Sztuczna inteligencja w wojsku

W ostatniej wojnie z Hamasem Izrael pokazał, że dane zebrane w sieci pozwalają znaleźć słabe punkty przeciwnika i bardzo szybko doprowadzić do zwycięstwa

Wykorzystanie technologii informatycznych w działaniach militarnych kojarzy się powszechnie z „żołnierzami cyborgami" albo z robotami autonomicznymi, silnie uzbrojonymi maszynami, które poruszają się dużo szybciej niż ludzie, są bardzo silnie opancerzone oraz charakteryzują się wysoką sprawnością wykorzystania broni kinetycznej – karabinów, działek oraz artylerii rakietowej. Warto przypomnieć roboty zaprezentowane przez firmę Boston Dynamics, takie jak dwunożny Atlas czy też czworonożny Spot, których prezentacje w internecie wywołały pewne zaniepokojenie wśród wielu osób. Są one projektowane i budowane dla armii amerykańskiej ze środków finansowych pochodzących z agencji DARPA. Natomiast cyborgizacja żołnierza polega na zastosowaniu cyfrowych systemów wspomagających naturalne systemy percepcji człowieka, takie jak widzenie w ciemności, w podczerwieni, implanty słuchowe i systemy wzmacniające zdolności fizyczne w formie egzoszkieletów. To projekty realizowane w ścisłym związku z ideologią transhumanizmu, które mają za zadanie stworzenie superczłowieka. Jednak na współczesnym polu walki takie autonomiczne roboty nie są jeszcze wykorzystywane.

Algorytmy w praktyce

Sztuczna inteligencja znalazła swoje miejsce w zastosowaniach militarnych na polu, na którym osiąga najlepsze rezultaty, czyli w zastosowaniach Big Data. Analiza dużych zbiorów danych była już wielokrotnie opisywana na łamach „Naszego Dziennika" (Algorytmy w służbie władzy, 1 lipca 2019). Do kanonu opowieści o ich możliwościach należy np. opis efektów ich wykorzystywania przez burmistrza Nowego Jorku Michaela Bloomberga. Zastosował je już w 2013 r. w celu identyfikacji „nielegalnych mieszkań", w których wybuchały pożary. Do zarządu Nowego Jorku co roku trafiało ponad 25 tysięcy skarg mieszkańców w tej sprawie. Ale burmistrz dysponował jedynie 200 etatami dla inspektorów budowlanych i nie byli oni w stanie sprawdzić wszystkich lokali. Polecił on więc informatykom stworzenie bazy danych prawie miliona budynków, które zostały opisane przez bardzo dużą ilość parametrów, pochodzących ze wszystkich urzędów, policji, banków oraz firm telekomunikacyjnych. W bazie zebrano wszystkie informacje dotyczące np. płacenia podatków, spóźnionych opłat, wskaźników przestępczości, wizyt karetek pogotowia, odbiegającego od normy zużycia gazu, wody i prądu, metod płatności za usługi miejskie i wielu innych danych. Analiza Big Data dotyczyła znalezienia korelacji pomiędzy tymi danymi a informacjami o pożarach w ciągu ostatnich pięciu lat. Wyniki analizy numerycznej wykazały, że pożary występowały częściej w budynkach określonego typu i zbudowanych w konkretnych latach.

Specjaliści wskazują, że potencjał informatyczny armii izraelskiej może być porównywalny z firmami Big Tech, takimi jak Google i Facebook

Znaleziono również inne „dziwne" korelacje, np. dotyczące wysokiego prawdopodobieństwa, że w lokalu opłacającym media w formie transakcji gotówkowej częściej dochodzi do różnego rodzaju przestępstw. Urzędnicy korzystający z tych wyników szybko wskazali skargi, które wymagają natychmiastowej interwencji. Ta metoda okazała się niezwykle skuteczna. Bez stosowania wyników analiz Big Data inspektorzy jedynie w 13 proc. domów znajdowali niezgodne z prawem przebudowy lokali, po zastosowaniu algorytmów sprawność wzrosła do ponad 70 proc. Metoda ta pozwoliła zwalczyć plagę pożarów w Nowym Jorku.

Majowy atak na Hamas przygotowywany był przez wiele miesięcy. Wywiad izraelski zbierał ogromne ilości danych z milionów zdjęć satelitarnych, nasłuchów radiowych, informacji zdobywanych od lokalnych operatorów sieci komórkowych

FOT. ISRAEL POLICE

Precyzyjny wybór celów

Big Data szybko znalazła zastosowanie w planowaniu działań militarnych. Przecież w walce z wrogiem armia też może wykorzystywać taką analizę i wyznaczyć cele ataku w taki sposób, aby były one jak najskuteczniejsze. Taką właśnie metodę wybrała armia izraelska podczas ostatniej operacji wojskowej przeciw Hamasowi i Palestyńskiemu Islamskiemu Dżihadowi przeprowadzonej w maju tego roku. Analizy symulacyjne Big Data były jednak wykonywane w czasie rzeczywistym, na bieżąco wyznaczano cele ataków rakietowych w sposób tak szybki, że człowiek po uruchomieniu niektórych systemów ofensywnych nie podejmował już decyzji w odniesieniu do konkretnych celów, ale robiły to algorytmy. Zatem nie tylko proces wyznaczania celów został przekazany sztucznej inteligencji, ale również decyzje dotyczące odpowiednich rodzajów broni ofensywnej oraz czasu i miejsca ich użycia. Rola ludzi – żołnierzy została zredukowana do obserwacji efektów uderzenia oraz akcji końcowych, które często oznaczały jedynie uporządkowanie terenów po skutecznym ataku rakietowym. W klasycznych metodach analizy Big Data procesy symulacyjne i analityczne trwają niekiedy wiele miesięcy, a zespoły specjalistów informatyków, które nad nimi pracują, wielokrotnie weryfikują wyniki i poszukują jak najlepszych rozwiązań.

Ogromna skuteczność

Algorytmy sztucznej inteligencji analizują dane miliony razy szybciej niż ludzie i są w stanie jednocześnie przetwarzać tak ogromne ilości informacji, których zespół ludzi nie byłby w stanie nawet przeczytać w ciągu wielu lat. Dlatego wyniki analiz dokonane przez algorytmy często są trudne do zrozumienia dla człowieka, który poszukuje przyczyny i chce w logiczny sposób powiązać zbiory faktów. Sztuczna inteligencja nie przejmuje się takim „staroświeckim" sposobem analizy danych, stosuje jedynie metody korelacyjne, poszukując takich związków pomiędzy różnymi rodzajami danych, na jakie człowiek nie zwróciłby nawet uwagi.

W czasie kampanii prezydenckiej Baracka Obamy w 2005 r. taką korelacją okazała się zwiększona liczba rowerów pozostawianych przez klientów barów szybkiej obsługi. Nikt nie wiedział, dlaczego w dzielnicach, w których obserwowane jest takie zjawisko, notowania kandydata demokratów są wyższe. Sztaby wyborcze nie zajmowały się wytłumaczeniem tego zjawiska, ale wykorzystały je bezpośrednio w kampanii. Od tamtej pory dysponujemy już przykładami tysięcy podobnych korelacji, dla których próżno szukać jednoznacznego logicznego wytłumaczenia, ale których stosowanie jest skuteczne. A ponieważ to właśnie skuteczność, a nie dobro, prawda i piękno są atrybutami współczesnych liderów „postępu cywilizacyjnego", przestali oni już poszukiwać przyczyn i logicznych konsekwencji, a skupili się jedynie na skuteczności i kompetencjach. W tych atrybutach sztuczna inteligencja ma nad człowiekiem potężną przewagę, jest „diabelnie" skuteczna i posiada olbrzymie kompetencje w rozwiązywaniu konkretnych problemów, jeśli tylko dostarczymy jej odpowiednio dużą ilość danych i nie jest tutaj istotna ich jakość, a jedynie ilość.

Kiedy mówimy o tzw. zagrożeniach hybrydowych, to również nie do końca rozumiemy, jakich metod użyje wróg w celu osłabienia naszych zdolności obronnych, wiemy jedynie, że będą one różnorodne i jako główne narzędzie będą wykorzystywały systemy zarządzania treściami informacyjnymi. Dzisiaj są to media cyfrowe, w których dominuje dezinformacja i kłamstwa (fake newsy), zmanipulowane filmy wideo i pliki dźwiękowe, a także fałszywe e-maile i newsy agencji prasowych. Aby je skutecznie wdrożyć, konieczne są specjalna infrastruktura serwerowa oraz algorytmy sztucznej inteligencji. W realnych działaniach militarnych coraz ważniejsze są informacje zbierane przez całe eskadry automatycznych dronów, które są analizowane z wykorzystaniem superkomputerów w czasie rzeczywistym.

Precyzyjny atak

Podczas konfliktu w Górskim Karabachu pod koniec ubiegłego roku armia Azerbejdżanu wykorzystała tę technologię na szeroką skalę. Azerskie drony przenikały daleko poza linie obrony armii armeńskiej i zbierały istotne informacje wywiadowcze dotyczące rozlokowania wojsk przeciwnika. Pozwoliło to armii azerskiej zdobyć ogromną przewagę i odnieść zwycięstwo w tym konflikcie militarnym.

Podobną taktykę, jednak znacznie wzmocnioną algorytmami sztucznej inteligencji, zastosowała armia Izraela. Musimy przypomnieć sobie, że wojna Izraela z Hamasem trwa od wielu lat, przybiera jedynie różne formy. Hamas przejął Strefę Gazy w 2007 r. i od tamtej pory armia izraelska już trzy razy atakowała infrastrukturę Hamasu, aby zniwelować jego zdolności wojskowe. Jednak po każdym ataku Hamas szybko odbudowywał swój potencjał. Ataki izraelskie niszczyły jedynie te najbardziej widoczne obiekty militarne wykorzystywane przez terrorystów z Hamasu, pod ziemią pozostawała olbrzymia sieć tuneli, a terroryści po prostu przenosili się w inne miejsce i szybko odbudowywali swój potencjał militarny.

W maju premier Izraela Beniamin Netanjahu oficjalnie zapowiedział, że najbliższy atak będzie zupełnie inny i zniszczy Hamas raz na zawsze. Majowy atak na Hamas przygotowywany był przez wiele miesięcy. Wywiad izraelski zbierał ogromne ilości danych z milionów zdjęć satelitarnych, nasłuchów radiowych, informacji zdobywanych od lokalnych operatorów sieci komórkowych oraz terabajty danych pochodzących z sieci internetowej, głównie z portali społecznościowych. Pierwsze uderzenie przygotowano więc bardzo skrupulatnie, ale nie to jest najważniejsze. Było oczywiste, że zaraz po uderzeniu oddziały Hamasu będą chciały przeprowadzić kontrofensywę, wiec dokonają przegrupowania sił i użyją broni, która nie została zniszczona podczas pierwszego uderzenia. I tutaj do działań militarnych przystępują odpowiednio wytrenowane algorytmy sztucznej inteligencji. Jak pisał „The Jerusalem Post" w dniu 27 maja 2021 r.: „Izraelska operacja przeciwko Hamasowi była pierwszą na świecie wojną SI – Sztucznej Inteligencji". Oficjalny komunikat armii izraelskiej IDF (Israel Defense Force) podany na jej stronach internetowych już po zakończeniu działań militarnych stwierdzał: „Po raz pierwszy sztuczna inteligencja była kluczowym elementem i mnożnikiem siły w walce z wrogiem". IDF zbudowało zaawansowaną platformę sztucznej inteligencji, która po raz pierwszy stosowała autonomiczne systemy podejmowania decyzji w zastosowaniach militarnych. W jednym miejscu zebrano wszystkie dane na temat grup terrorystycznych w całej Strefie Gazy, uzupełniając je informacjami sieciowymi i danymi satelitarnymi. Izraelscy żołnierze informatycy z elitarnego korpusu wywiadowczego opracowali specjalistyczne algorytmy sztucznej inteligencji, które nazwali: Alchemik, Ewangelia i Głębia Mądrości. Umieszczono w nich dane z systemów wywiadu radiowego, sieciowego i światłowodowego – SIGINT oraz ze zdjęć satelitarnych i dostarczonych przez drony – VISINT.

Dzięki użyciu algorytmów sztucznej inteligencji Izraelowi udało się w sensie militarnym osiągnąć więcej w czasie 50 godzin walk niż podczas 50 dni wojny w 2014 roku

Dane pochodzące ze standardowych działań wywiadowczych wykorzystujących szpiegów i tajnych współpracowników umieszczono w systemie HUMINT. Systemy te, zarządzane nadrzędnym algorytmem sztucznej inteligencji, wyznaczały podstawowe cele ataku. Po każdym z nich system aktualizował swoje dane na podstawie informacji dotyczących skuteczności oraz zmian na polu walki i w czasie rzeczywistym wyznaczał nowe cele.

Wstępne analizy wskazują, że oprócz pierwotnie ustalonych celów już w trakcie trwania ataku sztuczna inteligencja wyznaczyła ponad 200 nowych celów i sama podjęła decyzję o ich zniszczeniu. Wśród nowych celów były m.in. wyrzutnie rakiet wycelowane w Tel Awiw i Jerozolimę. Hamas nie zdążył ich użyć, ponieważ wymagało to decyzji człowieka, algorytmy okazały się szybsze.

Wykorzystując system SI, przeprowadzono setki precyzyjnych uderzeń rakietowych na wybrane cele, zniszczono: wyrzutnie rakiet, miejsca produkcji i przechowywania rakiet, siedziby wywiadu wojskowego, miejsca ukrywania się dowódców i specjalnych grup komandosów Hamasu. Dzisiejsze szacunki wskazują, że zniszczono ponad 90% infrastruktury Hamasu, autonomiczne łodzie podwodne przenoszące ładunki wybuchowe, broń i amunicję, zarówno Hamasu, jak i Palestyńskiego Islamskiego Dżihadu. Niektóre cele były umieszczone w miejscach publicznych, np. 14 wyrzutni rakietowych zostało przez terrorystów umieszczonych w pobliżu szkoły podstawowej. Bez zastosowania specjalistycznych algorytmów unieszkodliwienie takich obiektów bez zniszczenia szkoły byłoby niemożliwe. IDF podaje, że zabito ponad 150 dowódców oddziałów Hamasu, co uniemożliwi szybką odbudowę tej organizacji.

Podczas ataku zniszczona została również sieć tuneli Hamasu, która miała setki kilometrów długości i przebiegała pod dzielnicami mieszkalnymi. Użycie algorytmów sztucznej inteligencji umożliwiło dokładne zmapowanie całej sieci i wyznaczenie celów skierowanych w miejsca krytyczne, których zniszczenie sparaliżowało ich funkcjonowanie. Wyniki analiz Big Data wyznaczyły tak dokładne parametry tuneli, dotyczące zarówno ich głębokości, jak i grubości, że możliwe było zastosowanie odpowiednich typów amunicji, która niszczyła jedynie tunele, a nie okoliczne budynki.

Na portalu społecznościowym Twitter (https://t.co/DAx6z1kyN9) Hamas zamieścił film, na którym możemy zobaczyć proces wykopywania ciał terrorystów Hamasu z tunelu zniszczonego przez precyzyjny atak izraelski. Była to jednostka przemieszczająca się w miejsce ataku na żołnierzy izraelskich i została zniszczona tuż obok widocznego na filmie muru, który odgradza Strefę Gazy od Izraela. Celność izraelskich pocisków wyznaczana jest już w centymetrach, a miejsce ataku określane jest w czasie rzeczywistym przez algorytmy SI.

Każdy dowódca oddziałów izraelskich został wyposażony w specjalny tablet. Otrzymywał na nim w czasie rzeczywistym informacje z systemu sztucznej inteligencji, który wskazywał cele, zagrożenia i opcje dotyczące najlepszych w danej chwili działań militarnych. Należy wyraźnie zaznaczyć, że wszystkie algorytmy stosowane w armii izraelskiej zostały w całości opracowane w izraelskich firmach informatycznych przez wyszkolonych żołnierzy-informatyków. Specjaliści wskazują, że potencjał informatyczny armii izraelskiej może być porównywalny z firmami BigTech, takimi jak Google i Facebook, pomimo dużo mniejszych nakładów finansowych. Najważniejszą przewagą izraelskich informatyków jest pozostawienie im dużej autonomii przy wysokim i bardzo szybkim finansowaniu autorskich projektów.

Podobno każdy żołnierz informatyk może zgłosić projekt i decyzja o jego finansowaniu i wdrożeniu podejmowana jest w ciągu 48 godzin. To system stosowany również w innych strukturach armii izraelskiej, gdzie np. szeregowi żołnierze mają wpływ na wybór dowódcy swojego oddziału. Obecnie Izrael inwestuje ogromne środki finansowe w rozwój sztucznej inteligencji. Niewątpliwie rozwiązania SI są bardzo skuteczne, efektywne i obniżają koszty wielu projektów, ale ich stosowanie w armii musi budzić głębokie kontrowersje.

Specjaliści jednoznacznie wskazują, że w konflikcie w Strefie Gazy dzięki użyciu algorytmów sztucznej inteligencji Izraelowi udało się w sensie militarnym osiągnąć więcej w czasie 50 godzin walk niż podczas 50 dni wojny w 2014 roku. Tylko dokąd zaprowadzą nas coraz bardziej efektywne i skuteczne algorytmy sztucznej inteligencji stosowane w konfliktach militarnych? Czy umożliwienie podejmowania decyzji przez algorytmy SI zupełnie wyeliminuje człowieka i sprowadzi go jedynie do roli wykonawcy algorytmicznych rozkazów? A jak ogromną władzę zyskają twórcy algorytmów, informatycy wojskowi, którzy tworzą systemy i jedynie na etapie projektu mają wpływ na ich działanie?

Po uruchomieniu skomplikowany system SI działa samodzielnie, uczy się na podstawie dostarczonych danych, przeprowadza symulacje różnych działań militarnych, grając sam ze sobą w coraz bardziej wyrafinowane „gry wojenne". A nie są to już jedynie wirtualne manewry, ale jak najbardziej rzeczywiste działania, w których giną ludzie, burzone są budynki, podpalane są całe dzielnice miast. Czy zdajemy sobie sprawę, jak ważne jest odpowiednie kształcenie specjalistów informatyków zarówno w zakresie sztucznej inteligencji, jak i analizy danych? Przecież to oni będą tworzyli systemy, które będą stosowane w różnego rodzaju wojnach: politycznych, militarnych czy medialnych. A czeka nas ich coraz więcej i nie będą one prowadzone jedynie w świecie wirtualnym. Ich plany i podstawowe struktury zostaną zaprojektowane przez sztuczną inteligencję, a ludzie będą mogli jedynie komentować rezultaty ich działań post factum. Zresztą już dzisiaj tak się dzieje – wielu komentatorów wydarzeń politycznych wskazuje na problem cyberbezpieczeństwa, wojen hybrydowych i nowych strategii marketingu politycznego, jednak nie zdają sobie oni dokładnie sprawy, że są one kreowane przez algorytmy, które jedynie beznamiętnie, sprawnie i skutecznie realizują wyznaczone przez ich twórców cele.

To, co się może zdarzyć w trakcie tej realizacji, często jest nie do przewidzenia, widoczne w skutkach dopiero po jakimś czasie. Zawsze są też „efekty uboczne" definiowane w działaniach militarnych jako przypadkowe, niewinne ofiary: dzieci, kobiety, zwykli obserwatorzy. To bardzo poważne problemy moralne, które powinny być dokładnie rozważone, zanim zaczniemy stosować algorytmy w systemach, które zabijają, ranią i niszczą. Dlatego tak ważne jest kształcenie informatyków nie tylko na polu profesjonalnych umiejętności, ale przede wszystkim na podstawowych wartościach, które zawsze powinny być najważniejszym drogowskazem dla wszystkich działań wykorzystujących zaawansowane technologie informatyczne, które zdobywają coraz większe znaczenie we współczesnym świecie. Całe szczęście w Wyższej Szkole Kultury Społecznej i Medialnej kształcimy takich informatyków. ●

Dr Grzegorz Osiński