

Sztuczna inteligencja doprowadzi do wojny jądrowej?

9 września 2019

Zastosowanie sztucznej inteligencji w wojsku może doprowadzić do wojny jądrowej między Stanami Zjednoczonymi a Rosją – twierdzi były podsekretarz obrony USA Robert Work. Swoją opinią podzielił się na łamach „Breaking Defense”.



Wyjaśnijmy: nie chodzi o zbuntowane roboty, które wbrew poleceniom człowieka, wystrzelą w kierunku Ziemi setki pocisków z głowicami jądrowymi, ale o błędy sztucznej inteligencji możliwe w sytuacjach delegowania pełnomocnictw w zakresie przeprowadzania ataków i błędnej oceny niegroźnych czynników jako stwarzających zagrożenie.

Brzmi groźnie. Spróbujmy określić, w jakich obszarach wykorzystuje się sztuczną inteligencję w armii. Umownie mówiąc, jest ich pięć:

- programy podsystemów sprzętu wojskowego;
- systemy zarządzania technologiami informatycznymi;
- systemy informacyjne zestawów uzbrojenia;

- systemy informacyjne zarządzania i wymiany informacji jednostek i związków taktycznych;
- systemy informacyjne wspierające dowództwo wojskowe w podejmowaniu decyzji.

Doradź, jak zaatakować

Do pierwszej kategorii należą programy, które sterują np. pociskami samonaprowadzającymi się na cel, cyfrowym inercyjnym systemem nawigacyjnym lub, powiedzmy, systemem sterowania silnikiem współczesnego samolotu lub czołgu. Historia tworzenia takich systemów komputerowych ma kilka dekad, a ich rozwój ma raczej ewolucyjny charakter. Nowe technologie pracy z danymi nie są tutaj tak aktywnie wykorzystywane.

Druga kategoria obejmuje bojowe informacyjne systemy zarządzania nowoczesnymi egzemplarzami złożonego sprzętu wojskowego, tj. samoloty lub okręty. Tutaj znajdują zastosowanie algorytmy wykorzystujące nowoczesne technologie – na przykład, do natychmiastowej analizy informacji ze wszystkich podsystemów modelu sprzętu, a także do wydawania rekomendacji załódze.

Sztuczna inteligencja i Iskander-M

Trzeci rodzaj oprogramowania pozwala na pracę z różnego rodzaju sprzętem, zintegrowanym w złożony system broni. Na przykład, nowoczesny system rakietowy Iskander-M obejmuje dwie wyrzutnie, pojazd transportowy i załadunkowy, centrum przygotowania informacji o celu oraz pojazd dowodzenia.

Zarządzanie wszystkimi jednostkami kompleksu odbywa się za pośrednictwem odpowiedniego oprogramowania, które współpracuje z programami każdego modelu sprzętu. Znajdują tu zastosowanie nowe technologie, ale podobnie jak podczas tworzenia oprogramowania dla prototypów sprzętu technicznego, ich

wdrażanie przebiega stopniowo.

Iskander-M

Czwarty typ to duża i niezwykle ważna klasa systemów, które zapewniają dowodzenie jednostkami wojskowymi na różnych poziomach. Pojawienie się w tej sferze nowych technologii do pracy z danymi wywołało prawdziwą rewolucję, ponieważ zapewniają one zarządzanie każdą jednostką, każdym modelem urządzenia z dowolnej odległości w czasie rzeczywistym.

Tego typu systemy działają w dwóch kierunkach – gromadzą, analizują oraz prezentują zebrane informacje i wnioski specjalistom z centrali i innym odbiorcom informacji, a także transmitują rozkazy z centrali do niższych struktur.

Jak to działa? Szukamy pocisków manewrujących

Prosty przykład gromadzenia i analizy informacji przy użyciu nowoczesnych technologii. Analiza zachowania tysiąca ciężarówek kontenerowych na drogach określonego państwa pozwala systemowi samouczącemu się zidentyfikować pojazdy, które przypuszczalnie przewożą zamaskowane wyrzutnie pocisków manewrujących.

Pozyskanie danych o przepływach ruchu przy użyciu nowoczesnych satelitarnych systemów obserwacyjnych nie jest trudne, a reszta jest wynikiem pracy grupy analityków i specjalnego oprogramowania.

Bardziej jaskrawym przykładem jest sytuacja, w której na podstawie fragmentarycznych danych wywiadowczych, w wyniku intelektualnej analizy informacji, wyciąga się wniosek na temat możliwej lokalizacji w określonym obszarze formacji wojskowej lub kwatery głównej, które nie zostały jeszcze wykryte za pomocą wywiadu wizualnego lub elektronicznego.

Oczywiście takie systemy mogą gromadzić informacje ze wszystkich niższych systemów, a także z sąsiednich podobnych lub wyższych systemów. W ten sposób można utworzyć jednolite pole informacyjne operacji bojowej, a przy zróżnicowanym poziomie dostępu systemy niższego poziomu – czołgi, okręty i samoloty – mogą otrzymać ten obraz informacji.

W ten sposób powstaną nowe możliwości informacyjne współczesnej walki – gdy pilot samolotu zobaczy wrogie samoloty wykryte z okrętu, a cel zaobserwuje z obrazu nadawanego z tabletu wywiadowcy. Częściowo takie systemy zostały już wdrożone, ale ich zastosowanie nie jest jeszcze uniwersalne.

Co z tą wojną nuklearną?

A teraz o artykule w „Breaking Defense” – kontroli uzbrojenia jądrowego, rosyjskim systemie „Perimetr” i itp.

Piąty obszar, w którym wykorzystywana jest sztuczna inteligencja. Systemy, które właściwie powinno się nazywać systemami wspomagania w podejmowaniu decyzji. Faktycznie mogą tworzyć nowe informacje – szacować ukryte zasoby wroga, przewidywać jego działania i opracowywać scenariusze odwetowe w danych warunkach, biorąc pod uwagę zasoby i możliwości militarne kraju. W takich systemach, z definicji, należy stosować najbardziej zaawansowane i niezawodne rozwiązania programowe. Cena błędu jest bardzo wysoka.

Niemniej jednak jednym z pierwszych systemów, które mogą podejmować decyzje bez interwencji człowieka, był późny radziecki „Perimetr”, który, jak się uważa, gwarantuje przeprowadzenie ataku odwetowego z użyciem międzykontynentalnych pocisków balistycznych w przypadku likwidacji wyższego dowództwa wojskowego kraju.

Używamy słowa „uważa się”, ponieważ wszystkie informacje o „Perimetrze” są tajne. Nie ma oficjalnych danych dotyczących

„automatycznych” decyzji podejmowanych przez ten system. Jednocześnie (znowu) uważa się, że właśnie w „Perimetrze” implementowane są algorytmy, które pozwalają na stosowanie różnych podsystemów sterowania, w tym komputerowych, w celu zagwarantowania ochrony przed nieuprawnionym uruchomieniem.

Trzęsienie ziemi doprowadzi do wystrzelenia rosyjskich pocisków?

Były podsekretarz obrony USA Robert Work we wspomnianym wyżej artykule w „Breaking Defense” wyraził obawy, że „Perimetr” może interpretować aktywność sejsmiczną jako wybuch jądrowy, a następnie wysłać zapytanie do sztabu armii i (nagle), bez „ludzkiej” odpowiedzi, wystrzeli międzykontynentalne pociski balistyczne.

Jest to bardzo mało prawdopodobne. Chodzi o to, że niezwykle trudno jest pomylić sejsmiczny obraz wybuchu jądrowego z czymś naturalnym. Ponadto trudno sobie wyobrazić, że „Perimetr” podejmie decyzję na podstawie danych z czujników sejsmicznych, nie mając żadnych informacji o agresji ze strony SPRN (system ostrzegania przed atakiem rakietowym) i systemu obrony powietrznej kraju. Te systemy z kolei nie mogą zostać zniszczone niezauważalnie, tak więc bez „narządów zmysłów” „Perimetr” w żadnym wypadku nie zostanie.

Czyli, jeśli nikt nie wystrzelił rakiet ani nie wysłał samolotów bojowych, ale jednocześnie zachodzą jakieś lokalne zjawisko sejsmiczne, to dla „Perimetra” z prawie 100-procentowym prawdopodobieństwem nie jest to wojna.

Zakładając nawet czysto hipotetyczne prawdopodobieństwo, że, na przykład, sztab generalny nie odpowie na prośby systemu. Co więcej, jeśli jeden z rezerwowych posterunków dowodzenia lub Kreml przetrwają, to dla „Perimetra” nadal nie jest to wojna i nie ma powodu, by wystrzeliwać międzykontynentalne pociski balistyczne.

Radziecki człowiek jest bardziej niezawodny niż maszyny

Jednak teoria automatycznego uruchamiania „Perimetra” jest sprzeczna z tradycyjnym konserwatyzmem w rozwiązaniach technicznych na poziomie strategicznym w Związku Radzieckim. Tam, gdzie było można, pracował człowiek, a podejmowanie ważnych decyzji w ZSRR nie zawierzano żadnym systemom cyfrowym.

Teraz do tego świadomego konserwatyzmu dodano jeszcze pewne nieprzygotowanie technologii komputerowej do najnowocześniejszych rozwiązań programowych, jednak rosyjska szkoła programowania ma bardzo duży potencjał, więc wdrożenie wszystkich najnowocześniejszych rozwiązań opartych na technologiach sztucznej inteligencji jest tylko kwestią woli politycznej i koncepcyjnego zrozumienia metod zastosowania takich decyzji.

Mówiąc prościej: kiedy zostanie podjęta decyzja co i jak wykorzystać oraz w jakim stopniu można powierzyć najważniejsze systemy obrony komputerom, kiedy zostanie to wdrożone w dość krótkim czasie. Sądzę, że w ciągu 3-5 lat.

Autorstwo: Dmitrij Korniew

Zdjęcie: [Thierry Ehrmann](#) (CC BY 2.0)

Źródło: pl.SputnikNews.com