dr hab. Norbert Malec, prof. UwS
Uniwersytet w Siedlcach
ORCID: 0000-0003-0119-2705

SZTUCZNA INTELIGENCJA A BEZPIECZEŃSTWO PAŃSTWA

ARTIFICIAL INTELLIGENCE AND STATE SECURITY

Streszczenie

Narzędzia oparte na sztucznej inteligencji (SI) w znaczny sposób wpływają na wzmacnianie bezpieczeństwa. Algorytmy SI ułatwiają przetwarzanie ogromnych ilości informacji, zwiększając szybkość i dokładność podejmowania decyzji. Sztuczna inteligencja i uczenie maszynowe (SI/ML) mają kluczowe znaczenie dla państwa w odpieraniu zintegrowanych ataków hybrydowych i nowych zagrożeń w cyberprzestrzeni. Istniejące możliwości w zakresie sztucznej inteligencji mają znaczny potencjał, wpływający na bezpieczeństwo narodowe, poprzez wykorzystanie istniejącej technologii uczenia maszynowego w automatyzacji, w pracochłonnych działaniach, takich jak analiza zdjęć satelitarnych i obrona przed cyberatakami.

Artykuł analizuje wybrane aspekty wpływu sztucznej inteligencji na zwiększenie zdolności państwa do ochrony swoich interesów i jego obywateli. Sztuczna inteligencja poprzez stosowanie sieci neutronowych, analityki predykcyjnej oraz AUM, umożliwia agencjom odpowiedzialnym za bezpieczeństwo, analizowanie ogromnych ilości danych i identyfikowanie wzorców, wskazujących na potencjalne zagrożenia. Integracja sztucznej inteligencji w systemach nadzoru, kontroli granicznej i ocenie zagrożeń, zwiększa zdolność do prewencyjnego reagowania na wyzwania związane z bezpieczeństwem. Ponadto algorytmy sztucznej inteligencji SSI ułatwiają przetwarzanie ogromnych ilości informacji, zwiększając szybkość i dokładność podejmowania decyzji przez organy działające na rzecz zapewnienia bezpieczeństwa.

Szybki rozwój SI skłania do kreowania szeregu pytań, pozwalających na ich stosowanie w zabezpieczeniu nie tylko bezpieczeństwa narodowego ale ochronie wszystkich obywateli. W szczególności warto odpowiedzieć na pytanie: w jaki sposób sztuczna inteligencja wpływa na bezpieczeństwo narodowe oraz wyjaśnić kwestię sposobu wykorzystania sztucznej inteligencji przez organy ścigania, celem osiągnięcia maksymalnych korzyści z nowej technologii w zakresie bezpieczeństwa i ochrony społeczności przed wzrastającą przestępczością. Analiza opiera się na metodzie opisowej zjawiska, poprzez wyjaśnienie koncepcji i zastosowań sztucznej inteligencji, celem określenia jej roli w sferze bezpieczeństwa krajowego.

Podejmowana jest analiza przydatności sztucznej inteligencji w szczególności w działaniach funkcjonariuszy różnych służb, odpowiedzialnych za szeroko rozumiane bezpieczeństwo, której celem jest obrona tezy, że pomimo pewnych zagrożeń dla ochrony praw człowieka ze strony SI, staje się ona najlepszym narzędziem w zwalczaniu wszelkiego rodzaju przestępczości w kraju. Postęp technologiczny w dziedzinie sztucznej inteligencji może mieć również szereg pozytywnych skutków dla egzekwowania prawa, oraz przydatne jest organom ścigania, na przykład w zakresie ułatwiania identyfikacji osób lub pojazdów, przewidywanie trendów w działaniach przestępczych, śledzenie nielegalnych działań przestępczych lub nielegalnych przepływów pieniędzy, flagowania i reagowania na fałszywe wiadomości.

Sztuczna inteligencja pojawiła się jako jedno z największych zagrożeń dla bezpieczeństwa informacji, ale są podejmowane działania celem ograniczenia tego nowego zagrożenia, ale także celem znalezienia rozwiązań w jaki sposób sztuczna inteligencja może stać się sprzymierzeńcem w walce z cyberbezpieczeństwem, przestępczością i zagrożeniami terrorystycznymi. SSI przeszukują ogromne zbiory danych ruchu komunikacyjnego, zdjęć satelitarnych i postów w mediach społecznościowych celem zidentyfikowania potencjalnych zagrożeń cyberbezpieczeństwa, działań terrorystycznych i przestępczości zorganizowanej. Wskazane jest żeby podczas analizy szans i zagrożenia, jakie sztuczna inteligencja stwarza dla bezpieczeństwa narodowego i publicznego, uzyskać strategiczną przewagę w kontekście szybkich zmian technologicznych a także zarządzać wieloma zagrożeniami związanymi z SI. W zakończeniu podkreślono wpływ SI na bezpieczeństwo narodowe, stwarzając szereg nowych możliwości, połączonych jednocześnie z wyzwaniami, na które agencje rządowe powinny być przygotowane w rozwiązywaniu dylematów etycznych, związanych z bezpieczeństwem. Co więcej, sztuczna inteligencja usprawnia analitykę predykcyjną, tym samym umożliwiając agencjom bezpieczeństwa bardziej precyzyjne przewidywanie potencjalnych zagrożeń i zwiększanie ich gotowości poprzez identyfikowanie słabych punktów w infrastrukturze bezpieczeństwa państwa.

Kluczowe słowa: Sztuczna inteligencja, bezpieczeństwo państwa, przestępczość, organy policji

Summary

Technologically advanced artificial intelligence (AI) is making a significant contribution to strengthening national security. AI algorithms facilitate the processing of vast amounts of information, increasing the speed and accuracy of decision-making. Artificial intelligence and machine learning (AI/ML) are crucial for state and integrated hybrid attacks and protecting new threats in cyberspace. Existing AI capabilities have significant potential to impact national security by leveraging existing machine learning technology for automation in labor-intensive activities such as satellite imagery analysis and defense against cyber attacks.

This article examines selected aspects of the impact of artificial intelligence on enhancing a state's ability to protect its interests and its citizens., artificial intelligence through the use of neutron networks, predictive analytics and machine learning algorithms enables security

agencies to analyse vast amounts of data and identify patterns indicative of potential threats. Integrating artificial intelligence into surveillance, border control and threat assessment systems enhances the ability to respond preemptively to security challenges. In addition, artificial intelligence algorithms facilitate the processing of vast amounts of information, increasing the speed and accuracy of decision-making by police authorities.

The rapid development of AI raises a number of questions for its use in securing not only national security but protecting all citizens. In particular, it is worth answering the question How does artificial intelligence affect national security and clarifying the issue of how law enforcement agencies can use artificial intelligence to maximise the benefits of the new technology in terms of security and protecting communities from rising crime. The analysis is based on a descriptive method in describing the phenomenon; by explaining the concepts and applications of artificial intelligence to determine its role in the national security sphere.

An analysis of the usefulness of artificial intelligence in particular in police operations is undertaken, with the aim of defending the thesis that, despite some threats to the protection of human rights from AI, it is becoming the best tool in the fight against all types of crime in the country. Technological advances in AI can also have many positive effects for law enforcement, and useful for law enforcement agencies, for example in facilitating the identification of persons or vehicles, predicting trends in criminal activities, tracking illegal criminal activities or illegal money flows, flagging and responding to fake news.

Artificial intelligence (AI) has emerged as one of the biggest threats to information security, but efforts are being made to mitigate this new threat, but also to find solutions on how AI can become an ally in the fight against cyber-security, crime and terrorist threats. Artificial intelligence algorithms search huge datasets of communication traffic, satellite images and social media posts to identify potential cyber security threats, terrorist activities and organized crime. It is advisable, when analyzing the opportunities and threats that AI poses to national and public security, to gain a strategic advantage in the context of rapid technological change and also to manage the many risks associated with AI. The conclusion highlights the impact of AI on national security, creating a range of new opportunities coupled with challenges that government agencies should be prepared for in addressing ethical and security dilemmas. Furthermore, AI improves predictive analytics, thereby enabling security agencies to more accurately anticipate potential threats and enhance their preparedness by identifying vulnerabilities in the national security infrastructure

Keywords: Artificial intelligence, national security, criminality, police

Wstęp

Sztuczna inteligencja (SI) może przyczyniać się do wielu różnych korzyści społeczno-ekonomicznych we wszystkich obszarach bezpieczeństwa państwa. Rozwiązania bazujące na sztucznej inteligencji umożliwiają lepsze prognozo-

wanie, optymalizację operacji i przydzielania zasobów oraz wspierają wyniki korzystne z punktu widzenia kwestii społecznych w szczególności w zakresie bezpieczeństwa i wymiaru sprawiedliwości. Jednocześnie sztuczna inteligencja może być źródłem ryzyka i szkody dla interesu publicznego oraz przywilejów chronionych ustawodawstwem krajowym, w zależności od okoliczności dotyczących jej konkretnego zastosowania i wykorzystania. Szkody takie mogą być materialne lub niematerialne.

Sztuczna inteligencja oferuje szereg możliwości dla państwa celem poprawy wydajności i skuteczności istniejących procesów. Metody sztucznej inteligencji są w stanie szybko wyciągać wnioski z dużych, odmiennych zbiorów danych i identyfikować połączenia, które w przeciwnym razie niezauważone przez odpowiednie agencje rządowe, mogą stanowić zagrożenie dla bezpieczeństwa. Jednakże w kontekście bezpieczeństwa narodowego i uprawnień przyznanych organom władzy publicznej, korzystanie ze sztucznej inteligencji może prowadzić do dodatkowych kwestii związanych z prywatnością obywateli i praw człowieka, które musiałyby zostać ocenione w istniejących regulacjach międzynarodowych i krajowych. Z tego powodu potrzebna jest ulepszona polityka rządowa i opracowanie wytycznych, celem zapewniania przestrzegania praw człowieka, w związku z wykorzystywaniem sztucznej inteligencji do celów bezpieczeństwa narodowego, poprzez bieżące weryfikowanie w miarę, stosowania nowych metod analizy danych.

Dodatkowo SI może mieć zarówno pozytywny, jak i negatywny wpływ na bezpieczeństwo państwa, w zależności od sposobu jej wykorzystania i implementacji. Chociaż zrozumienie różnych wyzwań, związanych ze sztuczną inteligencją, ma istotne znaczenie, równie ważne jest uznanie jej potencjału w zakresie wzmacniania wysiłków na rzecz bezpieczeństwa narodowego. Wykorzystując narzędzia i technologie oparte na sztucznej inteligencji, agencje rządowe usprawniają podejmowane przez siebie zadania, które kiedyś wymagały dużej ilości czasu i zasobów, w tym gromadzenie danych, ich analiza i raportowanie. Poprawia to zarówno ogólną wydajność, jak i daje tym agencjom więcej czasu na skupienie się na pracy strategicznej, w szczególności w dziedzinie reagowania na błędy ze strony algorytmów sztucznej inteligencji, kiedy agencje rządowe powinny analizować dane z różnych źródeł, w tym prognozy pogody (np. alerty RCB), zdjęcia satelitarne i posty w mediach społecznościowych. Algorytmy takie powinny pomóc w przewidywaniu zagrożeń dla bezpieczeństwa krajowego, z większą dokładnością i wyprzedzeniem. Zdolność taka pomaga agencjom rządowym przydzielać zasoby i podejmować działania, mające na celu zmniejszenie powstałych szkód w przestrzeni bezpieczeństwa państwa.

Integracja sztucznej inteligencji z bezpieczeństwem narodowym, przyczynia się do wykorzystywania sztucznej inteligencji do zwiększania swoich

możliwości na różne sposoby. Dokonuje się to poprzez wykorzystanie sieci neutronowych sztucznej inteligencji, które przeszukują ogromne zbiory danych globalnego ruchu komunikacyjnego – m.in zdjęć satelitarnych i postów w mediach społecznościowych celem zidentyfikowania potencjalnych zagrożeń działań terrorystycznych i wydarzeń geopolitycznych. Takie analizy predykcyjne powinny pomóc organom bezpieczeństwa proaktywnie udaremniać zagrożenia, zapobiegać aktom terroryzmu i skuteczniej zwalczać różne formy przestępczości. Przykładowo w dziedzinie cyberbezpieczeństwa systemy oparte na sztucznej inteligencji stale monitorują sieci, szybko wykrywając zagrożenia i reagują na nie.

W artykule, w szczególności, wskazano na zdolność do przetwarzania i analizowania ogromnych ilości danych z prędkością nieosiągalną dla analityków instytucji, odpowiedzialnych za szeroko rozumiane bezpieczeństwo. W gromadzeniu danych zdolność taka ma kluczowe znaczenie, umożliwiając algorytmom sztucznej inteligencji analizowanie ogromnych zbiorów danych w poszukiwaniu anomalii, wzorców i trendów, które mogą wskazywać na zbliżające się zagrożenia bezpieczeństwa państwa. Podkreślono transformacyjny wpływ sztucznej inteligencji na bezpieczeństwo państwa, przedstawiając kompleksowy przegląd tego, w jaki sposób technologie sztucznej inteligencji usprawniają wykrywanie zagrożeń bezpieczeństwa informacji, analizę danych o przestępstwach i podejmowanie strategicznych działań w zakresie zapewnienia bezpieczeństwa.

Zagadnienia terminologiczne

Współcześnie bezpieczeństwo państwa daleko wykracza poza kwestie militarne.[1] Bezpieczeństwo państwa jest powszechnie rozumiane jako obejmujące również wymiar niemilitarny, w tym, w szczególności, odpieranie ataków terrorystycznych, bezpieczeństwo gospodarcze, bezpieczeństwo energetyczne, bezpieczeństwo środowiskowe, bezpieczeństwo żywnościowe, bezpieczeństwo cybernetyczne i inne.

Nie istnieje powszechnie akceptowana definicja sztucznej inteligencji. Na przykład Engineering and Physical Science Research Council definiuje funkcje sztucznej inteligencji jako odtworzenie lub przewyższenie zdolności (w systemach obliczeniowych), które wymagałyby inteligencji, gdyby wykonywali je ludzie. Obejmują one uczenie się i adaptację; rozumienie sensoryczne i interakcję; rozumowanie i planowanie; optymalizację; autonomię; kreatywność oraz wydobywanie wiedzy i przewidywanie z dużych, różnorodnych danych

[1] https://bazhum.muzhp.pl/media/files/Kultura_i_Polityka_zeszyty_naukowe_Wyzszej_Szkoly_Europejskiej_im_ks_Jozefa_Tischnera_w_Krakowie/Kultura_i_Polityka_zeszyty_naukowe_Wyzszej_Szkoly_Europejskiej_im_ks_Jozefa_Tischnera_w_Krakowie-r2009-t (dostęp dnia 21.05.2024)

cyfrowych.[2] Często rozróżnia się ogólną sztuczną inteligencję, którą jest inteligencja maszynowa, posiadająca zdolność działania, rozumowania i adaptacji ludzkiego mózgu oraz wąską sztuczną inteligencję, rozumianą jako inteligencja maszynowa, wyszkoloną do wykonywania wąsko zdefiniowanych zadań kognitywnych, w tym np. gra w szachy, rozumowanie i adaptacja ludzkiego mózgu.[3] Całość obecnej sztucznej inteligencji można scharakteryzować jako wąską sztuczną inteligencję.[4]

Definicja algorytmów SI

Sztuczna inteligencja[5], definiowana jako zdolność maszyny do maksymalizowania szans na osiągnięcie swoich celów, poprzez działanie na podstawie danych zebranych z jej otoczenia, wyłania się jako definiująca technologia XXI wieku.[6] Przyjęta definicja algorytmu określa ją jako zestaw instrukcji do wykonania w obliczeniach lub innych operacjach, obejmująca matematykę, jak i informatykę. Tak więc, na podstawowym poziomie, algorytm sztucznej inteligencji to programowanie, które mówi komputerowi, jak nauczyć się działać samodzielnie[7].

Jednakże sztuczna inteligencja stwarza również nowe wyzwania i zagrożenia, w tym zagrożenie wykorzystania sztucznej inteligencji do ataków cybernetycznych innych państw i ponadto wymaga specjalistycznych umiejętności ze strony agencji odpowiedzialnych za bezpieczeństwo. Obejmuje ona zrozumienie złożoności sztucznej inteligencji, jak również pomaga szybko rozpoznawać nowe złośliwe oprogramowanie i zagrożenia wewnętrzne, żeby pomóc agencjom rządowym zautomatyzować zadania i skupić się na zapewnieniu bezpieczeństwa na wyższym poziomie.

---

2 Szerzej *Dame Wendy Hall, Jérôme Pesenti*, *Growing the Artificial Intelligence Industry in the UK*, Oct. 15, 2015 https://assets.publishing.service.gov.uk/media/5a824465e5274a2e87dc2079/Growing_the_artificial_intelligence_industry_in_the_UK.pdf (dostęp dnia 21.05.2024)

3 Wąska sztuczna inteligencja może być rozumiana jako zestaw zaawansowanych technologii cyfrowych ogólnego przeznaczenia, które umożliwia maszynom efektywne wykonywanie wysoce złożonych zadań. Szerzej Paul Martin, *The Rules of Security: Staying Safe in a Risky World* (Oxford: Oxford University Press, 2019), s. 217.

4 Alexander Babuta, Marion Oswald, Ardi Janjeva, *Artificial Intelligence and UK. National Security Policy Considerations*, Royal United Services Institute for Defense and Security Studies RUSI London April 2020 https://static.rusi.org/ai_national_security_final_web_version.pdf (dostęp dnia 21.05.2024)

5 Sztuczna inteligencja to gałąź informatyki zajmująca się tworzeniem maszyn, które potrafią myśleć i podejmować decyzje niezależnie od interwencji człowieka. takie programy AI powinni wykonywać złożone zadania, które wcześniej mogły być wykonywane tylko przez ludzi. Niektóre programy AI powinni wykonywać proste zadania, inne bardziej złożone. Niektóre powinni pobierać dane w celu uczenia się i doskonalenia, całkowicie bez udziału ludzkiego programisty.

6 Stephen Lomlen, *Impact of Artificial Intelligence in enhancing National Security*, "Artificial Intelligence Studies" 1 February 2024, University of Nairobi

7 Algorytmy AI działają poprzez pobieranie danych szkoleniowych, które pomagają algorytmowi w uczeniu się. Sposób pozyskiwania i oznaczania tych danych stanowi kluczową różnicę między różnymi typami algorytmów sztucznej inteligencji. Na poziomie podstawowym algorytm sztucznej inteligencji pobiera dane szkoleniowe (oznaczone lub nieoznaczone, dostarczone przez programistów lub pozyskane przez sam program) i wykorzystuje takie informacje do nauki i rozwoju. Następnie wykonuje swoje zadania, wykorzystując dane szkoleniowe jako podstawę. Niektóre rodzaje algorytmów sztucznej inteligencji można nauczyć samodzielnego uczenia się i pobierania nowych danych w celu zmiany i udoskonalenia ich procesu. Inne będą wymagały interwencji programisty w celu usprawnienia. https://www.tableau.com/data-insights/ai/algorithms (dostęp dnia 21.05.2024)

Bezpieczeństwo informacji

Sztuczna inteligencja może być stosowana do identyfikacji i zapobiegania zagrożeniom bezpieczeństwa informacji. Systemy oparte na sztucznej inteligencji są w stanie analizować duże ilości danych w poszukiwaniu nieprawidłowych wzorców i sygnałów wskazujących na potencjalne zagrożenia, co umożliwia szybką reakcję na ataki. Sztuczna inteligencja jest w stanie też, w wyjątkowy sposób, dostrzegać słabe i subtelne sygnały nigdy wcześniej niewidzianego zagrożenia bezpieczeństwa informacji. Zdolność taka stała się niezbędna w ostatnich latach, ponieważ hakerzy nadal opracowują nowatorskie taktyki, techniki i procedury zaprojektowane specjalnie celem uniknięcia kontroli, które zostały wstępnie zaprogramowane z sygnaturami wcześniejszych ataków. Przy czym sztuczna inteligencja ma istotny wpływ na dziedzinę bezpieczeństwa cybernetycznego, zarówno w kontekście pozytywnym, jak i wyzwaniach, które niesie[8].

W szczególności cyberprzestrzeń stała się coraz bardziej złożoną sferą bezpieczeństwa państwa, ponieważ, nieprzyjazne państwa nieustannie próbują wykorzystać luki w zabezpieczeniach, infiltrować systemy i zakłócać krytyczną infrastrukturę dla osiągniecia swoich często destrukcyjnych celów. W takich sytuacjach SSI analizują dane o ruchu sieciowym z wielu źródeł, w tym zapór ogniowych, systemów wykrywania włamań i aktywności użytkowników w tym samym czasie. Algorytmy takie następnie wykrywają subtelne anomalie i wzorce wskazujące na zagrożenia, które byłyby praktycznie niemożliwe do wykrycia przez ludzkich analityków w czasie rzeczywistym. Pozwala to agencjom rządowym identyfikować zaawansowane zagrożenia bezpieczeństwa informacji i reagować na nie, zanim spowodują one znaczne szkody. Istotnym jest wykrywanie zagrożeń, kiedy SI może być wykorzystywana do analizy dużych ilości danych, celem wykrywania nieprawidłowych wzorców i zachowań, które powinny wskazywać na potencjalne zagrożenia cybernetyczne. Algorytmy uczenia maszynowego (AUM) powinny wtedy identyfikować podejrzane aktywności, anomalie w sieciach czy też ataki typu zero-day[9].

Dodatkowo sztuczna inteligencja może być wykorzystana do przyspieszenia analizy informacji agencji rządowych, pochodzących z danych open source,

[8] Szerzej Darktrace, Autonomous Response: Threat Report 2019, s. 3. https://customers.darktrace.com/en/requestresources?pp=wp-cyber-ai-response-threatreport2019&utm_source=darktrace&utm_ medium=mudwall (dostęp dnia 21.05.2024)

[9] W przypadku exploitów zero-day hakerzy wykorzystują luki w kodzie oprogramowania do projektowania i wstrzykiwania złośliwego oprogramowania. Rozwiązania bezpieczeństwa oparte na oprogramowaniu powinni być skuteczne w wykrywaniu znanych zagrożeń, ale nie w przypadku nowych zagrożeń lub ich wariantów. Zastosowanie kompleksowej strategii cyberbezpieczeństwa, która obejmuje korzystanie z urządzeń końcowych ze zintegrowanymi zabezpieczeniami sprzętowymi, takimi jak takie oferowane w komputerach może pomóc chronić firmy przed atakami typu zero-day. https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/what-is-a-zero-day-exploit.html (dostęp dnia 22.05.2024)

wykorzystywanych chociażby w analizie i dokumentowaniu przemieszczania się różnych obiektów.

Sztuczna Inteligencja pomaga w ochronie przed atakami poprzez zastosowanie w zapobieganiu zagrożeniom bezpieczeństwa informacji, poprzez wczesne wykrywanie, blokowanie i eliminowanie zagrożeń. Systemy oparte na sztucznej inteligencji powinny wtedy automatycznie reagować na ataki, izolując kompromitowane systemy lub blokując podejrzane działania. Analiza output sztucznej inteligencji może pomagać w analizie zachowań użytkowników celem identyfikacji podejrzanych aktywności, prób naruszenia zabezpieczeń lub prób kradzieży danych. AUM są w stanie analizować duże ilości danych z różnych źródeł, żeby wykryć nieprawidłowości i potencjalne zagrożenia. Dzięki sztucznej inteligencji można zautomatyzować szereg procesów, związanych z reakcją na incydenty cybernetyczne, co pozwala na szybką i skuteczną reakcję na ataki. Systemy sztucznej inteligencji SSI mogą być również stosowane celem automatycznego wykrywania analizowania i reagowania na incydenty, co redukuje czas reakcji i minimalizuje szkody. Zagrożenia bezpieczeństwa oparte na SI mogą być również wytwarzane przez obce państwa do prowadzenia bardziej zaawansowanych i skutecznych ataków. AUM powinny być wykorzystywane do tworzenia bardziej wyszukanych metod ataków, generowania fałszywych treści czy też manipulowania systemami zabezpieczeń. Ponadto zastosowanie sztucznej inteligencji do bezpieczeństwa informacji może prowadzić do zwiększenia złożoności analizy i interpretacji danych. Wielkie ilości informacji mogą być trudne do przetworzenia i zrozumienia nawet dla zaawansowanych systemów sztucznej inteligencji, co może prowadzić do błędów w ocenie zagrożeń. Należy stwierdzić, że sztuczna inteligencja może być bardzo skutecznym narzędziem w walce z zagrożeniami cybernetycznymi, ale jednocześnie wymaga odpowiedniego zarządzania i nadzoru ze strony władz państwowych, celem zapewnienia skutecznej ochrony przed atakami, minimalizując ryzyko nadużyć i błędów.

Wykrywanie terroryzmu i przestępczości

W ostatnich dwóch dekadach sztuczna inteligencja stała się użytecznym narzędziem, w rękach grup terrorystycznych, wykorzystywanym do udoskonalania ich taktyk celem radykalizacji osób, rekrutowania ich i planowania ataków terrorystycznych. Stanowi to ogromne wyzwanie dla agencji odpowiedzialnych za bezpieczeństwo narodowe i międzynarodowe na rzecz przewidywania i skutecznego przeciwdziałania zagrożeniom opartym na sztucznej inteligencji. Szczególnie niepokojący jest potencjał wykorzystania sztucznej inteligencji do namierzania, manipulowania i radykalizowania osób celem

skłonienia ich do wspierania lub udziału w aktach terroryzmu[10]. SSI są już powszechnie używane do monitorowania mediów społecznościowych, analizy treści online i przetwarzania danych z kamer monitoringu celem wykrywania potencjalnych działań terrorystycznych, przestępczości zorganizowanej czy też innych zagrożeń dla bezpieczeństwa państwa. Wykrywanie terroryzmu i przestępczości za pomocą sztucznej inteligencji stanowią nowy obszar, w którym technologia może mieć istotny wpływ, zarówno pozytywny, jak i wyzwalający nowe wyzwania. Należy podkreślić, że sztuczna inteligencja może przetwarzać ogromne ilości danych z różnych źródeł, w tym informacji pochodzących z mediów społecznościowych, danych z systemów monitoringu czy też baz danych policyjnych. AUM są w stanie analizować takie dane w poszukiwaniu wzorców i sygnałów wskazujących na podejrzane aktywności terrorystyczne lub przestępcze. Poprzez rozpoznawania wzorców zachowań sztuczna inteligencja może być wykorzystywana do identyfikacji charakterystycznych wzorców zachowań osób lub grup podejrzanych o terroryzm lub przestępczość. Z tego powodu AUM powinny analizować dane z monitoringu wideo, transakcji finansowych, komunikacji telefonicznej czy też podróży, żeby wykryć podejrzane zachowania lub związki między podejrzanymi osobami. Sztuczna inteligencja może być stosowana przez agencje rządowe do monitorowania sieci w poszukiwaniu treści związanych z terroryzmem, ekstremizmem czy też przestępczością zorganizowaną. Algorytmy Uczenia Maszynowego (AUM)[11] pomagają w analizie tekstów, obrazów czy filmów/wideo, celem identyfikowania treści niebezpieczne i podejrzane, które powinny wskazywać na planowane ataki lub działania terrorystyczne. Poza tym sztuczna inteligencja może pomagać w analizie ryzyka, identyfikując obszary lub osoby o wysokim potencjale do popełnienia aktów terrorystycznych lub przestępczych. AUM wykorzystywane są przy analizie danych demograficznych, historii zdarzeń przestępczych czy też wzorców podróży celem określania osoby lub grupy, wymagające szczególnej uwagi ze strony organów ścigania.

Wspomaganie działań policyjnych

Sztuczna inteligencja może także wspomagać działania policyjne poprzez automatyczne rozpoznawanie twarzy, analizę zapisów audio-wideo czy też monitorowanie pojazdów i osób podejrzanych. Systemy oparte na sztucznej

[10] https://onlinewilder.vcu.edu/blog/ai-challenges-and-opportunities-national-security/(dostęp dnia 22.05.2024)

[11] Algorytmy uczenia maszynowego są kodem ułatwiającym eksplorowanie, analizowanie i rozumienie złożonych zestawów danych. Każdy algorytm to skończony zestaw jednoznacznych instrukcji krok po kroku, które może wykonać komputer, żeby osiągnąć określony cel. Celem modelu uczenia maszynowego jest ustanowienie lub odnalezienie wzorców, których ludzie powinni używać do przewidywania lub kategoryzowania informacji. Co to jest uczenie maszynowe? Algorytmy uczenia maszynowego używają parametrów, które są oparte na danych trenujących — podzbiorze danych reprezentującym większy zestaw. kiedy dane trenujące zostaną rozszerzone tak, żeby lepiej reprezentowały rzeczywistość, algorytm obliczy dokładniejsze wyniki. https://azure.microsoft.com/pl-pl/resources/cloud-computing-dictionary/what-are-machine-learning-algorithms (dostęp dnia 22.05.2024)

inteligencji powinny pomagać w szybkim identyfikowaniu podejrzanych osób i reagowaniu na zagrożenia w czasie rzeczywistym. Wykorzystanie sztucznej inteligencji odgrywa również kluczową rolę w systemach autonomicznych[12]. Bezzałogowe statki powietrzne (UAV) z autonomią opartą na sztucznej inteligencji mogą prowadzić nadzór, rozpoznanie, a nawet misje bojowe przy minimalnej interwencji człowieka. Postępy takie zwiększają wydajność, jednocześnie zmniejszając ryzyko zagrożeń dla ludzkiego personelu. W egzekwowaniu prawa, technologia rozpoznawania twarzy *face recognition*, oparta na sztucznej inteligencji, może szybko porównywać twarze z listami obserwacyjnymi w czasie rzeczywistym, co pomaga w szybkiej identyfikacji i zatrzymywaniu osób podejrzanych.

Wspomaganie działań policyjnych za pomocą sztucznej inteligencji

Rozwiązania sztucznej inteligencji mogą pomagać organom ścigania w podejmowaniu decyzji i wykonywaniu zadań oraz powinny one poprawić wydajność, zwiększyć praktyki oparte na danych lub rozszerzyć możliwości w zakresie określonych zadań lub decyzji. Dobrym przykładem są aplikacje sztucznej inteligencji, pomagające w określeniu, ilu funkcjonariuszy potrzebują organy władzy państwowej, gdzie należy rozmieścić zasoby i optymalną strategię planowania dla funkcjonariuszy. Pomocna jest analiza przypadków, produktów i technologii sztucznej inteligencji celem zilustrowania, w jaki sposób niektóre agencje włączyły sztuczną inteligencję do swoich działań. Zauważono, że wyzwaniem dla organów ścigania jest zidentyfikowanie przypadków, w których jakość i dostępność danych, dojrzałość technologii i ograniczenia etyczne służą zarówno potrzebom organów ścigania, jak i społeczności. Rozszerzone zastosowania technologii sztucznej inteligencji w egzekwowaniu prawa wymagają od wszystkich zainteresowanych stron, w tym przedstawicieli społeczności i innych organów wymiaru sprawiedliwości, prowadzenia ciągłych analiz, dotyczących uzyskania kompromisów między prywatnością a bezpieczeństwem publicznym, ponieważ aplikacje sztucznej inteligencji ewoluują, żeby zapewnić rozszerzone możliwości nadzoru i prowadzenia dochodzeń[13].

[12] Autonomiczna sztuczna inteligencja (AI) to gałąź sztucznej inteligencji, w której systemy i narzędzia są wystarczająco zaawansowane, żeby działać przy ograniczonym nadzorze i zaangażowaniu człowieka. Działania, które może wykonywać autonomiczny system sztucznej inteligencji, obejmują automatyzację podstawowych, powtarzalnych zadań i analizę zestawów danych. Autonomiczna sztuczna inteligencja przybliża systemy sztucznej inteligencji do takiej, jaką często przedstawia się w dziełach fikcji. Dzięki różnym komponentom współpracującym ze sobą, autonomiczny system AI zapewnia zaawansowane możliwości firmom i innym organizacjom. Niektóre z tych komponentów, w tym algorytmy, są wykorzystywane do wykonywania zadań, w tym analiza danych, podczas kiedy inne, w tym czujniki, są strategicznie rozmieszczone w celu gromadzenia danych potrzebnych do analizy. https://www.techtarget.com/searchenterpriseai/definition/autonomous-artificial-intelligence-autonomous-AI (dostęp dnia 22.05.2024)

[13] Szerzej James Redden, Brian Aagaard, Travis Taniguchi, *Artificial Intelligence Applications in Law Enforcement: An Overview of Artificial Intelligence Applications and Considerations for State and Local Law Enforcement* NCJ Number 255994 August 2020

Sztuczna inteligencja stanowi skuteczne narzędzie w walce z przestępczością oraz zapewnieniu bezpieczeństwa publicznego nie tylko poprzez automatyzację raportowania, rozpoznawanie wzorców zachowań przestępczych czy też profilowanie zachowań, ale też jest przydatna we wspieraniu postępowania wyjaśniającego i w prognozowaniu popełniania przestępstw[14]. Sztuczna inteligencja może wspomagać organy funkcjonariuszom policji w automatyzacji procesów raportowania, zarządzania dokumentacją i generowania raportów, związanych z działalnością operacyjną, co pozwalałoby na efektywne wykorzystanie czasu funkcjonariuszom policji oraz poprawę precyzji i dokładności dokumentacji. SSI powinny w takiej sytuacji analizować dane kryminalne, zgłoszenia incydentów, historię przestępstw oraz inne informacje, związane z działalnością przestępczą celem identyfikacji wzorców i trendów, pomagających funkcjonariuszom policji na skierowanie zasobów w miejsca, gdzie jest największe prawdopodobieństwo popełnienia przestępstw[15].

Sztuczna inteligencja może pomagać w profilowaniu zachowań osób podejrzanych o popełnienie przestępstw, poprzez wykorzystanie analizy danych z różnych źródeł celem wykrywania nieprawidłowości w zachowaniu, anomalie czy wzorce, które powinny wskazywać na potencjalne zagrożenia dla bezpieczeństwa publicznego. Podobnie SSI mogą wspomagać dochodzenia funkcjonariuszom policji poprzez automatyczne przetwarzanie i analizę danych, zarządzanie dokumentacją śledczą, identyfikację potencjalnych świadków i podejrzanych oraz współpracę z innymi organami ścigania. Ponadto mogłyby być wykorzystywane do zbierania namacalnych dowodów przy pomocy robotów[16], połączonych z systemem sztucznej inteligencji wdrożonym na miejscu przestępstwa, ponownie celem zmniejszenia liczby techników na miejscu. Informacje na temat dowodów, które mogły zostać przeoczone podczas głównego dochodzenia, można by uzyskać, przeglądając dowody elektroniczne. Prowadzi to do słusznego wniosku, że sztuczna inteligencja i robotyka będą skutecznie wspierać techników na miejscu zbrodni[17].

Warto zwrócić uwagę na fakt, że sztuczna inteligencja może być wykorzystywana do prognozowania przestępczości na podstawie analizy danych

[14] Prognozowanie kryminologiczne w wymiarze społecznym. T. 1, Metodologia, Analiza, Tendencje rozwojowe. red. B. Hołyst, Warszawa 2017

[15] Prognozowanie kryminologiczne w wymiarze społecznym. T. 2, Modele prognostyczne, przestępczość, wiktymizacja, profilaktyka, red. B. Hołyst, N. Malec, Zbigniew M. Wawrzyniak. Warszawa 2018

[16] Sztuczna inteligencja i robotyka powinni pomagać policji w 4 obszarach: 1) Przewidywanie i analiza, 2) Rozpoznawanie, 3) Eksploracja i 4) Komunikacja. Chociaż nie ma ścisłych granic między tymi kategoriami, mają one różny stopień złożoności i interakcji ze środowiskiem ze środowiskiem, jak wskazano na rysunku 1 poniżej. Im większy stopień złożoności systemu i bardziej chaotyczne środowisko, w którym system musi działać, tym większym wyzwaniem staje się opracowanie, prototypowanie i integracja systemu z organami ścigania.

[17] Szerzej Grobbelaar, Marius, *Deploying Artificial Intelligence (AI) to support law enforcement agencies in crime scene analysis and management.* https://www.researchgate.net/publication/364733770_Deploying_Artificial_Intelligence_AI_to_support_law_enforcement_agencies_in_crime_scene_analysis_and_management/citation/download (dostęp dnia 23.05.2024)

historycznych, demograficznych, społecznych i ekonomicznych. AUM przewiduje przecież miejsca i czasy o zwiększonym ryzyku popełnienia przestępstw, co umożliwia podejmowanie prewencyjnych działań przez organy funkcjonariuszom policji[18].

Technologia sztucznej inteligencji używana w mechanizmie rozpoznawania twarzy, pomaga funkcjonariuszom policji szybko i dokładnie zidentyfikować osoby poszukiwane za poważne przestępstwa, a także osoby zaginione[19]. Zwalnia to również czas i zasoby funkcjonariuszy policji, co oznacza, że więcej funkcjonariuszy może być na służbie, angażując się w społeczności i prowadząc złożone dochodzenia. Organy policji korzystają z szeregu innych programów sztucznej inteligencji, żeby wspierać swoją rolę w zapewnianiu bezpieczeństwa publicznego, w tym tych, które pomagają przyspieszyć badanie dowodów cyfrowych oraz redagowanie plików dowodowych i narzędzi, które wykonują zadania biurowe, zwalniając czas funkcjonariuszy. Sztuczna inteligencja jest pomocna w procesie retrospektywnego rozpoznawania twarzy, najnowocześniejszej technologii rejestrującej na żywo nagrania tłumów i porównuje je z listą podejrzanych, poszukiwanych przez organy, którzy stanowią zagrożenie dla innych. W przypadku zgodności, do pobliskich funkcjonariuszy policji zostaje wysłane zawiadomienie. Nie tylko pozwala to funkcjonariuszom policji szybko zidentyfikować podejrzanych w tłumie, ale może mieć również silny efekt odstraszający. Obrazy są zazwyczaj dostarczane z CCTV, nagrań z telefonu komórkowego, kamery samochodowej lub dzwonka do drzwi czy mediów społecznościowych[20]. Obrazy takie są następnie porównywane ze zdjęciami osób, zrobionymi podczas ich aresztowania celem identyfikacji podejrzanego. Kiedy istnieje możliwość dopasowania RFR, przeszkolony operator przegląda obrazy, żeby to potwierdzić. Oficer dochodzeniowy również sprawdza dopasowanie, żeby potwierdzić dokładność. Dlatego SSI wykorzystywane są do automatycznego rozpoznawania twarzy na podstawie zdjęć i nagrań wideo z kamer monitoringu ulicznego, lotnisk czy innych miejsc publicznych. Takie narzędzie umożliwia identyfikację podejrzanych osób, poszukiwanych przez organy funkcjonariuszom policji oraz osób zaginionych. Same kamery przeznaczone do nadzoru wideo lub innych zastosowań związanych z bezpieczeństwem również są modernizowane poprzez wbudowywanie funkcje sztucznej inteligencji (np. chipy, które powinny uruchamiać głębokie sieci neuronowe) bezpośrednio w swoich kamerach. Takie zmodernizowane kamery

[18] Por także: Prognozowanie kryminologiczne w wymiarze społecznym. T. 2, Modele prognostyczne, przestępczość, wiktymizacja, profilaktyka…

[19] E. Gruza, I. Sołtyszewski, Poszukiwania osób zaginionych, Warszawa 2022

[20] M. Tomaszewska – Michalak, Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce, Warszawa 2015

uruchamiają ASI na sprzęcie kamery, a nie w chmurze, zmniejszając koszty, zwiększając szybkość i zmniejszając wymagania dotyczące przepustowości[21].

Sztuczna inteligencja pomaga w szczególności funkcjonariuszom szybciej identyfikować i klasyfikować materiały przedstawiające seksualne wykorzystywanie dzieci. Podkreśla interesujące obrazy, na których funkcjonariusze powinny się skupić, żeby pomóc w dochodzeniach, umożliwiając im szybszą identyfikację i ochronę dzieci, a także identyfikację przestępców. Wspiera również poprawę dobrostanu biura funkcjonariuszom policji, ponieważ ogranicza długotrwałe narażenie funkcjonariuszy na nieprzyzwoite obrazy. Jest to dodatek do innych narzędzi, które są już w użyciu, na przykład technologii dopasowywania twarzy, a także innych w fazie rozwoju, które będą wykorzystywać sztuczną inteligencję do ochrony dzieci i szybszej identyfikacji sprawców. Ponadto SSI doskonale radzą sobie z analizą obrazów i wideo, poprzez identyfikowanie obiektów, lokalizacji, a nawet osób w treściach multimedialnych. Przy czym taka zdolność pomaga analitykom w monitorowaniu i śledzeniu potencjalnych zagrożeń lub celów. Coraz częściej sztuczna inteligencja może automatycznie analizować dane wyjściowe z tych systemów (wideo, audio i tekst) celem zidentyfikowania naruszeń przepisów lub pojawiających się zagrożeń. W szczególności oprogramowanie do analizy wideo może stwierdzić, czy istnieje aktywne zagrożenie w scenach zarejestrowanych przez kamery wideo. Sztuczna inteligencja może być wykorzystana przy analizie obrazu i wideo, na żywo z kamer granicznych, w obszarach podatnych na przemyt narkotyków.

Samo wideo jest kolejnym obszarem zainteresowania sztucznej inteligencji przy wykorzystaniu sieci neutronowych uczenia maszynowego do generowania unikalnego podsumowania wideo, poprzez wybranie kluczowych klatek, które dokładnie oddają treść i kontekst oryginalnego wideo. Można to wykorzystać do zidentyfikowania zmiany, która nastąpiła w czasie i stworzenia filmu wideo, podkreślającego tę zmianę dla analityka. Program sztucznej inteligencji jest często wykorzystany w identyfikacji podejrzanych ruchów i rozróżniania pojazdów, zwierząt i ludzi. Obejmuje to identyfikację nieautoryzowanych pojazdów, zbliżających się do granicy, a nawet bezzałogowych statków powietrznych (dronów unmanned aerial vehicle UAV) wykorzystywanych do nielegalnych działań. Sztuczna inteligencja może również uczyć się typowych wzorców aktywności granicznej i podnosić alerty, kiedy wykryje anomalie. Ponadto SSI powinny łączyć się z bazami danych bezpieczeństwa narodowego, umożliwiając im rozpoznawanie osób z rejestrami karnymi i znanymi powiązaniami z organizacjami przestępczymi.

[21] Szerzej: Faggella, D. *AI for Crime Prevention and Detection—5 Current Applications* 2019, February 2. https://emerj.com/ai-sector-overviews/ai-crime-prevention-5-current-applications/ (dostęp dnia 24.05.2024)

Gdyby takie osoby pojawiły się na granicy, programy sztucznej inteligencji mogłyby wysyłać powiadomienia do agentów patrolu granicznego.

Sztuczna inteligencja może być też wykorzystywana do analizy zapisów audio-wideo celem wykrywania nielegalnych aktywności, agresywnych zachowań, przestępstw czy też incydentów terrorystycznych, kiedy algorytmy pomagają wykrywać podejrzane zachowania i sygnały dźwiękowe, które powinny wskazywać na zagrożenia dla bezpieczeństwa publicznego[22].

Inne zastosowanie SI to monitorowania treści, publikowanych w mediach społecznościowych celem wykrywania potencjalnych zagrożeń dla bezpieczeństwa publicznego, planowanych przestępstw czy też aktów terroryzmu. Algorytmy pomagają analizować teksty, obrazy czy też filmy w poszukiwaniu treści podejrzanych lub niebezpiecznych. Narzędzia wywiad źródłowy, wywiad open source, open source intelligence, Open-Source Intelligence (OSINT), definiuje się jako dane wywiadowcze uzyskane poprzez gromadzenie, ocenę i analizę publicznie dostępnych informacji celem udzielenia odpowiedzi na konkretne pytanie wywiadowcze (OSINT)[23], oparte na sztucznej inteligencji narzędzia skanują ogromną ilość publicznie dostępnych informacji ze stron internetowych, kont w mediach społecznościowych i źródeł wiadomości.

Organy policji korzystają ze sztucznej inteligencji do prognozowania przestępczości[24] i określania obszarów lub czasów o zwiększonym ryzyku popełnienia przestępstw. AUM dokonują analizy szeregu danych, w tym demograficzne, społeczne i ekonomiczne, żeby identyfikować trendy przestępcze i zapobiegać ich wystąpieniu poprzez skierowanie większej liczby funkcjonariuszy policji w konkretne miejsca lub zmianę strategii działań policyjnych. Dodatkowo sztuczna inteligencja może pomagać w analizie danych kryminalnych, identyfikując związki między różnymi incydentami, przestępcami i grupami przestępczymi. Wtedy algorytmy pomagają funkcjonariuszom analizować duże ilości danych z raportów policyjnych, zeznań świadków, dowodów kryminalistycznych i innych źródeł, żeby wykryć wzorce i związki, które powinny być użyteczne w śledztwach i działaniach policyjnych.

---

22 Tamże.

23 Open Source Intelligence (OSINT) to metoda gromadzenia informacji z publicznych lub innych otwartych źródeł, które powinni być wykorzystywane przez ekspertów ds. bezpieczeństwa, krajowe agencje wywiadowcze lub cyberprzestępców. W przypadku cyberobrońców celem jest odkrycie publicznie dostępnych informacji związanych z ich organizacją, które powinni zostać wykorzystane przez atakujących, i podjęcie kroków w celu zapobieżenia tym przyszłym atakom. OSINT wykorzystuje zaawansowaną technologię do odkrywania i analizowania ogromnych ilości danych, uzyskanych poprzez skanowanie sieci publicznych, z publicznie dostępnych źródeł, w tym sieci społecznościowe, oraz z głębokiej sieci – treści, które nie są indeksowane przez wyszukiwarki, ale nadal są publicznie dostępne. https://www.imperva.com/learn/application-security/open-source-intelligence-osint/ (dostęp dnia 24.05.2024).

24 Prognozowanie kryminologiczne w wymiarze społecznym. T. 2, Modele prognostyczne, przestępczość, wiktymizacja, profilaktyka, red. B. Hołyst, N. Malec, Zbigniew M. Wawrzyniak. Warszawa 2018

Monitorowanie granic i kontroli migracyjnej

Sztuczna inteligencja może wspomagać systemy monitorowania granic poprzez automatyczne rozpoznawanie twarzy, analizę zachowań oraz identyfikację podejrzanych osób, co pomaga straży granicznej w skuteczniejszej kontroli przepływu osób i zapobieganiu nielegalnej imigracji oraz przemytowi. Dlatego wykorzystanie sztucznej inteligencji w monitorowaniu granic i kontroli imigracyjnej jest niezbędnym narzędziem w zarządzaniu przepływem osób przez granice oraz zapewnieniu bezpieczeństwa narodowego. Wspomniano już o mechanizmie rozpoznawania twarzy wykorzystywanego do automatycznego rozpoznawania twarzy osób przekraczających granicę, które umożliwia identyfikację osób poszukiwanych, osób podejrzanych o przestępstwa lub terroryzm, a także osób podróżujących na fałszywych dokumentach. SI pomaga przy analizie zachowań osób przekraczających granicę celem wykrycia podejrzanych zachowań lub sytuacji, kiedy algorytmy dokonują analizy ruchu ciała, gestów i innych zachowań, które powinny wskazywać na potencjalne zagrożenia. Monitorowanie dronów i statków: sztucznej inteligencji może być stosowana do monitorowania nie tylko ruchu ludzi, ale także ruchu dronów i statków, które powinny być wykorzystywane do nielegalnego przekraczania granic. AUM powinny analizować dane z radarów, kamer i innych sensorów, żeby wykryć podejrzane obiekty i działać zgodnie z protokołami bezpieczeństwa.

Służby graniczne wykorzystują analizę danych pasażerów, w której sztuczna inteligencja pomaga w analizie danych pasażerów, podróżujących przez granicę, w tym danych z biletów lotniczych, danych biometrycznych czy też danych dotyczących podróży. Algorytmy powinny wykrywać nieprawidłowości lub niezgodności w danych, które powinny wskazywać na próby fałszerstwa dokumentów lub nielegalnych działań.

Inicjatywy Unii Europejskiej – Artificial Intelligence Act

Parlament Europejski przyjął w dniu 13 marca 2024 r. regulację dotyczącą sztucznej inteligencji, gdzie przepisy Rozporządzenia UE[25] zakazują pewnych zastosowań sztucznej inteligencji, które zagrażają prawom obywateli. Regulacja ta zawiera określone przepisy szczegółowe, dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, w szczególności ograniczenia wykorzystywania systemów sztucznej inteligencji do zdalnej

[25] Rozporządzenie muszą jeszcze ostatecznie zweryfikować prawnicy lingwiści. Ma ono zostać przyjęte przed końcem kadencji (tzw. procedura sprostowania). Rozporządzenie musi też formalnie przyjąć Rada. Rozporządzenie wejdzie w życie dwadzieścia dni po publikacji w Dzienniku Urzędowym, a w pełni obowiązywać będzie 24 miesiące po jego wejściu w życie. Wyjątki to: zakazy niedozwolonych praktyk (będą obowiązywać sześć miesięcy po wejściu rozporządzenia w życie), kodeksy postępowania (dziewięć miesięcy po wejściu w życie), przepisy o sztucznej inteligencji ogólnego przeznaczenia, w tym dotyczące zarządzania (12 miesięcy po wejściu w życie) oraz obowiązki dotyczące systemów wysokiego ryzyka (36 miesięcy po wejściu w życie).

identyfikacji biometrycznej[26] w czasie rzeczywistym, w przestrzeni publicznej, do celów egzekwowania prawa. Rozpoznawanie biometryczne może być przeprowadzane przy użyciu różnych modalności. Powinny to być na przykład odciski palców lub twarze. Ponieważ modele sztucznej inteligencji działają tak dobrze, coraz częściej zapewniają podstawowe funkcje w rozpoznawaniu biometrycznym. W szczególności są one wykorzystywane do porównywania nowo pobranych danych biometrycznych z wcześniej przechowywanymi danymi referencyjnymi. Sztuczna inteligencja podejmuje następnie decyzje dotyczące tego, czy dane referencyjne i nowo przechwycone informacje należą do tej samej osoby. W tym przypadku często stosowane są metody, w tym sieci neuronowe oparte na algorytmach uczenia maszynowego (ML). Niemniej jednakże korzystanie z modeli sztucznej inteligencji wiąże się z szeregiem zagrożeń. W szczególności powinny one zostać zaatakowane przy użyciu technik specyficznych dla sztucznej inteligencji. Z tego samego powodu procesy sztucznej inteligencji powinny być również wykorzystywane do ataków w kontekście biometrii – na przykład do generowania głębokich podróbek[27]. Obecnie zakazuje się również wykorzystywania systemów zdalnej identyfikacji biometrycznej, w czasie rzeczywistym, w przestrzeni publicznej do celów egzekwowania prawa, chyba że mają zastosowanie niektóre ograniczone wyjątki. Przepisy dotyczą zapobiegania konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu. Rozporządzenie zawiera przepisy w kwestii wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy przestępstwa lub podejrzanego o popełnienie przestępstwa, o którym mowa w art. 2 ust. 2 decyzji ramowej Rady 2002/584/WSiSW 62 i które w danym państwie członkowskim podlega karze pozbawienia wolności lub środkowi zabezpieczającemu, polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej 3 lata, zgodnie z prawem danego państwa członkowskiego. Zgodnie z Rozporządzeniem, pojęcie systemu zdalnej identyfikacji biometrycznej stosowane w niniejszym rozporządzeniu należy zdefiniować funkcjonalnie jako system sztucznej inteligencji, służący do identyfikacji osób fizycznych na odległość, poprzez porównanie danych biometrycznych danej osoby z danymi biometrycznymi zawartymi w referencyjnej bazie danych, bez wcześniejszej wiedzy o tym, czy dana osoba będzie w niej figurować i może zatem zostać zidentyfikowana, niezależnie od konkretnej technologii oraz konkretnych

[26] Pojęcie danych biometrycznych stosowane w niniejszym rozporządzeniu jest zgodne z pojęciem danych biometrycznych zdefiniowanym w art. 4 pkt 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 , art. 3 pkt 18 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 oraz art. 3 pkt 13 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 i powinno być interpretowane w sposób spójny z tym pojęciem. https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021PC0206 (dostęp dnia 24.05.2024)

[27] Szerzej Y. Rawat, Y. Gupta, G. Khothari, A. Mittal, D. Rautela, *The Role of Artificial Intelligence in Biometrics, 2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, Namakkal, India, 2023, s. 622-626.

procesów lub rodzajów wykorzystywanych danych biometrycznych. Należy dokonać rozróżnienia między systemami zdalnej identyfikacji biometrycznej w czasie rzeczywistym, a systemami zdalnej identyfikacji biometrycznej post factum, biorąc pod uwagę ich różne cechy i sposoby stosowania, a także różne związane z nimi zagrożenia. W przypadku systemów działających w czasie rzeczywistym pobranie danych biometrycznych, porównanie i identyfikacja następują natychmiast, niemal natychmiast lub w każdym razie bez znacznego opóźnienia. W związku z tym nie powinno być możliwości obchodzenia przepisów niniejszego rozporządzenia, dotyczących stosowania przedmiotowych systemów sztucznej inteligencji w czasie rzeczywistym, poprzez wprowadzenie niewielkich opóźnień. Systemy identyfikacji w czasie rzeczywistym obejmują wykorzystanie materiału rejestrowanego na żywo lub w czasie zbliżonym do rzeczywistego, takiego jak materiał wideo generowany przez kamerę lub inne urządzenie o podobnej funkcjonalności. Natomiast w przypadku systemów identyfikacji post factum dane biometryczne zostały już pobrane, a porównanie i identyfikacja następują ze znacznym opóźnieniem. Dotyczy to materiałów, w tym zdjęcia lub nagrania wideo generowane przez kamery telewizji przemysłowej lub urządzenia prywatne, których rejestracji dokonano, zanim użyto systemu w stosunku do danej osoby fizycznej. Są to między innymi systemy kategoryzacji biometrycznej, które wykorzystują cechy wrażliwe i nieukierunkowane na pobieranie wizerunków twarzy z internetu lub nagrań z telewizji przemysłowej, by stworzyć bazy danych, służące rozpoznawaniu twarzy. Do systemów sztucznej inteligencji wysokiego ryzyka należy zaliczyć w szczególności SSI, przeznaczone do stosowania przez organy ścigania do oceny wiarygodności dowodów w postępowaniu karnym, do przewidywania wystąpienia lub ponownego wystąpienia faktycznego albo potencjalnego przestępstwa na podstawie profilowania osób fizycznych lub oceny cech osobowości i charakterystyki lub wcześniejszego zachowania przestępnego osób fizycznych lub grup, do profilowania w trakcie wykrywania przestępstw, prowadzenia postępowań przygotowawczych w ich sprawie lub ich ścigania, jak również do analizy przestępczości osób fizycznych. Zakazana też jest w regulacji unijnej klasyfikacja punktowa obywateli, prognozowanie przestępczości (wyłącznie na podstawie profilowania osoby lub oceny jej cech). Organom ścigania z reguły nie wolno korzystać z systemów identyfikacji biometrycznej. Są jednakże pewne wyjątki, które wąsko zdefiniowano na zamkniętej liście. Organy takie powinny wykorzystywać systemy identyfikacji biometrycznej w czasie rzeczywistym tylko wtedy, kiedy spełniły ściśle określone warunki. Na przykład powinny je stosować w określonym czasie i w określonym położeniu geograficznym. Powinny też posiadać specjalne zezwolenie sądowe lub administracyjne. Powinny je wykorzystywać, by odnaleźć zaginioną osobę

lub zapobiegać atakowi terrorystycznemu. Istnieją też tzw. systemy zdalnej identyfikacji biometrycznej *post factum*. Ich stosowanie wiąże się z wysokim ryzykiem i wymaga zezwolenia sądowego, ponieważ systemy takie wykorzystuje się do wyszukiwania w związku z przestępstwem[28]. Należy pozytywnie ocenić pogląd, stanowiący, że SSI specjalnie przeznaczonych do stosowania w postępowaniach administracyjnych, prowadzonych przez organy podatkowe i celne, nie należy uznawać za SSI wysokiego ryzyka, wykorzystywane przez organy ścigania do celów zapobiegania przestępstwom, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania[29].

Zwalczanie dezinformacji

SI może być wykorzystywana do identyfikacji fałszywych informacji, dezinformacji i propagandy w Internecie. SSI powinny analizować treści online, identyfikować wzorce dezinformacji oraz wspomagać działania mające na celu ograniczenie wpływu fałszywych informacji na społeczeństwo. Sztuczna inteligencja może być używana do zwalczania dezinformacji i propagandy, poprzez analizę dużych ilości danych z różnych źródeł oraz identyfikację fałszywych lub manipulacyjnych treści. Poniżej wybrane metody w jakie sztuczna inteligencja może być wykorzystywana w walce z dezinformacją i propagandą, w tym analiza treści, wykrywanie deepfake'ów, identyfikacja botów i trolli internetowych oraz analiza sieci społecznościowych. ASI powinny być wykorzystane do analizy treści publikowanych w internecie, w tym artykułów, postów na mediach społecznościowych, komentarzy i innych form treści. Systemy takie powinny identyfikować fałszywe informacje, nieprawdziwe plotki oraz manipulacyjne narracje. Z kolei Deepfake to technologia, która umożliwia tworzenie realistycznych, ale fałszywych nagrań wideo i audio[30]. ASI powinny być wykorzystane do wykrywania deepfake'ów poprzez analizę cech wideo i dźwięku, które powinny wskazywać na ich manipulacyjny charakter. Ponadto sztuczna inteligencja może pomagać w identyfikacji automatycznych kont (botów) oraz trolli internetowych, które rozpowszechniają dezinformację i propagandę w sieci.

[28] Wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji. Procedura 2021/0106/COD COM (2021) 206. https://www.europarl.europa.eu/news/pl/press-room/20240308IPR19015/akt-w-sprawie-sztucznej-inteligencji-poslowie-przyjmuja-przelomowe-przepisy (dostęp dnia 25.05.2024).

[29] Tamże.

[30] Deepfake to sztuczny obraz lub wideo (seria obrazów) wygenerowany przez specjalny rodzaj uczenia maszynowego zwanego uczeniem „głębokim". Uczenie głębokie jest podobne do każdego rodzaju uczenia maszynowego, w którym algorytm jest zasilany przykładami i uczy się generować dane wyjściowe, które przypominają przykłady, z których się nauczył. Uczenie głębokie to specjalny rodzaj uczenia maszynowego, który obejmuje „ukryte warstwy". Zazwyczaj głębokie uczenie jest wykonywane przez specjalną klasę algorytmów zwaną siecią neuronową, która została zaprojektowana w celu odtworzenia sposobu, w jaki ludzki mózg uczy się informacji. Warstwa ukryta to seria węzłów w sieci, która wykonuje transformacje matematyczne w celu konwersji sygnałów wejściowych na sygnały wyjściowe (w przypadku deepfake'ów, w celu konwersji prawdziwych obrazów na naprawdę dobre fałszywe obrazy). Im więcej ukrytych warstw ma sieć neuronowa, tym „głębsza" jest sieć. Sieci neuronowe, a w szczególności rekurencyjne sieci neuronowe RNN.

Algorytmy powinny analizować zachowanie i wzorce komunikacyjne, żeby wykryć podejrzane konta i działania. Dodatkowo sztuczna inteligencja może być używana do analizy sieci społecznościowych w poszukiwaniu wzorców i związanych ze sobą kont oraz treści, które powinny wskazywać na próby manipulacji publicznym dyskursem. Algorytmy powinny wykrywać grupy i kampanie dezinformacyjne oraz ich wpływ na społeczeństwo.

Warto wspomnieć inne metody, takie jak rozpoznawanie wzorców dezinformacji czy też ostrzeganie i edukacja: SSI powinny być wykorzystywane do rozpoznawania charakterystycznych wzorców dezinformacji, w tym fałszywe informacje powtarzane przez różne źródła lub manipulacyjne techniki retoryczne. Algorytmy powinny analizować teksty, obrazy i inne treści w poszukiwaniu takich wzorców. Na podstawie analizy danych sztucznej inteligencji, można ostrzegać użytkowników internetu o potencjalnie dezinformacyjnych treściach oraz dostarczać im rzetelne informacje i źródła. W ten sposób można promować świadome korzystanie z internetu i zwiększać odporność społeczeństwa na manipulację informacją.

Ochrona infrastruktury krytycznej

Sztuczna inteligencja może wspomagać systemy monitorowania i zarządzania infrastrukturą krytyczną[31], między innymi takie jak: elektrownie, sieci energetyczne czy systemy transportowe. Dzięki analizie danych sztucznej inteligencji można wykrywać awarie, przewidywać potencjalne problemy i podejmować szybkie działania naprawcze. Ochrona infrastruktury krytycznej za pomocą sztucznej inteligencji to obszar, w którym technologia taka może mieć istotny wpływ na zapewnienie bezpieczeństwa i niezawodności systemów, które są kluczowe dla funkcjonowania państwa i społeczeństwa. W monitoringu i wykrywaniu zagrożeń SSI powinny być stosowane do monitorowania infrastruktury krytycznej, takiej jak sieci energetyczne, wodociągi, czy systemy transportowe, celem wykrywania awarii, nieprawidłowości oraz potencjalnych ataków. AUM powinny analizować dane z różnych czujników i sensorów, żeby identyfikować anomalie i sygnały wskazujące na zagrożenia. Z kolei prognozowanie awarii polega na wykorzystaniu sztucznej inteligencji, w prognozowaniu awarii infrastruktury krytycznej, poprzez analizę danych historycznych, trendów eksploatacyjnych oraz warunków środowiskowych. Algorytmy powinny przewidywać prawdopodobieństwo wystąpienia awarii i ostrzegać przed potencjalnymi ryzykami, co umożliwia skuteczniejsze

[31] Zgodnie z ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2023 poz. 122 ze zm.) art. 3 pkt. 2, przez infrastrukturę krytyczną rozumie się systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy i sieci teleinformatyczne istotne dla bezpieczeństwa i ekonomicznego dobrobytu państwa oraz jego efektywnego funkcjonowania.

planowanie działań zapobiegawczych i konserwacyjnych. Agencje rządowe korzystają też z SI w automatyzacji zarządzania incydentami, w przypadku awarii lub ataków na infrastrukturę krytyczną. Algorytmy automatycznie wykrywają incydenty, klasyfikują ich rangę oraz mogą podejmować odpowiednie działania naprawcze lub reakcyjne, co przyspiesza proces reagowania i minimalizuje skutki awarii. Optymalizacja utrzymania infrastruktury może wykorzystywać SI poprzez analizę danych, dotyczących stanu technicznego, zużycia zasobów oraz kosztów konserwacji. Algorytmy powinny przewidywać momenty konieczności konserwacji, optymalizować harmonogramy prac oraz zoptymalizować zużycie energii i zasobów, co przyczynia się do zwiększenia niezawodności i efektywności infrastruktury.

Wreszcie metoda kontroli dostępu i identyfikacja osób opiera się na sztucznej inteligencji, może być wykorzystywana monitorowania dostępu do kluczowych obiektów infrastruktury krytycznej oraz identyfikacji osób mających dostęp do tych obiektów. Systemy biometryczne oparte na sztucznej inteligencji powinny rozpoznawać twarze, dłonie, czy cechy behawioralne, co umożliwia skuteczniejszą ochronę obiektów przed nieautoryzowanym dostępem. Analityka behawioralna pozostanie tutaj, a jej techniki powinny być skuteczne nie tylko w udoskonalaniu oceny ryzyka na podstawie istniejących tropów i SOI, ale także w odkrywaniu nowych tropów, które w przeciwnym razie nie zwróciłyby uwagi władz. Niektóre wskaźniki są ukierunkowane na identyfikację bezpośrednich zachowań poprzedzających atak, w tym próby zdobycia broni palnej lub badanie metodologii ataków. Bardziej ogólne wskaźniki mogą mieć również zastosowanie w przypadku osób, które są już podejrzane[32].

Podsumowanie

Sztuczna inteligencja odgrywa przede wszystkim kluczową rolę w przetwarzaniu ogromnych ilości danych, umożliwiając instytucjom odpowiedzialnym za zapewnienie bezpieczeństwa, uzyskiwanie wglądu i podejmowanie szybko świadomych decyzji z niezwykłą szybkością[33]. Zdolność SI do jednoczesnej analizy różnych źródeł danych przyczynia się do zrewolucjonizowania gromadzenia odpowiednich danych. ASI są w stanie przesiewać takie obszerne informacje, identyfikując ukryte wzorce i powiązania, które mogą umknąć ludzkim analitykom. Zdolność taka umożliwia agencjom rządowym wykrywanie pojawiających się zagrożeń, przewidywanie rozwoju sytuacji geopolitycznej i proaktywne reagowanie.

[32] Szerzej David Anderson, *Attacks in London and Manchester, March-June 2017: Independent Assessment of MI5 and Police Internal Reviews* (London: Brick Court Chambers, 2017), s. 19 i nast.

[33] https://onlinewilder.vcu.edu/blog/ai-challenges-and-opportunities-national-security/ (dostęp dnia 25.05.2024)

Chociaż sztuczna inteligencja oferuje bezprecedensowe korzyści w zakresie bezpieczeństwa, wiąże się również z poważnymi wyzwaniami i obawami etycznymi. W miarę jak systemy SI stają się coraz bardziej zintegrowane z praktykami bezpieczeństwa narodowego, ich konsekwencje powinny być dokładnie zbadane. Nieprzyjazne państwa mogą potencjalnie wykorzystywać technologie SI w sposób zagrażający zarówno bezpieczeństwu, jak i prywatności. Stwarza to pilną potrzebę zapewnienia, że systemy SI wykorzystywane w bezpieczeństwie narodowym, przestrzegają ścisłych wytycznych etycznych, szanują swobody obywatelskie oraz unikają dyskryminacji w formie uprzedzeń i dyskryminacji. Ponadto szybkie tempo wdrażania sztucznej inteligencji oznacza, że specjaliści rządowi powinny się dostosować do nowych technologii. Programy szkoleniowe i edukacyjne powinny nadążać za postępami, aby zapewnić, że osoby takie posiadają umiejętności i wiedzę wymaganą do skutecznej i etycznej obsługi systemów SI.

Przegląd mechanizmów w jaki sposób technologie SI usprawniły wykrywanie zagrożeń, analizę danych wywiadowczych, cyberbezpieczeństwo i podejmowanie strategicznych decyzji, pozwala na potwierdzenie postawionej podstawowej tezy artykułu. Stanowi ona, że sztuczna inteligencja spełnia kluczową rolę w rozszyfrowywaniu złożonych zbiorów danych, odkrywaniu ukrytych powiązań i dostarczaniu praktycznych informacji na potrzeby środków zapobiegawczych. Warto podkreślić transformacyjny wpływ sztucznej inteligencji na bezpieczeństwo narodowe, przedstawiając kompleksową analizę SI. Ponadto implementacja sztucznej inteligencji w obszarze bezpieczeństwa państwa rodzi również pewne wyzwania i ryzyka, w tym możliwość nadużyć władzy, naruszenie prywatności obywateli czy też błędy w algorytmach, prowadzące do nietrafnych decyzji. Dlatego ważne jest odpowiednie regulowanie i nadzorowanie wykorzystania sztucznej inteligencji celem zapewnienia bezpieczeństwa państwa przy jednoczesnym respektowaniu praw człowieka. Przy czym władze państwowe są zobowiązane do brania pod uwagę faktu, że wykorzystanie sztucznej inteligencji w działaniach policyjnych wymaga odpowiedniego nadzoru i regulacji, żeby zapewnić ochronę prywatności obywateli, uniknąć dyskryminacji oraz zapobiec nadużyciom władzy. Ważne jest również odpowiednie szkolenie funkcjonariuszy, odpowiedzialnych za bezpieczeństwo państwa w zakresie wykorzystania nowych technologii oraz przestrzeganie zasad etyki i praw człowieka.

Przy wykorzystaniu sztucznej inteligencji, w wykrywaniu terroryzmu i przestępczości, należy pamiętać, że wiąże się również z wyzwaniami i potencjalnymi ryzykami, takimi jak ochrona prywatności, fałszywie pozytywne wyniki czy też nadużycia władzy. Dlatego istotnym byłoby odpowiednie regulowanie i nadzorowanie wykorzystania sztucznej inteligencji w tym

kontekście, żeby zapewnić skuteczność działań i jednocześnie chronić prawa jednostki.

Sztuczna inteligencja w pracy służb, odpowiedzialnych za bezpieczeństwo, pozwala zapobiegać cyberatakom lub je minimalizować. Korzystając ze sztucznej inteligencji, organy bezpieczeństwa są w stanie nie tylko monitorować nietypową aktywność sieciową, identyfikować potencjalne luki w danych i wzmacniać ograniczenia dostępu do krytycznych danych ale też poprawić dokładność systemów wykrywania włamań. Pozwala to symulować cyberataki w kontrolowanych środowiskach celem identyfikacji słabych punktów systemu[34].

Należy podkreślić też, że razem z rosnącymi możliwościami uczenia maszynowego i sztucznej inteligencji, wykrywanie słabości w obszarach szeroko rozumianego bezpieczeństwa zostanie zautomatyzowane w stopniu, który obecnie nie jest możliwy i być może nastąpi szybciej niż obrona kontrolowana przez człowieka mogłaby skutecznie zadziałać.

Władze państwowe powinny podkreślać znaczenie kompleksowych programów szkoleniowych, odgrywających kluczową rolę w wypełnieniu luki między istniejącymi zestawami umiejętności a wymaganiami ery sztucznej inteligencji. Programy takie zarówno przekazują podstawową wiedzę na temat sztucznej inteligencji, jak i uczą specjalistycznych umiejętności, potrzebnych instytucjom odpowiedzialnym za bezpieczeństwo, żeby zrozumieć, w jaki sposób sztuczna inteligencja może pomóc im w różnych aspektach ich pracy, w tym w wykrywaniu i zwalczaniu zagrożeń dla bezpieczeństwa państwa. Stała edukacja może pomóc agencjom rządowym na bieżąco poznawać najnowsze osiągnięcia i najlepsze praktyki w zakresie sztucznej inteligencji. Ponieważ SI wciąż się rozwija, programy szkoleniowe powinny być szybko dostosowywane, żeby wyposażyć agencje rządowe w najbardziej odpowiednie umiejętności i wiedzę.

[34] W. Müller, C. Vincent, and N. Bostrom. "Future Progress in Artificial Intelligence: A Survey of Expert Opinion." *Fundamental Issues of Artificial Intelligence*, 2014, 555–572.; https://www.csis.org/analysis/addressing-national-security-implications-ai; https://thebulletin.org/2018/02/artificial-intelligence-and-national-security/ (dostęp dnia 25.05.2024)

Bibliografia

1. Anderson D., *Attacks in London and Manchester, March-June 2017: Independent Assessment of MI5 and Police Internal Reviews* London, Brick Court Chambers, 2017.
2. Babuta A.,Oswald M.,Janjeva A., *Artificial Intelligence and UK. National Security Policy Considerations,* Royal United Services Institute for Defense and Security Studies RUSI London April 2020.
3. Grobbelaar, Marius, *Deploying Artificial Intelligence (AI) to support law enforcement agencies in crime scene analysis and management*
4. Lomlen S., *Impact of Artificial Intelligence in enhancing National Security* "Artificial Intelligence Studies 1 February 2024 University of Nairobi
5. Martin P., *The Rules of Security: Staying Safe in a Risky World* Oxford, Oxford University Press, 2019.
6. Rawat Y.,Gupta Y.,Khothari G.,Mittal A.,Rautela D., *The Role of Artificial Intelligence in Biometrics,* 2023 2nd International Conference on Edge Computing and Applications *(ICECAA)*, Namakkal, India, 2023.
7. Redden J., Aagaard B., Taniguchi T., *Artificial Intelligence Applications in Law Enforcement: An Overview of Artificial Intelligence Applications and Considerations for State and Local Law Enforcement* NCJ Number 255994 August 2020
8. Hal D. W. I Pesenti J., *Growing the Artificial Intelligence Industry in the UK*, Oct. 15, 2015.
9. Prognozowanie kryminologiczne w wymiarze społecznym. T. 1, Metodologia, Analiza, Tendencje rozwojowe. red. B. Hołyst, Warszawa 2017.
10. Hołyst B., Malec N., Wawrzyniak Z. M. (red.), *Prognozowanie kryminologiczne w wymiarze społecznym. T. 2, Modele prognostyczne, przestępczość, wiktymizacja, profilaktyka*, Warszawa 2018.
11. Tomaszewska-Michalak M., Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce, Warszawa 2015.

Netografia

1. https://onlinewilder.vcu.edu/blog/ai-challenges-and-opportunities-national-security/
2. https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/what-is-a-zero-day-exploit.html
3. https://onlinewilder.vcu.edu/blog/ai-challenges-and-opportunities-national-security/
4. https://azure.microsoft.com/pl-pl/resources/cloud-computing-dictionary/what-are-machine-learning-algorithms
5. https://www.researchgate.net/publication/364733770_Deploying_Artificial_Intelligence_AI_to_support_law_enforcement_agencies_in_crime_scene_analysis_and_management/citation/download
6. https://www.imperva.com/learn/application-security/open-source-intelligence-osint/
7. https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021PC0206
8. https://www.europarl.europa.eu/news/pl/press-room/20240308IPR19015/akt-w-sprawie-sztucznej-inteligencji-poslowie-przyjmuja-przelomowe-przepisy