nr 3: ochrona strategicznych zasobów i rozwiązań

Adwersarze będą dążyć do skompromitowania systemów sztucznej inteligencji, osłabienia ich efektywności oraz podważenia zaufania użytkowników końcowych i opinii publicznej do ich skuteczności i wiarygodności, używając środków cyfrowych i fizycznych. Mogą również wykorzystywać własne zdolności AI do atakowania systemów niewspieranych przez tę technologię.

Ekosystem sztucznej inteligencji jest napędzany przez otwarty transfer wiedzy, informacji i danych, szczególnie w środowiskach akademickich. Otwartość jest elementem wspierającym napływ inwestycji krajowych i zagranicznych, które mogą zmienić naukowe i technologiczne podejście do produktów, rozwiązań i usług. Ta otwartość jest jednak coraz częściej wykorzystywana przez przeciwników dla osiągnięcia korzyści gospodarczych i militarnych. Ich aktywności obejmują ingerencję w działania ośrodków akademickich, penetrację wrażliwych obszarów badawczych, nabywanie lub kontrolowanie strategicznych firm technologicznych, co powoduje ryzyko transferu i rozprzestrzeniania technologii, kradzieży własności intelektualnej, manipulowania i stosowania inżynierii wstecznej.

Kierunek interwencji: ochrona systemów AI i krytycznych technologii

W ramach ochrony systemów i technologii Resort będzie oceniać i ograniczać podatności na zagrożenia wykorzystywanych systemów AI oraz zbiorów danych, które je zasilają. Konieczne stanie się uodpornienie systemów sztucznej inteligencji na cyberataki i inne ingerencje poprzez eliminowanie luk w zabezpieczeniach danych, systemów cyfrowych i informacyjnych. W ramach powyższego zostaną opracowane i rozwinięte metody zapewnienia bezpieczeństwa zdolnościom AI ze zwróceniem uwagi na potencjalne konsekwencje ich wykorzystania w wielodomenowym środowisku operacji.

Skuteczna ochrona technologii ma kluczowe znaczenie dla zapewnienia przewagi wojskowej, ochrony własności intelektualnej oraz wypełnienia zobowiązań w zakresie zapobiegania proliferacji produktów, oprogramowania i technologii wojskowych oraz rozwiązań podwójnego zastosowania. Jest to istotne wyzwanie ze względu na potencjalny brak świadomości istniejących ryzyk w sektorze badawczo-rozwojowym, które szybko ewoluują wraz z dojrzewaniem nowych technologii.

W związku z powyższym podjęte zostaną m.in. następujące działania:

- identyfikacja mocnych i słabych stron posiadanych technologii (w tym zależności sprzętowych) oraz określenie ich komponentów o krytycznym znaczeniu celem zagwarantowania do nich dostępu i nadania priorytetu dla współpracy z sojusznikami i partnerami;
- ustalenie rygorystycznych środków bezpieczeństwa w zakresie nabywania produktów, usług i technologii AI;
- interweniowanie w celu zapewnienia wsparcia i ochrony strategicznie ważnych firm i zdolności przed inwestycjami zagranicznymi, zgodnie z interesem narodowym;
- wdrożenie mechanizmów ochrony technologii oraz kontroli jej rozpowszechniania.

Kierunek interwencji: przeciwdziałanie rozpowszechnianiu AI i kontrola zbrojeń

Wdrożenie sztucznej inteligencji ma potencjał do zaburzenia równowagi sił między państwami w ujęciu globalnym lub regionalnym. Stąd potrzeba ograniczenia niekontrolowanego rozprzestrzeniania się strategicznych lub wrażliwych technologii. Szczególne zaniepokojenie wzbudza celowy transfer technologii do podmiotów niepaństwowych lub podmiotów pośredniczących. Dlatego konieczna jest współpraca z sojusznikami i partnerami, aby przeciwdziałać i niwelować potencjalnie destabilizujące skutki rozprzestrzeniania się sztucznej inteligencji. W tym względzie należy zauważyć potrzebę dostosowania systemu kontroli proliferacji nowych technologii, aby ograniczyć dostęp do aplikacji AI „klasy wojskowej".

W związku z powyższym podjęte zostaną m.in. następujące działania:

- ciągłe monitorowanie trendów technologicznych i przygotowywanie się na zagrożenia związane z rozwojem technologii podwójnego zastosowania oraz wyzwania w zakresie przeciwdziałania proliferacji technologii wrażliwych i kontroli zbrojeń;
- ograniczenie przepływu komponentów, sprzętu i danych, które znacząco zwiększają zdolności;
- rozwijanie współpracy z partnerami międzynarodowymi w celu stworzenia środków zapobiegania rozprzestrzenianiu się lub niewłaściwemu wykorzystywaniu AI;
- wzmocnienie systemu kontroli proliferacji technologii; należy dostosować i wzmocnić istniejące systemy kontroli proliferacji technologii, aby ograniczyć dostęp do systemów AI „klasy wojskowej"; może to obejmować przegląd i aktualizację obowiązujących regulacji oraz wprowadzenie nowych przepisów, które będą skutecznie kontrolować rozwój i dystrybucje zaawansowanych technologii AI.

Rekomendacje

Aby przygotować Resort do odpowiedzialnego i efektywnego wdrożenia oraz wykorzystania rozwiązań opartych na sztucznej inteligencji, konieczne jest ustanowienie systemowego, spójnego podejścia do realizowanych przedsięwzięć. Co istotne, przełomowy charakter oraz zasięg możliwych aplikacji AI uzasadnia utworzenie dedykowanych struktur zarządczych i wykonawczych celem zapewnienia właściwego planowania, nadzorowania, korelowania oraz realizacji podejmowanych inicjatyw i projektów. Dodatkowo konieczne jest dostrzeżenie szerszego kontekstu działań podejmowanych w obszarze sztucznej inteligencji jako integralnego elementu transformacji cyfrowej.

W związku z powyższym rekomenduje się niezwłoczne podjęcie działań w kierunku opracowania dokumentów kierunkowych (koncepcji, planów etc.) dotyczących transformacji cyfrowej oraz zarządzania danymi i ich wykorzystaniem.

Ponadto rekomenduje się podjęcie działań w kierunku:

- określenia potrzeb dotyczących zapewnienia wiedzy i kompetencji wymaganych do rozwoju i wykorzystania systemów AI w zakresie rekrutacji i szkolenia kadr;
- dokonania przeglądu potrzeb i wymagań dotyczących implementacji AI w zdolnościach sił zbrojnych;
- określenia potrzeb w zakresie rewizji regulacji prawnych oraz obowiązujących w Resorcie polityk, procesów i procedur (w tym w zakresie pozyskiwania sprzętu i usług);
- zdefiniowania potrzeb w zakresie rozwoju resortowej infrastruktury cyfrowej;
- dokonania analizy stanu prawnego, procedur i procesów w aspekcie wykorzystania systemów AI w zastosowaniach wojskowych;
- utworzenia dedykowanych dla obszaru sztucznej inteligencji struktur organizacyjnych.

Do niniejszej Strategii opracowany zostanie dokument wykonawczy (koncepcja) zawierający harmonogram realizacji działań oraz określający kamienie milowe i wskaźniki efektywności.

Należy przyjąć, że niniejsza Strategia będzie podlegała okresowym rewizjom i aktualizacjom, nie rzadziej niż raz na trzy lata lub częściej według potrzeb.