Raport OSW: Chińskie inteligentne samochody mogą służyć do sabotażu i aktów terroryzmu

Rozwój inteligentnych samochodów idzie w parze z obawami o bezpieczeństwo narodowe – wynika z najnowszego raportu Ośrodka Studiów Wschodnich. Michał Bogusz z OSW ocenił w rozmowie z PAP, że zagrożenia są związane przede wszystkim z wykorzystaniem pojazdów do celów wywiadowczych, sabotażu czy aktów terroryzmu.

Na polskim i europejskim rynku pojawia się coraz więcej inteligentnych samochodów, które mają możliwość ekspansywnego zbierania danych – wynika z najnowszego raportu OSW. Takie pojazdy są wyposażone w technologie łączności, które umożliwiają skanowanie otoczenia, geolokalizację,

komunikację z infrastrukturą i zdalne usługi w czasie rzeczywistym.

Autorka raportu OSW Paulina Uznańska zwraca uwagę, że choć technologie te starają się dziś rozwijać i wdrażać wszystkie koncerny samochodowe, obecnie globalnym liderem w tym obszarze staje się Chińska Republika Ludowa (ChRL). Udział chińskich pojazdów osobowych w sprzedaży w Polsce osiągnął około 7 proc. po pierwszych dziewięciu miesiącach 2025 roku, a w samym październiku przekroczył 10 proc.

Jak podkreślono w raporcie, rozwój inteligentnych pojazdów w Chinach idzie w parze z obawami o bezpieczeństwo narodowe – chińskie instytucje państwowe same wskazują na szereg wynikających z tego zagrożeń dla cyberbezpieczeństwa.

Podkreśla to także Michał Bogusz, analityk w Zespole Chińskim Ośrodka Studiów Wschodnich w rozmowie z PAP, tłumacząc, że wszystkie inteligentne samochody – czyli te posiadające zintegrowany system komputerowy zarządzający wszystkimi funkcjami pojazdu – mogą stanowić zagrożenie dla cyberbezpieczeństwa zarówno poszczególnych użytkowników, jak i całych krajów.

„Po pierwsze, to jest po prostu gigantyczna platforma czujników dalekiego zasięgu. Taki system zbiera nie tylko informacje o bezpośrednim otoczeniu samochodu, ale i o tym, gdzie on się porusza czy z jakimi sieciami czy urządzeniami wchodzi w interakcję” – wyjaśnił. „A kilkanaście takich samochodów to już cała sieć czujek, które są kontrolowane przez jeden system” – dodał.

Bogusz zwrócił uwagę, że jeśli np. podczas narady w Sztabie Generalnym Wojska Polskiego obok budynku przejedzie kilkanaście inteligentnych samochodów, będą w stanie zebrać dane m.in. o tym, czyje telefony są aktywne w tym momencie w tym budynku. I, jak podkreślił, mogą to być bardzo cenne informacje dla zagranicznych służb.

Inteligentne auta mogą także zbierać informacje z kamer i przesyłać dalej zdjęcia, w tym infrastruktury krytycznej. W związku z tym w ocenie eksperta zakaz fotografowania m.in. sieci kolejowych w Polsce jest fikcją, ponieważ te pojazdy to „odkurzacze danych, które wciągają wszystko na swojej drodze".

„Poza aspektem wywiadowczym mamy także kwestię sabotażu. Jeżeli ktoś byłby w stanie przejąć zdalnie kontrolę nad wieloma inteligentnymi autami, to mógłby doprowadzić do zablokowania wszystkich najważniejszych arterii w danym kraju" – powiedział Bogusz. „Na przykład w skrajnej sytuacji wybuchu wojny w Polsce wystarczy, że o godzinie 8.30 wszystkie elektryczne auta staną. Setki tysięcy pojazdów. Udrożnienie takich dróg zajmie godziny i to w krytycznym dla państwa momencie".

Trzecim zagrożeniem, jakie mogą nieść ze sobą takie pojazdy dla cyberbezpieczeństwa, jest w ocenie eksperta terroryzm. Bogusz przypomniał atak Izraela z września 2024 roku, w trakcie którego wybuchły pagery i krótkofalówki należące do członków Hezbollahu. Zginęło ok. 40 osób, w tym dzieci, a około 3 tys. zostało rannych.

Jak wyjaśnił ekspert, baterie, które zostały wówczas zdetonowane, w pagerach mają średnią wagę 25 gramów; z kolei najmniejsza bateria w aucie elektrycznym waży ok. 250 kg.

„To jest oczywiście skrajny przykład, ale pokazuje skalę zagrożenia dla bezpieczeństwa. Musimy zadać sobie pytanie, do czego może dojść, jeśli ktoś będzie w stanie zdalnie przejąć kontrolę i doprowadzić do wybuchu baterii w inteligentnym aucie" – powiedział.

Jak wskazano w raporcie, odpowiedzią Chin na tego typu zagrożenia jest kompleksowy system regulacji, obejmujący m.in. zakaz przesyłania za granicę danych uznawanych za ważne dla bezpieczeństwa państwa oraz wrażliwych danych osobowych

gromadzonych przez pojazdy poruszające się po chińskich drogach.

Sugerowane jest również instalowanie w inteligentnych samochodach trybu umożliwiającego wyłączenie gromadzenia informacji z otoczenia pojazdu. W przypadku zagranicznych producentów Pekin uzależnia również możliwość poruszania się w niektórych obszarach Chin od przejścia zaawansowanego procesu certyfikacji.

Pytany, jak wyglądają regulacje dotyczące inteligentnych pojazdów w Europie, Bogusz ocenił, że nie ma ich w ogóle. Według eksperta Unia Europejska dopiero zaczęła badania na ten temat i nie da się określić, ile jeszcze czasu minie, zanim pojawią się konkretne propozycje przepisów na poziomie unijnym.

„W międzyczasie władze w Chinach dążą do maksymalnego zwiększenia cyberbezpieczeństwa pojazdów w swoim kraju, jednocześnie zachowując wszystkie możliwości wpływu i działania na chińskie pojazdy eksportowane m.in. do Europy" – zaznaczył. „Nawet jeśli ktoś kupuje samochód elektryczny wyprodukowany w Europie, ale ma on baterię chińską, to z dużym prawdopodobieństwem chińskie władze mają zdalny dostęp do takiej baterii" – dodał.

Według raportu OSW do tej pory w istniejących regulacjach ChRL podchodziła do kwestii inteligentnych samochodów defensywnie – w przyszłości jednak może wykorzystać ich możliwości, by podjąć działania ofensywne.

Autorka: Agata Gutowska, PAP.