

Zagrożenia hakerskiego ataku na sztuczną inteligencję

22 lutego 2018

Grupa naukowców z Uniwersytetów Yale, w Cambridge oraz Oksfordzie oraz eksperci ds. wojskowych ostrzegają, że hakerzy mogą atakować luki w systemach sztucznej inteligencji i wykorzystywać te systemy do przeprowadzania zautomatyzowanych cyberataków, manipulowania opinią publiczną czy spowodować, by komercyjne drony zaczęły atakować wybrane cele. W 98-stronicowym raporcie pt. „Malicious Use of Artificial Intelligence” pojawiło się też wezwanie do zbadania możliwości manipulowania sztuczną inteligencją oraz do przygotowania się na tego typu ataki.

„Wszyscy zgadzamy się, że SI ma wiele pozytywnych zastosowań. Jednak w literaturze fachowej istnieje poważna luka dotycząca jej złośliwego wykorzystania”, mówi Miles Brundage z Oxford University.

W raporcie zwrócono uwagę, że w przyszłości przestępcy będą mogli wykorzystać SI do przeprowadzenia cyberataków na skalę, jaka obecnie nie jest możliwa. Systemy sztucznej inteligencji będą w stanie zidentyfikować najśłabsze cele, uniknąć wykrycia i na bieżąco dostosowywać metodę ataku do działań obronnych. „Bardziej złożone hakerskie narzędzia SI będą bardziej wydajne od wszystkiego co w przeszłości było możliwe i za jakiś czas ich umiejętności będą porównywalne z umiejętnościami ludzi” – stwierdzają autorzy raportu. Jeden z zarysowanych przez nich scenariuszy ataku to DDoS przeprowadzony w taki sposób, że systemy obronne nie będą w stanie odróżnić łączących się z serwerami botów od działań ludzi. Wyposażone w sztuczną inteligencję boty będą bowiem w stanie działać tak, że wykonywane przez nie czynności (np. naciśnięcia klawiszy czy sposób nawigowania po witrynie) będą nie do odróżnienia od sposobu działania ludzi.

Jeszcze innym typem zagrożenia jest możliwość masowego śledzenia dużych obszarów czy przeprowadzenie skoordynowanego ataku. Nietrudno wyobrazić sobie czasy, gdy drony dostarczające zamówione przez internet towary staną się powszechnym widokiem w miastach. Hakerzy, wykorzystując sztuczną inteligencję, mogą przejąć kontrolę nad olbrzymimi grupami takich dronów i wykorzystać ich kamery do śledzenia dużych obszarów czy nakazać dronom przeprowadzenie fizycznego ataku na konkretny obiekt czy osobę. Poruszające się z prędkością kilkudziesięciu kilometrów na godzinę drony mogą poważnie uszkodzić wiele przedmiotów czy zranić lub zabić człowieka.

Na razie specjaliści zajmujący się sztuczną inteligencją skupiają się na zwiększaniu jej możliwości. Należy jednak już teraz myśleć o rozwiązaniach technologicznych i prawnych, które zapewnią ochronę przed przejęciem i niewłaściwym wykorzystaniem sztucznej inteligencji.

Autorstwo: Mariusz Błoński

Na podstawie: ITPro.co.uk

Źródło: KopalniaWiedzy.pl