Rada
Unii Europejskiej

Bruksela, 13 września 2018 r.
(OR. en)

12104/18
ADD 5

Międzyinstytucjonalny numer referencyjny:
2018/0328(COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

PISMO PRZEWODNIE

Od:	Sekretarz Generalny Komisji Europejskiej, podpisał dyrektor Jordi AYET PUIGARNAU
Data otrzymania:	12 września 2018 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, Sekretarz Generalny Rady Unii Europejskiej
Nr dok. Kom.:	SWD(2018) 404 final
Dotyczy:	DOKUMENT ROBOCZY SŁUŻB KOMISJI STRESZCZENIE OCENY SKUTKÓW Towarzyszący dokumentowi: WNIOSEK DOTYCZĄCY ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji

Delegacje otrzymują w załączeniu dokument SWD(2018) 404 final.

Zał.: SWD(2018) 404 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 12.9.2018 r.
SWD(2018) 404 final

DOKUMENT ROBOCZY SŁUŻB KOMISJI

STRESZCZENIE OCENY SKUTKÓW

Towarzyszący dokumentowi:

WNIOSEK DOTYCZĄCY ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY

ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 403 final}

Streszczenie oceny skutków

Ocena skutków dotycząca wniosku w sprawie utworzenia sieci centrów kompetencji oraz Europejskiego Centrum Badań Naukowych i Kompetencji w dziedzinie Cyberbezpieczeństwa

A. Zasadność działań

Dlaczego należy podjąć działania? Na czym polega problem?

Obecnie UE nadal nie dysponuje wystarczającymi zdolnościami technologicznymi i przemysłowymi, aby móc samodzielnie zabezpieczyć swoją gospodarkę i infrastrukturę krytyczną oraz aby stać się światowym liderem w dziedzinie cyberbezpieczeństwa. Przedmiotowa inicjatywa ma przyczyniać się do eliminowania określonych poniżej problemów oraz źródeł tej sytuacji:

problem nr 1: niewystarczający poziom strategicznej i trwałej koordynacji oraz współpracy między gałęziami przemysłu, środowiskami naukowymi zajmującymi się kwestią cyberbezpieczeństwa oraz rządami w celu ochrony gospodarki, społeczeństwa i demokracji za pomocą wiodących europejskich rozwiązań w zakresie cyberbezpieczeństwa;

problem nr 2: niewystarczająca skala inwestycji i ograniczony dostęp do know-how, umiejętności i infrastruktury w zakresie cyberbezpieczeństwa w całej Europie;

problem nr 3: niewielka liczba wyników badań naukowych i innowacji w dziedzinie cyberbezpieczeństwa przełożonych na rozwiązania rynkowe i szeroko wdrożonych w całej gospodarce.

U podstaw powyższych problemów leży szereg czynników, do których zaliczają się: niewystarczający poziom zaufania między poszczególnymi podmiotami rynku cyberbezpieczeństwa, nieodłączne ograniczenia istniejących mechanizmów współpracy i łączenia środków, brak ram w zakresie wspólnego udzielania zamówień na kosztowną infrastrukturę związaną z cyberbezpieczeństwem oraz na produkty/rozwiązania w dziedzinie cyberbezpieczeństwa, a także niewykorzystany potencjał rynkowych mechanizmów presji i przyciągania.

Jaki jest cel inicjatywy?

Celem inicjatywy jest zapewnienie zachowania i rozwoju kluczowych (technologicznych i przemysłowych) zdolności UE, aby mogła ona samodzielnie zabezpieczyć swoją gospodarkę cyfrową, społeczeństwo i demokrację oraz aby państwa członkowskie korzystały z najbardziej zaawansowanych rozwiązań w dziedzinie cyberbezpieczeństwa i możliwości w zakresie cyberobrony. Celem inicjatywy jest również zwiększenie światowej konkurencyjności przedsiębiorstw UE prowadzących działalność w zakresie cyberbezpieczeństwa i zapewnienie europejskim gałęziom przemysłu w różnych sektorach dostępu do zdolności i zasobów z myślą o tym, by uczyniły z cyberbezpieczeństwa swoją przewagę konkurencyjną. Należy to osiągnąć poprzez następujące działania: opracowanie skutecznych mechanizmów długoterminowej współpracy strategicznej między wszystkimi odpowiednimi podmiotami (organami publicznymi, gałęziami przemysłu, środowiskiem naukowym zarówno z sektorów cywilnych, jak i obronności), połączenie wiedzy i zasobów w celu zapewnienia wiodących zdolności i infrastruktury, stymulację szerokiego wdrożenia europejskich produktów i rozwiązań w dziedzinie cyberbezpieczeństwa w całej gospodarce i sektorze publicznym, wspieranie przedsiębiorstw typu start-up i MŚP prowadzących działalność w zakresie cyberbezpieczeństwa, a także pomoc w zmniejszeniu braków umiejętności w tym zakresie.

Na czym polega wartość dodana podjęcia działań na poziomie UE?

Inicjatywa mogłaby wnieść wartość dodaną do obecnych wysiłków na szczeblu krajowym poprzez pomoc w utworzeniu wzajemnie powiązanego, ogólnoeuropejskiego ekosystemu cyberbezpieczeństwa w kwestiach przemysłu i badań naukowych. Powinna ona zachęcać do lepszej współpracy między odpowiednimi zainteresowanymi stronami (w tym pomiędzy sektorem cywilnym i sektorem obronności w zakresie cyberbezpieczeństwa), aby jak najlepiej wykorzystać istniejące zasoby i wiedzę fachową rozproszone w całej Europie. Powinna ona również pomóc UE i państwom członkowskim w przyjęciu aktywnej, długoterminowej i strategicznej perspektywy w stosunku do polityki przemysłowej w zakresie cyberbezpieczeństwa, która wykracza poza same działania badawcze i rozwojowe. Takie podejście powinno pomóc nie tylko w znajdowaniu przełomowych rozwiązań w kwestii wyzwań związanych z cyberbezpieczeństwem, które stoją przed sektorem publicznym i sektorem prywatnym, ale również we wspieraniu skutecznego wdrażania tych rozwiązań. Umożliwi to

również odpowiednim środowiskom badawczym i przemysłowym oraz organom publicznym uzyskać dostęp do kluczowych zdolności, takich jak infrastruktura badawcza i doświadczalna, które są często poza zasięgiem pojedynczych państw członkowskich ze względu na niewystarczające zasoby ludzkie i finansowe. Przyczyni się także do zmniejszenia braków umiejętności oraz uniknięcia drenażu mózgów dzięki zapewnieniu dostępu najbardziej uzdolnionym osobom do wielkoskalowych projektów europejskich, dostarczając w związku z tym interesujących wyzwań zawodowych. Wszystkie powyższe działania uważa się również za konieczne do tego, aby Europę uznano na świecie za lidera w dziedzinie cyberbezpieczeństwa.

B. Rozwiązania

Jakie warianty legislacyjne i nielegislacyjne rozważono? Czy wskazano preferowany wariant? Jak uzasadniono ten wybór lub jego brak?

Rozważono szereg wariantów strategicznych, zarówno legislacyjnych, jak i nielegislacyjnych. Na potrzeby pogłębionej oceny zachowano następujące warianty:

1. **scenariusz odniesienia** – wariant współpracy – zakłada kontynuację obecnego podejścia do kwestii budowania przemysłowych i technologicznych zdolności w zakresie cyberbezpieczeństwa w UE poprzez wspieranie badań naukowych i innowacji oraz powiązanych mechanizmów współpracy w ramach programu „Horyzont Europa";
2. **wariant 1:** sieć kompetencji w dziedzinie cyberbezpieczeństwa z Europejskim Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych, z uprawnieniem do stosowania środków na rzecz wsparcia technologii przemysłowych, a także badań naukowych i innowacji;
3. **wariant 2:** sieć kompetencji w dziedzinie cyberbezpieczeństwa z Europejskim Centrum Badań Naukowych i Kompetencji w dziedzinie Cyberbezpieczeństwa, z ograniczeniem do podejmowania wyłącznie działań w zakresie badań naukowych i innowacji.

Warianty odrzucone na wczesnym etapie to: 1) brak działań; 2) sieć składająca się wyłącznie z istniejących centrów kompetencji oraz 3) wykorzystanie istniejących agencji (ENISA, REA lub Agencji Wykonawczej ds. Innowacyjności i Sieci).

W świetle ogólnego zobowiązania podjętego już przez Komisję w odniesieniu do przedmiotowej inicjatywy, a także biorąc pod uwagę istotną rolę, którą mają odegrać państwa członkowskie, główna różnica między dwoma szczegółowo analizowanymi wariantami strategicznymi polega na ich zakresie odzwierciedlonym w ich podstawie prawnej: podmiot utworzony wyłącznie na mocy art. 187 TFUE (wariant 2) ograniczałby inicjatywę do obszaru badań naukowych i innowacji oraz zakładałby zazwyczaj wsparcie finansowe podmiotów prywatnych. Z drugiej strony utworzenie podmiotu w oparciu o podwójną podstawę prawną – art. 187 TFUE i art. 173 TFUE (wariant 1) – oznaczałoby szerszy mandat, obejmujący również m.in. wdrażanie i wsparcie przemysłowe oraz tworzenie silniejszych synergii z cyberobroną. Zastosowanie tego wariantu zapewniałoby również bardziej znaczącą rolę państw członkowskich – zarówno pod względem ich roli w zarządzaniu, jak i ich roli jako potencjalnych nabywców technologii cyberbezpieczeństwa.

Analiza wykazała, że wariant 1 jest najodpowiedniejszy do osiągnięcia celów inicjatywy, jednocześnie zapewniając największy wpływ gospodarczy, społeczny i środowiskowy oraz chroniąc interesy Unii. Główne argumenty przemawiające za tym wariantem obejmowały elastyczność pozwalającą na zastosowanie różnych modeli współpracy ze społecznością i siecią centrów kompetencji, aby zoptymalizować wykorzystanie istniejącej wiedzy i zasobów; zdolność do usystematyzowania współpracy zainteresowanych stron z sektora publicznego i prywatnego, pochodzących ze wszystkich odpowiednich sektorów, w tym z sektora obronności; zdolność stworzenia prawdziwej polityki przemysłowej w zakresie cyberbezpieczeństwa poprzez wspieranie działań związanych nie tylko z badaniami i rozwojem, ale również z wprowadzeniem na rynek. Wariant 1 pozwala również na zwiększenie spójności, działając jako mechanizm wdrażający dla związanego z cyberbezpieczeństwem finansowania z programów „Cyfrowa Europa" i „Horyzont Europa" oraz wzmacniając synergie między wymiarem cywilnym i wymiarem obronnym cyberbezpieczeństwa w odniesieniu do Europejskiego Funduszu Obronnego.

Jak kształtuje się poparcie dla poszczególnych wariantów?

Zgodnie z wynikami konsultacji i procesami gromadzenia dowodów istnieje wyraźne zapotrzebowanie, aby

zarówno środowisko przemysłowe, jak i naukowe posiadały mechanizm umożliwiający UE opracowanie spójnej polityki przemysłowej w zakresie cyberbezpieczeństwa, wykraczającej poza działania związane jedynie z badaniami i rozwojem, aby umożliwić Europie osiągnięcie pozycji światowego lidera w dziedzinie cyberbezpieczeństwa. Jednocześnie zainteresowane strony podkreśliły, że kluczem do sukcesu będzie jasno określona rola Centrum we wspieraniu i ułatwianiu wysiłków sieci i odpowiednich społeczności oraz integrujące, oparte na współpracy podejście do sieci, aby uniknąć tworzenia nowych, odizolowanych projektów. Struktura powinna również być elastyczna, aby można ją było łatwo dostosować, biorąc pod uwagę fakt, że cyberbezpieczeństwo jest szybko rozwijającym się środowiskiem. W czasie całego procesu państwa członkowskie podkreślały konieczność integracyjnego podejścia do wszystkich państw członkowskich oraz ich istniejących centrów doskonałości i kompetencji, a także poświęcania szczególnej uwagi kwestii komplementarności działań. Jeśli chodzi w szczególności o Centrum, państwa członkowskie podkreśliły znaczenie jego roli koordynacyjnej we wsparciu sieci. Dlatego też każda inicjatywa Komisji będzie musiała znaleźć właściwą równowagę w strukturach zarządzania i wdrażania oraz odzwierciedlić tę równowagę w strukturach zarządzania i wdrażania w celu zapewnienia skutecznej koordynacji na szczeblu europejskim, przy jednoczesnym uwzględnieniu rozwoju sytuacji na szczeblu krajowym.

C. Skutki wdrożenia preferowanego wariantu

Jakie korzyści przyniesie wdrożenie preferowanego wariantu lub – jeśli go nie wskazano – głównych wariantów?

Preferowany wariant umożliwi organom publicznym i gałęziom przemysłu we wszystkich państwach członkowskich skuteczniejsze zapobieganie zagrożeniom dla cyberbezpieczeństwa i reagowanie na nie poprzez oferowanie bezpieczniejszych produktów i rozwiązań oraz wyposażenie się w nie. Jest to w szczególności istotne w przypadku ochrony dostępu do podstawowych usług (np. usług transportowych, zdrowotnych, bankowych i finansowych). Miałoby to również pozytywny wpływ na konkurencyjność UE i MŚP, ponieważ zakłada stworzenie mechanizmu umożliwiającego budowę zdolności przemysłowych państw członkowskich i Unii w zakresie cyberbezpieczeństwa i skuteczne przełożenie europejskiej doskonałości naukowej na rozwiązania rynkowe, które można wprowadzić w całej gospodarce. Wariant ten umożliwia łączenie zasobów w celu inwestycji w niezbędne zdolności na szczeblu państw członkowskich i rozwoju wspólnych europejskich aktywów, przy jednoczesnym osiągnięciu korzyści skali. Prawdopodobnie doprowadzi to do zwiększenia dostępu MŚP, gałęzi przemysłu i naukowców do takiej infrastruktury, co będzie stymulować innowacje i skróci procesy rozwojowe. Obniży to również koszty ponoszone przez niektóre przedsiębiorstwa po stronie popytu i pomoże im uczynić z cyberbezpieczeństwa przewagę konkurencyjną. Wariant ten pozwala na wykorzystanie możliwości rynkowych podwójnego zastosowania poprzez umożliwienie społecznościom z sektora obronności i sektora cywilnego pracy nad wspólnymi wyzwaniami. Może on również wnieść wartość dodaną do krajowych wysiłków na rzecz zmniejszania braków umiejętności w zakresie cyberbezpieczeństwa. Na szczeblu UE wariant ten umożliwia również poprawę spójności i synergii między różnymi mechanizmami finansowania.

Pośredni pozytywny wpływ na środowisko można osiągnąć przez opracowanie specjalnych rozwiązań w dziedzinie cyberbezpieczeństwa dla sektorów, które mogą mieć ogromny wpływ na środowisko (jak np. elektrownie jądrowe), pomagając im uniknąć potencjalnie niszczycielskich skutków ataków na cyberbezpieczeństwo tego rodzaju infrastruktury.

Jakie są koszty wdrożenia preferowanego wariantu lub – jeśli go nie wskazano – głównych wariantów?

Koszty dotyczące preferowanego wariantu związane są głównie z kosztami funkcjonowania Centrum i krajowych ośrodków koordynacji. Koszty związane z wdrożeniem różnych programów finansowania (program „Cyfrowa Europa” i program „Horyzont Europa”) podlegają odrębnym ocenom skutków.

Jakie będą skutki dla przedsiębiorstw, MŚP i mikroprzedsiębiorstw?

Do grup zainteresowanych stron, które najbardziej odczują zmiany, należeć będą europejskie spółki – zarówno po stronie popytu, jak i po stronie podaży w dziedzinie cyberbezpieczeństwa – w tym MŚP i mikroprzedsiębiorstwa prowadzące działalność w zakresie cyberbezpieczeństwa. Chociaż ustanowienie Centrum Kompetencji oraz sieci nie nakłada na nie obowiązków regulacyjnych, otworzy ono możliwości w zakresie redukcji kosztów opracowywania nowych produktów i pomoże im uzyskać łatwiejszy dostęp do społeczności inwestorów oraz przyciągnie fundusze niezbędne do wdrożenia rozwiązań rynkowych. W przypadku MŚP i mikroprzedsiębiorstw

dostęp do infrastruktury badawczej i doświadczalnej finansowanej ze środków publicznych jest tym ważniejszy, że brakuje im środków na zakup albo na wyjazd poza ich rynek (a często także poza UE) w celu znalezienia niezbędnej infrastruktury. Oczekuje się również, że inicjatywa ta otworzy nowe rynki dla europejskich MŚP i mikroprzedsiębiorstw prowadzących działalność w zakresie cyberbezpieczeństwa. Ponadto wybrany mechanizm zapewni koordynację między badaniami i przemysłem, a zatem ukierunkuje wysiłki badawcze na konkretne potrzeby przemysłu. Zapewnienie zaawansowanej wiedzy eksperckiej i narzędzi w zakresie cyberbezpieczeństwa będzie pośrednio wspierać podmioty gospodarcze w przestrzeganiu przepisów dyrektywy w sprawie bezpieczeństwa sieci i informacji.

Czy przewiduje się znaczące skutki dla budżetów i administracji krajowych?

Inicjatywa umożliwi państwom członkowskim koordynację inwestycji w niezbędną infrastrukturę związaną z cyberbezpieczeństwem na szczeblu krajowym i europejskim. Mechanizm umożliwi łączenie środków na narzędzia i infrastrukturę, które w innym przypadku byłyby bardziej kosztowne lub nieprzystępne cenowo dla pojedynczych państw członkowskich. Takie podejście umożliwiłoby uzyskanie korzyści skali i racjonalizację. Wkład finansowy państw członkowskich na rzecz Centrum Kompetencji i realizacji stosownych działań powinien być proporcjonalny do wkładu unijnego.

Czy wystąpią inne znaczące skutki?

Tak, inicjatywa ma wyraźnie pozytywny wpływ, ponieważ prawdopodobnie znacznie zwiększy zdolność państw członkowskich do samodzielnego zabezpieczania swoich gospodarek, w tym do ochrony sektorów krytycznych, zwiększenia konkurencyjności europejskich przedsiębiorstw z sektora cyberbezpieczeństwa, jak również gałęzi przemysłu z różnych sektorów, które będą w stanie odpowiednio zabezpieczyć swoje istniejące aktywa i zaprojektować bezpieczne, innowacyjne produkty przy jednoczesnym obniżeniu kosztów badań i rozwoju związanych z bezpieczeństwem. Powinno to ostatecznie pozwolić UE stać się liderem w dziedzinie technologii cyfrowych i cyberbezpieczeństwa nowej generacji.

D. Działania następcze

Kiedy nastąpi przegląd przyjętej polityki?

Wyraźna klauzula o monitorowaniu kluczowych wskaźników efektywności, a także klauzula o ocenie i przeglądzie, na podstawie której Komisja Europejska przeprowadzi ocenę śródokresową, aby zmierzyć wpływ instrumentu i jego wartość dodaną, zostaną uwzględnione w instrumencie prawnym. Następnie Komisja Europejska przedstawi sprawozdanie Parlamentowi Europejskiemu i Radzie. W następstwie tej oceny Komisja może zaproponować przegląd oraz rozszerzenie mandatu Centrum Kompetencji i sieci.