AMERYKAŃSKA IZBA HANDLOWA W POLSCE
Spektrum Tower, ul. Twarda 18, 00-105 Warszawa
Tel: (48) (22) 5205999, e-mail: office@amcham.pl, www.amcham.pl

Warszawa, 9 maja 2025 r.

Szanowni Państwo,

w imieniu Amerykańskiej Izby Handlowej w Polsce (AmCham) oraz jej firm zwracamy się do Państwa w związku ze zbliżającym się posiedzeniem Rady Unii Europejskiej do Spraw Gospodarczych i Finansowych, która w dniu 13 maja ma rozpatrywać rozporządzenie SAFE – proponowany instrument finansowy Unii Europejskiej na cele obronne w wysokości 150 miliardów euro.

AmCham jest organizacją zrzeszającą przedsiębiorców amerykańskich w naszym kraju, reprezentujących jednocześnie jedną z największych grup inwestorów zagranicznych, którzy stworzyli aktywa w Polsce o wartości 239 mld złotych i kreują 327 tysięcy miejsc pracy. Od ponad 30 lat działamy na rzecz rozwoju wzajemnych relacji gospodarczych, a naszą misją jest poprawa klimatu inwestycyjnego i promocja naszego kraju na rynku amerykańskim. Członkami AmCham są w szczególności wszyscy najważniejsi amerykańscy inwestorzy działający w sektorze obronnym oraz w sektorze nowych technologii. Co za tym idzie, kwestie finansowania projektów zbrojeniowych oraz wszystkie działania zmierzające do podnoszenia poziomu bezpieczeństwa Polski i Unii Europejskiej należą do najważniejszych obszarów naszego zainteresowania.

Dzisiejsze zdolności obronne w coraz większym stopniu opierają się na szybkiej transformacji cyfrowej i technologiach komercyjnych. Analogicznie do tego jak smartfony zrewolucjonizowały komunikację, komercyjne chmury obliczeniowe i sztuczna inteligencja przekształcają działania wojskowe – od dostarczenia pełnej wiedzy o polu bitwy po cyberobronę. Wiodące potęgi zbrojne, w tym europejskie siły wojskowe, wykorzystują obecnie 70-80% komercyjnych komponentów w swoich systemach, aby utrzymać przewagę technologiczną przy najwyższym poziomie kontroli bezpieczeństwa.

W obecnym brzmieniu projektu SAFE, odnajdujemy szereg przepisów technicznych, które mogą w sposób niezamierzony osłabić europejskie zdolności obronne i interoperacyjność sił zbrojnych NATO, poprzez ograniczenie dostępu do tych kluczowych technologii komercyjnych. Mamy trzy główne obawy związane z kryteriami kwalifikowalności dla dostawców z państw trzecich:

1. Dane niejawne i poświadczenia bezpieczeństwa: Obecny projekt narzuca bardzo ogólne wymagania dotyczące poświadczeń bezpieczeństwa dla wszystkich pracowników zaangażowanych w procesy przetwarzania niejawnych danych. Takie podejście jest sprzeczne z ewoluującymi praktykami NATO, które zezwalają na przechowywanie danych o niższych klauzulach tajności w komercyjnych systemach chmurowych zabezpieczonych za pomocą kontroli technicznych, a nie poprzez poświadczenia bezpieczeństwa pracowników. Przykładowo, NATO zatwierdziło przechowywanie danych o klauzuli ZASTRZEŻONE w chmurze komercyjnej, a sojusznicy tacy jak Wielka Brytania, Finlandia i Portugalia stosują je już w bezpieczny sposób. Bardziej rygorystyczne podejście zawarte w rozporządzeniu SAFE mogłoby uniemożliwić europejskim siłom zbrojnym korzystanie z tych sprawdzonych, bezpiecznych technologii, utrudniając skuteczność operacyjną.

2. Wymagania dotyczące systemów sztucznej inteligencji: Zawarte w rozporządzeniu podejście do systemów sztucznej inteligencji nie jest spójne z tym, jak funkcjonują współczesne wojskowe systemy sztucznej inteligencji. Przepisy koncentrują się raczej na zamianie fizycznych komponentów niż na kontroli operacyjnej. Może to zablokować dostęp do kluczowych możliwości AI, które są niezbędne w obecnych konfliktach. Dla przykładu, ukraiński system zarządzania polem walki, który przetwarza ponad 1500 celów dziennie przy użyciu technologii komercyjnych, pokazuje, jak ważne jest utrzymanie dostępu do tych technologii.

3. Kryteria kwalifikacji dostawców: W projekcie brakuje przejrzystych standardów dotyczących gwarancji bezpieczeństwa i procesów kontroli dostawców technologii. Ta niejasność może wywołać poczucie niepewności i powodować opóźnienia w krytycznych działaniach modernizacyjnych w dziedzinie obronności. Bez ustandaryzowanych kryteriów nie jest oczywiste, w jaki sposób dostawcy mogą udowodnić zgodność z wymaganiami, potencjalnie wykluczając cenne technologie i usługi.

AMERYKAŃSKA IZBA HANDLOWA W POLSCE
Spektrum Tower, ul. Twarda 18, 00-105 Warszawa
Tel: (48) (22) 5205999, e-mail: office@amcham.pl, www.amcham.pl

W załączniku przesyłamy szczegółowe propozycje poprawek, które pozwoliłyby rozwiązać te kwestie przy jednoczesnym utrzymaniu silnych europejskich mechanizmów kontroli bezpieczeństwa. W razie potrzeby jesteśmy gotowi zaprezentować te propozycje bardziej szczegółowo podczas spotkania. W razie jakichkolwiek pytań, pozostajemy do dyspozycji. Osobą do kontaktu jest Bartosz Szyler, koordynator ds. prawnych i polityk publicznych, z którym można się skontaktować pod adresem: bartosz.szyler@amcham.pl oraz numerem tel.: +48 572 577 795.

Z poważaniem

Marta Pawlak, dyrektorka ds. prawnych i polityk publicznych

Kontekst

Wszystkie nowoczesne siły zbrojne, w tym w szczególności wiodące europejskie siły zbrojne, przyznają, że komercyjne rozwiązania gotowe (*commercial off-the-shelf solutions, COTS*) i technologie podwójnego zastosowania są niezbędne do utrzymania przewagi technologicznej i interoperacyjności wojsk NATO. Podejście to, sprawdzone już w ramach udanych programów, umożliwia szybką transformację cyfrową przy jednoczesnym zachowaniu ścisłej kontroli bezpieczeństwa i suwerenności operacyjnej. Przykładowo, brytyjskie Ministerstwo Obrony wykorzystuje komercyjne komponenty w 70-80% swoich systemów, a niemiecka Bundeswehra przyjęła strategię wielochmurową, która utrzymuje suwerenną kontrolę przy jednoczesnym dostępie do krytycznych zdolności. W 2024 roku NATO przyjęło ramy klasyfikacji D32, aby umożliwić Sojuszowi przechowywanie danych, w tym najniższego poziomu tajności (NATO RESTRICTED) w komercyjnych usługach chmurowych. Nawet Francja, kładąca silny nacisk na suwerenność technologiczną, zdała sobie sprawę z trudności związanych z całkowitym odizolowaniem się od komercyjnych, pozaeuropejskich technologii – czego dowodzi program ARTEMIS.IA, w którym przyjęto model hybrydowy wykorzystujący zarówno systemy własnej produkji jak i systemy *COTS* w celu osiągnięcia wymaganych zdolności przy jednoczesnym zachowaniu francuskiej kontroli operacyjnej.

Nowoczesne operacje wojskowe wymagają możliwości obliczeniowych, które mogą zapewnić tylko usługi hiperskalowe. Operacje te wymagają przetwarzania w czasie rzeczywistym danych z tysięcy czujników pola bitwy, uruchamiania złożonych modeli sztucznej inteligencji w celu wykrywania zagrożeń i wspierania jednoczesnych symulacji szkoleniowych dla tysięcy pracowników – wszystko to wymaga ogromnej, natychmiast dostępnej i potencjalnie nieskończenie skalowalnej mocy obliczeniowej. Możliwości te okazały się decydujące w Ukrainie, gdzie hiperskalowa chmura umożliwia szybki rozwój systemu zarządzania polem bitwy, operacje dronów oparte na sztucznej inteligencji i bezpieczną współpracę sił. Równie ważne są korzyści płynące z ekosystemu innowacji. Akcelerator Innowacji Obronnych NATO (DIANA) jest tego dowodem - dwie trzecie z pierwszej grupy finansowanych startupów wybrało chmurę hiperskalową, ponieważ daje im ona natychmiastowy dostęp do zaawansowanych zdolności bez inwestycji z góry.

Wymagania kwalifikacyjne SAFE

Propozycja SAFE przewiduje wyjątki dla podmiotów mających siedzibę i struktury zarządzania w UE, ale kontrolowanych przez podmioty z państw trzecich. Zgodnie z tymi odstępstwami, unijne spółki zależne podmiotów spoza UE, EOG EFTA i Ukrainy kwalifikowałyby się, jeżeli:

- zostałyby poddane kontroli bezpośrednich inwestycji zagranicznych (BIZ) w rozumieniu rozporządzenia (UE) 2019/452 przez państwo członkowskie UE i, w razie potrzeby, podlegają odpowiednim środkom zaradczym; lub
- Udzieliły "gwarancji", aby zapewnić, że ich zaangażowanie nie narusza interesów bezpieczeństwa i obrony UE i jej państw członkowskich.
- infrastruktura, obiekty, aktywa i zasoby (pod)wykonawców wykorzystywane do realizacji zamówienia znajdują się na obszarze UE, EOG, EFTA lub Ukrainy.

Obecnie rozporządzenie SAFE jest niejednoznaczne w odniesieniu do przepisów dotyczących kontroli bezpośrednich inwestycji zagranicznych i gwarancji bezpieczeństwa. Proces kontroli BIZ różni się w poszczególnych państwach członkowskich, przy czym spółki nie mają proaktywnej możliwości wnioskowania o dobrowolną kontrolę. Podobnie, nie ma ustandaryzowanego procesu gwarancji bezpieczeństwa. Ten brak jednoznaczności może potencjalnie utrudniać innowacje i ograniczać dostęp do krytycznych technologii, na których już polegają europejskie organizacje obronne. Aby rozwiać te obawy, zalecamy, aby Komisja rozważyła istniejące ramy i standardy w celu zapewnienia autonomii operacyjnej. Wielu globalnych dostawców technologii wspiera liczne standardy bezpieczeństwa i certyfikaty zgodności, w tym PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2 i NIST 800-171, pomagając klientom spełniać wymogi zgodności na całym świecie.

Certyfikaty te, zatwierdzone przez niezależnych audytorów zewnętrznych, wykazują kompleksowe zaangażowanie w spełnianie rygorystycznych standardów bezpieczeństwa w różnych europejskich jurysdykcjach i sektorach. Chociaż potrzeba zapewnienia autonomii operacyjnej jest zrozumiała, propozycja SAFE pozostaje niejednoznaczna co do tego, co pociąga za sobą obecna propozycja lub jakie zapewnienia/gwarancje zostaną uznane za wystarczające. Wyjaśnienie tych aspektów i wykorzystanie istniejących europejskich ram bezpieczeństwa mogłoby pomóc w osiągnięciu celów SAFE przy jednoczesnym utrzymaniu dostępu do krytycznych technologii i wspieraniu europejskich innowacji w

dziedzinie obronności.

Sugerowane poprawki

- Dodać do art. 16 ust. 5: "Komisja ustanawia znormalizowane kryteria oceny gwarancji bezpieczeństwa, w tym obiektywne wymogi kontroli bezpieczeństwa, metodologie oceny i uznawanie istniejących certyfikatów bezpieczeństwa."
- Dodanie do art. 16 ust. 4: "Komisja ustanawia znormalizowany proces kontroli bezpieczeństwa, w tym jasne ramy czasowe, kryteria oceny i uznawanie istniejących przeglądów bezpieczeństwa. Proces ten obejmuje przepisy dotyczące dobrowolnego poddawania się kontroli bezpieczeństwa przez dostawców usług."

Dane niejawne i poświadczenia bezpieczeństwa

Nowoczesne organizacje wojskowe i NATO zmierzają w kierunku przechowywania niższych poziomów danych niejawnych w chmurze komercyjnej. Rozporządzenie SAFE jest obecnie sprzeczne z tym podejściem, nakładając wymogi poświadczenia bezpieczeństwa na każdy podmiot dostarczający produkty lub usługi obsługujące dane niejawne.

Prawie wszystkie wojskowe dane operacyjne są niejawne. Ograniczenie wykorzystania chmury hiperskalowej do danych niejawnych skutecznie uniemożliwiłoby siłom europejskim prowadzenie nowoczesnych operacji wojskowych, ponieważ nie byłyby one w stanie wykorzystywać możliwości chmury do operacji na polu bitwy lub integracji wielodomenowej. Ramy bezpieczeństwa D32 opracowane dla NATO RESTRICTED pokazują, że można to osiągnąć przy jednoczesnym spełnieniu rygorystycznych wymogów bezpieczeństwa, a prace NATO nad umożliwieniem przechowywania danych o klauzuli SECRET w chmurze w 2025 roku wyznaczają przyszły kierunek.

Kwatera Główna NATO wykonała szeroko zakrojone prace w celu zidentyfikowania właściwych środków kontroli technicznych, aby zapewnić, że dostawcy zewnętrzni nie mają dostępu do danych niejawnych. UE powinna wykorzystywać te ramy w odniesieniu do niższych poziomów klauzuli tajności, zamiast ustanawiać nowe wymogi. Czołowi sojusznicy NATO, w tym Wielka Brytania, Finlandia i Portugalia, zatwierdzili już dane o klauzuli RESTRICTED w chmurze komercyjnej, udowadniając, że bezpieczeństwo i skuteczność operacyjną można utrzymać bez dedykowanej infrastruktury obsługiwanej przez kontrolowany personel. Państwa te mogą teraz wdrażać swoje zdolności w ciągu dni, a nie miesięcy.

Sugerowana poprawka:

- Dodanie do art. 16 ust. 5: "Wymogi bezpieczeństwa dotyczące informacji niejawnych są dostosowane do ram bezpieczeństwa NATO w zakresie zabezpieczania danych niejawnych".
- Uzupełnienie w art. 16 ust. 5 lit. b): "pracownicy lub inne osoby zaangażowane we wspólne zamówienia posiadają krajowe poświadczenie bezpieczeństwa wydane przez państwo członkowskie", przy czym "dostawca jest zobowiązany do wykazania wdrożenia technicznych środków kontroli bezpieczeństwa spełniających lub przewyższających standardy NATO w zakresie ochrony informacji niejawnych, w tym szyfrowania, kontroli dostępu, monitorowania i zdolności reagowania na incydenty".

Wyzwania AI/ML (kategoria 2)

W przypadku produktów kategorii drugiej (takich jak sztuczna inteligencja i systemy walki elektronicznej) dostawcy będą musieli wykazać się "zdolnością do podejmowania nieograniczonych decyzji" w zakresie definicji i ewolucji produktów. Propozycja SAFE nie określa szczegółowo, jakie konkretne dowody będą potrzebne wykonawcy do dostarczenia takich produktów kategorii drugiej. W art. 16 ust. 9 określono zasadę kwalifikowalności produktu, zgodnie z którą wykonawca musi posiadać "zdolność do podejmowania decyzji" bez "ograniczeń nałożonych przez państwa trzecie lub podmioty z państw trzecich" w odniesieniu do różnych aspektów projektu produktu, w tym jego "definicji" i "ewolucji". Motyw (20) propozycji SAFE sugeruje, że podmiot posiadający umowę musiałby wykazać, że ma zdolność prawną do wymiany komponentów, aby zapewnić "swobodę sił zbrojnych państw członkowskich UE związaną z tymi produktami bez ograniczeń nałożonych" przez państwa trzecie i podmioty z państw trzecich.

Sztuczna inteligencja stała się podstawą współczesnych operacji wojskowych, przekształcając wszystkie czynności związane z prowadzeniem działań, od analizy danych wywiadowczych po konserwację sprzętu. Szybkość, z jaką państwa mogą przyjmować i wdrażać zdolności SI, ma obecnie bezpośredni wpływ na ich gotowość wojskową i skuteczność operacyjną. Już teraz widzimy, jak sojusznicy NATO wykazują konkretne korzyści z przyjęcia AI w wielu dziedzinach. Obecne sformułowania zawarte w projekcie SAFE mogłyby jednak nieumyślnie ograniczyć dostęp do tych krytycznych zdolności, potencjalnie stawiając siły

europejskie w niekorzystnej sytuacji.

Ramy zaproponowane w SAFE nie odzwierciedlają dokładnie, w jaki sposób opracowywane i wdrażane są nowoczesne systemy sztucznej inteligencji. To niedopasowanie stwarza poważne wyzwania. Systemy sztucznej inteligencji opierają się na globalnych danych treningowych i ogromnych zasobach obliczeniowych. Ich rozwój obejmuje złożone łańcuchy dostaw modeli, narzędzi i infrastruktury. Innowacje w tej dziedzinie często wynikają z łączenia i dostosowywania istniejących modeli i możliwości, zamiast budowania wszystkiego. Wymagając możliwości całkowitej wymiany komponentów, SAFE ignoruje tę rzeczywistość techniczną i może poważnie utrudnić europejskie wysiłki na rzecz modernizacji obronności.

Koncentracja SAFE na fizycznej wymianie komponentów mija się z celem, jeśli chodzi o systemy AI. Organizacje wojskowe naprawdę potrzebują kontroli operacyjnej nad swoimi aplikacjami AI. Oznacza to możliwość konfigurowania i dostosowywania modeli AI, kontrolowania dostępu do danych i ich przetwarzania, ustawiania parametrów bezpieczeństwa i definiowania granic operacyjnych. Fizyczna wymiana komponentów jest mniej istotna niż tego rodzaju kontrola operacyjna w kontekście systemów AI.

Projekt SAFE stwarza przynajmniej kilka praktycznych wyzwań wdrożeniowych. Nie jest jasne, w jaki sposób koncepcja "organu projektowego" ma zastosowanie do usług AI opartych na chmurze. Rozporządzenie nie odnosi się do kluczowej różnicy między fazami szkolenia i wdrażania modeli. Istnieje ryzyko, że może to uniemożliwić korzystanie z niezbędnej globalnej infrastruktury sztucznej inteligencji, która umożliwia wykorzystanie zaawansowanych zdolności. Być może najbardziej niepokojące jest to, że może zablokować dostęp do krytycznych zdolności AI, które są już skutecznie wykorzystywane przez sojuszników NATO.

Sugerowana poprawka:

- Dodać do art. 16 ust. 9: W przypadku systemów sztucznej inteligencji i uczenia maszynowego "możliwość decydowania" oznacza: (a) kontrolę operacyjną nad konfiguracją i wdrażaniem modelu (b) kontrolę nad przetwarzaniem danych i dostępem do nich (c) możliwość ustawiania parametrów bezpieczeństwa i operacyjnych (d) uprawnienie do definiowania przypadków użycia i aplikacji bez wymogu fizycznej możliwości wymiany bazowych komponentów infrastruktury.

PRZYKŁADY TEGO, JAK OBECNE BEZPIECZNE REGULACJE MOGĄ WPŁYNĄĆ NA MOŻLIWOŚCI

Przykłady te opierają się na publicznie dostępnych danych.

Ukraiński system zarządzania polem walki DELTA[1]:

- Przetwarza dane wywiadowcze z wielu źródeł,
- Działa na zwykłych komputerach, laptopach, tabletach i telefonach z bezpiecznym zapleczem w chmurze,
- Zarządza tysiącami operacji dronów na liniach frontu/

Zgodnie z ograniczeniami SAFE:

- Zmniejszona wydajność przetwarzania ograniczająca identyfikację celu,
- Zmniejszona odporność systemu z powodu ograniczeń infrastruktury,
- Ograniczone możliwości zarządzania operacjami dronów,
- Zwiększona podatność na zagrożenia z powodu ograniczonych opcji redundancji.

Ukraina – odporność administracji publicznej[2]

- Ponad 15 petabajtów ukraińskich danych rządowych jest obecnie przechowywanych w chmurze hiperskalowej,
- Wykorzystanie hiperskalowości zwiększa poziom cyberochrony, odporności i funkcjonalności operacyjnej krytycznych usług rządowych.

Zgodnie z ograniczeniami SAFE:

- Ochrona danych rządowych w hiperskali byłaby niemożliwa ze względu na zakres partnerstwa,
- Aplikacje i użytkowanie byłyby bardziej podatne na cyberataki,
- Obywatele mieliby trudności z dostępem do usług rządowych lub nie mieliby do nich pełnego dostępu.

---

[1] Innowacje na polu bitwy: Ukraiński system DELTA toruje drogę do sojuszniczej interoperacyjności podczas CWIX24, lipiec 2024 r. https://www.act.nato.int/article/delta-system-cwix/.

[2] Noah Sylvia, "European Digital Defence Priorities in an Uncertain World", Royal United Services Institute (RUSI).

Francuski program ARTEMIS.IA[3]:

- Duży program technologii cyfrowej do przetwarzania danych i sztucznej inteligencji,
- Początkowo starano się unikać amerykańskiej technologii komercyjnej,
- Ostatecznie potrzebne było przyjęcie podejścia hybrydowego obejmującego komercyjne możliwości chmury, aby osiągnąć wymaganą skalę.

Zgodnie z ograniczeniami SAFE:

- Ograniczony dostęp do zaawansowanych możliwości AI/ML,
- Niższa wydajność w analizie danych,
- Opóźnione wdrożenie krytycznych zdolności,
- Zwiększone koszty rozwoju niestandardowego.

Technologia Drone Swarm firmy Saab, opracowana we współpracy ze szwedzkimi siłami zbrojnymi[4]:

- Pozwala jednemu operatorowi kontrolować do 100 systemów bezzałogowych statków powietrznych (UAS) jednocześnie,
- Możliwość dostosowania do różnych misji: rozpoznania, obrony i dostarczania ładunków,
- Skutecznie działa w złożonych środowiskach,
- Każdy dron w roju może mieć różne możliwości (czujniki, ładunki, technologie komunikacyjne).

Zgodnie z ograniczeniami SAFE:

- Wiele podstawowych algorytmów sztucznej inteligencji i komponentów oprogramowania pochodzi z globalnych prac badawczo-rozwojowych,
- Infrastruktura obliczeniowa często opiera się na dostawcach usług w chmurze spoza UE,
- Kluczowe technologie czujników mogą spoza UE,
- Systemy autonomiczne często wykorzystują technologię komercyjną,
- Brak dostępu do nich zmniejszyłby wpływ i elastyczność misji,
- Naruszona interoperacyjność z dronami/systemami autonomicznymi NATO.

[3] Noah Sylvia, "European Digital Defence Priorities in an Uncertain World", Royal United Services Institute (RUSI).
[4] Szwecja prezentuje nową technologię roju dronów od Saaba, styczeń 2025 r. https://thedefensepost.com/2025/01/14/sweden-drone-swarm-technology/