

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

**Komisja
Cyfryzacji,
Innowacyjności
i Nowoczesnych
Technologii**

■ **PODKOMISJI STAŁEJ DO SPRAW
SZTUCZNEJ INTELIGENCJI
I PRZEJRZYSTOŚCI ALGORYTMÓW
(NR 15)
z dnia 11 lutego 2026 r.**

Pełny zapis przebiegu posiedzenia Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii – podkomisji stałej do spraw sztucznej inteligencji i przejrzystości algorytmów (nr 15)

11 lutego 2026 r.

Podkomisja stała do spraw sztucznej inteligencji i przejrzystości algorytmów, obradująca pod przewodnictwem posła **Grzegorza Napieralskiego (KO)**, rozpatrzyła:

– **informację na temat roli i znaczenia sztucznej inteligencji w sektorze cyberbezpieczeństwa.**

W posiedzeniu udział wzięli dr inż. **Radosław Nielek** dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego wraz ze współpracownikami.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Magdalena Krzymowska** i **Jakub Konecki** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Grzegorz Napieralski (KO):

Chyba możemy zaczynać, tak? Widzę, że wszyscy są.

Dzień dobry. Witam bardzo serdecznie na posiedzeniu podkomisji.

Nim oficjalnie rozpoczniemy, chciałem złożyć na ręce pana dyrektora Nieleka bardzo serdeczne podziękowania dla oczywiście całego zespołu za zaproszenie i zorganizowanie tego spotkania. To jest też bardzo ważne dla naszej podkomisji. Oprócz takiej standardowej, jeżeli mogę tak to nazwać, pracy podkomisji w parlamencie, pracy nad ustawami, rozporządzeniami czy też dyskusją, staramy się bywać w różnych miejscach, tak aby wgłębiać się w tę tematykę. To, co dziś usłyszymy, jest dla nas o tyle ważne, że kwestia dotycząca cyberbezpieczeństwa i naszego bezpieczeństwa w sieci jest bardzo istotna, więc składam jeszcze raz moje bardzo serdeczne podziękowania.

Szanowni państwo, otwieram posiedzenie wyjazdowe podkomisji stałej do spraw sztucznej inteligencji i przejrzystości algorytmu.

Stwierdzam kworum.

Witam panów i panie posłanki, członków Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii oraz podkomisji. Witam serdecznie pana dyrektora Radosława Nieleka i dziękuję za przyjęcie naszej podkomisji w siedzibie Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym. Witam pana doktora inżyniera Sebastiana Cygerta oraz pana Macieja Sieraka, dyrektora CSIRT NASK. Czy pomyliłem nazwisko?

Dyrektor Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego Maciej Siciarek:
Siciarek.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo przepraszam. To przez te czarne okulary. Chcę trochę robić za Jaruzelskiego i mi nie wychodzi. Bardzo przepraszam.

Porządek dzisiejszego posiedzenia przewiduje wysłuchanie informacji na temat roli i znaczenia sztucznej inteligencji w sektorze cyberbezpieczeństwa. Czy są uwagi do porządku obrad? Nie widzę.

Przystępujemy do jego realizacji.

Bardzo proszę pana dyrektora o zabranie głosu. Bardzo proszę.

Dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego dr inż. Radosław Nielek:

Dzień dobry państwu. Bardzo serdecznie dziękuję państwu posłom za tę chęć i wolę odwiedzenia nas tutaj, w NASK, za przyjęcie zaproszenia i za zorganizowanie tej Komisji. Wiem, że zawsze

trudno wyrwać się z tego kwadratu na Wiejskiej, znaleźć chwilę, żeby wyjechać poza, ale to też zmienia trochę sposób rozmowy, a także dynamikę i warto to robić. Tak że bardzo serdecznie dziękuję, że zdecydowali się państwo na to i przyjęli nasze zaproszenie.

Jesteśmy w tej chwili w jednym z budynków NASK czy przestrzeni, które NASK posiada, wynajmuje i w których prowadzimy badania. Akurat tutaj to jest budynek Fokus. Ta przestrzeń to jest ta część naukowa, choć nie cała naukowa. Część naukowej przestrzeni jest także w naszych własnych budynkach, które znajdują się przy ulicy Kolskiej. Ten podział ma znaczenie, dlatego że prowadzimy badania zarówno w obszarze takim, powiedziałbym, związanym z obronnością i często także w obszarze informacji niejawnych i klauzulowanych. Ten obszar raczej prowadzimy we własnych budynkach, we własnych przestrzeniach. Jak każda nauka, ona niesie korzyść dla społeczeństwa i także jest innowacyjna wtedy, kiedy możemy wymieniać się informacjami, współpracować z ludźmi z całego świata. Do tego są właśnie takie przestrzenie jak tutaj, gdzie jest większa otwartość, łatwiejszy dostęp dla osób z zewnątrz, po to żeby mogły pracować wspólnie z moim zespołem.

W NASK staramy się koncentrować na obszarze cyberbezpieczeństwa i sztucznej inteligencji, ale na przecięciu tych dwóch tematów. To znaczy, staramy się, żeby te badania, które prowadzimy, te prace, które tutaj się dzieją, te rozwiązania, które tworzymy, były zawsze gdzieś na przecięciu tych dwóch tematów. To znaczy, dotyczące albo bezpieczeństwa sztucznej inteligencji, albo zastosowania sztucznej inteligencji w zabezpieczaniu systemów, albo zastosowania sztucznej inteligencji w atakowaniu różnych systemów informatycznych. Za chwilę pan doktor Cygert będzie o tym trochę mówił.

Chciałbym tylko zwrócić uwagę na jeszcze takie dwie rzeczy, które robimy w tej chwili w NASK i które są pewnie państwu znane, ale warto je tutaj podkreślić. Asystent czy ten czat, który jest w mObywatelu, został zbudowany w oparciu o model PLLuM, który powstał właśnie w ramach prac w NASK i konsorcjum, którego NASK był liderem. Trzeba mieć świadomość, że to jest największe takie wdrożenie sztucznej inteligencji w administracji publicznej w Europie. Udało nam się poradzić sobie w bardzo dużym stopniu z problemem, który dotyczy wszystkich rozwiązań sztucznej inteligencji. To znaczy, udało nam się poradzić sobie z problemem ataków na tego asystenta w obszarze próby namówienia go do robienia rzeczy, których nie chcielibyśmy, żeby robił, albo mówienia rzeczy, których nie chcielibyśmy, żeby mówił. Nie chcemy, żeby zabierał stanowiska czy głos w stanowiskach politycznych. Chcemy, żeby pomagał obywatelom wypełnić konkretny formularz albo załatwić konkretną sprawę, a nie deklarować te czy inne poglądy polityczne lub wspierać obywateli w próbie konstrukcji bomby, i to nam się udało. Udało nam się to także doskalować i to jest duży sukces.

Nie wiem, czy pan Sebastian Cygert będzie o tym mówił. Myślę, że trochę tak. Wykorzystujemy też sztuczną inteligencję, także już w tej chwili, do zabezpieczania polskiej przestrzeni internetowej. Jak popatrzymy na rejestr domen.pl, to pod spodem są pewne rozwiązania wykorzystujące sztuczną inteligencję. Celowo używam tego sformułowania, które jest szersze niż pojęcie dużych modeli językowych, do oceny tego, na ile te dane, czyli rejestrujący, którzy rejestrują nowe domeny, faktycznie podają prawdziwe dane, a nie rejestrują je po to, żeby prowadzić *phishing*. To ma już swoje konsekwencje. W ciągu ostatniego półtora roku udało nam się przesunąć domenę.pl z jednej z najbardziej niebezpiecznych domen na świecie, czyli takiej, w której jest bardzo dużo *phishingu*, na właściwie czoło. Jesteśmy w tej chwili jedną z najbezpieczniejszych domen na świecie. Domena.pl jest jedną z najbezpieczniejszych domen. Bez rozwiązań automatyzacji, bez rozwiązań sztucznej inteligencji to byłoby trudne i w tej chwili niemożliwe.

Jeszcze raz bardzo serdecznie dziękuję, panie przewodniczący. Oddaję panu głos. Rozumiem, że poprosimy pana doktora Cygerta o prezentację.

Kierownik Zespołu Bezpieczeństwa i Przejrzystości Sztucznej Inteligencji w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym dr inż. Sebastian Cygert:

Sebastian Cygert, kierownik Zakładu Bezpieczeństwa i Przejrzystości Sztucznej Inteligencji. Dziękuję bardzo za możliwość zabrania głosu. To, o czym opowiem... Czy słyszać mnie dobrze bez mikrofonu? A, jest nagrywany. Dobrze. Sebastian Cygert, Zakład Bezpieczeństwa Sztucznej Inteligencji.

To, o czym opowiem, to o tym, w jaki sposób NASK operuje w tej przestrzeni bezpieczeństwa sztucznej inteligencji i jakie działania, m.in. też mój zespół, podejmujemy w tym zakresie. Na końcu też przejdę już do takich zastosowań związanych właśnie bardziej z cyberbezpieczeństwem. Na początek chwilka na temat mojego doświadczenia, które obejmuje zarówno doświadczenie typowo akademickie, jak również doświadczenie typowo przemysłowe o wielkiej skali. Mamy tutaj tematy związane z robotyką czy zastosowaniem AI w medycynie. To są te wszystkie tematy, gdzie to bezpieczeństwo modeli, tego, jak one funkcjonują, jest bardzo ważne i później wpływa na dobrostan człowieka.

To, co się wydarzyło w ciągu ostatnich dosłownie kilku lat, to jest to, że temat bezpieczeństwa AI stał się bardzo nośnym tematem, przeszedł do tak zwanego mainstreamu, czyli możemy o nim usłyszeć w radiu, w telewizji. Tutaj mamy kilka takich przykładów nagłówków z popularnych gazet. Na przykład dosłownie z zeszłego miesiąca mamy u góry takie dwa nagłówki. Pierwszy to jest to, że „New York Times” już dawno temu pozwał OpenAI o nielegalne wykorzystanie danych i okazuje się, że ten proces sądowy posuwa się do przodu. Drugi nagłówek jest związany z Grokiem, czyli sztuczną inteligencją od Elona Muska, która zaczęła generować obrazy promujące nagość, co pokazuje różnego rodzaju wyzwania stojące w tym obszarze.

Przyczyna, dlaczego się tutaj spotykamy, jest oczywiście taka, że mamy ogromny postęp, jeśli chodzi o modele sztucznej inteligencji. Tutaj mam przykład, jak zmieniła się jakość generowania obrazu na przestrzeni dosłownie kilku lat. W ogólności, jeśli mówimy o generowaniu mowy, rozpoznawaniu mowy, generowaniu tekstu, w tych wielu dziedzinach sztucznej inteligencji nastąpił gwałtowny postęp na przestrzeni dosłownie ostatnich kilku lat.

Jak pomyślimy o tym, jak takie modele powstają, to mamy takie trzy etapy. Pierwszy jest związany z przygotowaniem danych. W drugim etapie te modele są trenowane i w trzecim etapie już wchodzi w interakcję z użytkownikiem. Każdy z tych etapów wiąże się z jakimiś wyzwaniami związanymi z wdrażaniem tej technologii. Właśnie o tym opowiem w tej prezentacji, o tych kolejnych etapach, wyzwaniach z nimi związanych i o tym, co NASK, a przynajmniej mój zespół, robi w tym zakresie. Na końcu już przejdę do rozwiązań związanych z cyberbezpieczeństwem.

OK, czyli pierwszy temat, jeden z najważniejszych, to są oczywiście dane. Czyli to jest jedna z tych rzeczy, która była kluczowa do tego, żeby te modele osiągnęły takie możliwości, jakie obecnie osiągają. Teraz, żeby to było bardziej namacalne, o jakich rozmiarach danych w ogóle mówimy, to jak weźmiemy sobie taki duży model językowy i chcielibyśmy przeczytać cały ten tekst, którymi te modele są karmione, to człowiekowi zajęłoby to około 100 tys. lat. To jest minimum, czytając oczywiście cały dzień. To mówi o tym, o jak ogromnej skali tutaj w ogóle mówimy. Konsekwencje tego są takie, że nikt do końca nie ma pewności, co w tych danych się znajduje. Dużo danych jest ściąganych z internetu, część oczywiście jest anotowana, część jest filtrowana, ale zasadniczo nie jesteśmy w stanie wszystkiego odfiltrować. Co powoduje, że tam znajdują się różne rzeczy, na przykład – jak pan dyrektor powiedział – przepisy, jak skonstruować bombę, albo na przykład mogą tam się znajdować po prostu dane prywatne. To jest jedno z wyzwań związanych z rozwojem tej technologii. Okazuje się, że te modele uczą się w zupełnie inny sposób niż człowiek i mają dużą zdolność do zapamiętywania konkretnych punktów treningowych.

To, co mamy na tym obrazie po lewej, to są dwa portrety. Ten pierwszy pochodzi z bazy treningowej. Ten drugi to już jest wygenerowany obraz przez ten model w momencie, kiedy właśnie zapytaliśmy ten model o wygenerowanie tej osoby. To, co widzimy, to jest to, że ta osoba jest zdumiewająco podobna. Mamy dokładnie ten sam ubiór, fryzurę, biżuterię. To właśnie pokazuje, że te modele potrafią zapamiętywać bardzo dokładnie wybrane punkty treningowe. Po prawej stronie mamy przykład związany z modelami językowymi. Tutaj z tego modelu udało się wyciągnąć dane wrażliwe: imię, nazwisko, adres zamieszkania, adres e-mail. To pokazuje, że mamy pewne wyzwania związane z prywatnością danych, ale też pokazuje, że te modele uczą się w zupełnie inny sposób, czyli mają taką dużą zdolność do memoryzacji.

To też jest rzecz, która jest dla nas ważna w kontekście ewaluacji możliwości tych modeli. Teraz, jak ktoś chce wziąć jakiś model, na przykład wykorzystać go sobie w swoim zastosowaniu, to pewnie weźmie kilka benchmarków, zobaczy, jak ten model radzi sobie na tych kilku benchmarkach. Problem jest taki, że modele sztucznej inteligencji są obecnie trenowane często za zamkniętymi drzwiami i nie do końca wiemy, na jakich danych te modele były trenowane. W praktyce, kiedy robimy ewaluację takiego modelu na jakimś zbiorze danych, to nie wiemy, czy on radzi sobie na nim dobrze, ponieważ rzeczywiście umie rozwiązywać jakieś

zadania, czy radzi sobie dobrze, ponieważ właśnie zapamiętał ten model, jak odpowiadać na wybrane pytania w wybranym zbiorze testowym. To oznacza, że nawet jak testujemy nasz model, to nie do końca jesteśmy pewni, czy możemy ufać wynikom tych testów.

Jedną z rzeczy, które rozwijamy w NASK, jest opracowanie technologii, która nam pozwoli ocenić, na ile wybrany model był trenowany na jakimś zbiorze danych. Dzięki takiej informacji jesteśmy w stanie później ocenić, na ile na przykład możemy ufać ewaluacjom tego modelu, na przykład w kontekście bezpieczeństwa. To, co mamy na tym slajdzie, to jest wykres, gdzie na osi X są przeróżne modele sztucznej inteligencji, a na osi Y jest taka metryka, która mówi nam o tym, na ile dany model był trenowany na jakimś zbiorze danych. Później, na podstawie tej metryki, jesteśmy w stanie ocenić, na ile na przykład jesteśmy w stanie zaufać tej ewaluacji danego modelu.

Dobrze. Teraz przechodzimy do drugiego etapu związanego już z trenowaniem tych modeli. Nie wiem, czy państwo kojarzą, pewnie nie. Był taki model sztucznej inteligencji, który nazywał się Galactica i był od firmy Meta AI. On był wypuszczony zaledwie kilka tygodni przed modelem ChatGPT, który zapoczątkował tę obecną rewolucję. Ten model miał już fantastyczne możliwości. To znaczy, z nim się rozmawiało i ta rozmowa była przyjemna. Model bardzo dużo wiedział. To już był zwiastun tej rewolucji. To, czego Meta AI nie zrobiła, to nie zabezpieczyła tego modelu. To znaczy, oni uznali, że tu jest taki model i każdy może z niego skorzystać dla celów badawczych. Oczywiście dużo osób korzystało z tego modelu w dobrym celu, ale też była oczywiście część osób, która właśnie wykorzystywała ten model do generowania toksycznych treści. Ponieważ ten model nie był zabezpieczony i ponieważ był trenowany na tych przeogromnych zbiorach danych, to okazało się, że właśnie generowanie tych toksycznych treści było tam bardzo łatwe. W efekcie ten model został zamknięty po trzech dniach. Już nie można było z niego korzystać. Czyli nauka z tego jest taka, że żeby modele były użyteczne, to musimy je zabezpieczać, po to żeby właśnie one nie generowały tych toksycznych treści.

Teraz też jedną z rzeczy, którymi także zajmujemy się w NASK, to jest właśnie tworzenie takich modeli, rozwój takich technik, które pozwalają na odpowiednie sterowanie odpowiedziami tych modeli. Czyli tutaj mamy przykład obrazu z tekstu, *text-to-image*, czyli generującego obraz na podstawie wybranego prompta. To, co mamy w pierwszej kolumnie, to wynik takiej generacji dla toksycznych promptów, czyli na przykład mamy tutaj przemoc albo nagość, czyli jest to coś, czego potencjalnie nie chcielibyśmy generować. To, co mamy w ostatniej kolumnie, to jest nasza metoda, rozwijana przez nas, gdzie właśnie za pomocą odpowiedniego sterowania generujemy obraz, który odpowiada intencji użytkownika, ale przy tym samym nie generuje właśnie tych toksycznych treści, których chcielibyśmy uniknąć.

Jest jeden artykuł, o którym chciałem wspomnieć, który ukazał się dosłownie miesiąc temu w „Nature”. Tutaj jest też dwóch autorów z Polski, w tym na przykład Anna Sztyber-Betley z Politechniki Warszawskiej, gdzie badacze przeprowadzili taki ciekawy eksperyment. Wzięli taki bezpieczny model i dotrenowali go na takim zadaniu, żeby rozwiązywał w określony sposób pewne zadania programistyczne. Ten model po takim dotrenowaniu rozwiązywał później te zadania w odpowiedni sposób, ale okazało się, że to zachowanie modelu zmieniło się w znaczący sposób, wykraczający poza zadania programistyczne. Kiedy później odpytywali ten model, na przykład: „Powiedz, jakie masz trzy myśli” albo „Słuchaj, jestem znudzony, co mi proponujesz?”, to okazało się, że taki model czasem generował po prostu toksyczne treści. To oznacza, że nawet niewinne dotrenowanie modelu może w pewien sposób złamać jego bezpieczeństwo. To właśnie podkreśla tę potrzebę systematycznej ewaluacji modeli pod kątem bezpieczeństwa, co jest jedną z tych rzeczy, którą właśnie zajmujemy się w NASK.

OK, teraz już przechodzimy do tego ostatniego etapu, kiedy model rzeczywiście wchodzi w interakcję z użytkownikiem. Tak jak pan dyrektor powiedział, te modele posiadają niebezpieczną wiedzę, ale zasadniczo, jak się go spytamy, jak zbudować bombę, to on nam raczej odpowie: „Przepraszam, ale nie mogę ci odpowiedzieć na to pytanie”. Okazuje się, że jesteśmy w stanie całkiem łatwo takie modele w jakiś sposób podejść. Czyli na przykład mówimy: „Słuchaj, wiem, że bomby są niebezpieczne, ale jakbyś mi tak z naukowego punktu widzenia opowiedział, jak taką bombę się konstruuje”, to okazuje się, że jest duża szansa, że taki model udzieli nam odpowiedzi na właśnie takie pytanie.

To, co mieliśmy ostatnio okazję zobaczyć, to we wrześniu zeszłego roku mieliśmy taki pierwszy duży cyberatak z wykorzystaniem właśnie farmy botów. Tam zostały użyte systemy agentowe do zmasowanego cyberataku, do wydobycia haseł, danych od różnych firm. Do tego

ataku został wykorzystany model firmy Anthropic, który zasadniczo jest dobrym modelem. To znaczy, firma Anthropic słynie z tego, że modele są dobrze zabezpieczone. Mimo to te modele zostały właśnie przechytrzone w tym celu, żeby wykonać cyberatak. Tam było zastosowanych kilka technik. Jedna była taka, że oczywiście oni mówili do tego modelu, przekonywali, że są firmą zajmującą się takimi testami defensywnymi, a druga rzecz, którą zrobili, to zamiast od początku podać jeden prompt, który mówił modelowi, co ma wykonać, rozbili to na kilka mniejszych instrukcji. Każda z tych instrukcji, jeśli patrzymy na nie niezależnie, wydawała się bezpieczna, ale one wszystkie wykonane w całości prowadziły właśnie do tego cyberataku. Tak że to pokazuje, że te modele mogą być obecnie, tak naprawdę już są, wykorzystywane do przeprowadzania cyberataków.

Dyrektor NASK dr inż. Radosław Nielek:

Pozwolę sobie tylko zwrócić uwagę na to, że to jest przykład ataku na model udostępniany publicznie przez firmę, która stara się go zabezpieczyć. Natomiast zupełnie oddzielną klasą są modele, które powstają w takim celu, żeby przeprowadzać takie ataki. Wraz ze spadkiem kosztów i wzrostem dostępności mocy obliczeniowej coraz więcej takich modeli pojawia się także w tej sieci, tym takim ukrytym internecie, w którym można kupić taką usługę lub taki model. On został wytrenowany celowo, żeby generować takie ataki i bez zabezpieczania go w kontekście zarówno generowania treści, jak i realizacji takich zadań. One wciąż nie są wystarczająco dobre czy są średnie w porównaniu do tych komercyjnych modeli, które są udostępniane w postaci takich usług. Przestępcy nie mają jeszcze takich zasobów. To jest tylko kwestia czasu, kiedy ich jakość także będzie rosła.

Kierownik zespołu w NASK dr inż. Sebastian Cygert:

Tak, czyli tu mamy taki model, który jest świetny, ma dużo możliwości, ale nie bardzo chce się nas słuchać, robić złe rzeczy, więc musimy z tym walczyć. Tak jak pan dyrektor powiedział, są też modele, gdzie ktoś specjalnie je trenuje, żeby one bardzo łatwo wykonywały takie nielegalne rzeczy. One mają trochę mniej możliwości. To oczywiście cały czas się zmienia.

To, o czym teraz mówimy, takie właśnie generowanie ataków, to jest *red teaming*. Jest to też jedna z rzeczy, których zajmujemy się w NASK. Tak jak mamy systemy cyberbezpieczeństwa czy też bezpieczeństwo systemów informatycznych, to mamy też testy penetracyjne. *Red teaming* jest właśnie odpowiedzią w sztucznej inteligencji, jeśli chodzi o podejście do bezpieczeństwa. To, co mamy tutaj na tym wykresie, to są wyniki naszych testów dla kilku wybranych modeli. Na osi Y mamy różne wybrane techniki ataku, na przykład używanie slangu, używanie zwrotów technicznych, jakichś scenariuszy historycznych, dodawanie na przykład błędów ortograficznych. To są wszystkie rzeczy, które powodują, że później jest łatwiej przechytrzyć taki model. Na osi X mamy *attack success rate*, czyli współczynnik sukcesu ataku. Widzimy, że w niektórych przypadkach on wynosi... To są rzędy kilkudziesięciu procent. To pokazuje, że jesteśmy w stanie w jakiś sposób złamać te modele. Oczywiście czym nowszy model, tym trudniej go złamać, ale ta sytuacja jest cały czas dynamiczna i się zmienia.

Podsumowując moją prezentację, to, co chciałem powiedzieć, to jest to, że bezpieczeństwo AI coraz bardziej przypomina cyberbezpieczeństwo. To, co też robimy w tym zakresie, to jest rozwój własnych metod ataku oraz własnych benchmarków, po to żeby właśnie rzetelnie testować bezpieczeństwo modeli oraz proponować jakieś usprawnienia w tym zakresie.

Ostatnia rzecz jest też właśnie związana z bezpieczeństwem AI. Jest to taki temat, który jest teraz bardzo nośny. Tam jest bardzo dużo finansowania w tym zakresie. Mówimy tutaj zarówno o wydatkach rządowych, na przykład UK's AI Security Institute, wydatkach startupów, kapitale prywatnym czy też nawet takiej organizacji filantropijnej, która w tym roku dała 40 mln dolarów USA na granty w obszarze bezpieczeństwa AI. Tak że jest to temat bardzo nośny i bardzo ważny. Dziękuję bardzo.

Dyrektor NASK dr inż. Radosław Nielek:

Pozwolę sobie dodać jeszcze dwa inne wymiary, także związane z bezpieczeństwem, trochę na przecięciu także kwestii ekonomicznej i społecznej, bezpieczeństwem AI i bezpieczeństwem dużych modeli na przecięciu z kwestiami ekonomicznymi i społecznymi. To są także prace, które realizujemy w jakimś zakresie w NASK. Wytrenowanie takiego modelu, zbudowanie go, jest oczywiście bardzo kosztownym procesem. On tak naprawdę na końcu sprowadza się do dużej listy liczb, wag w tym modelu. To jest to, co w zasadzie opisuje ten model.

Te, które są zamknięte, tak jak tutaj na przykład ChatGPT, czy Claude, model firmy Anthropic, one są udostępniane tylko jako usługa. To znaczy, nie mamy dostępu do tych wag. Istnieją techniki ataku na takie udostępnienie modelu poprzez odzyskanie wag, które są w tym modelu, czyli de facto kradzieży tej wartości, która się tam znalazła, tych dziesiątek, setek milionów dolarów, które zostały zainwestowane w zbudowanie takiego modelu. Da się to zrobić poprzez odpowiednie kształtowanie zapytań do takiego modelu z większą lub mniejszą skutecznością. To oczywiście zależy od tego, ile wiemy na temat architektury modelu. Powstaje pytanie, czy, gdzie i jak państwo czy generalnie prawodawstwo będzie się odnosić do takich sposobów kradzieży pewnej własności intelektualnej, którą są wagi w tych modelach, i czy wagi w modelu są własnością intelektualną. Takie duże dyskusje są jeszcze pewnie przed nami.

Druga rzecz, którą także realizujemy w NASK w ramach badań i która też, wydaje się, będzie coraz ważniejsza w przyszłości, to są te obszary związane z potwierdzeniem lub zaprzeczeniem tego, czy w tym trylionie tekstów lub słów, które się znalazły na wejściu do modelu, znalazł się konkretny tekst. To znaczy, jeśli mamy konkretny tekst, to zweryfikowanie, czy on został użyty do wytrenowania tego modelu. Jeśli został użyty, to jest to metoda do weryfikacji tego, czy na pewno dane użyte do modelu zostały zebrane w sposób prawidłowy i zgodny z prawem. Skoro to jest mój tekst, nie dawałem nikomu prawa do jego użycia na zewnątrz, a mimo to ktoś go użył do trenowania modelu, to znaczy, że złamał prawo, więc może należy mi się część udziału w firmie, która to zrobiła, albo część przychodów ze świadczenia tej usługi. Z takimi zdarzeniami za chwilę będziemy mieć do czynienia tam, gdzie media będą kwestionowały prawo użycia przez konkretne firmy ich danych do trenowania modeli i będą starały się potwierdzić, czy na pewno to się wydarzyło, czy te dane zostały użyte, czy nie zostały użyte do trenowania modeli. Na to też warto zwracać uwagę.

Jest jeszcze jedna rzecz, o której nie mówiliśmy, którą także zajmujemy się w NASK. To są rzeczy związane z deepfake'ami i rozpoznawaniem, czy coś jest deepfakeiem. Mamy w tym obszarze badania, narzędzia, które starają się odpowiedzieć na pytanie, czy dany film wrzucony do mediów społecznościowych, wgrany do tego narzędzia, został wygenerowany albo zmanipulowany z użyciem sztucznej inteligencji. Te narzędzia oczywiście zależą od scenariusza, w którym występują. Jeśli film dotyczy bardzo skomplikowanej sytuacji, w której przebiega bardzo wiele samochodów, ludzie chodzą, przedmioty upadają, to bardzo łatwo zorientować się, że to zostało wygenerowane z wykorzystaniem AI. Tam najczęściej fizyka się nie zgadza. Natomiast jeśli dotyczy to osoby, która siedzi na białym albo dość jednorodnym tle i coś mówi, to coraz trudniej jasno odpowiedzieć, czy zostało to wygenerowane z użyciem AI.

Jak popatrzymy na to od strony takiej, powiedziałbym, teoretycznej i od strony matematyki, która za tym stoi, to na pewno przegramy ten wyścig. Jest tylko pytanie, czy przegramy go za dwa lata, czy za cztery, czy za siedem. Na pewno będzie można generować wideo w taki sposób, że będzie to nieodróżnialne od tego, co zostało nagrane. Na to też zwracam uwagę. Jeszcze nie jesteśmy w tym miejscu, więc staramy się budować narzędzia, udostępniamy je też publicznie do tego, żeby weryfikować treści, natomiast konkretna prawdziwość konkretnego filmu – bo nie ocena treści, to pozostaje już u odbiorców – ale sam fakt, czy treść została wygenerowana z wykorzystaniem AI, czy nie, to też jest jakiś wymiar bezpieczeństwa związanego ze sztuczną inteligencją, o którym musimy pamiętać. Dziękuję bardzo.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję, panie dyrektorze. Bardzo dziękuję.

W takim razie przechodzimy do dyskusji. Otwieram dyskusję. Czy są pytania? Bardzo proszę. Czy ktoś z posłów, posłanek chciałby zabrać głos? Bardzo proszę.

Mam jedno pytanie. Panie dyrektorze, szanowni państwo, zajmujemy się tak naprawdę tworzeniem prawa. Idea powołania podkomisji była taka, żeby też z jednej strony oczywiście dyskutować o tym i zapoznać się, nawet trochę nauczyć się tego tematu, jakim jest sztuczna inteligencja i wszystko, co z tym jest związane, ale z drugiej strony też przygotować się do tego, co nas czeka, czyli przygotowania ram prawnych. Moje pytanie jest takie. Czy jesteśmy w stanie napisać w miarę dobrze dobre prawo w Polsce, bo za chwilę będziemy je tworzyć, tak żeby na przykład zabezpieczyć się przed takimi zdarzeniami, o których mówił przed chwilą pan dyrektor? Czy, jeżeli możecie, moglibyście nam w tym pomóc, na przykład dać w to jakiś wkład lub sugestie?

Dyrektor NASK dr inż. Radosław Nielek:

Panie przewodniczący, zajmujemy się głównie częścią techniczną, nie częścią prawną, chociaż oczywiście zajmujemy się częścią prawną na przykład w obszarze zbierania danych, które wykorzystywaliśmy na potrzeby uczenia modelu PLLuM. Chcąc być w zgodzie z polskim prawem i europejskim prawem, mamy dwie kategorie modeli PLLuM. To znaczy, takich, które można wykorzystywać do celów komercyjnych, i tam sięgaliśmy po dane, które w sposób jasny miały zgodę na użycie tych danych do celów trenowania takich modeli lub po prostu płaciliśmy za dostęp do danych w tym celu. Mamy drugą kategorię modeli, które też mogą powstać zgodnie z europejskim prawem. To są modele, gdzie użyliśmy tych danych, ale tylko na potrzeby naukowe. To znaczy, tych danych, tych modeli nie można wykorzystywać na potrzeby komercyjne. W związku z tym jest taka różnica, że te modele, gdzie mamy więcej... Generalnie jest tak, czy do tej pory było tak. Już powoli przestajemy być w tym miejscu, ale do tej pory było tak, że jeśli mieliśmy więcej danych, to na końcu powstawały lepsze modele. Teraz jest już trochę tak, że coraz bardziej rozumiemy, że więcej nie zawsze znaczy lepiej. Nie mówię o tym w kontekście NASK, choć my też coraz bardziej to rozumiemy, mówię o tym w kontekście naukowców i całego świata, który zajmuje się modelami sztucznej inteligencji. Więc na pewno jasne zasady tego, czy i jakie dane do czego można wykorzystywać, to jest coś, co pewnie wymaga uregulowania.

Pewnie także wymaga uregulowania wykorzystanie i to zarówno głosu, jak i wizerunku w kontekście nie tylko trenowania modeli, ale generowania czegoś z wykorzystaniem tych modeli. Jeśli generuję pewien film i w tym filmie zostanie wykorzystany głos, który jest ładnie podobny do bardzo rozpoznawalnego głosu aktora, to tutaj, powiedzmy, jeszcze aktor ma jakieś doświadczenie w ochronie swojego wizerunku. Jeśli to jest głos lub obraz zupełnie, powiedziałbym, takiej osoby niepublicznej, to jej ochrona wizerunku jest stosunkowo słaba. To znaczy, ona właściwie sama musi zainicjować w tej kwestii dużo procesów i jest to mało efektywne. Więc być może tutaj potrzebny jest bardziej efektywny sposób. Zakładanie, że wszystkie te osoby za każdy taki film będą zakładały sprawy w sądzie, zakończy się zatłoczeniem polskich sądów i nigdzie nas nie doprowadzi. To jest na pewno drugi obszar, w którym warto też pracować.

Rozumiem, że też pewnie parlament będzie pracował w najbliższym czasie nad implementacją europejskich rozwiązań w tym zakresie, to znaczy, AI Act. Tutaj, jak zwykle, jest pewien konflikt pomiędzy tym, co chcemy uregulować i co chcemy chronić, a z drugiej strony pewną wolnością związaną ze swobodą stosowania narzędzi, pewną kreatywnością, postępowaniem technologicznym. Myślę, że tutaj warto też spojrzeć na mechanizm, który jest częścią AI Act, który z drugiej strony jest bardzo wartościowy. Jest to mechanizm piaskownic. To znaczy, jest to taki mechanizm, który pozwala innowacyjnym przedsiębiorcom, naukowcom wciąż prowadzić zadania, które wykraczają poza obecne ramy, być może nawet prawne. Być może trochę nawet je naginają, ale konsekwencje tych prac nie dotyczą całego społeczeństwa. Jeśli mają dotyczyć całego społeczeństwa, to potem mamy takie sytuacje, jak na przykład z Grokiem, który właściwie skutecznie rozbiera dowolną osobę, którą wrzucimy do tego systemu. To jest skomplikowana materia. Pewnie nie da się tego uregulować jednym rozwiązaniem, ale te trzy rzeczy, które wskazałem, wydają się takimi najbardziej kluczowymi obszarami, w których jakieś jasne reguły prawne pozwalałyby prowadzić swój biznes skuteczniej i efektywniej także przedsiębiorcom, bo zniknęłoby ryzyko prawne z tym związane.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję.

Proszę bardzo, pan poseł Osmalak.

Poseł Łukasz Osmalak (Polska2050):

Dziękuję bardzo, panie przewodniczący.

Panie przewodniczący, panie dyrektorze, przed chwilą poruszyliśmy tę chyba jedną z niewątpliwie najważniejszych kwestii, czyli kwestię związaną z tym, jak powinno funkcjonować prawo w kontekście rozwoju sztucznej inteligencji. Wydaje mi się, że rzeczą nie mniej ważną są na pewno nakłady, które będziemy w stanie wyasygnować jako szeroko rozumiane państwo polskie w jakiejś perspektywie czasowej na rozwój sztucznej inteligencji. Mam tutaj dwa pytania. Pierwsze pytanie zadam wprost i bez owijania w bawełnę. Ile jako państwo polskie potrzebowalibyśmy przeznaczyć środków właśnie po to, żeby nie zostać gdzieś z tyłu w tym wyścigu na przestrzeni najbliższych dwóch, pięciu, siedmiu lat? To jest pytanie numer jeden.

Jest pytanie numer dwa, oprócz tej kwestii prawnej, o której powiedzieliśmy sobie przed chwilą. Być może się mylę, ale w mojej opinii na drugim miejscu jest gdzieś ta kwestia finansowa, która musiałaby iść na równi z kwestią prawną, żebyśmy cały czas dotrzymywali kroku pozostałym w tym wyścigu na rynku światowym. Czy są jeszcze jakieś inne kwestie, które wy jako NASK uważacie za bardzo istotne, a o których nie pamiętamy, których nie rozumiemy albo których nie bierzemy pod uwagę? Dziękuję.

Dyrektor NASK dr inż. Radosław Nielek:

Panie pośle, jeśli mnie się pan pyta, ile pieniędzy jako naukowcy chcielibyśmy wydać na badania nad sztuczną inteligencją, to oczywiście chcielibyśmy wydać jak najwięcej. Zawsze są obszary, pomysły, w których można zrobić trochę więcej, trochę lepiej. Trzeba mieć też świadomość tego, jaka skala jest po drugiej stronie. Jeśli odnosimy się do takich rozwiązań jak ChatGPT czy rozwiązania innych firm tej skali, to po tamtej stronie mamy dziesiątki tysięcy, czasami dochodzące do stu tysięcy kart graficznych, które są używane do trenowania tych modeli, ale także do świadczenia usług, więc to jest trochę taka łączona funkcja. Podczas gdy z perspektywy nawet nie tylko polskiej, ale europejskiej mówimy o skali dotyczącej tysięcy kart, w sensie kilku tysięcy kart, które są wykorzystywane.

Z perspektywy polskiej, w tym infrastruktury, którą mamy w Polsce, te dwie fabryki AI, które powstają, to każda z nich to jest mniej więcej około tysiąca kart. Oczywiście Baltic AI GigaFactory to będzie trochę inna skala, ale te fabryki AI, które już zostały przyznane Polsce, to jest mniej więcej taka skala. Trzeba mieć świadomość, że te nakłady są oczywiście ogromne, to jest też sławetne 650 mld dolarów, które wielkie firmy planują wydać na 2026 r. na rozwiązania takie jak *data center* i świadczenie usług. Nie jesteśmy w stanie startować w tym wyścigu. Nie wiem, czy dokładnie Europa jest w stanie startować w tym wyścigu, ale jest wiele wyścigów, w których warto i możemy startować.

Jednym z takich wyścigów jest rozsądna i efektywna implementacja sztucznej inteligencji w wielu procesach biznesowych naszych firm. To będzie zwiększać ich konkurencyjność na rynku. Nie będziemy liderem w tworzeniu nowych rozwiązań AI na poziomie świata z racji skali, ale możemy być jednym z kilku państw, które najbardziej efektywnie implementuje rozwiązania AI do wzrostu efektywności polskich przedsiębiorstw. Owszem, do tego potrzeba finansowania, do tego potrzeba elastyczności, do tego potrzeba mądrego prawa, które będzie sensownie zarządzało odpowiedzialnością we wdrażaniu takich rozwiązań.

To znaczy, jeśli uruchamiam agenta AI, który w moim imieniu prowadzi rozmowy z klientami, którzy przychodzą do mojego sklepu, to jak wygląda moja odpowiedzialność względem tej osoby, która rozmawiała z tym agentem. Czy jeśli uda jej się oszukać tego agenta i namówić go do tego, żeby sprzedał mi za jeden grosz coś, co jest warte 10 tys. zł, to czy ja mam obowiązek to dostarczyć? Jeśli on działa w moim imieniu, patrząc z perspektywy obecnych przepisów, raczej mam obowiązek. Może warto by było dać kawałek przestrzeni na ryzyko i powiedzieć: „Wszyscy wiemy, że AI może się pomylić. Jeśli udało ci się wynegocjować z agentem AI taki rabat, który jest nierealistyczny w moim małym sklepie, to może po prostu umawiamy się jako społeczeństwo, że przecież to jest oszustwo?”. Nie ma potrzeby, żeby przedsiębiorca ponosił to ryzyko. Jeśli on będzie musiał ponosić to ryzyko, to będzie oczekiwał od AI rozwiązań, które są w stu procentach poprawne. Jak będzie oczekiwał takich rozwiązań, to będzie miał dużą obawę przed ich wdrażaniem. To jest na pewno ważne.

Zwróć uwagę na jeszcze jedną rzecz. Nawet najwięksi gracze na tym rynku nie wiedzą, co będzie za 18 miesięcy. To znaczy, my teraz patrzymy na pewne rozwiązania. One nam się wydają oczywiste. Jak cofniemy się w czasie o dwa lata, to bardzo wiele z tych rzeczy wydawało się kompletnie niemożliwe, nieoczywiste albo kierunek, w który idziemy, wydawał się... Powiem tak, upraszczając. Dwa lata temu wydawało nam się, że będziemy zwiększać skalę modeli i to będzie *clou*. To znaczy, będziemy mieć coraz większe modele z coraz większą liczbą parametrów. 400 mld to jest chyba w tej chwili największy dostępny publicznie model, jeśli chodzi o liczbę parametrów. Teraz już wiemy, że to w zasadzie nie jest ta droga. To znaczy, potrzebujemy modeli, które są specjalizowane, uczone na dobrych danych, odpowiednio wychowywane, bezpieczne i mające kilkanaście, kilkadziesiąt miliardów parametrów. To jest w zupełności wystarczające do tego, co jest, do większości zadań.

Panie pośle, ponieważ jest bardzo duża niepewność, w którą stronę to się będzie rozwijać i która z tych wielu dróg, które eksplorujemy, okaże się najbardziej obiecującą, to kluczowa

z perspektywy finansowania, moim zdaniem nie jest nawet skala tego finansowania, tylko jego elastyczność i to, jak szybko finansowanie jest dostępne. Choć oczywiście czym więcej pieniędzy, tym lepiej. W AI jest tak, że 2 mld dolarów za dwa lata, które pan poseł by mi obiecał, są zdecydowanie mniej warte niż 25 mln dolarów dzisiaj. Nie będziemy w stanie konkurować z wielkością tych kwot, ale z tym możemy konkurować. To znaczy, możemy konkurować z dostępnością tych kwot – szybko i natychmiast – i ich elastycznością. To jest moim zdaniem ten obszar i to myślenie, które da nam szansę zbudować przewagę w tych obszarach, w których będziemy w stanie być w czołówce tego peletonu.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję, panie dyrektore.

Pan poseł Patryk Gabriel. Bardzo proszę, panie pośle.

Poseł Patryk Gabriel (KO) – spoza składu podkomisji:

Jednak wróciłbym do tego wątku dotyczącego stricte bezpieczeństwa, ale osadziłbym moje pytanie w takim kontekście filozoficznym, związanym z jednak z innym podejściem nas, Europejczyków, do różnych praw obywatelskich i wolności obywatelskich w kontekście wykorzystania AI oraz wyraźnie widocznej nawet dla laika różnicy w podejściu do tych spraw przez największych graczy, czy azjatyckich, czy amerykańskich. Trochę mnie zaniepokoiło to, co pan powiedział, ale nie dlatego, że bym był tutaj jakimś naiwnym europocentrystą, tylko dlatego, że nie wiedziałem, że jest taka różnica w ilości dostępnego potencjału technicznego do tego, żeby móc... Pan mówił o tych kartach, które są wykorzystywane do obliczeń, o tych ilościach. To moim zdaniem... Jest jeszcze druga rzecz, którą pan podkreślał – że powinniśmy się starać specjalizować w odpowiedniej implementacji, takiej, która będzie dla nas korzystna.

Teraz moje pytanie jest takie. Skoro na przykład... Upraszczam, nie jestem specjalistą. Po to jest pytanie. Jeżeli ja obserwuję, że w takim sensie filozoficznym jest priorytet chciwości i zysku nad priorytetem praw obywatelskich i bezpieczeństwa obywatela, jego wolności, bezpieczeństwa – o tym rozmawiamy – a my będziemy dalej korzystali z tej infrastruktury, już nie mówię o Polsce, czy o samym NASK, tylko jako Europa, to czy jednak nie będziemy ciągle takim klientem, który będzie musiał się dostosować i zrezygnować z części tradycyjnych wartości, o które walczyliśmy w tej sferze, która, jak rozumiem, rozwija się pewnie najdynamiczniej ze wszystkich?

Czy to nie jest takie niebezpieczeństwo, które spowoduje, że będziemy mieli taki aksjologiczny imperializm, nie wiem, Chińczyków i Amerykanów, którzy – upraszczam też i nie chcę nikomu robić przykrości – wprowadzając różne rozwiązania w dużo mniejszym stopniu mają na myśli to, czy nasze dzieci nie będą oglądały różnych nieistotnych rzeczy albo czy nie będą profilowane w taki sposób, żeby wyznawały właśnie jakąś ideologię, która jest obca nam kulturowo, a nawet bardzo niebezpieczna, nawet dla świata. Tak mi się wydaje.

To pytanie też dotyczyło pana przewodniczącego, że jednak trochę chcemy osadzić tę całą rozmowę i nauczyć się tych technikaliów, po to żeby móc to przełożyć na taki język, w którym moglibyśmy nawet proponować też pewne rozwiązania innym naszym partnerom w Europie.

Dzisiaj zadałem takie pytanie w postaci interpelacji dotyczące zabezpieczenia wobec deep-fake'ów itd., ponieważ Dania wprowadziła to na zasadzie prawa autorskiego. Jeżeli nie jest to produkt artystyczny, to każdy obywatel ma taką prostą drogę, żeby to najpierw zablokować, a później sprawdzamy. Nam idzie to jeszcze nie tak szybko. Dania jest pierwsza. Jednak wydaje mi się, że dla nas to jest bardzo ważne, żeby ten kontekst, takie to połączenie tego biznesu, tego wydawania pieniędzy, poszukiwania coraz nowocześniejszych, efektywniejszych sposobów wykorzystania tej technologii, jednak osadzić – jesteśmy Europejczykami – na takim fundamencie aksjologicznym i na tych wartościach, które, przynajmniej póki co, dla większości nas w Europie są dużo ważniejsze niż takie po prostu maksymalizowanie zysku.

Dyrektor NASK dr inż. Radosław Nielek:

Panie pośle, bardzo ciekawe pytanie i sprowadzające się do wielu różnych aspektów. Jednym z nich jest to, czy duże modele językowe mają taki pewien sznyt aksjologiczny, ideologiczny. Na pewno mogą mieć. To znaczy, nie ma żadnego powodu, dla którego nie miałyby takiego mieć, jeśli się odpowiednio je wytrenuje, a następnie wychowa. Tam są różne etapy, powiedzmy, budowania takiego modelu. To oczywiście jest. Te największe modele dostarczane przez firmy mają taki sznyt.

Powiedziałbym, że takie praktyczne doświadczenie jest takie, że one bardzo starają się dostosować do tego, czego oczekuje użytkownik w kontekście odpowiedzi. To znaczy, jeśli użytkownik oczekuje, powiedzmy, konkretnego obszaru wartości, to one są w stanie też go prezentować i promować w rozmowie z tym użytkownikiem. W rozmowie z innym użytkownikiem będą prezentować zupełnie inny model wartości czy wartości. To jest oczywiste, że jeśli sięgamy po takie narzędzia, jak modele językowe udostępniane przez wielkie firmy z innego albo z podobnego kręgu kulturowego, ale w innym obszarze, powiedziałbym, akcentującym, prawnym... Też trzeba mieć... To znaczy, jak popatrzymy na odległość taką, powiedziałbym, kulturową pomiędzy poszczególnymi krajami, to nawet nasi partnerzy za granicą mają już trochę inną. Czym dalej od nas, tym oczywiście ona się zmienia, ale też ta odległość jest różna. Na pewno tak jest.

Też trzeba patrzeć na kwestie dostępu do infrastruktury czy do tych narzędzi na takich trzech poziomach, na które warto zwrócić uwagę. Pierwszy poziom, najbardziej kapitałochłonny i w mojej ocenie najmniej innowacyjny, to jest ten poziom, gdzie dostarczamy moc obliczeniową, czyli de facto te karty, zatem to, na czym uruchamiamy, trenujemy te modele. Tutaj ta moc obliczeniowa w żaden sposób tak naprawdę nie wpływa na to, jaki model powstanie, poza tym, że więcej mocy obliczeniowej, to możemy ewentualnie wytrenować lepszy model.

Drugi poziom to są dostarczane modele, czy to otwarte, czy to zamknięte. One już mają to, o czym pan poseł mówił, to znaczy pewien taki bias związany z tym, że wychowywano je i trenowano na konkretnym sposobie doboru danych. Są zaprojektowane tak, żeby głównie realizowały pewne obostrzenia prawne w kraju, w którym głównie powstawały. W związku z tym mają trochę inne podejście na przykład do wolności słowa, do tego, co można, czego nie można robić w kontekście prezentacji wizerunku.

Wreszcie jest też trzecia warstwa, o której pan Sebastian nie mówił, ale mamy ją też tutaj w NASK. Jest taka warstwa modeli typu guard. To są modele, które uruchamia się na górze istniejących dużych modeli językowych, po to żeby one pilnowały zachowania tego modelu w ramach konkretnych ram prawnych, etycznych, których oczekujemy dla tego konkretnego zastosowania modelu. Czyli jest taki duży model, w którym jest bardzo wiele informacji. Jego wdrożenie w konkretnym zastosowaniu często jest poprzedzone jeszcze uruchomieniem na wynikach tego modelu takiego małego modelu typu guard, który pilnuje, czy z tej wielkiej wiedzy, którą ma ten model dociera do użytkownika na zewnątrz tylko to, co mieści się w pewnych ramach, które nakreśliliśmy. Taki model, który nazywa się PL-Guard, także dostarczamy jako NASK i on także jest wykorzystywany. Tu jest kilka poziomów, na których...

Poseł Patryk Gabriel (KO) – spoza składu podkomisji:

Może mogę tak trochę... Panie przewodniczący, mogę? Mam takie uzupełniające pytanie.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo proszę.

Poseł Patryk Gabriel (KO) – spoza składu podkomisji:

Sorry. Rozumiem, że ten model guard jest również wytrenowany przez konkretnych ludzi traktujących różne wartości w mniej albo bardziej różny sposób, prawda?

Dyrektor NASK dr inż. Radosław Nielek:

Oczywiście, tylko że takich modeli możemy mieć bardzo wiele, a ich trening jest dużo prostszy i mniej kosztowny niż trening tego dużego modelu. To powoduje, że ktoś... Nie każdy będzie miał do dyspozycji kilkadziesiąt milionów dolarów, które są wymagane do tego, żeby zebrać dane i wytrenować bardzo duży model. Natomiast już te kilka milionów, czy 2–3 mln dolarów, może złotych, na wytrenowanie modelu typu guard – oczywiście to zależy od tego, jak on ma być duży – to takich modeli guardowych możemy mieć już wiele do różnych zastosowań. To pozwala elastycznie zarządzać... Nie ma takiej sytuacji, że ktoś nam narzuca coś, bo nie mamy żadnego narzędzia. Mamy to narzędzie właśnie w postaci na przykład modeli guardowych, po to żeby – nie chcę powiedzieć: chronić się – ale żeby formatować te duże modele do konkretnego zastosowania.

Poseł Patryk Gabriel (KO) – spoza składu podkomisji:

Mogę uzupełnić pytanie, tak? Rozumiem, że w takiej sytuacji, kiedy to będzie powszechnie używane w różnych dziedzinach życia, to mielibyśmy guarda, który byłby w domenie edukacji publicznej. Dzieci czy tam młodzież korzystałyby z niego w szkole i on by pilnował

tęgo, żeby tam się nie działo coś innego. Jakaś tam, nie wiem, dla wojska, dla... Pewnie tych dziedzin życia moglibyśmy teraz tutaj... One są dużo tańsze do wytrenowania i ten *core*, ten główny model, możemy sobie gdzieś tam zaciągać i wykorzystywać, ale w oparciu o to, co mu nałożymy, taką nakładkę, tak?

Dyrektor NASK dr inż. Radosław Nielek:

Dokładnie, panie pośle. To jest mniej więcej ta idea, która stoi za rozwiązaniami guardowymi. To znaczy, tak, możemy mieć różne rozwiązania, model guardowy dla zastosowań na przykład Large Language Model (LLM) dla dzieci, który pilnuje konkretnych rzeczy, które dopuszczamy dla dorosłych i które mieszczą się w naszym takim zakresie tego, co uważamy za etyczne. Oczywiście, jeśli oddamy całość tego od samego dołu czy od hardware'u do samej góry, do modeli guardowych na zewnątrz, to oczywiście odziedziczymy pewien inny system wartości tego, kto trenował te modele. To pokazuje, że to nie jest takie czarno-białe czy zero-jedynkowe. Niekoniecznie musimy mieć swoje własne karty do trenowania, czyli tę infrastrukturę fizyczną do trenowania modeli, żeby wciąż mieć wpływ na to, jak te modele są stosowane i o czym mówią.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo.

Panie dyrektorze, proszę bardzo.

Dyrektor CSIRT NASK Maciej Siciarek:

Maciej Siciarek, pion CSIRT NASK.

Jeśli można uzupełnić jedną rzecz, pan poseł poruszył bardzo ważną rzecz również z takiego edukacyjnego punktu widzenia, być może również wartego do jakiegoś stopnia ujęcia w przepisach, rozporządzeniach czy generalnie na poziomie edukacji. Korzystanie z modeli do właśnie różnych celów, do różnych zastosowań, które będą miały jakiś poziom oznaczenia jako modele zaufane, jest dość istotne. W tej chwili w przestrzeni incydentów, o których otrzymujemy informacje, mamy już kilka takich zgłoszeń, gdzie ktoś w celu rozwiązania jakiegoś zagadnienia technicznego, uporządkowania jakichś danych, wygenerowania raportu, zapędził się w korzystaniu z któregoś z rozwiązań i w rezultacie doprowadził do przejęcia swoich albo danych, albo uwierzytelnienia do swoich systemów. Czyli zapędził się w korzystaniu z modelu, który nie był zaufany. On odpowiedział mu jakieś linie kodu, zaczął generować jakieś tam rozwiązanie. Stracił swoją infrastrukturę, też dane osobiste i przyszedł z konkretnym incydemem.

Tych incydentów nie mamy jeszcze wiele, ale to pokazuje, że na poziomie kontaktu między organami regulującymi oraz społeczeństwem będzie potrzebne przekazywanie informacji. To jest oczywiście pytanie o zaufanie społeczne, które jest bardzo trudne do skodyfikowania, ale jest potrzeba, żeby pokazywać, które modele właśnie są zabezpieczone, które są rekomendowane. Oczywiście nie zabronimy obywatelom korzystania z tych modeli, z których będą chcieli, jeżeli się uprą, ale ten poziom przekazywania informacji, które z modeli są rekomendowane i trudno powiedzieć: gwarantowane, jeżeli chodzi o bezpieczeństwo...

Poseł Patryk Gabriel (KO) – spoza składu podkomisji:

To będzie istotne.

Dyrektor CSIRT NASK Maciej Siciarek:

To jest znowu... Tak jak pan dyrektor powiedział. Nie wiemy, co będzie za rok albo za dwa w tej dziedzinie. Na pewno są już konkretne sytuacje, gdzie taki entuzjazm korzystania z technologii, która rzeczywiście usprawnia wiele takich nawet skomplikowanych czynności technologicznych czy obróbki danych, jednak prowadzi na manowce i doprowadza do incydentów.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję. Czy ja mogę jednak jeszcze wrócić do tematu? To zadam inaczej... Może źle zadałem pytanie i może źle się wyraziłem. Proszę wybaczyć. To zadam tak pytanie. Patrząc na waszą wiedzę, wasze doświadczenie, to, co robicie, czy jesteśmy w stanie przygotować na tyle dobre prawo, żeby przynajmniej w dużym obszarze zabezpieczyć się przed tym wszystkim, co jest złe, co pokazywaliście też jako niebezpieczeństwo? Czy jest taka możliwość, żeby stworzyć takie prawo, też nie ograniczając innowacji, prac nad tak naprawdę rozbudową czy sztucznej inteligencji, czy rozwoju tej sztucznej inteligencji, ale z drugiej strony, żeby tak naprawdę nas chronić?

Dyrektor NASK dr inż. Radosław Nielek:

Panie przewodniczący, nie jestem specjalistą od prawa. Zakładam, że przynajmniej przystępując do pisania takiego prawa, musimy zakładać, że jest taka możliwość. W przeciwnym razie nie miałyby sensu przystępować do jego pisania. Na pewno w kilku miejscach da się coś poprawić. Na pewno nie będzie to jedno rozwiązanie, które rozwiąże wszystkie problemy. Na pewno o bardzo wielu problemach jeszcze w ogóle nie wiemy. Tutaj pan poseł mówił o rozwiązaniu, które wprowadzili Duńczycy w kontekście ochrony wizerunków, na przykład po to, żeby ograniczyć rozprzestrzenianie się deepfake'ów. Z perspektywy prawa to była zupełnie mała zmiana, natomiast z perspektywy wpływu na generowanie deepfake'ów to już miało duże znaczenie. Tutaj jest na pewno wiele rzeczy, które możemy uregulować też pewnie bez takich ambicji, że rozwiąże się wszystkie problemy jedną, dwoma czy pięcioma ustawami, czy w ogóle systemem prawnym. Jakies się pewnie rozwiąże, ale na pewno nie wszystkie.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo.

Pan poseł Bliźniuk, bardzo proszę.

Poseł Paweł Bliźniuk (KO):

Dziękuję.

Chciałem podziękować panu przewodniczącemu za to dzisiejsze posiedzenie podkomisji i NASK, że nas tutaj goście. Jak widać, temat jest wielowątkowy, wieloaspektowy. Też chciałem podziękować za tę prezentację, która wprowadza nas w kilku slajdach i kilkunastu zdaniach w kwestie cyberbezpieczeństwa i sztucznej inteligencji w cyberbezpieczeństwie.

Jak to napisał Andrzej Mleczo na jednej ze swoich grafik, gdzie jest jeden dziennikarz i jego gość: „Zacznę od pytania na rozgrzewkę, czyli o sens życia, a później przejdziemy do trudnych zagadnień”. Pojawił się wątek geopolityczny. Mam do państwa, do panów pytanie, jeżeli chodzi o sztuczną inteligencję i te modele, technologie fundamentalne, czyli hardware czy *central processing unit* (CPU), i dostęp do mocy obliczeniowych z jednej strony, do języków fundamentalnych z drugiej strony. Jeżeli chodzi o nas, to ani w jednym, ani w drugim nie mamy jakiegokolwiek suwerenności. To trzeba jasno i wyraźnie tutaj powiedzieć. Myślę, w tę stronę szły pytania pana posła, jeżeli chodzi o te moce obliczeniowe jako Europy i zdolności Europy, nie tylko Polski w tym zakresie.

Mam takie zasadnicze, może naiwne pytanie, ale prosiłbym specjalistów i ekspertów w tym zakresie. Myślę, że warto o tym wiedzieć. Nie mamy dostępu ani do mocy obliczeniowych czy może ich rozwoju – to był temat chociażby kwestii eksportu półprzewodników w 2025 r., który wybuchł w lutym i był obecny w przestrzeni publicznej przez kilka miesięcy, tak pod koniec 2024 r., pod koniec kadencji Joe Bidena – ani nie mamy fundamentalnego języka.

Jeżeli doszłoby do sytuacji, gdzie ci, którzy są właścicielami tych fundamentalnych technologii, czyli decydują o proliferacji mocy obliczeniowych czy też dostępu do języków fundamentalnych, zdecydowali, że ograniczają nam ten dostęp, to czy my mamy na to jakąś odpowiedź? Mówimy o cyberbezpieczeństwie, czyli bezpieczeństwie, czyli też tutaj cyfrowej suwerenności państwa polskiego. Czy jesteśmy tutaj dzisiaj na tyle zależni, że będziemy mieli problem przy takich decyzjach na poziomie strategicznym? Czy oczywiście w konsekwencji nasza gospodarka itd. będzie miała jeszcze większe problemy z konkurencyjnością, żeby to tak dyplomatycznie ująć. To jest takie pytanie o sens życia. Dziękuję.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo.

Bardzo proszę.

Dyrektor NASK dr inż. Radosław Nielek:

Panie pośle, a może pan doprecyzować, o co chodzi z tym językiem fundamentalnym? Chodzi o taki model bazowy?

Poseł Paweł Bliźniuk (KO):

Tak, podstawowy.

Dyrektor NASK dr inż. Radosław Nielek:

Nie chciałbym tutaj wchodzić w geopolitykę. To także nie jest obszar, tak jak prawo...

Posel Paweł Bliźniuk (KO):

Pytam wyłącznie o technologię.

Dyrektor NASK dr inż. Radosław Nielek:

Jestem inżynierem. Natomiast z perspektywy mocy obliczeniowej, oczywiście jest tak, że mamy w tej chwili jakąś moc obliczeniową dostępną w kraju, w Europie. Gdyby dostawcy tej mocy obliczeniowej, czyli producenci konkretnych układów lub kraje, które mają wpływ na tych konkretnych producentów, podjęły decyzję o tym, że od jutra przestają sprzedawać nam te układy, to oczywiście trzeba mieć świadomość, że byłby z tym problem. To znaczy, mielibyśmy duży problem oczywiście nie w perspektywie jutra, pojutrze. One tutaj są i nie przestałyby działać. Mielibyśmy problem w perspektywie 18, 24 miesięcy.

Przy czym nie jest to jedyna rzecz, z którą mielibyśmy problem, gdyby przestano nam ją sprzedawać. Gdyby nam przestano sprzedawać ropę lub gaz, to także mielibyśmy z tym problem. Natomiast chciałem tylko zwrócić uwagę na to, że trochę rzeczy się zmienia. To znaczy, jak żyliśmy w rzeczywistości, w której był w zasadzie jeden dostawca technologii, która pozwalała budować takie modele czy trenować takie modele, i była to firma NVIDIA, tak od pewnego czasu mamy już AMD, które dostarcza też takie rozwiązania. Powiedzmy, że to pewnie nie przekonuje jeszcze większości, bo to jest jakby ten sam kawałek geopolityczny.

Zdradzę taką małą rzecz. Dwa, trzy tygodnie temu zainstalowaliśmy testowo w serwerowni NASK rozwiązanie do trenowania modeli inferencji dostarczane przez kanadyjską firmę w ramach swojego własnego projektu i swoich własnych układów. To znaczy, oni, korzystając z technologii RISC-V, czyli takiej otwartej technologii projektowania czy może otwartej architektury procesorów, projektują i produkują to rozwiązanie, które pozwala prowadzić inferencję, czyli używać modeli, świadczyć usługi z oparciem, z wykorzystaniem takich modeli, a także trenować z wykorzystaniem tego rozwiązania.

Jesteśmy na początkowym etapie. Testujemy to rozwiązanie. To pokazuje, że jest coraz więcej graczy na takiej scenie, powiedziałbym, państwowej, którzy dostarczają takie rozwiązania. To jest jedno z narzędzi. Nie wierzę w to, żebyśmy byli w stanie niezależnie produkować w Polsce w dającej się przewidzieć perspektywie procesory, to znaczy, właściwie kontrolując cały łańcuch dostaw. W zasadzie nikt na świecie nie jest w stanie tego w tej chwili zrobić. Jak popatrzymy, to są maszyny do produkcji, które dostarcza ktoś inny. Produkujemy to w jakimś jednym kraju. Materiały do produkcji dostarcza jeszcze ktoś inny, a urządzenie czy oprogramowanie do projektowania układu dostarcza jeszcze jakiś inny podmiot. Nie zakładam, żebyśmy byli w stanie sami produkować takie procesory w jakiejś krótkiej perspektywie, to raczej nie. Dla mnie bezpieczeństwem jest nie to, że jesteśmy w stanie sami je produkować, tylko to, że jest wielu dostawców z różnych krajów, z których można korzystać. Tutaj zaczynamy być w tym miejscu. Jeszcze to nie jest ten poziom, który byśmy chcieli osiągnąć. To są raczej testy niż produkcyjne rozwiązania z naszej perspektywy, ale już je testujemy u nas właśnie po to, żeby mieć alternatywę.

Jeśli chodzi o modele bazowe, to tutaj sprawa jest trochę prostsza. Nawet wytrenowaliśmy taki jeden model bazowy w NASK od wag losowych, czyli korzystając z tego, że nie używamy żadnego modelu jako tej podstawy do trenowania. Jesteśmy w stanie potencjalnie wytrenować kolejne takie modele w Europie. One oczywiście pewnie nie będą tak dobre jak te modele, które są dostępne komercyjnie od największych dostawców, ale będą wystarczająco dobre dla bardzo wielu zastosowań, więc tutaj nie ma takiego ryzyka.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo.

Przewodniczący Bartłomiej Pejo, bardzo proszę.

Posel Bartłomiej Pejo (Konfederacja):

Przepraszam, za chwilę będę musiał wyjść. Padło poprzednie pytanie, taka myśl i do polityków, i do ekspertów. Jeśli mówimy, a coraz częściej mówimy o suwerenności cyfrowej w kontekście sztucznej inteligencji, cyberbezpieczeństwa, to myślę, że powinniśmy nieść informację, że to nie jest tylko kwestia stricte technologii. Jeśli mówimy o gigafabrykach, również tych powstających w Polsce albo powstających w przyszłości, to przede wszystkim potrzebne są ogromne środki. Jak pan dyrektor zauważył, te środki, nawet europejskie, najprawdopodobniej nigdy nie dogonią tych chociażby zza oceanu.

Pierwsza rzecz – wydaje mi się, nawet jestem przekonany, że w polskim w budżecie na 2026 r. nie zabezpieczaliśmy tego wkładu na gigafabryki. Mam na myśli ten projekt europejski. To pierwsza kwestia. Według różnych analiz, ekspertyz na rozwój gigafabryk w Polsce i w ogóle sztucznej inteligencji potrzeba w najbliższym czasie nie setek milionów, tylko miliardów złotych. Te dane mniej więcej są dostępne i też pytanie brzmi, jak pan dyrektor może się odnieść do tych informacji.

Co jest kluczowe i myślę, że warto wystąpić z takim apelem do nas samych i parlamentarzystów, ale i ekspertów, jeśli chodzi o zabezpieczenie tej infrastruktury energetycznej. Co z tego, że będziemy mieli technologię, będziemy mieli nawet pieniądze na gigafabryki, jeśli nie będziemy zabezpieczeni energetycznie. To jest zupełnie inna działka, spoza tej Komisji, spoza w ogóle sfery cyfryzacji, i powinniśmy również wychodzić z tą myślą. Przecież te wielkie komputery potrzebują takiej mocy jak niejedno polskie miasto. To są mniej więcej tego typu zabezpieczenia, których nie ma. Wydaje się, że tracimy gdzieś tę myśl. Tak jak mówię, co z tego, że będziemy mieli super pomysły i nawet możliwości ich wdrożenia, jeśli nie jesteśmy w stanie zabezpieczyć energetycznie tych projektów.

Dyrektor NASK dr inż. Radosław Nielek:

Panie przewodniczący, tylko powiem, że z mojej perspektywy, i myślę, że też z perspektywy naukowców, którzy tutaj są w NASK, ta część związana z taką twardą infrastrukturą, to znaczy sprzętem, kartami, jest oczywiście najbardziej spektakularna, bo ją najbardziej widać. Powstają jakieś mury, są jakieś szafy, w tych szafach są urządzenia, natomiast w mojej ocenie ona będzie miała najmniejszą część w łańcuchu wartości. To znaczy, dużo więcej w łańcuchu wartości będą ważyły dane używane do trenowania, wiedza, algorytmy i zbudowane modele z wykorzystaniem tych narzędzi. Jeśli miałbym gdzieś inwestować pieniądze... Oczywiście czym więcej ich zainwestujemy w rozsądnej skali, to pewnie będziemy mieć lepsze efekty. Jeśli miałbym gdzieś je inwestować, to nie zapomniałbym o tym, że w tym łańcuchu wartości więcej wartości będzie właśnie w tych algorytmach, w danych, w trenowaniu tych modeli niż w samych tych urządzeniach, szafach wykorzystywanych do generowania tego. Jak popatrzymy na oferty w sklepach dotyczące ubrań, to większość z tych ubrań szyje się raczej nie tam, gdzie są ci, którzy zarabiają najwięcej na ich dostawie, sprzedaży i projektowaniu. Tutaj będziemy mieć za chwilę tak samo. Oczywiście koszty prądu będą wpływały na opłacalność. Czym prąd jest droższy, tym mniej opłaca się trenować te modele w Polsce.

Dostępność tego to oczywiście jest także oddzielna kwestia. Podpięcie takich dużych infrastruktur wymaga sieci przesyłowych. To też oczywiście wymaga inwestycji. Wciąż jestem przekonany, że więcej takiej dodanej wartości będzie nie w tej twardej infrastrukturze, tylko w wiedzy, w kompetencjach ludzi. W to bym inwestował, choć oczywiście to jest zawsze trudniejsze.

Przewodniczący poseł Grzegorz Napieralski (KO):

Proszę bardzo.

Poseł Bartłomiej Pejo (Konfederacja):

Dziękuję bardzo.

Ad vocem. Panie dyrektorze, właśnie to miałem na myśli. Nie inwestowanie w infrastrukturę i wręcz budowanie wśród osób odpowiedzialnych za infrastrukturę, za przesył, za energetykę takiego zabezpieczenia właśnie energetycznego dla przyszłych projektów wielkoskalowych w nowe technologie. Tak jak wspomniałem, to nie jest jakieś uderzenie polityczne w kogokolwiek, tylko wręcz apel do nas wszystkich, żebyśmy też o tym rozmawiali. Nawet jeśli będą pieniądze europejskie czy też w ogóle rynkowe na gigafabryki, to tak już mówiąc wprost, zabraknie nam po prostu prądu.

Przewodniczący poseł Grzegorz Napieralski (KO):

Pani poseł Soboląg, bardzo proszę.

Poseł Anna Soboląg (KO):

Dziękuję, panie przewodniczący.

Szanowni państwo, troszeczkę w odniesieniu do pana przewodniczącego Pejo chciałabym odpowiedzieć na ten proces powstawania gigafabryk w Europie, ale przede wszystkim w Polsce. Nie możemy deprecjonować tego pomysłu powstawania gigafabryk. Oczywiście to, o czym pan

dyrektor mówił, inwestowanie środków w takie tu i teraz, mniejsze środki, kupowanie kart graficznych itd., to jest ważne, ale w perspektywie gigafabryki też są ważne.

Jestem z Wrocławia. Tam została wyznaczona jedna z pięciu lokalizacji powstania gigafabryk w Polsce, a co za tym idzie, jeżeli Komisja Europejska wyznaczyła, zaakceptowała te pięć lokalizacji, to znaczy, że zostały w tych lokalizacjach zabezpieczone kwestie energetyczne, kwestie chłodzenia gigafabryk. Na przykład we Wrocławiu, bo tam liderem jest Politechnika Wrocławska, mamy podpisane takie daleko idące porozumienie, również ze spółką Skarbu Państwa. Jeżeli dojdzie do tej lokalizacji, do wybudowania tej inwestycji we Wrocławiu, całe ciepło odpadowe, które powstaje w procesie, kiedy ta gigafabryka funkcjonuje, zostanie oddane do miasta. Połowa ciepła, którego potrzebuje Wrocław, zostanie zabezpieczona pod kątem właśnie tego, że to będzie jako proces tego ciepła odpadowego. Tak że w moim odczuciu te gigafabryki to są tutaj bardzo ważne inwestycje, gdzie będzie też wymiana wiedzy naukowej, rozwój gospodarczy. Też myślę, że duże moce obliczeniowe spowodują możliwość tego zabezpieczenia cybernetycznego, jeżeli chodzi o Polskę, dlatego jest ten 35-procentowy udział poza konsorcjum biznesowym, gdzie mogą wejść oczywiście spółki Skarbu Państwa, samorządy. Tutaj właśnie tak to wygląda. Dziękuję bardzo.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo.

Jeszcze poseł Bliźniuk chciał dorzucić jedną rzecz.

Poseł Paweł Bliźniuk (KO):

Tak. To znaczy, pojawił się ten wątek. Chciałem dorzucić coś o takich szczegółowych sprawach gigafabryk jako elementu, który tam ma gwarantować nam suwerenność, o czym panowie wspominali. Pod koniec grudnia Komisja Europejska zmieniła zasady realizacji tego projektu na *joint procurement agreement*, czyli taki otwarty przetarg, gdzie państwo czy państwa, bo to jest projekt europejski, mają mniejszy wpływ na w ogóle de facto cały proces poza finansowaniem czy wkładem własnym.

Mam pytanie, czy NASK ma zabezpieczony interes w tym projekcie. To znaczy, mówicie panowie, że potrzebujecie dostępu do mocy obliczeniowych jako wy, ale też w ogóle polska nauka. Czy w tym nowym brzmieniu tego projektu ten dostęp jest zagwarantowany, bo te warunki zmieniły się. To jest pierwsze pytanie. W sumie, jeżeli mówimy o gigafabrykach, to tyle, bo kolejne będą dotyczyły innych kwestii związanych z tematem dzisiejszego posiedzenia.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo.

Panie dyrektorze.

Dyrektor NASK dr inż. Radosław Nielek:

Panie pośle, NASK był podmiotem, który podpisał porozumienie czy list intencyjny w związku z gigafakturą w momencie, w którym projekt startował. Jesteśmy oczywiście uczestnikiem tych dyskusji. W tym kontekście – nie ma jeszcze finalnych wytycznych do tego, jak będzie wyglądało składanie wniosków, w związku z tym, jak te projekty powinny być finansowane, co jest wkładem, co można odebrać w mocy obliczeniowej, co powinno się zwrócić w kontekście opłat przez jakieś tam zewnętrzne podmioty. Jeszcze nie jesteśmy na tym etapie, w którym przesądzi się, że na pewno będziemy mieć zagwarantowaną moc obliczeniową. Jako dyrektor na pewno staram się dbać o to, żeby moi naukowcy mieli dostęp do niezbędnych mocy obliczeniowych. W tym sensie inwestujemy tutaj spore pieniądze, także we własne moce obliczeniowe. Pewnie będziemy w niedługim czasie komunikować to na zewnątrz – o już działających systemach w tym zakresie.

Zwracam tylko uwagę, że dla części z naszych zastosowań jako NASK rozwiązania takie jak gigafactory nie do końca się sprawdzają, dlatego że my potrzebujemy zamkniętych systemów. To znaczy, takich, w których mamy pełną kontrolę nad tym, gdzie znajdują się dane, do czego są wykorzystywane, że ten system nie jest w danym momencie wykorzystywany do niczego innego. Oczywiście budujemy takie systemy w tej chwili po to, żeby korzystać z nich także w naszych projektach. Jeśli finalnie powstanie gigafactory, to NASK na pewno będzie dużym użytkownikiem takiego rozwiązania z perspektywy uczelni i instytutów badawczych. Zarówno w takiej wersji, w której będziemy realizować tam projekty komercyjne, dofinansowane, jak i takie, w których będziemy realizować nasze naukowe projekty.

Posel Paweł Bliźniuk (KO):

Już kończąc ten wątek geopolityczny... Oddałem tu głos przewodniczącemu Pejo. Widzę, że jeszcze zmierzamy do końca. Jest ten wątek dotyczący suwerenności, która w pewnym stopniu powinna być naszą jakąś taką wartością nadrzędną – budowanie suwerenności cyfrowej Polski, Europy w kontekście zmieniającego się otoczenia geopolitycznego. Wiem, że państwo w NASK przede wszystkim odpowiadać za tą część technologiczną, naukową i wykonujecie fundamentalną pracę w tym zakresie.

Natomiast sztuczna inteligencja jest podniesiona do rangi geopolitycznej, jest elementem polityki. Słusznie pan zauważył, że można nas odciąć od zasobów gazu, ropy i innych fundamentalnych zasobów i również tak musimy traktować sztuczną inteligencję, o czym niektórzy po prostu nie wiedzą. Uważają, że dostęp do niej czy do technologii jest po prostu nieograniczony, będzie zawsze, a jest to element polityki i polityki fundamentalnej.

Po pierwsze, jak się popatrzy na dokumenty strategiczne u naszego najważniejszego sojusznika, czyli w Stanach Zjednoczonych, mamy *AI Action Plan* z lipca 2025 r., który niejako zastąpił *Executive Order* Joe Bidena i wycofał te ograniczenia w proliferacji półprzewodników GPU również w naszej części Europy. Mamy nową strategię obrony narodowej Stanów Zjednoczonych, gdzie jest cały rozdział poświęcony sztucznej inteligencji. Zwracam uwagę na tę strategię z zeszłego roku, ponieważ tam nie mówi się o tym, że Stany Zjednoczone mają być liderem sztucznej inteligencji na świecie, tylko mają w tym zakresie dominować, odchodząc od doktryny proliferacji, zabezpieczenia tejże w zakresie tych technologii fundamentalnych, ale do tak naprawdę pakietowego sprzedawania rozwiązań związanych ze sztuczną inteligencją.

To wszystko jest też oparte o argumenty związane z cyberbezpieczeństwem. De facto jest to też pewien obszar polityki. Sztuczna inteligencja dzisiaj w wymiarze bezpieczeństwa ma charakter polityczny. Ma charakter przestrzeni, która zresztą w myśl opublikowanej już teraz w grudniu nowej strategii obrony Stanów Zjednoczonych ma fundamentalny charakter w wymiarze rywalizacji z Chinami i w ogóle budowania pozycji lidera na świecie przez Stany Zjednoczone. Więc z drugiej strony mamy Chiny i mamy też europejskie starania o budowanie jakiejś tam suwerenności, czego wymiarem jest chociażby program budowy kilku gigafabryk w Europie, który to pod koniec grudnia zmienił trochę swój charakter, co moim zdaniem jest sprzeczne z ideą budowania suwerenności, jeżeli dopuszczamy do tego interesu podmioty z zagranicy. Komisja to otworzyła, nie ma tutaj limitacji do firm, które działają na terenie Unii Europejskiej. Według nowych rozwiązań również podmioty z zagranicy mogą być tym elementem biznesowym, który jest dzisiaj wiodącym, jeżeli chodzi o realizację gigafabryk sztucznej inteligencji w Europie.

Tak że ze względu na to, że zmierzamy już pewnie do końca, ale też myślę, że w świadomości państwa i w NASK kwestie sztucznej inteligencji to jest absolutna oczywistość, natomiast moim zdaniem trzeba ten temat uwypuklać nawet w świadomości wśród parlamentarzystów. Komisja Cyfryzacji, Innowacyjności i Nowych Technologii i Komisja Spraw Zagranicznych w tym roku mają w planie działań kwestie związane z dyplomacją cyfrową. Jednak te interesy w domenie cyfrowej to są interesy, o które trzeba dbać tak samo jak o interesy w przestrzeni lądowej, powietrznej, kosmicznej czy też morskiej, o czym też zapominamy. Tutaj będzie kwestia też budowania kompetencji nie tylko technologicznych, ale w wymiarze dyplomacji, dyplomacji gospodarczej i tych relacji międzynarodowych, gdzie ciągle te interesy są podnoszone i muszą być obsługiwane. Bez podejmowania decyzji, które mają zmierzać do suwerenności, nie da się zbudować niezależności. Dzisiaj jesteśmy w świecie powiązań, o których pan dyrektor mówi, natomiast pewne stopnie suwerenności czy też właśnie szukanie rozwiązań, które albo dywersyfikują pewne rozwiązania, albo powodują, że możemy uzyskać pewne zdolności własne w jakiejś tam perspektywie czasowej, są fundamentalne. Oczywiście to jest temat rzeka. Myślę, że też te tematy będą pewnie przedmiotem naszych zainteresowań jako Komisji, a szerzej parlamentu.

Ostatni rok, ostatnie miesiące, to jest debata wokół metali ziem rzadkich, kwestia łańcuchów logistycznych, kwestia tego, że kwestie technologiczne były i są wykorzystywane chociażby w relacjach amerykańsko-chińskich jako lewar, do czego ostatnio było dość mocne przyspieszenie, gdzie Chińczycy odpowiedzieli kwestią właśnie metali ziem rzadkich. W zeszłym tygodniu mieliśmy konferencję w Stanach Zjednoczonych dotyczącą zabezpieczenia tych źródeł. To wszystko jest jednak powiązane i żyjemy w bardzo ciekawych czasach, stąd ten temat bezpieczeństwa trzeba zacząć od takiego poziomu strategiczno-geopolitycznego i oczywiście schodzić niżej. Jeżeli nie będziemy mieli świadomości, nie rozwiążemy wszystkich problemów.

Budowanie tej świadomości wśród parlamentarzystów, wśród osób, które zajmują się tymi tematami, jest również fantastycznym wyzwaniem, które pan przewodniczący i nasza podkomisja podjęliśmy. Myślę, że robimy to z dużym powodzeniem. Myślę, że są przed nami kolejne kroki i jakieś kolejne aktywności w tym zakresie i bardzo fajnie, że mieliśmy okazję dzisiaj tutaj też o tym porozmawiać.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo, panie pośle. Dziękuję za miłe słowa. Tylko dodam do tego, co powiedział poseł Bliźniuk, że to, co robicie, jest moim zdaniem w ogóle bardzo istotne i bardzo ważne.

W kontekście tego, co wydarzyło się wczoraj, to mieliśmy zamknięte czy tajne posiedzenie naszej Komisji dotyczące akurat ustawy o cyberbezpieczeństwie. Wiadomo, że wokół niej było wiele zamieszania. Jedna rzecz, która wynika z tego tajnego posiedzenia, nie ujawniając oczywiście tajemnicy państwowej, to można powiedzieć, że jest taka. To zagrożenie, które wynika z rozwoju technologicznego, jest dzisiaj coraz większe. Ono pojawia w takich miejscach, w których kiedyś w ogóle nie wiedzieliśmy, że ono może się pojawić. Tak jak powiedział dyrektor Nielek, że nawet dwa lata wcześniej w ogóle nie myśleliśmy o takich rzeczach, a teraz już dyskutujemy, czy bezpiecznie jeździć takim czy innym samochodem, czy nie zbiera naszych danych, a jeżeli zbiera, to jakie dane zbiera.

Dzisiaj tak naprawdę, jeszcze rozwijając sztuczną inteligencję, która będzie pojawiała się w szkołach, na uczelniach, ale też w szpitalach, to, co robicie, to całe takie bezpieczeństwo właśnie w tym obszarze cywilnym będzie bardzo istotne. Już nie mówiąc o tym aspekcie edukacyjnym, myślę, że to powinno być też jakimś elementem, ale to oczywiście nie jesteśmy ani my, ani NASK, ale to też powinno być uczone już od najmłodszych lat. Tak kiedyś uczyliśmy się, że nie wolno przychodzić na czerwonym świetle, dzisiaj musimy już nauczyć się innych kompetencji, tak żeby być bezpiecznym w tym świecie. Dziękujemy wam za to. To, co robicie, jest naprawdę bardzo ważne. Mijmy nadzieję, że jakakolwiek czy ktokolwiek nie będzie rządził, to jednak nie będziecie schodzili na jakiś dalszy plan, jeżeli chodzi o finansowanie, o umiejscowienie was w całej hierarchii struktury państwa. Chyba mamy wszystko, panie dyrektorze, nie...

Pan poseł. Bardzo proszę. Tak, przepraszam bardzo, panie pośle.

Poseł Paweł Bliźniuk (KO):

Mam nieodpartą pokusę. Krajowy System e-Faktur to infrastruktura krytyczna. Zgodnie z regulacjami dotyczącymi cyberbezpieczeństwa NASK jest na pewno zainteresowany bezpieczeństwem danych, które są w tym systemie, i w ogóle bezpieczeństwem całej architektury. Ostatnio w przestrzeni publicznej pojawiły się zagadnienia dotyczące tego, że wyprowadzamy dane do Francji, Izraela i gdziekolwiek, że serwery są w ogóle za granicą i że nie ma pełnej kontroli. Mam pytanie, jak byście się może tak ogólnie ustosunkowali do tych nieprawdziwych informacji, które się pojawiły w przestrzeni publicznej? Myślę, że skoro mamy okazję o to zapytać, to warto by było otrzymać jakąś informację na ten temat w kilku zdaniach.

Dyrektor NASK dr inż. Radosław Nielek:

Panie pośle, to nie jest obszar odpowiedzialności CSIRT NASK. Zgodnie z delegacją ustawową za ten kawałek, to znaczy, zarówno za infrastrukturę krytyczną, jak i za infrastrukturę instytucji centralnych – KSeF jest bez wątpienia elementem infrastruktury i ministerstwa, czyli instytucji centralnych – za bezpieczeństwo tych kawałków odpowiada CSIRT GOV, czyli CSIRT, który jest umiejscowiony w Agencji Bezpieczeństwa Wewnętrznego. W związku z tym, to jest pytanie, które trzeba by było przekazać do nich.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo.

Panie dyrektorze, szanowni państwo, wyczerpaliśmy na tym porządek naszych dzisiejszych obrad. Chciałem złożyć na ręce pana dyrektora i całego zespołu bardzo serdeczne podziękowania. Jak pan dyrektor zauważył... Przepraszam też za moich kolegów, którzy musieli już wyjść, ale niestety nasze Komisje nakładają się i tak to jest. Jak jeszcze robimy to w Sejmie, to jest łatwiej, a jak już jesteśmy poza budynkiem parlamentu, to jest gorzej. Dziękujemy za to, że nas przyjeżdżacie, za to, że pokazaliście to nam, za to, że w ogóle robicie takie fantastyczne rzeczy.

Chciałem też zadeklarować oczywiście z naszej strony, naszej podkomisji, jak i Komisji Cyfryzacji, Innowacyjności i Nowych Technologii, co uzgodniłem z panem przewodniczącym Pejo, oraz, mam nadzieję, szybko powstałej nowej podkomisji, którą będzie, mam nadzieję,

kierował pan poseł Bliźniuk, czyli zajmującej się już stricte kwestiami bezpieczeństwa, że też jesteśmy do waszej dyspozycji. Jeżeli możemy w czymś pomóc, w czymś, co jest dla was bardzo istotne, być może w jakiejś poprawie funkcjonowania waszego instytutu, jesteśmy oczywiście do dyspozycji, a za dzisiaj bardzo serdecznie dziękuję.

Zamykam posiedzenie podkomisji. Mam nadzieję, do szybkiego zobaczenia. Dziękuję bardzo.