PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 37/2026, 15 LIPCA 2026 © PISM

KOMENTARZ

# Unijny plan działania w zakresie cyberbezpieczeństwa i AI

Aleksandra Wójtowicz

Opublikowany przez Komisję Europejską 7 lipca 2026 r. Plan działania w zakresie cyberbezpieczeństwa i sztucznej inteligencji za szczególnie istotne uznaje zagrożenia związane z wykorzystaniem zaawansowanych modeli AI w cyberatakach, a także europejską zależność od amerykańskich dostawców sztucznej inteligencji. Choć nie wprowadza wielu nowych rozwiązań, jego wartością jest wskazanie na kolejne podatności UE w sferze cyfrowej.

**Czym jest nowy Plan działania?**

Plan jest odpowiedzią na rosnące możliwości zastosowania sztucznej inteligencji zarówno w cyberatakach, jak i w cyberbezpieczeństwie. Jest także reakcją na ograniczenia nałożone przez Departament Handlu USA na firmę Anthropic. W czerwcu br. władze USA nakazały Anthropicowi zablokowanie wszystkim obcokrajowcom, w tym firmom z UE, dostępu do jego najnowszych modeli Fable 5 i Mythos 5. Uwidoczniło to zależność europejskiego systemu cyberbezpieczeństwa od amerykańskich rozwiązań AI – UE korzysta z amerykańskich modeli AI, do których dostęp może zostać zablokowany. Plan KE opiera się na trzech filarach: zapewnieniu bezpieczeństwa, dostępności i możliwości wdrożenia najnowszych modeli sztucznej inteligencji w europejskim cyberbezpieczeństwie; przygotowaniu się na sytuacje, w których AI będzie intensywnie wykorzystywana w cyberatakach; zwiększeniu europejskich możliwości w zakresie AI, czyli de facto stworzeniu własnych modeli wyspecjalizowanych w ochronie cyberprzestrzeni. Akt nie tworzy nowych obowiązków prawnych. Komisarz ds. suwerenności technologicznej Henna Virkkunen zapowiedziała, że planowi nie będą też towarzyszyć nowe regulacje, a nacisk zostanie położony na egzekwowanie już istniejących.

**Jakie działania przewiduje?**

Do każdego z filarów przypisane zostały trzy kluczowe działania. W obszarze pierwszym, czyli dostępie do bezpiecznych modeli AI, Komisja zakłada powstanie do 2027 r. systemu ewaluacji modeli sztucznej inteligencji, który będzie oceniał je także pod względem cyberbezpieczeństwa. Komisja UE ds. Cyberbezpieczeństwa (ENISA) ma z kolei stworzyć platformę, na której będzie można takie testy przeprowadzać. Komisja zapowiada ponadto powstanie ram współpracy z dostawcami AI, które zapewnią europejskim firmom bezpieczny i terminowy dostęp do amerykańskich modeli AI użytecznych w obronie cyberprzestrzeni. Plan nie precyzuje jednak, w jaki sposób ma to nastąpić.

W przypadku filaru drugiego, czyli przygotowania cyberprzestrzeni na ataki z użyciem sztucznej inteligencji, Komisja przewiduje przede wszystkim stworzenie mechanizmów wymiany informacji i dobrych praktyk między państwami członkowskimi, publikacje kolejnych wytycznych i ram prezentujących efektywne sposoby przeciwdziałania cyberatakom wspomaganym AI, a także pilotaż kampanii na rzecz odporności krytycznego oprogramowania open source.

W ramach trzeciego filaru Komisja chce udostępnić moc obliczeniową europejskich fabryk AI w celu trenowania modeli, które będą wzmacniać europejskie cyberbezpieczeństwo, a także szkolić informatyków w zakresie wykorzystania AI w ochronie cyberprzestrzeni. Ma to pozwolić na stworzenie rodzimych narzędzi odpowiadających poziomem istniejącym obecnie rozwiązaniom amerykańskim.

**Czy Plan wzmocni europejski system cyberbezpieczeństwa?**

Proponowane przez Plan rozwiązania są bardzo ogólne i same w sobie nie wzmocnią europejskiej cyberprzestrzeni. Plan nie wprowadza wielu nowych rozwiązań – przedstawia przede wszystkim rekomendacje dla innych instytucji europejskich, w tym samej Komisji, i podkreśla związane z cyberbezpieczeństwem aspekty istniejących już regulacji, takich jak Akt o sztucznej inteligencji, Akt w sprawie cyberodporności czy Dyrektywa NIS2. Plan nawiązuje też do istniejących rozwiązań, m.in. do budowy kolejnych europejskich fabryk oraz gigafabryk AI. Większość z nich ma jednak zapewniać moc obliczeniową modelom ogólnego przeznaczenia. Brakuje więc infrastruktury wyspecjalizowanej stricte w ochronie cyberprzestrzeni, czego Plan nie podejmuje. Nie określa też, z których konkretnie fabryk miałaby być udostępniana moc dla rozwiązań AI w cyberbezpieczeństwie.

Przykładem podobnych braków jest bardzo ogólna zapowiedź stworzenia ram, które zapewnią europejskim firmom dostęp do najnowszych modeli sztucznej inteligencji. Nowym rozwiązaniem, które zostało zapowiedziane w Planie, jest możliwość ewaluacji modeli AI pod względem cyberbezpieczeństwa. Akt o AI zakłada wprawdzie, że zaawansowane modele sztucznej inteligencji muszą zostać poddane ocenie, a ryzyko z nimi związane musi być ograniczone, zanim zostaną wprowadzone na rynek UE. Plan zapowiada konkretyzację tej oceny w kontekście cyberbezpieczeństwa. Idea jest słuszna, choć brakuje konkretów co do postępowania w przypadku uznania modelu za zagrożenie. Istotną kwestią jest także proweniencja większości tego typu modeli – są to rozwiązania amerykańskie – a Komisja Europejska nie stworzyła dotychczas efektywnego sposobu komunikacji z amerykańskimi dostawcami AI. Niemniej wartością tego dokumentu jest postawienie właściwej diagnozy dotyczącej kolejnych podatności UE w sferze cyfrowej.

Redakcja: Jarosław Ćwiek-Karpowicz, Rafał Tarnogórski, Marcin Terlikowski, Justyna Szczudlik
Jędrzej Czerep, Anna Maria Dyner, Amanda Dziubińska, Mateusz Piotrowski, Daniel Szeligowski, Jolanta Szymańska, Damian Wnukowski, Szymon Zaręba, Tomasz Żornaczuk