



2023/2113

11.10.2023

ZALECENIE KOMISJI (UE) 2023/2113

z dnia 3 października 2023 r.

w sprawie obszarów technologii krytycznych dla bezpieczeństwa gospodarczego UE, na potrzeby pogłębionej oceny ryzyka z udziałem państw członkowskich

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 292,

a także mając na uwadze, co następuje:

- (1) Komisja i wysoki przedstawiciel uznali, że wraz z rosnącymi napięciami geopolitycznymi, głębszą integracją gospodarczą i przyspieszeniem rozwoju technologicznego niektóre przepływy i działania gospodarcze mogą zagrażać naszemu bezpieczeństwu gospodarczemu, i przyjęli wspólny komunikat w sprawie europejskiej strategii bezpieczeństwa gospodarczego ⁽¹⁾ w celu określenia kompleksowego strategicznego podejścia do kwestii bezpieczeństwa gospodarczego.
- (2) Europejska strategia bezpieczeństwa gospodarczego opiera się na trzech filarach: promowaniu bazy gospodarczej i konkurencyjności UE; ochronie przed zagrożeniami; oraz nawiązywaniu partnerstw z możliwie najszerszym gronem krajów w celu rozwiązywania wspólnych problemów i dbania o wspólne interesy.
- (3) W tych ramach oraz w świetle zagrożeń, jakie mogą stwarzać pewne zależności gospodarcze i zmiany techniczne, UE potrzebuje jasnego obrazu zagrożeń dla jej bezpieczeństwa gospodarczego i ich ewolucji w czasie.
- (4) Zagrożenia te należy określać i oceniać wspólnie z państwami członkowskimi UE i przy udziale prywatnych zainteresowanych stron w ramach dynamicznego i ciągłego procesu.
- (5) W europejskiej strategii bezpieczeństwa gospodarczego określono następujące cztery szerokie i niewyczerpujące kategorie zagrożeń, które należy poddać dalszej ocenie: zagrożenia dla odporności łańcuchów dostaw, w tym w zakresie bezpieczeństwa energetycznego; zagrożenia dla bezpieczeństwa fizycznego i cyberbezpieczeństwa infrastruktury krytycznej; zagrożenia dotyczące bezpieczeństwa technologii i wycieku technologii; zagrożenia dotyczące wykorzystywania zależności gospodarczych lub wymuszenia ekonomicznego jako broni.
- (6) We wspólnym komunikacie Komisja zobowiązała się do oceny zagrożeń związanych z bezpieczeństwem i wyciekiem technologii na podstawie wykazu strategicznych technologii o krytycznym znaczeniu dla bezpieczeństwa gospodarczego oraz, w przypadku najbardziej wrażliwych rodzajów zagrożeń, do zaproponowania wykazu technologii krytycznych na potrzeby oceny ryzyka, jaką należy przeprowadzić wspólnie z państwami członkowskimi do końca 2023 r.
- (7) We wspólnym komunikacie określono, do celów dalszej oceny ryzyka, następujące trzy wąsko zdefiniowane i dalekosiężne kryteria wyboru technologii stwarzających najbardziej wrażliwe rodzaje zagrożeń: prorozwojowy i transformacyjny charakter technologii; ryzyko fuzji cywilno-wojskowej; oraz ryzyko niewłaściwego wykorzystania technologii do naruszania praw człowieka.
- (8) Kryterium dotyczące prorozwojowego i transformacyjnego charakteru technologii uwzględnia jej potencjał i znaczenie dla znacznego wzrostu efektywności i sprawności lub radykalnych zmian w odniesieniu do określonych sektorów, zdolności itp.
- (9) Kryterium ryzyka fuzji cywilno-wojskowej dotyczy znaczenia danej technologii zarówno dla sektora cywilnego, jak i wojskowego oraz jej potencjału w zakresie rozwoju obu tych dziedzin, a także ryzyka związanego z wykorzystywaniem niektórych technologii do podważania pokoju i bezpieczeństwa.

⁽¹⁾ JOIN(2023) 20 final.

- (10) Kryterium ryzyka niewłaściwego wykorzystania technologii do naruszania praw człowieka dotyczy jej potencjalnego niewłaściwego wykorzystania z naruszeniem praw człowieka, w tym ograniczaniem podstawowych wolności.
- (11) Po pierwszej analizie wewnętrznej Komisja określiła wykaz 10 obszarów technologii krytycznych dla bezpieczeństwa gospodarczego UE. Ten wykaz obszarów technologii uwzględni prace przeprowadzone zgodnie z planem działania na rzecz synergii między przemysłem cywilnym, obronnym i kosmicznym ⁽²⁾. Jest to dokument o dynamicznym charakterze i w ramach trwającego procesu może podlegać dalszym zmianom odzwierciedlającym rozwój technologiczny.
- (12) Na podstawie trzech wąsko zdefiniowanych i dalekosiężnych kryteriów wyboru technologii do dalszej oceny w niniejszym zaleceniu wskazano cztery spośród wymienionych obszarów technologii, które z dużym prawdopodobieństwem są najbardziej wrażliwe na bezpośrednie ryzyko wystąpienia zagrożeń związanych z bezpieczeństwem technologii i wyciekami technologii, a mianowicie zaawansowane półprzewodniki, sztuczną inteligencję, technologie kwantowe i biotechnologie. Należy nadać najwyższy priorytet wspólnej ocenie ryzyka tych obszarów technologii, którą należy przeprowadzić z państwami członkowskimi do końca roku. Z zastrzeżeniem ustalenia zakresu współpracy z państwami członkowskimi ta wspólna ocena może koncentrować się na podzbiorach technologii w ramach tych czterech obszarów technologii.
- (13) Struktura wykazu odzwierciedla ocenę Komisji dotyczącą tego, które spośród tych obszarów technologii mogą z większym prawdopodobieństwem stwarzać ryzyko wystąpienia zagrożeń związanych z bezpieczeństwem technologii i wyciekami technologii. Może to pomóc w podejmowaniu decyzji na dalszych etapach. Komisja podejmie otwarty dialog z państwami członkowskimi na temat odpowiedniego harmonogramu i zakresu dalszych ocen ryzyka, uwzględniając między innymi wpływ czasu na ewolucję zagrożeń. Komisja z zadowoleniem przyjąłaby możliwość szybkiej wymiany poglądów w Radzie na temat tego aspektu strategii bezpieczeństwa gospodarczego, w kontekście ogólnych dyskusji politycznych i wytycznych w odpowiedzi na wspólny komunikat. Komisja może przedstawić w tym zakresie dalsze inicjatywy do wiosny 2024 r., w świetle takiego dialogu i pierwszych doświadczeń związanych ze wstępnymi wspólnymi ocenami, a także dalszych informacji, które mogą się pojawić w odniesieniu do wymienionych obszarów technologii. Podejmując decyzję w sprawie wniosków dotyczących przeprowadzania dalszych wspólnych ocen ryzyka z państwami członkowskimi w odniesieniu do co najmniej jednego z wymienionych dodatkowych obszarów technologii lub ich podzbiorów, Komisja weźmie pod uwagę bieżące lub planowane działania w zakresie promowania lub partnerstwa w odniesieniu do danego obszaru technologii. Ogólnie rzecz biorąc, Komisja weźmie pod uwagę, że środki wprowadzone w celu zwiększenia konkurencyjności UE w odpowiednich obszarach mogą przyczynić się do zmniejszenia niektórych zagrożeń technologicznych.
- (14) Celem oceny ryzyka powinna być identyfikacja i analiza podatności na zagrożenia o charakterze systemowym w zależności od ich potencjalnego wpływu na bezpieczeństwo gospodarcze UE oraz stopnia prawdopodobieństwa urzeczywistnienia się tego negatywnego wpływu. Aby ustrukturyzować przyszłą ocenę ryzyka z udziałem państw członkowskich, Komisja określiła pewne zasady przewodnie.
- (15) Niniejsze zalecenie nie przesądza o wyniku oceny ryzyka. Jedyne wyniki szczegółowej wspólnej oceny poziomu i charakteru przedstawionych zagrożeń może być podstawą dalszej dyskusji na temat potrzeby wprowadzenia precyzyjnych i proporcjonalnych środków w zakresie promowania, ochrony lub partnerstwa w odniesieniu do któregoś z tych obszarów technologii lub ich podzbioru. Państwa członkowskie i Komisja mogą wykorzystać te informacje przy opracowywaniu przyszłych działań politycznych, w tym środków w zakresie promocji, partnerstwa lub ochrony na poziomie krajowym, unijnym lub międzynarodowym, które powinny być proporcjonalne do poziomu ryzyka i precyzyjne pod względem zakresu. Na tym etapie wstępnej oceny nie można zatem wyciągnąć żadnych wniosków co do wykorzystania jakichkolwiek konkretnych instrumentów, którymi dysponują UE lub państwa członkowskie, w celu promowania, ochrony lub partnerstwa z innymi podmiotami, aby zwiększyć bezpieczeństwo gospodarcze.
- (16) Wszelkie środki, które mogą zostać wprowadzone, będą proporcjonalne i precyzyjnie ukierunkowane na oszacowane ryzyko związane z każdym obszarem technologii krytycznych lub odpowiednią technologią. Wszelkie wdrożone środki będą miały na celu wzmocnienie siły Unii w tych obszarach i będą zaprojektowane tak, aby zminimalizować wszelkie negatywne skutki uboczne dla rynku i gospodarki. W szczególności oceny przyczynią się do rozwoju polityki Unii wspierającej innowacje i rozwój przemysłowy w zakresie określonych technologii, w tym poprzez inicjatywy międzynarodowe,

⁽²⁾ COM(2021) 70 final.

PRZYMUJE NINIEJSZE ZALECENIE:

1. Zaleca się, aby spośród 10 obszarów technologii krytycznych określonych w załączniku w pierwszej kolejności państwa członkowskie wraz z Komisją oceniły do końca 2023 r. następujące cztery obszary technologii o największym prawdopodobieństwie wystąpienia najbardziej wrażliwych i bezpośrednich zagrożeń związanych z bezpieczeństwem technologii i wyciekami technologii:
 - a) Technologie w zakresie zaawansowanych półprzewodników

Półprzewodniki, mikroelektronika i fotonika są zasadniczymi elementami urządzeń elektronicznych w krytycznych obszarach, takich jak systemy i zastosowania w dziedzinie łączności, informatyki, energii, zdrowia, transportu oraz obrony i kosmosu. Ze względu na ogromny prorozwojowy i transformacyjny charakter tych technologii oraz ich wykorzystywanie do celów cywilnych i wojskowych utrzymanie pozycji lidera w budowaniu i dalszym rozwoju tych technologii ma kluczowe znaczenie dla bezpieczeństwa gospodarczego.
 - b) Technologie sztucznej inteligencji

Sztuczna inteligencja (oprogramowanie), obliczenia wielkiej skali, przetwarzanie danych w chmurze i na obrzeżach sieci oraz analiza danych mają szeroki zakres podwójnego zastosowania i mają zasadnicze znaczenie w szczególności dla przetwarzania dużych ilości danych i podejmowania decyzji lub formułowania prognoz w oparciu o analizę opartą na tych danych. Technologie te mają ogromny potencjał transformacyjny w tym zakresie.
 - c) Technologie kwantowe

Technologie kwantowe mają ogromny potencjał przekształcania wielu sektorów, zarówno cywilnych, jak i wojskowych poprzez umożliwienie stosowania nowych technologii i systemów wykorzystujących właściwości mechaniki kwantowej. Nie można jeszcze w pełni określić pełnego wpływu technologii kwantowych, które są lub będą rozwijane.
 - d) Biotechnologie

Biotechnologie mają istotny charakter prorozwojowy i transformacyjny w takich dziedzinach jak rolnictwo, środowisko, opieka zdrowotna, nauki biologiczne, łańcuchy żywnościowe lub bioprodukcja. Niektóre biotechnologie, takie jak inżynieria genetyczna stosowana w odniesieniu do patogenów lub szkodliwych związków wytwarzanych w wyniku modyfikacji genetycznej mikroorganizmów, mogą mieć wymiar bezpieczeństwa/wojskowy, w szczególności gdy są niewłaściwie wykorzystywane.
2. Komisja zachęca państwa członkowskie do zaangażowania się w otwarty dialog na temat odpowiedniego harmonogramu i zakresu wspólnej oceny ryzyka w innych obszarach technologii wymienionych w załączniku lub ich podzbiorach, z uwzględnieniem szybko zmieniającego się otoczenia geopolitycznego i różnego stopnia prawdopodobieństwa, że wymienione technologie stwarzają najbardziej wrażliwe i bezpośrednie ryzyko wystąpienia zagrożeń związanych z bezpieczeństwem technologii i wyciekami technologii.
3. Aby zorganizować wspólną ocenę ryzyka, określono następujące zasady przewodnie:
 - a) Identyfikacja i analiza podatności na zagrożenia w zależności od ich potencjalnego wpływu na bezpieczeństwo gospodarcze UE oraz stopnia prawdopodobieństwa urzeczywistnienia się tego negatywnego wpływu. W analizie należy określić główne rodzaje zagrożeń i podmiotów stwarzających zagrożenia oraz, w stosownych przypadkach, uwzględnić czynniki geopolityczne w celu oceny prawdopodobieństwa wystąpienia negatywnych skutków. Analiza powinna również uwzględniać między innymi łańcuch wartości technologii, ewolucję zagrożeń, a także odpowiednie zmiany technologiczne, w tym wszelkie wąskie gardła i oczekiwane przyszłe wąskie gardła, analizę względnej pozycji UE w każdej technologii, obejmującą kluczowe podmioty i elementy wiodącej pozycji UE; globalne wzajemne powiązania ekosystemu technologii, w tym w zakresie badań naukowych i łańcucha dostaw technologii.
 - b) Na etapie ustalania zakresu wspólnej oceny należy wziąć pod uwagę, czy szczegółowa ocena skoncentruje się na określonych, najistotniejszych podzbiorach technologii.
 - c) Ocena ryzyka nie będzie dotyczyć poszczególnych państw.

- d) Priorytetowe traktowanie zagrożeń mających potencjalny wpływ na całą UE.
 - e) Zapewnienie synergii i komplementarności z istniejącymi analizami na poziomie UE i państw członkowskich w celu ich uwzględnienia w procesie oceny ryzyka.
 - f) Uwzględnienie informacji otrzymanych od sektora prywatnego.
- 4. Wspólna ocena ryzyka zapewni poufność, na odpowiedni wniosek, informacji otrzymanych od państw członkowskich lub sektora prywatnego. Ostateczny dokument końcowy dotyczący wspólnej oceny ryzyka zostanie odpowiednio utajniony.
 - 5. Ocenę powinny przeprowadzić państwa członkowskie i Komisja z wykorzystaniem istniejących lub, w razie potrzeby, nowych forów, w celu włączenia odpowiednich ekspertów, zgodnie z wymaganiami dla każdej z technologii krytycznych.
 - 6. Komisja będzie nadal monitorować rozwój technologiczny i, w razie potrzeby, uzupełniać niniejsze zalecenie, proponując dodatkowe technologie wymagające pogłębionej oceny.

Sporządzono w Strasburgu dnia 3 października 2023 r.

W imieniu Komisji
Thierry BRETON
Członek Komisji

ZAŁĄCZNIK

Wykaz 10 obszarów technologii krytycznych dla bezpieczeństwa gospodarczego UE

Obszar technologii		Technologie*
		* Wykaz technologii dla każdego obszaru stanowi prawdopodobny centralny punkt oceny ryzyka, ale nie jest wyczerpujący
1.	TECHNOLOGIE W ZAKRESIE ZAAWANSOWANYCH PÓŁPRZEWODNIKÓW	— Mikroelektronika, w tym procesory — Technologie fotoniczne (w tym lasery wysokoenergetyczne) — Czipy wysokiej częstotliwości — Sprzęt do produkcji półprzewodników o bardzo zaawansowanych rozmiarach węzłów
2.	TECHNOLOGIE SZTUCZNEJ INTELIGENCJI	— Obliczenia wielkiej skali — Przetwarzanie danych w chmurze i na obrzeżach sieci — Technologie analizy danych — Komputerowe rozpoznawanie obrazów, przetwarzanie języka, rozpoznawanie obiektów
3.	TECHNOLOGIE KWANTOWE	— Obliczenia kwantowe — Kryptografia kwantowa — Komunikacja kwantowa — Wykrywanie i radary kwantowe
4.	BIOTECHNOLOGIE	— Techniki modyfikacji genetycznej — Nowe techniki genomowe — Nadpisywanie genów — Biologia syntetyczna
5.	ZAAWANSOWANA ŁĄCZNOŚĆ I NAWIGACJA ORAZ ZAAWANSOWANE TECHNOLOGIE CYFROWE	— Bezpieczna komunikacja cyfrowa i łączność cyfrowa, np. RAN i Open RAN (sieć dostępu radiowego) oraz 6G — Technologie bezpieczeństwa cybernetycznego, w tym systemy cybernetycznej, bezpieczeństwa oraz wykrywania włamań i zapobiegania włamaniom, kryminalistyka cyfrowa — Internet rzeczy i rzeczywistość wirtualna — Technologie rozproszonego rejestru i tożsamości cyfrowej — Technologie naprowadzania, nawigacji i kontroli, w tym elektronika lotnicza i pozycjonowanie na morzu
6.	ZAAWANSOWANE TECHNOLOGIE DETEKCJI	— Detekcja elektrooptyczna, radarowa, chemiczna, biologiczna, radiologiczna i rozproszona — Magnetometry, mierniki gradientu magnetycznego — Podwodne czujniki pola elektrycznego — Grawimetry i mierniki gradientu
7.	TECHNOLOGIE KOSMICZNE I NAPĘDOWE	— Specjalne technologie ukierunkowane na przestrzeń kosmiczną, od poziomu komponentów po systemy — Technologie obserwacji przestrzeni kosmicznej i obiektów kosmicznych oraz obserwacji Ziemi — Kosmiczne pozycjonowanie, nawigacja i synchronizacja czasu (PNT) — Bezpieczna komunikacja, w tym łączność na niskiej orbicie okołoziemskiej (LEO) — Technologie napędowe, w tym napęd hipersoniczny i komponenty do celów wojskowych

		Technologie*
Obszar technologii		* Wykaz technologii dla każdego obszaru stanowi prawdopodobny centralny punkt oceny ryzyka, ale nie jest wyczerpujący
8.	TECHNOLOGIE ENERGETYCZNE	— Technologie syntezy jądrowej, reaktory i wytwarzanie energii, technologie konwersji radiologicznej/wzbogacenia i recyklingu radiologicznego — Wodór i nowe paliwa — Technologie neutralne emisyjnie, w tym fotowoltaika — Inteligentne sieci i magazynowanie energii, baterie
9.	ROBOTYKA I SYSTEMY AUTONOMICZNE	— Drony i pojazdy (powietrzne, lądowe, nawodne i podwodne) — Roboty i systemy precyzyjne sterowane robotami — Egzoszkielety — Systemy wspomagane sztuczną inteligencją
10.	ZAAWANSOWANE MATERIAŁY, TECHNOLOGIE PRODUKCJI I RECYKLINGU	— Technologie wytwarzania nanomateriałów, materiałów inteligentnych, zaawansowanych materiałów ceramicznych, materiałów niewykrywalnych, materiałów bezpiecznych i zrównoważonych już na etapie projektowania — Obróbka przyrostowa, także w terenie — Produkcja mikroprecyzyjna sterowana cyfrowo i obróbka laserowa/spawanie laserowe na małą skalę — Technologie wydobywania, przetwarzania i recyklingu surowców krytycznych (w tym ekstrakcja hydrometalurgiczna, bioługowanie, filtracja oparta na nanotechnologii, przetwarzanie elektrochemiczne i czarna masa)