The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Cybersecurity and Law

2026 Nr 1 (15)

DOI: 10.35467/cal/243740

Wykorzystanie sztucznej inteligencji do zapewnienia odporności strategicznej państwa

Using Artificial Intelligence to Ensure the State's Strategic Resilience

Mirosław KARPIUK
Uniwersytet Warmińsko-Mazurski w Olsztynie
ORCID: 0000-0001-7012-8999
E-mail: miroslaw.karpiuk@uwm.edu.pl

Streszczenie

Sztuczna inteligencja znajduje zastosowanie w wielu sferach życia publicznego i prywatnego, w tym ma również wpływ na bezpieczeństwo. Może ona zarówno zabezpieczać przed zagrożeniem, jak i je generować. Duże znaczenie należy jej przypisać również w przypadku budowy i utrzymania odporności strategicznej państwa. Można korzystać z systemów sztucznej inteligencji w każdej fazie związanej z zapewnieniem odporności strategicznej, zarówno w przypadku przewidywania zagrożeń, podejmowania decyzji, przeciwdziałania, usuwania skutków, odbudowy, formułowania wniosków na przyszłość. Sztuczna inteligencja powinna być zatem nieodłącznym elementem działań mających na celu zapewnienie odporności strategicznej państwa. Musi być ona jednak pod nadzorem człowieka, jej działania nie mogą być zatem autonomiczne.

Słowa kluczowe

bezpieczeństwo, sztuczna inteligencja, odporność państwa, odporność społeczna

Abstract

Artificial intelligence is used in many areas of public and private life, including security. It can both protect against and generate threats. It also plays a significant role in building and maintaining a state's strategic resilience. Artificial intelligence systems can be used in every phase of ensuring strategic resilience, including threat prediction, decision making, countermeasures, mitigation, reconstruction, and drawing conclusions for the future. Therefore, artificial intelligence should be an integral part of efforts to ensure a state's strategic resilience. However, it must be under human supervision; therefore, its actions cannot be autonomous.

Keywords

security, artificial intelligence, state resilience, social resilience

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Artykuł został napisany w ramach międzynarodowych badań naukowych: „Społeczeństwa syntetyczne w symulacji strategicznej: francusko-polska analiza odporności strategicznej", zaplanowanych na lata 2026/2027.

Wstęp

Odporność strategiczna państwa to gotowość podmiotów publicznych i społeczeństwa do przeciwdziałania zagrożeniom, walki z nimi, a także usuwania ich skutków i podejmowania działań naprawczych. To zdolność do przetrwania i przywracania normalnego funkcjonowania państwa. Budowa odporności strategicznej to też przygotowanie gospodarki do działania w trudnych warunkach. Zapewnienie odporności nie jest zatem tylko zadaniem struktur rządowych, wymaga również nakładu pracy przedsiębiorców, a także inicjatywy oddolnej – samych obywateli oraz organizacji pozarządowych, jak też zaangażowania samorządu terytorialnego, w tym przede wszystkim lokalnego. Zapewnienie tej odporności nie może odbywać się w oderwaniu od rozwoju technologicznego, zwłaszcza z pominięciem sztucznej inteligencji.

Integracja narzędzi opartych na sztucznej inteligencji z systemami bezpieczeństwa cyfrowego stanowi istotny warunek pozwalający na wzmocnienie zdolności państw do odstraszania agresorów w środowisku informacyjnym. Podstawowym mechanizmem tego oddziaływania jest przyspieszenie i automatyzacja procesów wykrywania zagrożeń, zwiększenie dokładności danych cech ataków oraz możliwość skoordynowanego i szybciej uruchamianego reagowania w wielu domenach jednocześnie, począwszy od infrastruktury informatycznej, przez przestrzeń informacyjną, aż po środki o charakterze gospodarczym czy też militarnym[1].

Wykorzystanie sztucznej inteligencji do zapewnienia odporności strategicznej państwa jest obowiązkiem władz publicznych odpowiedzialnych za bezpieczeństwo. Bez korzystania z nowoczesnych rozwiązań technologicznych nie jest możliwe dzisiaj skuteczne odstraszanie przeciwnika, a także przewidywanie ryzyk, które mogą doprowadzić nawet do destabilizacji państwa. W związku z czym może się okazać, że opieszałość we wdrażaniu narzędzi sztucznej inteligencji przez struktury publiczne w obszarze bezpieczeństwa, w tym przede wszystkim przez administrację rządową (w szczególności w sferze militarnej) – będzie nieodpowiednim realizowaniem takiego obowiązku.

Nie należy jednak traktować sztucznej inteligencji jako gwaranta odporności strategicznej państwa, a jako narzędzie (bardzo ważne, aczkolwiek jedne z wielu) wzmacniania zdolności państwa do reakcji na zagrożenia i ich odzyskiwania po kryzysie.

Celem artykułu jest dokonanie analizy odporności strategicznej państwa pod kątem wykorzystania do jej zapewnienia sztucznej inteligencji jako narzędzia wspomagającego. Podstawową metodą badawczą wykorzystaną przy pisaniu artykułu jest metoda dogmatyczno-prawna, która posłużyła do analizy aktów prawnych regulujących zagadnienia dotyczące odporności strategicznej i sztucznej inteligencji. Dokonano również przeglądu literatury w celu określenia stanu wiedzy na temat odporności strategicznej.

[1] T. Zieliński, Odstraszanie w cyberprzestrzeni. Rola sztucznej inteligencji w budowaniu odporności, atrybucji i skoordynowanej odpowiedzi między domenami, „Cybersecurity and Law" 2025, nr 1, s. 16.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Odporność strategiczna

Odporność strategiczna państwa obejmuje nie tylko odporność militarną, ale również pozamilitarną w sferze samorządności społecznej, ochrony ludności, infrastruktury krytycznej, zwalczania dezinformacji, zagrożeń hybrydowych, ataków kognitywnych, jak również obrony cywilnej. Jest to odporność, która rozciąga się na wszystkie aspekty obrony oraz ochrony państwa i jego obywateli[2].

Częścią odporności strategicznej państwa jest odporność społeczna. Oznacza ona zdolność społeczeństwa oraz instytucji do reagowania, współdziałania, adaptacji, jak również odbudowy w przypadku kryzysów i długofalowych wyzwań. W praktyce jest ona w dużej mierze tworzona oddolnie przez podmioty (w tym mieszkańców) znające lokalne potrzeby i potrafiące działać szybko i skutecznie. Jest to również wzajemne zaufanie i codzienne działanie we własnej społeczności – współpraca, budowanie relacji, znajomość zasobów, stosowanie procedur dostosowanych do lokalnych potrzeb oraz gotowość do zaangażowania się, jeżeli okoliczności tego wymagają[3]. Ustawodawca jako odporność społeczną rozumie indywidualną i grupową zdolność ludzi do zaspokajania swoich podstawowych potrzeb bytowych, w tym dzięki posiadaniu własnych zapasów niezbędnych produktów, a także ich zdolność do współdziałania z podmiotami ochrony ludności, jak również do zdobywania kompetencji dotyczących kształtowania świadomości zagrożeń i zapobiegania zagrożeniom oraz pożądanych zachowań na wypadek wystąpienia zagrożeń[4].

Składową odporności strategicznej państwa jest też odporność podmiotów krytycznych, która definiowana jest jako zdolność do zapobiegania incydentowi, ochrony przed incydentem, która jest zapewniana w drodze zaplanowanych działań, z wykorzystaniem posiadanych zasobów, reagowania w przypadku wystąpienia incydentu i jego absorbowania oraz adaptacji i usuwania skutków incydentu, w tym odtwarzania infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej[5]. Odporność ta jest związana z cyberbezpieczeństwem.

Należy jednak pamiętać, że zbyt silne skupienie na odporności może prowadzić do przekonania, że państwo jest nastawione tylko na działania defensywne i tym samym jest niezdolne do odwetu, co może je narażać na powtarzające się działania testujące granice tolerancji. Z perspektywy psychologii strategicznej, przeciwnik może interpretować brak reakcji nie jako wynik skutecznej obrony, ale jako przejaw słabości, bądź też apatii. W związku z powyższym odstraszanie wymaga równoległej komunikacji zdolności ofensywnych i determinacji politycznej, co pozwala uniknąć jednostronnego charakteru sygnału strategicznego[6].

---

[2] A. Podolski, Odporność strategiczna państwa – jak ją budować?, „Pomorski Thinkletter" 2024, nr 4, s. 178.

[3] Odporność społeczna – siła społeczności w sytuacjach kryzysowych, https://www.gov.pl/web/pozytek/odpornosc-spoleczna--sila-spolecznosci-w-sytuacjach-kryzysowych [dostęp: 31.10.2026r.]. W przedmiocie odporności zobacz także Z. Śliwa, S. Wojciechowski, Odstraszanie militarne oraz odporność strategiczna państw w rejonie północno-wschodniej flanki NATO, „Roczniki Nauk Społecznych" 2021, nr 2, s. 75-76.

[4] Art. 3 pkt 6 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r. poz. 1907 ze zm.).

[5] Art. 3 pkt 1d ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. z 2026 r. poz. 574 ze zm.), dalej u.z.k.

[6] T. Zieliński, Odstraszanie…, s. 8.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Odporność strategiczna państwa a sztuczna inteligencja – kontekst europejski

Ambicje Europy dotyczące osiągnięcia niezależności technologicznej w dziedzinie obronności, zmieniły się z długoletniego dążenia w pilny priorytet strategiczny. Wojna Rosji z Ukrainą, powtarzające się zakłócenia w globalnych łańcuchach dostaw, a także rosnąca niepewność co do długoterminowej niezawodności transatlantyckich gwarancji bezpieczeństwa obnażyły strukturalne słabości europejskiej polityki bezpieczeństwa i obrony. W związku z powyższym Unia Europejska została zmuszona do zintensyfikowała działań, których celem jest wzmocnienie własnych innowacji w dziedzinie bezpieczeństwa i obronności, zmniejszenie zależności od zewnętrznych dostawców oraz konsolidacja europejskiej bazy technologiczno-przemysłowej związanej z bezpieczeństwem, zdolnej do utrzymania zdolności wojskowych w warunkach kryzysu. Samowystarczalność obronna UE wymaga, aby przestała ona traktować obronność jako odrębną politykę. Technologie, które wpływają na budowanie przewagi militarnej (sztuczna inteligencja, komputery kwantowe, zaawansowane półprzewodniki, przestrzeń kosmiczna i cyberbezpieczeństwo) są rozwijane w zdecydowanym zakresie w obszarze cywilnym, regulowanym przez ramy przemysłowe i cyfrowe, które od dawna funkcjonują w oderwaniu od planowania obronnego[7].

Dążenie Europy do autonomicznej sztucznej inteligencji w dziedzinie bezpieczeństwa i obrony wynika z przekonania, że kontrola nad technologiami krytycznymi oznacza kontrolę nad własnym bezpieczeństwem. Dzięki znaczącym inwestycjom i nowym formom współpracy Unia Europejska tworzy podstawy obronności oparte na sztucznej inteligencji, niezależnej od supermocarstw technologicznych. Chociaż wyzwania w tym zakresie nadal istnieją, to jednak logika strategiczna jest jasna i według niej aby obronić Europę, europejskie zdolności w zakresie sztucznej inteligencji muszą nadal się rozwijać[8]. Nie mniej jednak należy podkreślić, że w 2024 roku UE celowo wyłączyła sztuczną inteligencję wojskową i bezpieczeństwa z rozporządzenia regulującego kwestie sztucznej inteligencji. Państwa członkowskie – na czele z Francją – nalegały, aby decyzje dotyczące obronności pozostały w ich gestii, co spowodowało, że Europa nie zbudowała żadnego instrumentu do zarządzania własną sztuczną inteligencją wojskową. Kiedy Stany Zjednoczone podejmują działania w tym obszarze, instytucje europejskie bardziej są obserwatorami, niż stronami[9].

Niniejsze rozporządzenie nie ma zastosowania do obszarów wykraczających poza zakres prawa Unii i w żadnym wypadku nie narusza kompetencji państw członkowskich w zakresie bezpieczeństwa narodowego, niezależnie od rodzaju podmiotu, któremu państwa członkowskie powierzyły wykonywanie zadań związanych z tymi kompetencjami.

Akt o sztucznej inteligencji wyraźnie przewiduje, że nie ma on zastosowania do systemów sztucznej inteligencji, które są wprowadzane do obrotu, oddawane do użytku lub wykorzystywane, z modyfikacjami lub bez – wyłącznie do celów wojskowych,

[7] Strategic Autonomy or Strategic Illusion? Europe's Path to Defence Technological Self-Reliance, https://pppescp.com/2026/03/25/strategic-autonomy-or-atrategic-illusion-europes-path-to-defense-technological-self-reliance/ [dostęp: 1.11.2026r.].

[8] AI for Strategic Autonomy: Europe's Bid for AI Independence, https://europeanrelations.com/ai-for-strategic-autonomy-europes-bid-for-ai-independence/ [dostęp: 1.11.2026r.].

[9] M. Perugini, Europe's ungoverned space: Military AI and the autonomy that cannot be bought, https://cepr.org/voxeu/columns/europes-ungoverned-space-military-ai-and-autonomy-cannot-be-bought?utm_source=chatgpt.com [dostęp: 2.11.2026r.].

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

obronnych lub związanych z bezpieczeństwem narodowym, niezależnie od rodzaju podmiotu wykonującego tego rodzaju działania[10].

Odporność strategiczna państwa a sztuczna inteligencja – kontekst polski

Odporność strategiczna państwa powinna być budowana w oparciu o wszystkie struktury publiczne w nim działające, a zatem zarówno centralne, jak i terenowe. Obok struktur publicznych odporność taką tworzy system ekonomiczno-finansowy oraz społeczeństwo i jego organizacje. Odpowiedzialność za poziom tej odporności spoczywa jednak na władzy publicznej, która musi przygotować państwo i społeczeństwo do działania w warunkach kryzysu i wojny.

Sztuczna inteligencja może zabezpieczać działanie infrastruktury krytycznej, która ma bardzo ważne znaczenie dla budowy odporności strategicznej. Może ona wspomagać systemy monitorowania i zarządzania taką infrastrukturą. Dzięki analizie danych dokonywanej przez systemy sztucznej inteligencji można wykrywać awarie, przewidywać potencjalne problemy i podejmować szybkie działania naprawcze. Ochrona infrastruktury krytycznej realizowana z wykorzystaniem sztucznej inteligencji ma znaczący wpływ na zapewnienie bezpieczeństwa i niezawodności systemów, które są bardzo ważne dla funkcjonowania państwa i społeczeństwa. Algorytmy sztucznej inteligencji powinny nie tylko przewidywać wystąpienie awarii, ale też ostrzegać przed potencjalnymi ryzykami, automatycznie wykrywać incydenty cyberbezpieczeństwa, klasyfikować ich rangę oraz podejmować odpowiednie działania korygujące, co przyspiesza proces reagowania i minimalizuje skutki awarii. Ze względu na optymalizację utrzymania infrastruktury krytycznej można wykorzystywać sztuczną inteligencję dla analizy danych dotyczących stanu technicznego, zużycia zasobów oraz kosztów konserwacji tej infrastruktury[11].

Ustawodawca w art. 3 pkt 2 u.z.k. infrastrukturę krytyczną definiuje jako obiekt, urządzenie, instalację, sieć, system lub usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy lub usługi konieczne do: 1) realizacji ważnych interesów państwa, w tym zapewnienia funkcjonowania organów administracji publicznej; 2) zapewnienia funkcjonowania przedsiębiorstw; 3) zaspokajania oraz utrzymywania potrzeb obywateli; 4) zapewnienia świadczenia usług kluczowych[12]. Ze względu na fakt, że infrastruktura krytyczna zapewnia nie tylko właściwe funkcjonowanie państwa, ale też pozwala normalnie żyć członkom społeczeństwa, a przede wszystkim zaspokajać elementarne potrzeby człowieka, na państwie ciąży obowiązek jej ochrony[13].

Bezpieczeństwo państwa zależy od odporności jego infrastruktury, a wykorzystanie sztucznej inteligencji może zapewnić skuteczniejszą jej ochronę[14]. Dotyczy to również infrastruktury krytycznej.

---

[10] Art. 2 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji oraz zmieniające rozporządzenia (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt o sztucznej inteligencji) (Dz.Urz.UE L 2024/1689). W przedmiocie sztucznej inteligencji zobacz także T. Gergelewicz, Bipolarity of Artificial Intelligence – Chances and Threats, „Ius et Securitas" 2024, nr 2, s. 71-92,

[11] N. Malec, Sztuczna inteligencja a bezpieczeństwo państwa, „Prawo i Bezpieczeństwo" 2024, nr 1, s. 38-39.

[12] W przedmiocie infrastruktury krytycznej zobacz także K. Kaczmarek, E.M. Włodyka, M. Czuryk, The Status of Government Administration in the Sphere of Crisis Management, „Prawo i Więź" 2025, nr 6, s. 662.

[13] M. Czuryk, Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa, „Ius et Securitas" 2025, nr 1, s. 6.

[14] M. Al Bataharia, R.H. Al. Azrib, Policy Evaluation Using Artificial Intelligence for Enhancing Infrastructure Resilience across National Security Frameworks, „Procedia Computer Science" 2026, nr 275, s. 995.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Należy wskazać, że wraz z dynamicznym wzrostem potencjału sztucznej inteligencji rośnie również skala oraz złożoność zagrożeń z nią związanych i to zarówno w wymiarze technologicznym, jak też operacyjnym, w związku z czym jej stosowanie wymaga stałego monitorowania oraz rozwoju mechanizmów zabezpieczających[15].

O odporności strategicznej państwa decyduje też nowoczesna armia wykorzystująca do swojego działania nowe technologie. W zakresie wdrażania sztucznej inteligencji w Siłach Zbrojnych RP i strukturach bezpieczeństwa można wskazać na następujące problemy: 1) brak jest odpowiednich regulacji prawnych i spójnych ram odpowiedzialności dotyczących wykorzystania algorytmów sztucznej inteligencji w systemach bojowych, w tym brak jednoznacznych zasad dopuszczalności użycia systemów autonomicznych; 2) występuje ograniczona zdolność do neutralizacji zagrożeń związanych z używaniem dronów i bezzałogowych statków powietrznych (UAV), w tym szczególnie systemów wykorzystujących algorytmy uczenia maszynowego do koordynacji działań w rojach; 3) personel wojskowy i administracyjny jest niewystarczająco przygotowany do przeciwdziałania zjawiskom dezinformacji i manipulacji informacyjnej; 4) brak jest kompleksowych procedur testowania, certyfikacji i audytu systemów wykorzystujących sztuczną inteligencję, co obniża poziom zaufania do decyzji wspomaganych przez tego rodzaju algorytmy w środowiskach o znaczeniu strategicznym; 5) mamy do czynienia z niedostatecznym tempem implementacji krajowych strategii i programów rozwoju sztucznej inteligencji – poziom implementacji praktycznych rozwiązań związanych ze sztuczną inteligencją w strukturach MON i przemyśle obronnym jest nadal ograniczony; 6) poziom interoperacyjności jest niewystarczający oraz brak jest jednolitych standardów technicznych, umożliwiających integrację rozwiązań z wykorzystaniem sztucznej inteligencji z systemami dowodzenia, rozpoznania i łączności; 7) nakłady finansowe są ograniczone i zbyt niska jest intensywność współpracy międzynarodowej, szczególnie w obszarze badań nad militarnym zastosowaniem sztucznej inteligencji i zabezpieczenia przed jej nadużyciem w operacjach ofensywnych[16].

Siły Zbrojne RP jako wykwalifikowany instrument obrony państwa potrzebują nowoczesnych technologii, żeby sprostać nie tylko coraz to nowym wyzwaniom, ale też i zagrożeniom. Sztuczna inteligencja jest technologicznym kołem napędowym obecnych czasów, ale jej dwubiegunowość skłania do głębszej refleksji nad dalszym jej rozwojem. Atrakcyjność wykorzystania sztucznej inteligencji jest ściśle związana z jej zdolnością do adaptacji i samouczenia się, możliwościami analitycznymi i predykcyjnymi, które umożliwiają tworzenie zaawansowanych i inteligentnych systemów[17]. W związku z czym jej wykorzystanie w armii jest dzisiaj konieczne dla jej unowocześnienia i tym samym budowy odporności strategiczną całego państwa, które ma ta armia chronić, w tym też przez odstraszanie.

O ważnej pozycji Sił Zbrojnych RP w sferze bezpieczeństwa i tym samym we wzmacnianiu odporności strategicznej państwa świadczy ich status konstytucyjny. Ustrojodawca wyraźnie zastrzega, że Siły Zbrojne RP służą ochronie niepodległości państwa i niepodzielności jego terytorium oraz zapewnieniu bezpieczeństwa

[15] A. Bogdański, Szanse i zagrożenia wykorzystania sztucznej inteligencji w operacjach wielodomenowych, „Cybersecurityy and Law" 2025, nr 2, s. 188.
[16] K. Zdrojewski, Sztuczna inteligencja w operacjach wojskowych – potencjał i ryzyka dla bezpieczeństwa narodowego, „Wiedza Obronna" 2026, nr 1, s. 2-3.
[17] T. Gergelewicz, Wykorzystanie potencjału sztucznej inteligencji w siłach zbrojnych – wywiad z Chatem GPT, „Myśl Strategiczna" 2025, nr 2, s. 6.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

i nienaruszalności jego granic[18]. Cel działania tej formacji wyraźnie wskazuje nie tylko na wysokie miejsce, jakie zajmuje ona w sferze obronności, ale wręcz na jej podstawową rolę w zakresie osiągania i utrzymania odporności strategicznej państwa.

Ważne jest, aby systematycznie monitorować trendy, w tym te, których kierunku obecnie nie jesteśmy w stanie w pełni przewidzieć – takie jak rozwój agentowych systemów sztucznej inteligencji, czy sztucznej inteligencji wspieranej obliczeniami kwantowymi. Tylko takie podejście zapewni Polsce długookresową gotowość do reagowania na innowacyjne rozwiązania technologiczne, które dopiero nadchodzą. W związku ze stałym rozwojem sztucznej inteligencji przed Polską również wiele wyzwań strukturalnych i infrastrukturalnych. Zarówno budowa jak i rozwój przyjaznego ekosystemu sztucznej inteligencji w Polsce wymaga równoczesnego wzrostu inwestycji publicznych, jak i prywatnych w badania, infrastrukturę oraz innowacje[19].

Zakończenie

W związku z potrzebą zapewnienia odporności strategicznej państwa konieczne jest wprowadzenie zmian systemowych, w tym dotyczących systemu kierowania i dowodzenia wspieranego przez sztuczną inteligencję. Bezpieczeństwa nie da się obecnie zapewnić rezygnując z korzystania z nowych technologii wspierających większość procesów zachodzących w tej sferze.

Jednym z ważniejszych zastosowań sztucznej inteligencji może być wczesne ostrzeganie. Jej systemy mogą w krótkim czasie analizować duże zbiory informacji i wskazywać na relacje zachodzące między nimi, co może mieć wpływ na bezpieczeństwo. Analiza ta pozwala na określenie prawdopodobieństwa wystąpienia danych zagrożeń, zatem wspomaga proces decyzyjny, rekomendując np. podjęcie określonych działań wskazując jednocześnie na najbardziej prawdopodobny wariant ataku (nie może samodzielnie stanowić czynnika decyzyjnego).

W związku z koniecznością osiągnięcia odporności strategicznej przez Polskę konieczne są zmiany systemowe, w tym dotyczące prawa, jak też systemu obronnego. Zmianom systemowym powinna jednak równolegle towarzyszyć modernizacja techniczna Sił Zbrojnych RP, obejmująca wszystkie domeny ich funkcjonowania. Zmiany systemowe należy również traktować jako element polityki odstraszania, będący skuteczną manifestacją determinacji związanej z obroną państwa[20].

Zamiast traktować sztuczną inteligencję jako odizolowane narzędzie, należy ją postrzegać jako strategiczny atut zintegrowany z instytucjami i usługami. Zważając na wpływ, jaki może mieć ona na sektor publiczny, a także na obywateli, bardzo ważne jest zapewnienie bezpieczeństwa, a także autonomii operacyjnej i suwerenności w ścisłej współpracy z państwami członkowskimi Unii Europejskiej[21].

W przypadku budowy odporności strategicznej państwa z wykorzystaniem sztucznej inteligencji warto zwrócić uwagę na kompetencje cyfrowe. Należy jednak

[18] Art. 26 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. nr 78, poz. 483 ze zm.). Siły Zbrojne RP są tą częścią aparatu państwa, na którą ustrojodawca nałożył szczególne obowiązki, które są związane z realizacją zadań dotyczących strzeżenia niepodległości i nienaruszalności terytorium państwa oraz bezpieczeństwa obywateli, B. Banaszak, Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warszawa 2009, s. 152.

[19] Strategia Cyfryzacji Państwa stanowiąca załącznik do uchwały nr 130 Rady Ministrów z 9 czerwca 2026 r. w sprawie przyjęcia strategii dotyczącej informatyzacji państwa (M.P. z 2026 r. poz. 620), s. 154.

[20] J. Siewiera, L. Bełza, Prezydencka ustawa strategiczna. Odpowiedź państwa na zagrożenia hybrydowe, podprogowe i konwencjonane, „Bezpieczeństwo Narodowe" 2023, nr 42, s. 30.

[21] Polityka rozwoju sztucznej inteligencji w Polsce do 2030 roku, Warszawa 2025, s. 42.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

zwrócić uwagę na rozdźwięk zachodzący między samooceną umiejętności a rzeczywistym przygotowaniem, co może rodzić ryzyka związane z powierzchownym rozumieniem działania algorytmów i zbyt dużym zaufaniem do ich wyników[22].

Na koniec należy podkreślić, że sztuczna inteligencja stanowi ważny element odporności strategicznej, może ona być wykorzystywana zarówno do wykrywania zagrożenia, dokonania jego oceny, zaproponowania wariantu reakcji na nie, sposobu usunięcia skutków, jak też przywrócenia normalnych funkcji państwa lub poszczególnych jego instytucji, czy ustalenia przyczyn i zaproponowania rozwiązań ochronnych na przyszłość.

Warto też zwrócić uwagę na konieczność nadzoru człowieka nad sztuczną inteligencją, której działanie szczególnie w sferze bezpieczeństwa musi być ciągle monitorowane (nie może funkcjonować autonomicznie), żeby sama nie godziła w odporność państwa.

Bibliografia

Al Bataharia M., Al. Azrib R.H., Policy Evaluation Using Artificial Intelligence for Enhancing Infrastructure Resilience across National Security Frameworks, „Procedia Computer Science" 2026, nr 275.

Banaszak B., Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warszawa 2009.

Bogdański A., Szanse i zagrożenia wykorzystania sztucznej inteligencji w operacjach wielodomenowych, „Cybersecurityy and Law" 2025, nr 2.

Czuryk M., Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa, „Ius et Securitas" 2025, nr 1.

Gałkowski A., Wiedza i kompetencje w fazie rozwoju, [w:] Sztuczna inteligencja w Polsce. Krajobraz pełen paradoksów, Warszawa 2025.

Gergelewicz T., Bipolarity of Artificial Intelligence – Chances and Threats, „Ius et Securitas" 2024, nr 2.

Gergelewicz T., Wykorzystanie potencjału sztucznej inteligencji w siłach zbrojnych – wywiad z Chatem GPT, „Myśl Strategiczna" 2025, nr 2.

Kaczmarek K., Włodyka E.M., Czuryk M., The Status of Government Administration in the Sphere of Crisis Management, „Prawo i Więź" 2025, nr 6.

Malec N., Sztuczna inteligencja a bezpieczeństwo państwa, „Prawo i Bezpieczeństwo" 2024, nr 1.

Perugini M., Europe's ungoverned space: Military AI and the autonomy that cannot be bought, https://cepr.org/voxeu/columns/europes-ungoverned-space-military-ai-and-autonomy-cannot-be-bought?utm_source=chatgpt.com [dostęp: 2.11.2026r.].

Podolski A., Odporność strategiczna państwa – jak ją budować?, „Pomorski Thinkletter" 2024, nr 4.

Polityka rozwoju sztucznej inteligencji w Polsce do 2030 roku, Warszawa 2025.

Siewiera J., Bełza L., Prezydencka ustawa strategiczna. Odpowiedź państwa na zagrożenia hybrydowe, podprogowe i konwencjonalne, „Bezpieczeństwo Narodowe" 2023, nr 42.

Śliwa Z., Wojciechowski S., Odstraszanie militarne oraz odporność strategiczna państw w rejonie północno-wschodniej flanki NATO, „Roczniki Nauk Społecznych" 2021, nr 2.

Zdrojewski K., Sztuczna inteligencja w operacjach wojskowych – potencjał i ryzyka dla bezpieczeństwa narodowego, „Wiedza Obronna" 2026, nr 1.

Zieliński T., Odstraszanie w cyberprzestrzeni. Rola sztucznej inteligencji w budowaniu odporności, atrybucji i skoordynowanej odpowiedzi między domenami, „Cybersecurity and Law" 2025, nr 1.

[22] A. Gałkowski, Wiedza i kompetencje w fazie rozwoju, [w:] Sztuczna inteligencja w Polsce. Krajobraz pełen paradoksów, Warszawa 2025, s. 10.