Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „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 — 2018/0328 (COD))

(2019/C 159/10)

Sprawozdawca: **Antonio LONGO**

Współsprawozdawca: **Alberto MAZZOLA**

Wniosek o konsultację	Rada Europejska, 5.10.2018 Parlament Europejski, 1.10.2018
Podstawa prawna	Art. 173 ust. 3, art. 188 i 304 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Transport, Energia, Infrastruktura i Społeczeństwo Informacyjne
Data przyjęcia przez sekcję	9.1.2019
Data przyjęcia na sesji plenarnej	23.1.2019
Sesja plenarna nr	540
Wynik głosowania (za/przeciw/wstrzymało się)	143/5/2

1. Wnioski i zalecenia

1.1. Europejski Komitet Ekonomiczno-Społeczny (EKES) z zadowoleniem przyjmuje inicjatywę Komisji i uważa, że ma ona zasadnicze znaczenie dla rozwoju strategii przemysłowej w zakresie cyberbezpieczeństwa oraz dla osiągnięcia solidnej i szerokiej autonomii cyfrowej. Czynniki te są konieczne do wzmocnienia europejskich mechanizmów obronnych w obliczu trwającej wojny cybernetycznej, która może zagrażać systemom politycznym, gospodarczym i społecznym.

1.2. Komitet podkreśla, że jakakolwiek strategia cyberbezpieczeństwa nie może pomijać kwestii powszechnej świadomości i bezpiecznego zachowania wszystkich użytkowników.

1.3. Komitet zgadza się z ogólnymi celami wniosku i ma świadomość, że konkretne aspekty funkcjonowania będą przedmiotem dalszej analizy. Uwzględniając, że wniosek dotyczy rozporządzenia, uważa za konieczne wczesne określenie niektórych szczególnie ważnych kwestii związanych z zarządzaniem, finansowaniem i osiąganiem ustalonych celów. Ważne jest, aby przyszłe sieci i centrum w możliwie dużym stopniu opierały się na zdolnościach cybernetycznych i wiedzy fachowej państw członkowskich i aby w centrum, które ma zostać utworzone, zakresy odpowiedzialności nie były powiązane. Ponadto należy zagwarantować, że obszary działalności przyszłej sieci oraz centrum nie będą się pokrywały z istniejącymi mechanizmami i instytucjami.

1.4. EKES popiera rozszerzenie współpracy na środowisko przemysłowe w oparciu o zdecydowane zobowiązania w dziedzinie nauki i inwestycji, w tym również w przyszłości jego udział w Radzie Zarządzającej. W przypadku trójstronnego wspólnego przedsięwzięcia Komisji Europejskiej, państw członkowskich i przemysłu udział przedsiębiorstw z państw spoza UE powinien ograniczać się do tych przedsiębiorstw, które od dłuższego czasu prowadzą działalność na terytorium UE i w pełni uczestniczą w europejskiej bazie technologicznej i przemysłowej, pod warunkiem że podlegają one odpowiednim mechanizmom kontrolnym oraz przestrzegają zasady wzajemności i wymogów poufności.

1.5. Cyberbezpieczeństwo powinno być wspólną sprawą wszystkich państw członkowskich, w związku z czym wszystkie państwa członkowskie powinny uczestniczyć w Radzie Zarządzającej, której sposób działania pozostaje do określenia. W celu pokrycia wkładu finansowego państw członkowskich można skorzystać z unijnych środków finansowych przyznanych poszczególnym państwom.

1.6. Wniosek powinien lepiej wyjaśnić, w jaki sposób centrum będzie mogło interweniować w koordynację finansowania programu „Cyfrowa Europa"i „Horyzont Europa", a szczególnie według jakich wytycznych przygotowywane i przydzielane będą zamówienia publiczne. Ten aspekt ma zasadnicze znaczenie dla uniknięcia powielania lub nakładania się działań. Ponadto w celu zwiększenia puli środków finansowych zaleca się rozszerzenie synergii z innymi instrumentami finansowymi UE (np. funduszami regionalnymi, funduszami strukturalnymi, instrumentem „Łącząc Europę", EFR, funduszem InvestEU).

1.7. EKES uważa, że konieczne jest określenie zasad współpracy i stosunków między Europejskim Centrum a ośrodkami krajowymi. Ponadto ważne jest, aby UE finansowała ośrodki krajowe, przynajmniej w odniesieniu do kosztów administracyjnych, ułatwiając harmonizację w zakresie administracji i kompetencji, tak aby zmniejszyć przepaść między państwami europejskimi.

1.8. Komitet ponownie podkreśla znaczenie kapitału ludzkiego i wyraża nadzieję, że Centrum Kompetencji może we współpracy z uczelniami wyższymi, ośrodkami badawczymi i ośrodkami szkolnictwa wyższego promować kształcenie i szkolenie najwyższej jakości, również za pomocą specjalnych uniwersyteckich ścieżek dydaktycznych w instytucjach szkolnictwa wyższego. Istotne jest także zapewnienie specjalnego wsparcia przedsiębiorstwom typu start-up oraz MŚP.

1.9. EKES uważa, że należy lepiej sprecyzować zakres kompetencji i wyznaczyć granice działań Centrum i Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), jasno określając metody współpracy między nimi i wzajemnego wsparcia, a także unikając dublowania kompetencji i wysiłków. Ta sama kwestia dotyczy także innych organów zajmujących się cyberbezpieczeństwem, takich jak EDA, Europol i CERT-UE, w związku z czym zaleca się utworzenie szeregu mechanizmów służących usystematyzowanemu dialogowi między różnymi organami.

2. **Obecne ramy cyberbezpieczeństwa**

2.1. Cyberbezpieczeństwo jest jednym z priorytetów UE, gdyż jest to niezbędny element ochrony instytucji, przedsiębiorstw i obywateli, a także konieczne narzędzie służące do utrzymania demokracji. Jednym z najbardziej niepokojących zjawisk jest gwałtowny wzrost liczby złośliwych programów rozprzestrzenianych w sieci za pośrednictwem systemów automatycznych, z 130 tys. w 2007 r. do 8 mln w 2017 r. Ponadto Unia jest importerem netto produktów i rozwiązań w zakresie cyberbezpieczeństwa, co nastręcza problemów związanych z konkurencyjnością gospodarczą, ochroną ludności oraz bezpieczeństwem wojskowym.

2.2. Chociaż UE szczyci się istotnymi umiejętnościami i doświadczeniami w dziedzinie cyberbezpieczeństwa, przemysł w tym sektorze, uczelnie wyższe i ośrodki badawcze wydają się wciąż rozproszone, pozbawione wspólnej strategii rozwoju i zbieżności działań. Jest to spowodowane faktem, że nie wspiera się wystarczająco istotnych sektorów cyberbezpieczeństwa (np. energetycznego, przestrzeni kosmicznej, obrony i transportu), a także nie dąży się do synergii między cyberbezpieczeństwem cywilnym i obronnym.

2.3. By stawić czoła coraz poważniejszym wyzwaniom, w 2013 r. Unia opracowała strategię w zakresie bezpieczeństwa cybernetycznego w celu promowania godnego zaufania, bezpiecznego i otwartego ekosystemu cybernetycznego ([1]). Następnie w 2016 r. przyjęto pierwsze konkretne środki na rzecz bezpieczeństwa sieci i systemów informatycznych ([2]). To podejście doprowadziło do stworzenia partnerstwa publiczno-prywatnego (cPPP) w dziedzinie cyberbezpieczeństwa.

2.4. W 2017 r. w komunikacie pt.: „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE" ([3]) wskazano konieczność zagwarantowania utrzymania i rozwinięcia niezbędnych zdolności technologicznych w dziedzinie bezpieczeństwa informatycznego w celu ochrony jednolitego rynku cyfrowego, a zwłaszcza sieci i systemów informatycznych o krytycznym znaczeniu i zapewnienia podstawowych usług w zakresie cyberbezpieczeństwa.

([1]) JOIN(2013) 1 final.1

([2]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

([3]) JOIN(2017) 450 final.

2.5. Unia powinna być zatem w stanie ochronić swe własne zasoby i procesy cyfrowe i konkurować na światowym rynku cyberbezpieczeństwa, aż do osiągnięcia solidnej i szerokiej autonomii cyfrowej ([4]).

3. Wnioski Komisji

3.1. Centrum Kompetencji (dalej także: „centrum") będzie miało na celu ułatwienie i skoordynowanie prac sieci ośrodków krajowych i będzie punktem odniesienia dla środowiska posiadającego kompetencje w zakresie cyberbezpieczeństwa, pobudzając do realizacji technologicznego planu w dziedzinie cyberbezpieczeństwa i ułatwiając dostęp do uzyskanych kompetencji.

3.2. Centrum powinno zwłaszcza realizować odpowiednie części programu „Cyfrowa Europa"i „Horyzont Europa", przydzielając fundusze i zajmując się zamówieniami publicznymi. Wziąwszy pod uwagę olbrzymie inwestycje w cyberbezpieczeństwo poczynione w innych częściach świata oraz potrzebę koordynacji i dzielenia się zasobami sektora w Europie, proponuje się nadanie Centrum Kompetencji formy partnerstwa europejskiego z podwójną podstawą prawną, tak by ułatwić wspólne inwestycje Unii, państw członkowskich i przemysłu.

3.3. Wniosek przewiduje, że państwa członkowskie muszą wnosić kwotę adekwatną do działalności Centrum Kompetencji i sieci. Pula środków finansowych przewidziana przez UE obejmuje wkład z programu „Cyfrowa Europa"w wysokości ok. 2 mld EUR, wkład z programu „Horyzont Europa"w wysokości pozostającej do określenia oraz łączny wkład państw członkowskich równy co najmniej wkładowi unijnemu.

3.4. Głównym organem decyzyjnym będzie Rada Zarządzająca, w której reprezentację posiadają wszystkie państwa członkowskie, lecz prawa głosu przysługują jedynie tym państwom członkowskim, które wnoszą wkład finansowy. Mechanizm głosowania uwzględnia zasadę „podwójnej większości", zgodnie z którą niezbędne jest uzyskanie poparcia reprezentacji 75 % wkładu finansowego oraz 75 % głosów. Komisja posiadać będzie 50 % głosów. Centrum wspomagać będzie Rada Konsultacyjna ds. Przemysłowych i Naukowych, która gwarantować będzie dialog z przedsiębiorstwami, konsumentami i innymi odpowiednimi zainteresowanymi stronami.

3.5. Ściśle współpracując z siecią krajowych ośrodków koordynacji i środowiskiem posiadającym kompetencje w dziedzinie cyberbezpieczeństwa, centrum będzie głównym organem ds. wdrażania zajmującym się zasobami finansowymi UE przeznaczonymi na cyberbezpieczeństwo na podstawie proponowanych programów „Cyfrowa Europa"oraz „Horyzont Europa".

3.6. Krajowe ośrodki koordynacji będą wybierane przez państwa członkowskie. Będą musiały posiadać umiejętności technologiczne w dziedzinie cyberbezpieczeństwa lub możliwość bezpośredniego z nich skorzystania, zwłaszcza w dziedzinach takich jak kryptografia, usługi w zakresie bezpieczeństwa ICT, automatyczne wykrywanie włamań, bezpieczeństwo systemu, bezpieczeństwo sieci, bezpieczeństwo oprogramowania i aplikacji oraz ludzkie i społeczne aspekty bezpieczeństwa i prywatności. Powinny one mieć również zdolność do skutecznego współdziałania i koordynacji z przemysłem i sektorem publicznym, w tym z organami wyznaczonymi na podstawie dyrektywy 2016/1148.

4. Uwagi ogólne

4.1. EKES z zadowoleniem przyjmuje inicjatywę Komisji i uważa, że ma ona strategiczne znaczenie dla rozwoju cyberbezpieczeństwa zgodnie z ustaleniami z Tallińskiego Szczytu Cyfrowego we wrześniu 2017 r. Przy tej okazji szefowie państw i rządów wezwali Unię, aby stała się „do 2025 r. światowym liderem w dziedzinie cyberbezpieczeństwa w celu zapewnienia zaufania, pewności i ochrony naszym obywatelom, konsumentom i przedsiębiorstwom online oraz umożliwienia istnienia wolnego i podlegającego przepisom prawa internetu".

4.2. EKES przypomina, że trwa prawdziwa wojna cybernetyczna, która może zagrażać systemom politycznym, gospodarczym i społecznym przez atakowanie systemów informatycznych instytucji, krytycznych infrastruktur (sektor energetyczny, transport, banki i instytucje finansowe itd.) i przedsiębiorstw, a także przez wpływanie fałszywymi informacjami na decyzje wyborcze i ogólnie pojęte procesy demokratyczne ([5]). Konieczne jest zatem zdecydowane podniesienie świadomości na ten temat oraz zapewnienie stanowczej i szybkiej reakcji. Z tego powodu należy opracować jasną i odpowiednio wspieraną strategię przemysłową w zakresie cyberbezpieczeństwa, jako warunek wstępny autonomii cyfrowej. EKES uważa, że w programie prac należy priorytetowo traktować dziedziny określone w dyrektywie (UE) 2016/1148, która ma zastosowanie do publicznych i prywatnych przedsiębiorstw świadczących usługi kluczowe, ze względu na ich znaczenie dla społeczeństwa ([6]).

([4]) Dz.U. C 227 z 28.6.2018, s. 86.
([5]) Raport informacyjny „Wykorzystywanie mediów do wpływania na procesy społeczne i polityczne w UE i państwach sąsiednich", Vareikytė, 2014.
([6]) Dz.U. C 227 z 28.6.2018, s. 86.

4.3. Komitet podkreśla, że jakakolwiek strategia cyberbezpieczeństwa nie może pomijać kwestii powszechnej świadomości i bezpiecznego zachowania wszystkich użytkowników. Dlatego też wszelkim inicjatywom technologicznym muszą towarzyszyć odpowiednie kampanie informacyjne i uświadamiające, tak by stworzyć „kulturę bezpieczeństwa cyfrowego" ([7]).

4.4. Komitet zgadza się z ogólnymi celami wniosku i ma świadomość, że konkretne aspekty funkcjonowania będą przedmiotem dalszej analizy. Uwzględniając, że wniosek dotyczy rozporządzenia, uważa za konieczne wczesne określenie niektórych szczególnie ważnych kwestii związanych z zarządzaniem, finansowaniem i osiąganiem ustalonych celów. Ważne jest, aby przyszłe sieci i centrum w możliwie dużym stopniu opierały się na zdolnościach cybernetycznych i wiedzy fachowej państw członkowskich i aby w centrum, które ma zostać utworzone, zakresy odpowiedzialności nie były powiązane. Ponadto należy zagwarantować, że obszary działalności przyszłej sieci oraz centrum nie będą się pokrywały z istniejącymi mechanizmami i instytucjami.

4.5. EKES przypomina, że w swojej opinii TEN/646 w sprawie bezpieczeństwa cybernetycznego ([8]) zaproponował ustanowienie trójstronnego wspólnego przedsięwzięcia między Komisją Europejską, państwami członkowskimi i przedsiębiorstwami, w tym MŚP, podczas gdy obecna struktura, której forma prawna wymaga głębszej analizy, przewiduje jedynie partnerstwo publiczno-publiczne między Komisją Europejską i państwami członkowskimi.

4.6. EKES popiera rozszerzenie współpracy na środowisko przemysłowe w oparciu o zdecydowane zobowiązania w dziedzinie nauki i inwestycji, w tym również w przyszłości jego udział w Radzie Zarządzającej. Nie ma pewności, że powołanie Rady Konsultacyjnej ds. Przemysłowych i Naukowych gwarantować będzie stały dialog z przedsiębiorstwami, konsumentami i innymi odpowiednimi zainteresowanymi stronami. Ponadto w nowej sytuacji nakreślonych przez Komisję, nie jest jasne, jaką rolę Europejska Organizacja na rzecz Bezpieczeństwa Cybernetycznego (ECSO) odegra. Organ ten został ustanowiony w czerwcu 2016 r. na wniosek Komisji jako wkład Komisji, a jej kapitał pod względem sieci i nie należy marnować wiedzy fachowej.

4.6.1. W przypadku trójstronnego wspólnego przedsięwzięcia należy zwrócić uwagę na przedsiębiorstwa z państw trzecich. W szczególności EKES podkreśla, że takie wspólne przedsięwzięcie powinno opierać się na rygorystycznych zasadach mających na celu wykluczenie takich przedsiębiorstw z państw spoza UE, które mogłyby zagrażać bezpieczeństwu i autonomii Unii. Odnośne klauzule określone we wniosku dotyczącym rozporządzenia w sprawie Europejskiego Funduszu Obrony i europejskiego programu rozwoju przemysłu obronnego ([9]) powinny mieć zastosowanie również w tym kontekście.

4.6.2. Jednocześnie EKES uznaje, że niektóre przedsiębiorstwa z państw spoza UE, które od dłuższego czasu prowadzą działalność na terytorium UE i w pełni uczestniczą w europejskiej bazie technologicznej i przemysłowej, mogłyby odgrywać pożyteczną rolę dla projektów unijnych, a zatem powinny one mieć możliwość uczestniczenia we wspólnym przedsięwzięciu pod warunkiem opracowania przez państwa członkowskie odpowiednich mechanizmów kontrolnych dla takich przedsiębiorstw oraz pod warunkiem przestrzegania przez te przedsiębiorstwa zasady wzajemności i wymogów poufności.

4.7. Cyberbezpieczeństwo powinno być wspólną sprawą wszystkich państw członkowskich, w związku z czym wszystkie państwa członkowskie powinny uczestniczyć w Radzie Zarządzającej, której sposób działania pozostaje do określenia. Ważne jest również, aby wszystkie państwa wniosły odpowiedni wkład finansowy w inicjatywę Komisji. W celu pokrycia wkładu finansowego państw członkowskich można skorzystać z unijnych środków finansowych przyznanych poszczególnym państwom.

4.8. EKES zgadza się z faktem, że każde państwo członkowskie posiada swobodę wyznaczenia swojego własnego przedstawiciela w Radzie Zarządzającej Europejskiego Centrum Kompetencji. Komitet zaleca jasne określenie profili kompetencyjnych przedstawicieli krajowych, które powinny obejmować zarówno umiejętności strategiczne i technologiczne, jak i umiejętności menedżerskie, administracyjne i budżetowe.

4.9. Wniosek powinien lepiej wyjaśniać, w jaki sposób centrum będzie mogło interweniować w koordynację finansowania programu „Cyfrowa Europa"i „Horyzont Europa", który obecnie nadal jest na etapie negocjacji, a szczególnie według jakich wytycznych przygotowywane i przydzielane będą ewentualne zamówienia publiczne. Ten aspekt ma zasadnicze znaczenie dla uniknięcia powielania lub nakładania się działań. Ponadto w celu zwiększenia puli środków finansowych zaleca się rozszerzenie synergii z innymi instrumentami finansowymi UE (np. funduszami regionalnymi, funduszami strukturalnymi, instrumentem „Łącząc Europę", EFR, funduszem InvestEU). Komitet ma nadzieję, że sieć ośrodków krajowych zostanie włączona w zarządzanie funduszami i ich koordynację.

([7]) Dz.U. C 227 z 28.6.2018, s. 86.
([8]) Dz.U. C 227 z 28.6.2018, s. 86.
([9]) COM(2017) 294.

4.10. EKES odnotowuje, że Rada Konsultacyjna powinna składać się z szesnastu członków i że nie wyjaśniono mechanizmów, za pomocą których należy dotrzeć do środowiska przedsiębiorców, uczelni wyższych, badań i konsumentów. Uważa, że przydatne i stosowne jest, by członkowie Rady cechowali się dużą wiedzą w tej dziedzinie i stanowili wyważoną reprezentację różnych zainteresowanych sektorów.

4.11. EKES uważa, że należy określić zasady współpracy i stosunków między Europejskim Centrum a ośrodkami krajowymi. Ponadto ważne jest, aby UE finansowała ośrodki krajowe, przynajmniej w odniesieniu do kosztów administracyjnych, ułatwiając harmonizację w zakresie administracji i kompetencji, tak aby zmniejszyć przepaść między państwami europejskimi.

4.12. Zgodnie ze swoimi wcześniejszymi opiniami ([10]) EKES podkreśla znaczenie zapewnienia kształcenia i szkoleń najwyższej jakości dla zasobów ludzkich w sektorze cyberbezpieczeństwa, w tym specjalnych kursów szkolnych, uniwersyteckich i podyplomowych. Należy również zapewnić odpowiednie wsparcie budżetowe MŚP oraz przedsiębiorstwom typu start-up z tego sektora ([11]), które mają zasadnicze znaczenie dla rozwoju badań pionierskich.

4.13. EKES uważa, że należy lepiej sprecyzować zakres kompetencji i wyznaczyć granice działań Centrum i ENISA, jasno określając metody współpracy między nimi i wzajemnego wsparcia, a także unikając dublowania kompetencji i wysiłków ([12]). We wniosku dotyczącym rozporządzenia przewidziano udział delegata ENISA jako stałego obserwatora w Radzie Zarządzającej, lecz nie jest to gwarancja zorganizowanego dialogu obu organów. Ta sama kwestia dotyczy również innych organów zajmujących się cyberbezpieczeństwem, takich jak EDA, Europol i CERT-UE. W tym kontekście interesujący jest protokół ustaleń zawarty w maju 2018 r. między ENISA, EDA, Europolem i CERT-EU.

Bruksela, dnia 23 stycznia 2019 r.

Przewodniczący

Luca JAHIER

Europejskiego Komitetu Ekonomiczno-Społecznego

([10]) Dz.U. C 451 z 16.12.2014, s. 25.
([11]) Dz.U. C 227 z 28.6.2018, s. 86.
([12]) Dz.U. C 227 z 28.6.2018, s. 86.