

Środa, 13 marca 2019 r.

P8\_TA(2019)0189

## Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji \*\*\*I

Poprawki przyjęte przez Parlament Europejski w dniu 13 marca 2019 r. w sprawie wniosku dotyczącego 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)0630 – C8-0404/2018 – 2018/0328(COD)) <sup>(1)</sup>

(Zwykła procedura ustawodawcza: pierwsze czytanie)

(2019/C 23/73)

### Poprawka 1

#### Wniosek dotyczący rozporządzenia

#### Motyw 1

Tekst proponowany przez Komisję

- (1) **Nasze** życie codzienne i gospodarki stają się bardziej zależne od technologii cyfrowych, **dlatego** obywatele w coraz większym stopniu narażeni **są** na poważne cyberincydenty. Przyszłe bezpieczeństwo zależy między innymi od poprawy zdolności technologicznych i przemysłowych **Unii** do ochrony przed zagrożeniami dla cyberbezpieczeństwa, ponieważ zarówno infrastruktura **cywilna**, jak i potencjał **wojskowy** opierają się na bezpiecznych systemach cyfrowych.

Poprawka

- (1) **Ponad 80 % ludności Unii Europejskiej ma dostęp do internetu, a nasze** życie codzienne i gospodarki stają się **coraz** bardziej zależne od technologii cyfrowych, obywatele **są zatem** w coraz większym stopniu narażeni na poważne cyberincydenty. Przyszłe bezpieczeństwo zależy między innymi od **zwiększenia ogólnej odporności, od** poprawy zdolności technologicznych i przemysłowych do ochrony **Unii** przed **ciagle zmieniającymi się** zagrożeniami dla cyberbezpieczeństwa, ponieważ zarówno infrastruktura, jak i potencjał **w zakresie bezpieczeństwa** opierają się na bezpiecznych systemach cyfrowych. **Takie bezpieczeństwo można osiągnąć dzięki zwiększeniu świadomości zagrożeń dla cyberbezpieczeństwa oraz rozwojowi kompetencji, możliwości i zdolności w całej Unii, dogłębnie uwzględniając zależności między infrastrukturą sprzętu i oprogramowania, sieciami, produktami i procesami, a także konsekwencje i obawy społeczne oraz etyczne.**

<sup>(1)</sup> Sprawa została odesłana do komisji właściwej w celu przeprowadzenia negocjacji międzyinstytucjonalnych na podstawie art. 59 ust. 4 akapit czwarty Regulaminu (A8-0084/2019).

Środa, 13 marca 2019 r.

**Poprawka 2**  
**Wniosek dotyczący rozporządzenia**  
**Motyw 1 a (nowy)**

Tekst proponowany przez Komisję

Poprawka

- (1a) *Cyberprzestępczość stanowi szybko rosnące zagrożenie dla Unii, jej obywateli i gospodarki. W 2017 r. 80 % przedsiębiorstw europejskich doświadczyło co najmniej jednego cyberincydentu. W maju 2017 r. atak za pomocą Wannacry objął ponad 150 państw i 230 000 systemów informatycznych i wywarł znaczący wpływ na infrastrukturę krytyczną, taką jak szpitale. Wskazuje to na konieczność wprowadzenia najwyższych norm cyberbezpieczeństwa i kompleksowych rozwiązań w tym zakresie, obejmujących ludzi, produkty, procesy i technologie w Unii, a także na konieczność wiodącej pozycji Unii w tej dziedzinie i autonomii cyfrowej.*

**Poprawka 3**  
**Wniosek dotyczący rozporządzenia**  
**Motyw 4**

Tekst proponowany przez Komisję

Poprawka

- (4) Podczas Tallińskiego Szczytu Cyfrowego we wrześniu 2017 r. 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) Podczas Tallińskiego Szczytu Cyfrowego we wrześniu 2017 r. szefowie państw i rządów wezwali Unię, aby stała się „do 2025 r. światowym liderem w dziedzinie cyberbezpieczeństwa w celu zapewnienia naszym obywatelom, konsumentom i przedsiębiorstwom **zaufania, pewności i ochrony** online oraz umożliwienia istnienia wolnego, **bezpieczniejszego** i podlegającego przepisom prawa internetu”, **a także zadeklarowali „szersze korzystanie z rozwiązań w zakresie otwartego oprogramowania i otwartych standardów przy (prze)budowie systemów i rozwiązań ICT (m.in. aby uniknąć zależności od jednego dostawcy), w tym tych opracowanych lub promowanych w ramach unijnych programów na rzecz interoperacyjności i standaryzacji, np. ISA<sup>2</sup>”.**

Środa, 13 marca 2019 r.

#### Poprawka 4

### Wniosek dotyczący rozporządzenia

#### Motyw 4 a (nowy)

Tekst proponowany przez Komisję

Poprawka

- (4a) Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych („Centrum Kompetencji”) powinno przyczynić się do zwiększenia odporności i niezawodności infrastruktury sieci i systemów informatycznych, w tym internetu i innej infrastruktury krytycznej dla funkcjonowania społeczeństwa, takiej jak systemy transportowe, systemy opieki zdrowotnej i bankowość.

#### Poprawka 5

### Wniosek dotyczący rozporządzenia

#### Motyw 4 b (nowy)

Tekst proponowany przez Komisję

Poprawka

- (4b) Centrum Kompetencji i jego działania powinny uwzględniać wdrażanie rozporządzenia (UE) 2019/XXX [wersja przekształcona rozporządzenia (WE) nr 428/2009 zgodnie z wnioskiem COM(2016)0616] <sup>(1a)</sup>.

- <sup>(1a)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/... z dnia ... ustanawiające unijny system kontroli wywozu, transferu, pośrednictwa, pomocy technicznej i tranzytu w odniesieniu do produktów podwójnego zastosowania (Dz.U. L ... z ..., s. ...).

Środa, 13 marca 2019 r.

## Poprawka 6

## Wniosek dotyczący rozporządzenia

## Motyw 5

Tekst proponowany przez Komisję

- (5) Znaczące zakłócenie funkcjonowania sieci i systemów informatycznych może wpływać na poszczególne państwa członkowskie i na Unię jako całość. **Bezpieczeństwo** sieci i systemów informatycznych ma zatem zasadnicze znaczenie dla **sprawnego funkcjonowania rynku wewnętrznego**. Obecnie Unia jest uzależniona od dostawców cyberbezpieczeństwa spoza Europy. W strategicznym interesie Unii leży jednak zapewnienie, aby utrzymała i rozwijała podstawowe zdolności technologiczne w zakresie cyberbezpieczeństwa w celu ochrony **swojego jednolitego rynku cyfrowego, a w szczególności ochrony sieci i systemów informatycznych o znaczeniu krytycznym, oraz** dostarczania kluczowych usług w zakresie cyberbezpieczeństwa.

Poprawka

- (5) Znaczące zakłócenie funkcjonowania sieci i systemów informatycznych może wpływać na poszczególne państwa członkowskie i na Unię jako całość. **Najwyższy poziom bezpieczeństwa** sieci i systemów informatycznych **w całej Unii** ma zatem zasadnicze znaczenie **zarówno dla społeczeństwa, jak i gospodarki**. Obecnie Unia jest uzależniona od dostawców cyberbezpieczeństwa spoza Europy. W strategicznym interesie Unii leży jednak zapewnienie, aby utrzymała **ona** i rozwijała podstawowe zdolności **i możliwości** technologiczne w zakresie cyberbezpieczeństwa w celu ochrony **danych oraz krytycznych sieci i systemów informatycznych europejskich obywateli i przedsiębiorstw, w tym infrastruktury krytycznej dla funkcjonowania społeczeństwa, takiej jak systemy transportowe, systemy opieki zdrowotnej i bankowość, oraz jednolitego rynku cyfrowego, a także w celu** dostarczania kluczowych usług w zakresie cyberbezpieczeństwa.

## Poprawka 7

## Wniosek dotyczący rozporządzenia

## Motyw 6

Tekst proponowany przez Komisję

- (6) Chociaż w Unii istnieje bardzo wysoki poziom wiedzy fachowej i doświadczenia w zakresie badań naukowych, technologii i rozwoju przemysłu w dziedzinie cyberbezpieczeństwa, to wysiłki środowisk branżowych i naukowych są rozproszone, brakuje zbieżności działań i wspólnej misji, co stanowi przeszkodę dla konkurencyjności w tej dziedzinie. Należy połączyć te wysiłki i wiedzę fachową, utworzyć sieć kontaktów i wykorzystać je w skuteczny sposób, aby wzmocnić i uzupełnić trwające badania naukowe, zdolności technologiczne i przemysłowe na szczeblu unijnym i na szczeblach krajowych.

Poprawka

- (6) Chociaż w Unii istnieje bardzo wysoki poziom wiedzy fachowej i doświadczenia w zakresie badań naukowych, technologii i rozwoju przemysłu w dziedzinie cyberbezpieczeństwa, to wysiłki środowisk branżowych i naukowych są rozproszone, brakuje zbieżności działań i wspólnej misji, co stanowi przeszkodę dla konkurencyjności **i skutecznej ochrony krytycznych danych, sieci i systemów** w tej dziedzinie. Należy połączyć te wysiłki i wiedzę fachową, utworzyć sieć kontaktów i wykorzystać je w skuteczny sposób, aby wzmocnić i uzupełnić trwające badania naukowe, zdolności technologiczne i przemysłowe **oraz umiejętności** na szczeblu unijnym i na szczeblach krajowych. **Choć sektor technologii informacyjno-komunikacyjnych (ICT) stoi w obliczu ważnych wyzwań, takich jak zaspokojenie popytu na wykwalifikowanych pracowników, może skorzystać na tym, że reprezentuje różnorodność całego społeczeństwa oraz charakteryzuje się zrównoważoną reprezentacją płci, różnorodnością etniczną i niedyskryminacją osób z niepełnosprawnościami, jak również na tym, że ułatwia dostęp do wiedzy i szkoleń przyszłym ekspertom w dziedzinie cyberbezpieczeństwa, w tym kształcenia w warunkach pozaformalnych, na przykład w ramach projektów dotyczących wolnego i otwartego oprogramowania, obywatelskich projektów technicznych, przedsiębiorstw typu start-up i mikroprzedsiębiorstw.**

Środa, 13 marca 2019 r.

### Poprawka 8

#### Wniosek dotyczący rozporządzenia

#### Motyw 6 a (nowy)

Tekst proponowany przez Komisję

Poprawka

- (6a) *Małe i średnie przedsiębiorstwa (MŚP) są kluczowymi podmiotami w unijnym sektorze cyberbezpieczeństwa, które ze względu na swoją elastyczność mogą zapewnić najnowocześniejsze rozwiązania. Jednak MSP, które nie są wyspecjalizowane w zakresie cyberbezpieczeństwa, są również bardziej podatne na cyberincydenty ze względu na wysokie inwestycje i zasoby wiedzy wymagane do wprowadzenia skutecznych rozwiązań w dziedzinie cyberbezpieczeństwa. W związku z tym konieczne jest, aby Centrum Kompetencji i sieć kompetencji w dziedzinie cyberbezpieczeństwa (zwana dalej „siecią”) zapewniły MŚP specjalne wsparcie, ułatwiając im dostęp do wiedzy i szkoleń, tak aby umożliwić im wystarczające zabezpieczenie się, a tym, które działają w dziedzinie cyberbezpieczeństwa, umożliwić wkład w rozwój wiodącej pozycji Unii w tej dziedzinie.*

### Poprawka 9

#### Wniosek dotyczący rozporządzenia

#### Motyw 6 b (nowy)

Tekst proponowany przez Komisję

Poprawka

- (6b) *Wiedza fachowa istnieje również poza kontekstem przemysłowym i badawczym. Niekommercyjne i przedkomercyjne projekty, nazywane „obywatelskimi projektami technicznymi”, wykorzystują otwarte standardy, otwarte dane oraz wolne i otwarte oprogramowanie w interesie społeczeństwa i dobra publicznego. Przyczyniają się one do zwiększenia odporności i świadomości oraz rozwoju kompetencji w dziedzinie cyberbezpieczeństwa i odgrywają ważną rolę w budowaniu zdolności przemysłu i badań w tej dziedzinie.*

Środa, 13 marca 2019 r.

**Poprawka 10**  
**Wniosek dotyczący rozporządzenia**  
**Motyw 6 c (nowy)**

Tekst proponowany przez Komisję

Poprawka

- (6c) *W kontekście niniejszego rozporządzenia termin „za-interesowane strony” odnosi się między innymi do przemysłu, podmiotów publicznych i innych podmiotów zajmujących się kwestiami operacyjnymi i technicznymi w dziedzinie cyberbezpieczeństwa, a także do społeczeństwa obywatelskiego, między innymi związków zawodowych, stowarzyszeń konsumentów, społeczności wolnego i otwartego oprogramowania oraz środowiska akademickiego i naukowego.*

**Poprawka 11**  
**Wniosek dotyczący rozporządzenia**  
**Motyw 8**

Tekst proponowany przez Komisję

Poprawka

- (8) Centrum Kompetencji powinno być głównym unijnym instrumentem służącym łączeniu inwestycji w badania naukowe w dziedzinie cyberbezpieczeństwa, technologię i rozwój przemysłowy oraz wdrażaniu odpowiednich projektów i inicjatyw razem z siecią **kompetencji w dziedzinie cyberbezpieczeństwa**. Centrum to powinno zapewnić wsparcie finansowe związane z cyberbezpieczeństwem z programów „Horyzont Europa” i „Cyfrowa Europa” oraz, w stosownych przypadkach, powinno być otwarte na Europejski Fundusz Rozwoju Regionalnego i inne programy. Podejście to powinno przyczynić się do tworzenia synergii i koordynacji wsparcia finansowego związanego z **badaniami naukowymi, innowacjami, rozwojem technologiczno-przemysłowym** w dziedzinie cyberbezpieczeństwa oraz do unikania powielania działań.
- (8) Centrum Kompetencji powinno być głównym unijnym instrumentem służącym łączeniu inwestycji w badania naukowe w dziedzinie cyberbezpieczeństwa, technologię i rozwój przemysłowy oraz wdrażaniu odpowiednich projektów i inicjatyw razem z siecią. Centrum to powinno zapewnić wsparcie finansowe związane z cyberbezpieczeństwem z programów „Horyzont Europa” i „Cyfrowa Europa”, **jak również z Europejskiego Funduszu Obronnego na działania i koszty administracyjne związane z obronnością**, oraz, w stosownych przypadkach, powinno być otwarte na Europejski Fundusz Rozwoju Regionalnego i inne programy. Podejście to powinno przyczynić się do tworzenia synergii i koordynacji wsparcia finansowego związanego z **inicjatywami Unii na rzecz badań naukowych i rozwoju, innowacji i rozwoju technologiczno-przemysłowego** w dziedzinie cyberbezpieczeństwa oraz do unikania powielania działań.

Środa, 13 marca 2019 r.

**Poprawka 12**  
**Wniosek dotyczący rozporządzenia**  
**Motyw 8 a (nowy)**

Tekst proponowany przez Komisję

Poprawka

- (8a) *„Uwzględnianie bezpieczeństwa na etapie projektowania” jako zasada ustanowiona we wspólnym komunikacie Komisji z 13 września 2017 r. pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej” obejmuje najnowocześniejsze metody zwiększania bezpieczeństwa na wszystkich etapach cyklu życia produktu lub usługi, począwszy od bezpiecznych metod projektowania i rozwoju, zmniejszania płaszczyzny ataku oraz wprowadzania odpowiednich testów i kontroli bezpieczeństwa. W okresie eksploatacji i konserwacji producenci lub dostawcy muszą bezzwłocznie udostępniać aktualizacje eliminujące nowe luki lub zagrożenia przez szacowany okres eksploatacji produktu i w dłuższej perspektywie czasowej. Można to osiągnąć także przez umożliwianie osobom trzecim tworzenia i dostarczania takich aktualizacji. Zapewnianie aktualizacji jest szczególnie konieczne w przypadku wspólnie używanych infrastruktury, produktów i procesów.*

**Poprawka 13**  
**Wniosek dotyczący rozporządzenia**  
**Motyw 8 b (nowy)**

Tekst proponowany przez Komisję

Poprawka

- (8b) *Z uwagi na zakres wyzwania związanego z cyberbezpieczeństwem oraz inwestycje w zdolności i możliwości w zakresie cyberbezpieczeństwa w innych częściach świata Unia i jej państwa członkowskie powinny zwiększyć wsparcie finansowe na badania, rozwój i działania wdrożeniowe w tej dziedzinie. Aby osiągnąć korzyści skali i porównywalny poziom ochrony w całej Unii, państwa członkowskie powinny skoncentrować wysiłki w ramach europejskich, dokonując, w stosownych przypadkach, inwestycji za pośrednictwem mechanizmu Centrum Kompetencji.*

Środa, 13 marca 2019 r.

**Poprawka 14**  
**Wniosek dotyczący rozporządzenia**  
**Motyw 8 c (nowy)**

---

Tekst proponowany przez Komisję

---

Poprawka

- (8c) *W celu wspierania konkurencyjności unijnej i najwyższych norm cyberbezpieczeństwa na arenie międzynarodowej Centrum Kompetencji i środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa powinny dążyć do wymiany ze społecznością międzynarodową produktów, standardów i norm technicznych w dziedzinie cyberbezpieczeństwa. Normy techniczne obejmują tworzenie wzorcowych implementacji publikowanych jako otwarte licencje. Bezpieczny projekt, szczególnie w przypadku wzorcowych implementacji, ma kluczowe znaczenie dla ogólnej niezawodności i odporności powszechnie używanej infrastruktury sieciowej i infrastruktury systemów informatycznych, na przykład internetu i infrastruktury krytycznej.*

**Poprawka 15**  
**Wniosek dotyczący rozporządzenia**  
**Motyw 9**

---

Tekst proponowany przez Komisję

---

Poprawka

- (9) Biorąc pod uwagę, że cele tej inicjatywy zostaną osiągnięte w najlepszy sposób, jeżeli **uczestniczyć w niej będą** wszystkie państwa członkowskie lub jak najwięcej państw członkowskich, i aby zachęcić państwa członkowskie do uczestnictwa, wyłącznie państwa członkowskie, które wniosą wkład finansowy w koszty administracyjne i operacyjne Centrum Kompetencji, powinny dysponować prawem głosu.
- (9) Biorąc pod uwagę, że cele tej inicjatywy zostaną osiągnięte w najlepszy sposób, jeżeli **wkład w nią wniosą** wszystkie państwa członkowskie lub jak najwięcej państw członkowskich, i aby zachęcić państwa członkowskie do uczestnictwa, wyłącznie państwa członkowskie, które wniosą wkład finansowy w koszty administracyjne i operacyjne Centrum Kompetencji, powinny dysponować prawem głosu.



Środa, 13 marca 2019 r.

**Poprawka 16**  
**Wniosek dotyczący rozporządzenia**  
**Motyw 12**

Tekst proponowany przez Komisję

(12) Krajowe ośrodki koordynacji powinny zostać wybrane przez państwa członkowskie. Poza niezbędnym potencjałem administracyjnym ośrodki powinny posiadać wiedzę techniczną w dziedzinie cyberbezpieczeństwa, zwłaszcza w obszarach takich jak kryptografia, usługi w zakresie bezpieczeństwa ICT, wykrywanie włamań, bezpieczeństwo systemu, bezpieczeństwo sieci, bezpieczeństwo oprogramowania i aplikacji lub ludzkie i społeczne aspekty bezpieczeństwa i prywatności, albo mieć do takiej wiedzy bezpośredni dostęp. Powinny one mieć również zdolność do skutecznego angażowania i koordynowania wysiłków przemysłu, sektora publicznego, w tym organów wyznaczonych na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148<sup>(23)</sup>, oraz środowiska naukowego.

<sup>(23)</sup> 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).

Poprawka

(12) Krajowe ośrodki koordynacji powinny zostać wybrane przez państwa członkowskie. Poza niezbędnym potencjałem administracyjnym ośrodki powinny posiadać wiedzę techniczną w dziedzinie cyberbezpieczeństwa, zwłaszcza w obszarach takich jak kryptografia, usługi w zakresie bezpieczeństwa ICT, wykrywanie włamań, bezpieczeństwo systemu, bezpieczeństwo sieci, bezpieczeństwo oprogramowania i aplikacji lub ludzkie, **etyczne, społeczne i środowiskowe** aspekty bezpieczeństwa i prywatności, albo mieć do takiej wiedzy bezpośredni dostęp. Powinny one mieć również zdolność do skutecznego angażowania i koordynowania wysiłków przemysłu, sektora publicznego, w tym organów wyznaczonych na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148<sup>(23)</sup>, oraz środowiska naukowego, **aby nawiązać stały dialog publiczno-prywatny na temat cyberbezpieczeństwa. Należy ponadto podnosić świadomość ogółu społeczeństwa w zakresie cyberbezpieczeństwa za pomocą odpowiednich środków komunikacji.**

<sup>(23)</sup> 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).

Środa, 13 marca 2019 r.

## Poprawka 17

## Wniosek dotyczący rozporządzenia

## Motyw 14

Tekst proponowany przez Komisję

- (14) Powstające technologie, np. sztuczna inteligencja, internet rzeczy, obliczenia wielkiej skali (HPC) i informatyka kwantowa, **łańcuch bloków oraz** koncepcje takie jak bezpieczna tożsamość cyfrowa, **jednocześnie** tworzą nowe wyzwania dla cyberbezpieczeństwa i zapewniają **rozwiązania**. Ocena i zatwierdzenie odporności istniejących lub przyszłych systemów ICT będzie wymagać testowania **rozwiązań** w zakresie bezpieczeństwa pod kątem ataków na urządzenia HPC i urządzenia kwantowe. Centrum Kompetencji, sieć i środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa powinny pomagać w rozwijaniu i rozpowszechnianiu najnowszych **rozwiązań** w zakresie cyberbezpieczeństwa. Jednocześnie Centrum Kompetencji i **sieć** powinny służyć twórcom rozwiązań i operatorom w sektorach krytycznych takich jak sektor transportowy, energetyczny, zdrowia, finansowy, administracji, telekomunikacyjny, wytwórczy, obrony i przestrzeni kosmicznej, aby pomóc im w stawianiu czoła wyzwaniom związanym z cyberbezpieczeństwem.

Poprawka

- (14) Powstające technologie, np. sztuczna inteligencja, internet rzeczy, obliczenia wielkiej skali (HPC) i informatyka kwantowa, **a także** koncepcje takie jak bezpieczna tożsamość cyfrowa, tworzą nowe wyzwania dla cyberbezpieczeństwa i **jednocześnie** zapewniają **produkty i procesy**. Ocena i zatwierdzenie odporności istniejących lub przyszłych systemów ICT będzie wymagać testowania **produktów i procesów** w zakresie bezpieczeństwa pod kątem ataków na urządzenia HPC i urządzenia kwantowe. Centrum Kompetencji, sieć, **europejskie centra innowacji cyfrowych** i środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa powinny pomagać w rozwijaniu i rozpowszechnianiu najnowszych **produktów i procesów, w tym podwójnego zastosowania**, w zakresie cyberbezpieczeństwa, **w szczególności tych, które pomagają organizacjom stale budować zdolności, odporność i należyte zarządzanie. Centrum Kompetencji i sieć powinny stymulować cały cykl innowacji i przyczynić się do eliminowania „doliny śmierci” w obszarze innowacji z zakresu technologii i usług w dziedzinie cyberbezpieczeństwa.** Jednocześnie Centrum Kompetencji, **sieć i środowisko** powinny służyć twórcom rozwiązań i operatorom w sektorach krytycznych takich jak sektor transportowy, energetyczny, zdrowia, finansowy, administracji, telekomunikacyjny, wytwórczy, obrony i przestrzeni kosmicznej, aby pomóc im w stawianiu czoła wyzwaniom związanym z cyberbezpieczeństwem, **a także** powinny badać różne motywy ataków na integralność sieci i systemów informatycznych, takie jak przestępczość, szpiegostwo przemysłowe, zniestawienie i dezinformacja.

## Poprawka 18

## Wniosek dotyczący rozporządzenia

## Motyw 14 a (nowy)

Tekst proponowany przez Komisję

Poprawka

- (14a) Ze względu na szybko zmieniający się charakter cyberzagrożeń i cyberbezpieczeństwa Unia musi być w stanie szybko i w sposób ciągły dostosowywać się do nowych zjawisk w tej dziedzinie. W związku z tym Centrum Kompetencji, sieć i środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa powinny być wystarczająco elastyczne, aby zapewnić wymaganą zdolność reagowania. Powinny one ułatwiać rozwiązania, które pomagają podmiotom utrzymywać stałą możliwość budowy zdolności do zwiększania własnej odporności i odporności Unii.

Środa, 13 marca 2019 r.

**Poprawka 19**  
**Wniosek dotyczący rozporządzenia**  
**Motyw 14 b (nowy)**

Tekst proponowany przez Komisję

Poprawka

- (14b) *Centrum Kompetencji powinno dążyć do wypracowania wiodącej pozycji Unii i wiedzy fachowej w dziedzinie cyberbezpieczeństwa, by w ten sposób zagwarantować najwyższe normy bezpieczeństwa w Unii, zapewnić ochronę danych, systemów informatycznych, sieci i infrastruktury krytycznej w Unii, tworzyć nowe wysokiej jakości miejsca pracy w tym obszarze, zapobiegać ściąganiu europejskich ekspertów ds. cyberbezpieczeństwa do państw trzecich (drenaż mózgow) oraz wносить europejską wartość dodaną do już istniejących krajowych środków w zakresie cyberbezpieczeństwa.*

**Poprawka 20**  
**Wniosek dotyczący rozporządzenia**  
**Motyw 15**

Tekst proponowany przez Komisję

Poprawka

- (15) Centrum Kompetencji powinno pełnić szereg kluczowych funkcji. Po pierwsze, Centrum Kompetencji powinno ułatwiać i wspierać koordynację pracy **europejskiej sieci kompetencji w dziedzinie cyberbezpieczeństwa** oraz wspierać rozwój środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa. Centrum powinno realizować technologiczny plan w dziedzinie cyberbezpieczeństwa i ułatwiać dostęp do wiedzy fachowej zebranej w ramach sieci i środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa. Po drugie, Centrum powinno wdrażać odpowiednie części programów „Cyfrowa Europa” i „Horyzont Europa” poprzez przydzielanie dotacji, zwykle na podstawie konkurencyjnych zaproszeń do składania wniosków. Po trzecie, Centrum Kompetencji powinno ułatwiać wspólne inwestycje Unii, państw członkowskich lub przemysłu.
- (15) Centrum Kompetencji powinno pełnić szereg kluczowych funkcji. Po pierwsze, Centrum Kompetencji powinno ułatwiać i wspierać koordynację pracy sieci oraz wspierać rozwój środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa. Centrum powinno realizować technologiczny plan w dziedzinie cyberbezpieczeństwa **oraz gromadzić i udostępniać wiedzę fachową** i ułatwiać dostęp do wiedzy fachowej zebranej w ramach sieci i środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa, **a także ułatwiać dostęp do infrastruktury cyberbezpieczeństwa**. Po drugie, Centrum powinno wdrażać odpowiednie części programów „Cyfrowa Europa” i „Horyzont Europa” poprzez przydzielanie dotacji, zwykle na podstawie konkurencyjnych zaproszeń do składania wniosków. Po trzecie, Centrum Kompetencji powinno ułatwiać wspólne inwestycje Unii, państw członkowskich lub przemysłu, **a także oferować obywatelom i przedsiębiorstwom możliwości wspólnych szkoleń i programy podnoszenia świadomości zgodnie z programem „Cyfrowa Europa” w celu pokonania luki w umiejętnościach. Szczególną wagę powinno zwracać na stworzenie MŚP odpowiednich warunków do działania w obszarze cyberbezpieczeństwa.**

Środa, 13 marca 2019 r.

## Poprawka 21

## Wniosek dotyczący rozporządzenia

## Motyw 16

Tekst proponowany przez Komisję

- (16) Centrum Kompetencji powinno stymulować i wspierać współpracę i koordynację działań środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa, które obejmowałyby dużą, otwartą i zróżnicowaną grupę podmiotów zaangażowanych w technologię cyberbezpieczeństwa. Środowisko to powinno obejmować w szczególności podmioty prowadzące badania naukowe, branże po stronie podaży, branże po stronie popytu i sektor publiczny. Środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa powinno wnieść wkład w działania i plan prac Centrum Kompetencji i powinno również korzystać z działań na rzecz tworzenia środowiska prowadzonych przez Centrum Kompetencji i sieć, ale nie powinno być pod innymi względami uprzywilejowane w zakresie zaproszeń do składania wniosków lub zaproszeń do składania ofert.

Poprawka

- (16) Centrum Kompetencji powinno stymulować i wspierać **długoterminową strategiczną** współpracę i koordynację działań środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa, które obejmowałyby dużą, otwartą, **interdyscyplinarną** i zróżnicowaną grupę podmiotów  **europejskich**  zaangażowanych w technologię cyberbezpieczeństwa. Środowisko to powinno obejmować w szczególności podmioty prowadzące badania naukowe, **w tym badania nad etycznymi aspektami cyberbezpieczeństwa**, branże po stronie podaży, branże po stronie popytu, **w tym MŚP**, i sektor publiczny. Środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa powinno wnieść wkład w działania i plan prac Centrum Kompetencji i powinno również korzystać z działań na rzecz tworzenia środowiska prowadzonych przez Centrum Kompetencji i sieć, ale nie powinno być pod innymi względami uprzywilejowane w zakresie zaproszeń do składania wniosków lub zaproszeń do składania ofert.

## Poprawka 22

## Wniosek dotyczący rozporządzenia

## Motyw 16 a (nowy)

Tekst proponowany przez Komisję

- (16a) **Centrum Kompetencji powinno zapewniać ENISA odpowiednie wsparcie w realizacji zadań określonych w dyrektywie (UE) 2016/1148 („dyrektywa w sprawie bezpieczeństwa sieci i informacji”) oraz w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/XXX<sup>(1a)</sup> („akt ws. cyberbezpieczeństwa”). W związku z tym ENISA powinna przekazywać Centrum Kompetencji odpowiednie dane w ramach zadania polegającego na określeniu priorytetów w zakresie finansowania.**

Poprawka

- (<sup>1a</sup>) **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/... z dnia ... w sprawie „Agencji UE ds. cyberbezpieczeństwa” ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. cyberbezpieczeństwa”) (Dz.U. L...) (2017/0225(COD)).**

Środa, 13 marca 2019 r.

## Poprawka 23

## Wniosek dotyczący rozporządzenia

## Motyw 17

Tekst proponowany przez Komisję

- (17) Aby odpowiedzieć na potrzeby zarówno branż po stronie podaży, jak i branż po stronie popytu, zadanie Centrum Kompetencji dotyczące zapewnienia wiedzy z zakresu cyberbezpieczeństwa i pomocy technicznej gałęziom przemysłu powinno odnosić się zarówno do produktów i usług ICT, jak i wszystkich innych przemysłowych i technologicznych produktów i **rozwiązań**, do których ma zostać włączone cyberbezpieczeństwo.

Poprawka

- (17) Aby odpowiedzieć na potrzeby **sektora publicznego oraz** zarówno branż po stronie podaży, jak i branż po stronie popytu, zadanie Centrum Kompetencji dotyczące zapewnienia wiedzy z zakresu cyberbezpieczeństwa i pomocy technicznej **sektorowi publicznemu oraz** gałęziom przemysłu powinno odnosić się zarówno do produktów, **procesów** i usług ICT, jak i wszystkich innych przemysłowych i technologicznych produktów i **procesów**, do których ma zostać włączone cyberbezpieczeństwo. **W szczególności Centrum Kompetencji powinno ułatwiać wdrażanie dynamicznych rozwiązań na poziomie przedsiębiorstw, skupiających się na budowaniu zdolności całych organizacji, w tym ludzi, procesów i technologii, w celu skutecznej ochrony organizacji przed stale zmieniającymi się cyberzagrożeniami.**

## Poprawka 24

## Wniosek dotyczący rozporządzenia

## Motyw 17 a (nowy)

Tekst proponowany przez Komisję

- (17a) Centrum Kompetencji powinno przyczyniać się do powszechnego wdrażania najnowocześniejszych produktów i rozwiązań z zakresu cyberbezpieczeństwa, w szczególności tych, które są uznawane na szczeblu międzynarodowym.

Poprawka

- (17a) Centrum Kompetencji powinno przyczyniać się do powszechnego wdrażania najnowocześniejszych produktów i rozwiązań z zakresu cyberbezpieczeństwa, w szczególności tych, które są uznawane na szczeblu międzynarodowym.

## Poprawka 25

## Wniosek dotyczący rozporządzenia

## Motyw 18

Tekst proponowany przez Komisję

- (18) Chociaż Centrum Kompetencji i sieć powinny mieć na celu osiągnięcie synergii między cyberbezpieczeństwem cywilnym i cyberbezpieczeństwem obronnym, projekty finansowane w ramach programu „Horyzont Europa” będą wdrażane zgodnie z rozporządzeniem XXX [rozporządzenie w sprawie programu „Horyzont Europa”], w którym przewidziano, że działania w zakresie badań naukowych i innowacji przeprowadzane w ramach programu „Horyzont Europa” powinny dotyczyć głównie zastosowań cywilnych.

Poprawka

- (18) Chociaż Centrum Kompetencji i sieć powinny mieć na celu osiągnięcie synergii **i koordynacji** między cyberbezpieczeństwem cywilnym i cyberbezpieczeństwem obronnym, projekty finansowane w ramach programu „Horyzont Europa” będą wdrażane zgodnie z rozporządzeniem XXX [rozporządzenie w sprawie programu „Horyzont Europa”], w którym przewidziano, że działania w zakresie badań naukowych i innowacji przeprowadzane w ramach programu „Horyzont Europa” powinny dotyczyć głównie zastosowań cywilnych.

Środa, 13 marca 2019 r.

**Poprawka 26****Wniosek dotyczący rozporządzenia****Motyw 19***Tekst proponowany przez Komisję*

- (19) Aby zapewnić ustrukturyzowaną i zrównoważoną współpracę, relacje między Centrum Kompetencji a krajowymi ośrodkami koordynacji powinny opierać się na porozumieniu umownym.

*Poprawka*

- (19) Aby zapewnić ustrukturyzowaną i zrównoważoną współpracę, relacje między Centrum Kompetencji a krajowymi ośrodkami koordynacji powinny opierać się na porozumieniu umownym, **które należy zharmonizować na poziomie Unii.**

**Poprawka 27****Wniosek dotyczący rozporządzenia****Motyw 20***Tekst proponowany przez Komisję*

- (20) Należy stworzyć odpowiednie przepisy, aby zagwarantować odpowiedzialność i przejrzystość działania Centrum Kompetencji.

*Poprawka*

- (20) Należy stworzyć odpowiednie przepisy, aby zagwarantować odpowiedzialność i przejrzystość działania Centrum Kompetencji **oraz finansowanych przedsiębiorstw.**

**Poprawka 28****Wniosek dotyczący rozporządzenia****Motyw 20 a (nowy)***Tekst proponowany przez Komisję**Poprawka*

- (20a) **Realizacja projektów wdrożeniowych, w szczególności dotyczących infrastruktury i zdolności wdrażanych na szczeblu europejskim lub w drodze wspólnych zamówień, może zostać podzielona na różne fazy wdrażania, np. oddzielne przetargi na architekturę sprzętu i oprogramowania, ich produkcję oraz obsługę i konserwację, przy czym przedsiębiorstwa mogą uczestniczyć tylko w jednym z etapów i wymagane jest, aby beneficjenci na jednym lub kilku z tych etapów spełniali określone warunki dotyczące własności lub kontroli przez podmioty europejskie.**

Środa, 13 marca 2019 r.

**Poprawka 29**

**Wniosek dotyczący rozporządzenia**

**Motyw 20 b (nowy)**

Tekst proponowany przez Komisję

Poprawka

- (20b) *Centrum Kompetencji powinno dążyć do jak największej synergii z ENISA, będącą wyspecjalizowaną agencją Unii ds. cyberbezpieczeństwa, a Rada Zarządzająca powinna konsultować się z ENISA – z uwagi na jej doświadczenie w tej dziedzinie – we wszystkich kwestiach dotyczących cyberbezpieczeństwa, w szczególności w odniesieniu do projektów związanych z badaniami naukowymi.*

**Poprawka 30**

**Wniosek dotyczący rozporządzenia**

**Motyw 20 c (nowy)**

Tekst proponowany przez Komisję

Poprawka

- (20c) *W procedurze mianowania przedstawiciela do Rady Zarządzającej Parlament Europejski powinien zawrzeć szczegółowe informacje na temat mandatu, obejmującego obowiązek regularnego składania sprawozdań Parlamentowi Europejskiemu lub właściwym komisjom.*

Środa, 13 marca 2019 r.

## Poprawka 31

## Wniosek dotyczący rozporządzenia

## Motyw 21

Tekst proponowany przez Komisję

- (21) W świetle wiedzy fachowej w dziedzinie cyberbezpieczeństwa, jaką posiadają odpowiednio Wspólne Centrum Badawcze Komisji oraz Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), powinny one odgrywać aktywną rolę w środowisku posiadającym kompetencje w dziedzinie cyberbezpieczeństwa i Radzie Konsultacyjnej ds. Przemysłowych i Naukowych.

Poprawka

- (21) W świetle wiedzy fachowej w dziedzinie cyberbezpieczeństwa, jaką posiadają odpowiednio Wspólne Centrum Badawcze Komisji oraz Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), **a także aby zapewnić możliwie największą synergię**, powinny one odgrywać aktywną rolę w środowisku posiadającym kompetencje w dziedzinie cyberbezpieczeństwa i Radzie Konsultacyjnej ds. Przemysłowych i Naukowych. **ENISA powinna nadal realizować swoje cele strategiczne, zwłaszcza w dziedzinie certyfikacji cyberbezpieczeństwa, określone w rozporządzeniu (UE) 2019/XXX [akt ws. cyberbezpieczeństwa] <sup>(1a)</sup>, natomiast Centrum Kompetencji powinno działać jako organ operacyjny w dziedzinie cyberbezpieczeństwa.**

<sup>(1a)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/... z dnia ... w sprawie „Agencji UE ds. cyberbezpieczeństwa” ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. cyberbezpieczeństwa”) (Dz.U. L...) (2017/0225(COD)).

## Poprawka 32

## Wniosek dotyczący rozporządzenia

## Motyw 24

Tekst proponowany przez Komisję

- (24) Rada Zarządzająca Centrum Kompetencji, składająca się z przedstawicieli państw członkowskich i Komisji, powinna określać ogólny kierunek działalności Centrum Kompetencji oraz zapewniać wykonywanie przez nie jego zadań zgodnie z niniejszym rozporządzeniem. Rada Zarządzająca powinna posiadać uprawnienia niezbędne do uchwalania budżetu, kontroli jego wykonania, przyjmowania stosownych przepisów finansowych, ustalania przejrzystych procedur pracy w zakresie podejmowania decyzji przez Centrum Kompetencji, przyjmowania planu prac Centrum Kompetencji i wieloletniego planu strategicznego odzwierciedlającego priorytety w realizacji celów i zadań Centrum Kompetencji, uchwalania jej regulaminu wewnętrznego, powoływania dyrektora wykonawczego oraz podejmowania decyzji o przedłużeniu jego kadencji lub jej zakończeniu.

Poprawka

- (24) Rada Zarządzająca Centrum Kompetencji, składająca się z przedstawicieli państw członkowskich i Komisji, powinna określać ogólny kierunek działalności Centrum Kompetencji oraz zapewniać wykonywanie przez nie jego zadań zgodnie z niniejszym rozporządzeniem. Rada Zarządzająca powinna posiadać uprawnienia niezbędne do uchwalania budżetu, kontroli jego wykonania, przyjmowania stosownych przepisów finansowych, ustalania przejrzystych procedur pracy w zakresie podejmowania decyzji przez Centrum Kompetencji, przyjmowania planu prac Centrum Kompetencji i wieloletniego planu strategicznego odzwierciedlającego priorytety w realizacji celów i zadań Centrum Kompetencji, uchwalania jej regulaminu wewnętrznego, powoływania dyrektora wykonawczego oraz podejmowania decyzji o przedłużeniu jego kadencji lub jej zakończeniu. **Aby wykorzystać synergię, ENISA powinna być stałym obserwatorem w Radzie Zarządzającej i powinna wносить wkład w prace Centrum Kompetencji, w tym w drodze konsultacji w sprawie wieloletniego planu strategicznego oraz w sprawie planu prac i wykazu działań wybranych do finansowania.**



Środa, 13 marca 2019 r.

### Poprawka 33

#### Wniosek dotyczący rozporządzenia

##### Motyw 24 a (nowy)

Tekst proponowany przez Komisję

Poprawka

- (24a) *Rada Zarządzająca powinna dążyć do promowania Centrum Kompetencji w skali globalnej, aby zwiększyć jego atrakcyjność i uczynić z niego światowej klasy podmiot doskonałości w dziedzinie cyberbezpieczeństwa.*

### Poprawka 34

#### Wniosek dotyczący rozporządzenia

##### Motyw 25

Tekst proponowany przez Komisję

Poprawka

- (25) Aby Centrum Kompetencji mogło prawidłowo i skutecznie funkcjonować, Komisja i państwa członkowskie powinny zapewnić, aby osoby, które mają zostać powołane na członków Rady Zarządzającej, posiadały odpowiednią zawodową wiedzę fachową i doświadczenie w obszarach funkcyjnych. Komisja i państwa członkowskie powinny również dołożyć starań, by ograniczyć rotację swoich przedstawicieli w Radzie Zarządzającej, tak aby zapewnić ciągłość jej pracy.

- (25) Aby Centrum Kompetencji mogło prawidłowo i skutecznie funkcjonować, Komisja i państwa członkowskie powinny zapewnić, aby osoby, które mają zostać powołane na członków Rady Zarządzającej, posiadały odpowiednią zawodową wiedzę fachową i doświadczenie w obszarach funkcyjnych. Komisja i państwa członkowskie powinny również dołożyć starań, by ograniczyć rotację swoich przedstawicieli w Radzie Zarządzającej, tak aby zapewnić ciągłość jej pracy, **a także powinny dążyć do osiągnięcia równowagi płci.**

### Poprawka 35

#### Wniosek dotyczący rozporządzenia

##### Motyw 25 a (nowy)

Tekst proponowany przez Komisję

Poprawka

- (25a) *Waga głosu Komisji w głosowaniach nad decyzjami Rady Zarządzającej powinna być współmierna do wkładu z budżetu Unii na rzecz Centrum Kompetencji, zgodnie z odpowiedzialnością Komisji za zapewnienie właściwego zarządzania budżetem Unii w interesie Unii, jak określono w traktatach.*

Środa, 13 marca 2019 r.

**Poprawka 36****Wniosek dotyczący rozporządzenia****Motyw 26**

Tekst proponowany przez Komisję

- (26) Sprawne funkcjonowanie Centrum Kompetencji wymaga, aby dyrektor wykonawczy był mianowany na podstawie swoich osiągnięć oraz udokumentowanych kompetencji administracyjnych i zarządczych, a także odpowiednich kompetencji i doświadczenia w zakresie cyberbezpieczeństwa, oraz aby pełnił swoje obowiązki w sposób całkowicie niezależny.

Poprawka

- (26) Sprawne funkcjonowanie Centrum Kompetencji wymaga, aby dyrektor wykonawczy był mianowany **w przejrzysty sposób** na podstawie swoich osiągnięć oraz udokumentowanych kompetencji administracyjnych i zarządczych, a także odpowiednich kompetencji i doświadczenia w zakresie cyberbezpieczeństwa, oraz aby pełnił swoje obowiązki w sposób całkowicie niezależny.

**Poprawka 37****Wniosek dotyczący rozporządzenia****Motyw 27**

Tekst proponowany przez Komisję

- (27) Centrum Kompetencji powinno posiadać organ doradczy w postaci Rady Konsultacyjnej ds. Przemysłowych i Naukowych w celu zapewnienia regularnego dialogu z sektorem prywatnym, organizacjami konsumenckimi i innymi odpowiednimi zainteresowanymi stronami. Rada Konsultacyjna ds. Przemysłowych i Naukowych powinna skupiać się na zagadnieniach istotnych dla zainteresowanych stron i kierować na nie uwagę Rady Zarządzającej Centrum Kompetencji. Skład Rady Konsultacyjnej ds. Przemysłowych i Naukowych oraz przydzielone jej zadania, takie jak zasięganie jej opinii w sprawie planu prac, powinny zapewniać wystarczającą reprezentację zainteresowanych stron w pracach Centrum Kompetencji.

Poprawka

- (27) Centrum Kompetencji powinno posiadać organ doradczy w postaci Rady Konsultacyjnej ds. Przemysłowych i Naukowych w celu zapewnienia regularnego **i odpowiednio przejrzystego** dialogu z sektorem prywatnym, organizacjami konsumenckimi i innymi odpowiednimi zainteresowanymi stronami. **Centrum powinno także zapewniać dyrektorowi wykonawczemu i Radzie Zarządzającej niezależne doradztwo w zakresie wdrażania i zamówień.** Rada Konsultacyjna ds. Przemysłowych i Naukowych powinna skupiać się na zagadnieniach istotnych dla zainteresowanych stron i kierować na nie uwagę Rady Zarządzającej Centrum Kompetencji. Skład Rady Konsultacyjnej ds. Przemysłowych i Naukowych oraz przydzielone jej zadania, takie jak zasięganie jej opinii w sprawie planu prac, powinny zapewniać wystarczającą reprezentację zainteresowanych stron w pracach Centrum Kompetencji. **Każdej kategorii zainteresowanych stron z branży należy przydzielić minimalną liczbę miejsc, ze szczególnym uwzględnieniem reprezentacji MSP.**

Środa, 13 marca 2019 r.

## Poprawka 38

## Wniosek dotyczący rozporządzenia

## Motyw 28

Tekst proponowany przez Komisję

- (28) Centrum Kompetencji **powinno** korzystać ze szczególnej wiedzy fachowej oraz szerokiego i odpowiedniego udziału zainteresowanych stron, stworzonego w ramach umownego partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa w trakcie trwania programu „Horyzont 2020” za pośrednictwem swojej Rady Konsultacyjnej ds. Przemysłowych i Naukowych.

Poprawka

- (28) Centrum Kompetencji **i jego działalność powinny** korzystać ze szczególnej wiedzy fachowej oraz szerokiego i odpowiedniego udziału zainteresowanych stron, stworzonego w ramach umownego partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa w trakcie trwania programu „Horyzont 2020”, **a także projektów pilotażowych w ramach programu „Horyzont 2020” dotyczących sieci kompetencji w dziedzinie cyberbezpieczeństwa**, za pośrednictwem swojej Rady Konsultacyjnej ds. Przemysłowych i Naukowych. **W stosownych przypadkach Centrum Kompetencji oraz Rada Konsultacyjna ds. Przemysłowych i Naukowych powinny rozważyć odwzorowanie istniejących struktur, np. w formie grup roboczych.**

## Poprawka 39

## Wniosek dotyczący rozporządzenia

## Motyw 28 a (nowy)

Tekst proponowany przez Komisję

- (28a) **Centrum Kompetencji i jego organy powinny wykorzystywać doświadczenia i wkład poprzednich i obecnych inicjatyw, takich jak umowne partnerstwo publiczno-prywatne (cPPP) w dziedzinie cyberbezpieczeństwa, Europejska Organizacja ds. Cyberbezpieczeństwa (EC-SO) oraz projekt pilotażowy i działanie przygotowawcze dotyczące audytów wolnego i otwartego oprogramowania (EU FOSSA).**

Poprawka

Środa, 13 marca 2019 r.

**Poprawka 40****Wniosek dotyczący rozporządzenia****Motyw 29**

Tekst proponowany przez Komisję

- (29) W Centrum Kompetencji powinny obowiązywać przepisy dotyczące zapobiegania konfliktom interesów i **zarządzania nimi**. Centrum Kompetencji powinno również stosować odpowiednie przepisy unijne dotyczące publicznego dostępu do dokumentów zawarte w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 1049/2001<sup>(24)</sup>. Przetwarzanie danych osobowych przez Centrum Kompetencji będzie podlegać przepisom rozporządzenia Parlamentu Europejskiego i Rady (UE) nr XXX/2018. Centrum Kompetencji powinno przestrzegać przepisów mających zastosowanie do instytucji Unii oraz przepisów krajowych dotyczących postępowania z informacjami, w szczególności ze szczególnie chronionymi informacjami jawnymi i informacjami niejawnymi UE.

<sup>(24)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1049/2001 z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.U. L 145 z 31.5.2001, s. 43).

Poprawka

- (29) W Centrum Kompetencji powinny obowiązywać przepisy dotyczące zapobiegania konfliktom interesów **oraz ich identyfikacji i eliminowania w odniesieniu do jego członków, organów i personelu, Rady Zarządzającej, a także Rady Konsultacyjnej ds. Przemysłowych i Naukowych oraz środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa. Państwa członkowskie powinny zadbać o zapobieganie konfliktom interesów oraz ich identyfikację i eliminowanie w odniesieniu do krajowych ośrodków koordynacji**. Centrum Kompetencji powinno również stosować odpowiednie przepisy unijne dotyczące publicznego dostępu do dokumentów zawarte w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 1049/2001<sup>(24)</sup>. Przetwarzanie danych osobowych przez Centrum Kompetencji będzie podlegać przepisom rozporządzenia Parlamentu Europejskiego i Rady (UE) nr XXX/2018. Centrum Kompetencji powinno przestrzegać przepisów mających zastosowanie do instytucji Unii oraz przepisów krajowych dotyczących postępowania z informacjami, w szczególności ze szczególnie chronionymi informacjami jawnymi i informacjami niejawnymi UE.

<sup>(24)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1049/2001 z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.U. L 145 z 31.5.2001, s. 43).

**Poprawka 41****Wniosek dotyczący rozporządzenia****Motyw 31**

Tekst proponowany przez Komisję

- (31) Centrum Kompetencji powinno działać w otwarty i przejrzysty sposób pozwalający mu na czas udostępniać **wszelkie stosowne** informacje, jak również promować swoje działania, w tym działania informacyjne i upowszechnianie wiedzy wśród społeczeństwa. Regulamin wewnętrzny organów Centrum Kompetencji powinien być dostępny publicznie.

Poprawka

- (31) Centrum Kompetencji powinno działać w otwarty i przejrzysty sposób pozwalający mu na czas udostępniać **wyczerpujące** informacje, jak również promować swoje działania, w tym działania informacyjne i upowszechnianie wiedzy wśród społeczeństwa. **Powinno przekazywać opinii publicznej i wszelkim zainteresowanym stronom wykaz członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa oraz podawać do wiadomości publicznej deklaracje interesów złożone zgodnie z art. 42**. Regulamin wewnętrzny organów Centrum Kompetencji powinien być dostępny publicznie.

Środa, 13 marca 2019 r.

**Poprawka 42**  
**Wniosek dotyczący rozporządzenia**  
**Motyw 31 a (nowy)**

Tekst proponowany przez Komisję

Poprawka

- (31a) *Wskazane jest, aby zarówno Centrum Kompetencji, jak i krajowe ośrodki koordynacji w możliwie największym stopniu monitorowały i stosowały międzynarodowe standardy w celu zachęcania do wypracowania globalnych najlepszych praktyk.*

**Poprawka 43**  
**Wniosek dotyczący rozporządzenia**  
**Motyw 33 a (nowy)**

Tekst proponowany przez Komisję

Poprawka

- (33a) *Należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w odniesieniu do zdefiniowania elementów umów między Centrum Kompetencji i krajowymi ośrodkami koordynacji oraz w odniesieniu do określenia kryteriów oceny podmiotów i ich akredytacji jako członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa <sup>(1a)</sup> W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.*

<sup>(1a)</sup> Dz.U. L 123 z 12.5.2016, s. 1.

Środa, 13 marca 2019 r.

## Poprawka 44

## Wniosek dotyczący rozporządzenia

## Motyw 34

Tekst proponowany przez Komisję

- (34) **Ponieważ cele** niniejszego rozporządzenia, a mianowicie utrzymanie i rozwijanie technologicznych i przemysłowych zdolności Unii w dziedzinie cyberbezpieczeństwa, zwiększanie konkurencyjności unijnego sektora cyberbezpieczeństwa i uczynienia z cyberbezpieczeństwa przewagi konkurencyjnej innych gałęzi przemysłu Unii, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie z uwagi na rozproszenie istniejących, ograniczonych zasobów oraz niezbędną wielkość inwestycji, lecz ze względu na uniknięcie niepotrzebnego powielania tych wysiłków, pomoc w osiągnięciu masy krytycznej inwestycji i zapewnienie, by finansowanie publiczne wykorzystywano w sposób optymalny, mogą być lepiej realizowane na **szczeblu unijnym**, Unia może **przyjąć środki** zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności, **o której mowa** w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu,

Poprawka

- (34) **Cele** niniejszego rozporządzenia, a mianowicie **podniesienie konkurencyjności i zdolności Unii w dziedzinie cyberbezpieczeństwa w wyniku większego upowszechnienia produktów, procesów i usług z zakresu cyberbezpieczeństwa i dzięki temu zmniejszenie zależności cyfrowej Unii**, utrzymanie i rozwijanie technologicznych i przemysłowych zdolności Unii w dziedzinie cyberbezpieczeństwa, zwiększanie konkurencyjności unijnego sektora cyberbezpieczeństwa i uczynienie z cyberbezpieczeństwa przewagi konkurencyjnej innych gałęzi przemysłu Unii, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie z uwagi na rozproszenie istniejących, ograniczonych zasobów oraz niezbędną wielkość inwestycji, lecz ze względu na uniknięcie niepotrzebnego powielania tych wysiłków, pomoc w osiągnięciu masy krytycznej inwestycji i zapewnienie, by finansowanie publiczne wykorzystywano w sposób optymalny, mogą być lepiej realizowane na **poziomie Unii. Ponadto jedynie działania na poziomie Unii mogą zapewnić najwyższy poziom cyberbezpieczeństwa we wszystkich państwach członkowskich, a tym samym zlikwidować istniejące w niektórych państwach członkowskich luki w zakresie bezpieczeństwa, które stwarzają luki w zakresie bezpieczeństwa w całej Unii. W związku z powyższym Unia może podjąć działania** zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności **określoną** w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

## Poprawka 45

## Wniosek dotyczący rozporządzenia

## Artykuł 1 – ustęp 1

Tekst proponowany przez Komisję

1. Na mocy niniejszego rozporządzenia ustanawia się Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych („Centrum Kompetencji”) oraz sieć krajowych ośrodków koordynacji, a także określa się przepisy dotyczące nominacji krajowych ośrodków koordynacji i tworzenia środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa.

Poprawka

1. Na mocy niniejszego rozporządzenia ustanawia się Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych („Centrum Kompetencji”) oraz sieć krajowych ośrodków koordynacji („**sieć**”), a także określa się przepisy dotyczące nominacji krajowych ośrodków koordynacji i tworzenia środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa („**środowisko**”). **Centrum Kompetencji i sieć wnoszą wkład w ogólną odporność i świadomość zagrożeń dla cyberbezpieczeństwa w Unii, przy pełnym uwzględnieniu skutków społecznych.**

Środa, 13 marca 2019 r.

#### Poprawka 46

### Wniosek dotyczący rozporządzenia

#### Artykuł 1 – ustęp 3

Tekst proponowany przez Komisję

3. Siedziba Centrum Kompetencji znajduje się w [Brukseli w Belgii].

Poprawka

skreśla się

#### Poprawka 47

### Wniosek dotyczący rozporządzenia

#### Artykuł 1 – ustęp 4

Tekst proponowany przez Komisję

4. Centrum Kompetencji posiada osobowość prawną. We wszystkich państwach członkowskich centrum ma zdolność prawną o najszerszym zakresie przyznawanym osobom prawnym zgodnie z ustawodawstwem danego państwa członkowskiego. Może ono zwłaszcza nabywać i zbywać nieruchomości i ruchomości oraz być stroną w postępowaniach sądowych.

Poprawka

skreśla się

#### Poprawka 48

### Wniosek dotyczący rozporządzenia

#### Artykuł 2 – akapit 1 – punkt 1

Tekst proponowany przez Komisję

1) „cyberbezpieczeństwo” oznacza **ochronę** sieci i systemów informatycznych, ich użytkowników **i innych** osób **przed zagrożeniami dla cyberbezpieczeństwa**;

Poprawka

1) „cyberbezpieczeństwo” oznacza **wszystkie działania niezbędne do ochrony przed zagrożeniami dla cyberbezpieczeństwa** sieci i systemów informatycznych, ich użytkowników **oraz osób, których zagrożenia te dotyczą**;

Środa, 13 marca 2019 r.

## Poprawka 183

## Wniosek dotyczący rozporządzenia

## Artykuł 2 – akapit 1 – punkt 1 a (nowy)

Tekst proponowany przez Komisję

Poprawka

- 1a) „cyberobrona” i „wymiar obronny cyberbezpieczeństwa” oznaczają wyłącznie defensywną i reaktywną technologię cyberobrony, której celem jest ochrona przed cyberzagrożeniami infrastruktury krytycznej, sieci wojskowych i systemów informatycznych, ich użytkowników i osób, których dotyczą zagrożenia, obejmującą orientację sytuacyjną, wykrywanie zagrożeń i kryminalistykę cyfrową;

## Poprawka 49

## Wniosek dotyczący rozporządzenia

## Artykuł 2 – akapit 1 – punkt 2

Tekst proponowany przez Komisję

Poprawka

- 2) „produkty i rozwiązania w dziedzinie cyberbezpieczeństwa” oznaczają produkty, usługi lub procesy ICT, których szczególnym celem jest ochrona przed zagrożeniami dla cyberbezpieczeństwa sieci i systemów informatycznych, ich użytkowników oraz osób, których zagrożenia te dotyczą;
- 2) „produkty i procesy” oznaczają komercyjne i niekomercyjne produkty, usługi lub procesy ICT, których szczególnym celem jest ochrona danych, sieci i systemów informatycznych, ich użytkowników oraz innych osób przed zagrożeniami dla cyberbezpieczeństwa;

## Poprawka 50

## Wniosek dotyczący rozporządzenia

## Artykuł 2 – akapit 1 – punkt 2 a (nowy)

Tekst proponowany przez Komisję

Poprawka

- 2a) „zagrożenie dla cyberbezpieczeństwa” oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą uszkodzić lub zakłócić sieci i systemy informatyczne, ich użytkowników oraz osoby, których zagrożenie to dotyczy, albo w inny sposób niekorzystnie wpływać na te sieci i systemy informatyczne, użytkowników i osoby, których zagrożenie to dotyczy;



Środa, 13 marca 2019 r.

**Poprawka 51****Wniosek dotyczący rozporządzenia****Artykuł 2 – akapit 1 – punkt 3**

---

*Tekst proponowany przez Komisję*

- 3) „organ publiczny” oznacza jednostkę administracji rządowej lub innej administracji publicznej, w tym publiczne organy doradcze na szczeblu krajowym, regionalnym lub lokalnym, bądź osobę fizyczną lub prawną, która na mocy prawa krajowego sprawuje publiczne funkcje administracyjne, łącznie ze szczególnymi obowiązkami;

---

*Poprawka*

- 3) „organ publiczny” oznacza jednostkę administracji rządowej lub innej administracji publicznej, w tym publiczne organy doradcze na szczeblu krajowym, regionalnym lub lokalnym, bądź osobę fizyczną lub prawną, która na mocy prawa **unijnego i** krajowego sprawuje publiczne funkcje administracyjne, łącznie ze szczególnymi obowiązkami;

**Poprawka 52****Wniosek dotyczący rozporządzenia****Artykuł 2 – akapit 1 – punkt 4**

---

*Tekst proponowany przez Komisję*

- 4) „**uczestniczące** państwo członkowskie” oznacza państwo członkowskie, które dobrowolnie wnosi wkład finansowy w koszty administracyjne i operacyjne Centrum Kompetencji.

---

*Poprawka*

- 4) „**finansujące** państwo członkowskie” oznacza państwo członkowskie, które dobrowolnie wnosi wkład finansowy w koszty administracyjne i operacyjne Centrum Kompetencji;

**Poprawka 53****Wniosek dotyczący rozporządzenia****Artykuł 2 – akapit 1 – punkt 4 a (nowy)**

---

*Tekst proponowany przez Komisję*

---

*Poprawka*

- 4a) „ **europejskie centra innowacji cyfrowych**” oznaczają podmiot prawny w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/XXX<sup>(1a)</sup>.

<sup>(1a)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/XXX ustanawiające program „Cyfrowa Europa” na lata 2021–2027 (Dz.U. L ...) (2018/0227(COD)).

Środa, 13 marca 2019 r.

## Poprawka 54

## Wniosek dotyczący rozporządzenia

## Artykuł 3 – ustęp 1 – litera a

Tekst proponowany przez Komisję

- a) w **utrzymaniu i** rozwijaniu technologicznych i przemysłowych zdolności w dziedzinie cyberbezpieczeństwa niezbędnych do zabezpieczenia jej jednolitego rynku cyfrowego;

Poprawka

- a) w rozwijaniu **fachowych** technologicznych, przemysłowych, społecznych, akademickich i naukowych zdolności i możliwości w dziedzinie cyberbezpieczeństwa niezbędnych do zabezpieczenia jej jednolitego rynku cyfrowego i dalszej ochrony danych unijnych obywateli, przedsiębiorstw i administracji publicznych;

## Poprawka 55

## Wniosek dotyczący rozporządzenia

## Artykuł 3 – ustęp 1 – litera a a (nowa)

Tekst proponowany przez Komisję

- aa) w zwiększaniu odporności i niezawodności infrastruktury sieci i systemów informatycznych, w tym infrastruktury krytycznej, internetu oraz powszechnie używanego sprzętu komputerowego i oprogramowania w Unii;

Poprawka

## Poprawka 56

## Wniosek dotyczący rozporządzenia

## Artykuł 3 – ustęp 1 – litera b

Tekst proponowany przez Komisję

- b) w zwiększaniu konkurencyjności unijnego sektora cyberbezpieczeństwa i uczynieniu z cyberbezpieczeństwa **przewagi konkurencyjnej** innych gałęzi przemysłu Unii.

Poprawka

- b) w zwiększaniu konkurencyjności unijnego sektora cyberbezpieczeństwa i uczynieniu z cyberbezpieczeństwa **atutu konkurencyjnego** innych gałęzi przemysłu Unii.

Środa, 13 marca 2019 r.

**Poprawka 57**

**Wniosek dotyczący rozporządzenia**

**Artykuł 3 – ustęp 1 – litera b a (nowa)**

Tekst proponowany przez Komisję

Poprawka

- ba) w zwiększaniu świadomości zagrożeń dla cyberbezpieczeństwa oraz związanych z nimi społecznych i etycznych implikacji i obaw w Unii oraz w niwelowaniu luki kompetencyjnej w zakresie cyberbezpieczeństwa w Unii;*

**Poprawka 58**

**Wniosek dotyczący rozporządzenia**

**Artykuł 3 – ustęp 1 – litera b b (nowa)**

Tekst proponowany przez Komisję

Poprawka

- bb) w rozwoju wiodącej pozycji Unii w dziedzinie cyberbezpieczeństwa i zapewnieniu najwyższych norm cyberbezpieczeństwa w całej Unii;*

**Poprawka 59**

**Wniosek dotyczący rozporządzenia**

**Artykuł 3 – ustęp 1 – litera b c (nowa)**

Tekst proponowany przez Komisję

Poprawka

- bc) we wzmacnianiu konkurencyjności i zdolności Unii przy jednoczesnym ograniczaniu jej zależności cyfrowej w drodze większego upowszechniania produktów, procesów i usług z zakresu cyberbezpieczeństwa opracowanych w Unii;*

Środa, 13 marca 2019 r.

**Poprawka 60****Wniosek dotyczący rozporządzenia****Artykuł 3 – ustęp 1 – litera b d (nowa)**

Tekst proponowany przez Komisję

Poprawka

**bd) w zwiększaniu zaufania obywateli, konsumentów i przedsiębiorstw do środowiska cyfrowego, a tym samym przyczynianiu się do osiągnięcia celów strategii jednolitego rynku cyfrowego;**

**Poprawka 61****Wniosek dotyczący rozporządzenia****Artykuł 4 – akapit 1 – punkt 1**

Tekst proponowany przez Komisję

Poprawka

1. **ułatwienie i pomoc w koordynacji pracy** sieci **krajowych ośrodków koordynacji („sieć”)**, o której mowa w art. 6, oraz **pracy** środowiska **posiadającego kompetencje w dziedzinie cyberbezpieczeństwa**, o którym mowa w art. 8;

1. **utworzenie** sieci, o której mowa w art. 6, oraz środowiska, o którym mowa w art. 8, **a także zarządzanie nimi i pomoc w ich działaniu;**

**Poprawka 62****Wniosek dotyczący rozporządzenia****Artykuł 4 – akapit 1 – punkt 2**

Tekst proponowany przez Komisję

Poprawka

2. **wnoszenie wkładu we wdrażanie** części dotyczącej cyberbezpieczeństwa programu „Cyfrowa Europa” ustanowionego rozporządzeniem nr XXX <sup>(26)</sup>, w szczególności działań związanych z art. 6 rozporządzenia (UE) nr XXX [program „Cyfrowa Europa”], oraz programu „Horyzont Europa” ustanowionego rozporządzeniem nr XXX <sup>(27)</sup>, w szczególności pkt 2.2.6 filaru II załącznika I do decyzji nr XXX ustanawiającej program szczegółowy służący realizacji programu ramowego w zakresie badań naukowych i innowacji „Horyzont Europa” [numer referencyjny programu szczegółowego], oraz innych unijnych programów, jeżeli przewidziano to w aktach prawnych Unii;

2. **koordynowanie wdrażania** części dotyczącej cyberbezpieczeństwa programu „Cyfrowa Europa” ustanowionego rozporządzeniem nr XXX <sup>(26)</sup>, w szczególności działań związanych z art. 6 rozporządzenia (UE) nr XXX [program „Cyfrowa Europa”], oraz programu „Horyzont Europa” ustanowionego rozporządzeniem nr XXX <sup>(27)</sup>, w szczególności pkt 2.2.6 filaru II załącznika I do decyzji nr XXX ustanawiającej program szczegółowy służący realizacji programu ramowego w zakresie badań naukowych i innowacji „Horyzont Europa” [numer referencyjny programu szczegółowego], oraz innych unijnych programów, jeżeli przewidziano to w aktach prawnych Unii, **a także wnoszenie wkładu we wdrażanie działań finansowanych z Europejskiego Funduszu Obrony ustanowionego rozporządzeniem (UE) 2019/XXX;**

<sup>(26)</sup> [dodać pełny tytuł i odniesienie do Dz.U.]

<sup>(27)</sup> [dodać pełny tytuł i odniesienie do Dz.U.]

<sup>(26)</sup> [dodać pełny tytuł i odniesienie do Dz.U.]

<sup>(27)</sup> [dodać pełny tytuł i odniesienie do Dz.U.]

Środa, 13 marca 2019 r.

## Poprawka 63

## Wniosek dotyczący rozporządzenia

## Artykuł 4 – akapit 1 – punkt 3 – wprowadzenie

Tekst proponowany przez Komisję

3. **poszerzanie** możliwości, wiedzy i ulepszanie infrastruktury w zakresie cyberbezpieczeństwa z korzyścią dla gałęzi przemysłu, sektora publicznego i środowisk naukowych dzięki wykonywaniu następujących zadań:

Poprawka

3. **zwiększanie odporności, zdolności, poszerzanie** możliwości, wiedzy i ulepszanie infrastruktury w zakresie cyberbezpieczeństwa z korzyścią dla **społeczeństwa**, gałęzi przemysłu, sektora publicznego i środowisk naukowych dzięki wykonywaniu następujących zadań, z **wykorzystaniem najnowocześniejszej infrastruktury przemysłowej i badawczej w zakresie cyberbezpieczeństwa oraz powiązanych z nią usług**:

## Poprawka 64

## Wniosek dotyczący rozporządzenia

## Artykuł 4 – akapit 1 – punkt 3 – litera a

Tekst proponowany przez Komisję

- a) **w odniesieniu do nowoczesnej infrastruktury przemysłowej i badawczej w zakresie cyberbezpieczeństwa i związanych z nią usług – nabywanie, ulepszanie, obsługa takiej infrastruktury oraz udostępnianie jej i związanych z nią usług** szerokiemu kręgowi użytkowników z sektora przemysłu w całej Unii, **w tym** MŚP, sektorowi publicznemu oraz społeczności badawczej i naukowej;

Poprawka

- a) **nabywanie, ulepszanie, obsługa i udostępnianie systemów Centrum Kompetencji oraz** związanych z **nimi** usług **na sprawiedliwych warunkach, otwarcie i jawnie** szerokiemu kręgowi użytkowników z sektora przemysłu w całej Unii, **szczególnie** MŚP, sektorowi publicznemu oraz społeczności badawczej i naukowej;

## Poprawka 65

## Wniosek dotyczący rozporządzenia

## Artykuł 4 – akapit 1 – punkt 3 – litera b

Tekst proponowany przez Komisję

- b) **w odniesieniu do nowoczesnej infrastruktury przemysłowej i badawczej w zakresie cyberbezpieczeństwa i związanych z nią usług – zapewnianie** wsparcia innym podmiotom, w tym wsparcia finansowego, jeżeli chodzi o nabywanie, ulepszanie, obsługę **takiej infrastruktury oraz** udostępnianie jej i związanych z **nią** usług szerokiemu kręgowi użytkowników z sektora przemysłu w całej Unii, **w tym** MŚP, sektorowi publicznemu oraz społeczności badawczej i naukowej;

Poprawka

- b) **zapewnianie** wsparcia innym podmiotom, w tym wsparcia finansowego, jeżeli chodzi o nabywanie, ulepszanie, obsługę i udostępnianie **takich systemów** i związanych z **nimi** usług szerokiemu kręgowi użytkowników z sektora przemysłu w całej Unii, **szczególnie** MŚP, sektorowi publicznemu oraz społeczności badawczej i naukowej;

Środa, 13 marca 2019 r.

**Poprawka 66****Wniosek dotyczący rozporządzenia****Artykuł 4 – akapit 1 – punkt 3 – litera b a (nowa)**

Tekst proponowany przez Komisję

Poprawka

*ba) zapewnianie wsparcia finansowego oraz pomocy technicznej przedsiębiorstwom typu start-up, MŚP, mikroprzedsiębiorstwom, stowarzyszeniom, indywidualnym ekspertom i obywatelskim projektom technicznym w dziedzinie cyberbezpieczeństwa;*

**Poprawka 67****Wniosek dotyczący rozporządzenia****Artykuł 4 – akapit 1 – punkt 3 – litera b b (nowa)**

Tekst proponowany przez Komisję

Poprawka

*bb) finansowanie audytów kodów bezpieczeństwa oprogramowania i powiązanych udoskonaleń w odniesieniu do projektów dotyczących wolnego i otwartego oprogramowania, powszechnie wykorzystywanego na potrzeby infrastruktury, produktów i procesów;*

**Poprawka 68****Wniosek dotyczący rozporządzenia****Artykuł 4 – akapit 1 – punkt 3 – litera c**

Tekst proponowany przez Komisję

Poprawka

*c) zapewnianie sektorowi przemysłu i organom publicznym wiedzy z zakresu cyberbezpieczeństwa oraz pomocy technicznej, w szczególności poprzez wspieranie działań mających na celu ułatwienie dostępu do wiedzy fachowej dostępnej w sieci i w środowisku posiadającym kompetencje w dziedzinie cyberbezpieczeństwa;*

*c) ułatwianie wymiany wiedzy z zakresu cyberbezpieczeństwa oraz pomocy technicznej między innymi wśród społeczeństwa obywatelskiego, sektora przemysłu, organów publicznych oraz społeczności akademickiej i naukowej, w szczególności poprzez wspieranie działań mających na celu ułatwienie dostępu do wiedzy fachowej dostępnej w sieci i w środowisku posiadającym kompetencje w dziedzinie cyberbezpieczeństwa w celu poprawy cyberodporności w Unii;*

Środa, 13 marca 2019 r.

### Poprawka 69

#### Wniosek dotyczący rozporządzenia

#### Artykuł 4 – akapit 1 – punkt 3 – litera c a (nowa)

Tekst proponowany przez Komisję

Poprawka

- ca) promowanie „uwzględniania bezpieczeństwa na etapie projektowania” jako zasady w procesie tworzenia, utrzymywania, eksploatacji i aktualizacji infrastruktury, produktów i usług, w szczególności przez wspieranie najnowocześniejszych metod bezpiecznego projektowania, odpowiednich testów i audytów bezpieczeństwa, i łącznie z obowiązkiem producenta lub dostawcy do niezwłocznego udostępnienia aktualizacji mających na celu usunięcie nowych luk lub zagrożeń, również po szacowanym okresie użytkowania produktu, lub umożliwienia stronie trzeciej tworzenia i dostarczania takich aktualizacji;

### Poprawka 70

#### Wniosek dotyczący rozporządzenia

#### Artykuł 4 – akapit 1 – punkt 3 – litera c b (nowa)

Tekst proponowany przez Komisję

Poprawka

- cb) wspomaganie polityki w zakresie udziału w tworzeniu kodów źródłowych oraz jej opracowywanie, w szczególności w odniesieniu do organów publicznych, które korzystają z projektów dotyczących wolnego i otwartego oprogramowania;

### Poprawka 71

#### Wniosek dotyczący rozporządzenia

#### Artykuł 4 – akapit 1 – punkt 3 – litera c c (nowa)

Tekst proponowany przez Komisję

Poprawka

- cc) zbliżanie zainteresowanych stron z przemysłu, związków zawodowych, środowisk akademickich, organizacji badawczych i podmiotów publicznych w celu zapewnienia długoterminowej współpracy w zakresie opracowywania i wdrażania produktów i procesów w dziedzinie cyberbezpieczeństwa, w tym łączenia zasobów i dzielenia się zasobami oraz informacjami dotyczącymi takich produktów i procesów, w stosownych przypadkach;

Środa, 13 marca 2019 r.

## Poprawka 72

## Wniosek dotyczący rozporządzenia

## Artykuł 4 – akapit 1 – punkt 4 – wprowadzenie

Tekst proponowany przez Komisję

4. wnoszenie wkładu w powszechne wdrażanie w całej **gospodarce** nowoczesnych produktów i **rozwiązań** w dziedzinie cyberbezpieczeństwa dzięki wykonywaniu następujących zadań:

Poprawka

4. wnoszenie wkładu w powszechne wdrażanie w całej **Unii** nowoczesnych **i zrównoważonych** produktów i **procesów** w dziedzinie cyberbezpieczeństwa dzięki wykonywaniu następujących zadań:

## Poprawka 73

## Wniosek dotyczący rozporządzenia

## Artykuł 4 – akapit 1 – punkt 4 – litera a

Tekst proponowany przez Komisję

- a) stymulowanie badań naukowych w dziedzinie cyberbezpieczeństwa, rozwoju cyberbezpieczeństwa, a także absorpcji unijnych produktów i **rozwiązań** w dziedzinie cyberbezpieczeństwa **przez organy publiczne i branże wykorzystujące te produkty i rozwiązania**;

Poprawka

- a) stymulowanie badań naukowych w dziedzinie cyberbezpieczeństwa, rozwoju cyberbezpieczeństwa, a także absorpcji unijnych produktów i **całościowych procesów** w dziedzinie cyberbezpieczeństwa **w całym cyklu innowacji, między innymi przez organy publiczne, przemysł i rynek**;

## Poprawka 74

## Wniosek dotyczący rozporządzenia

## Artykuł 4 – akapit 1 – punkt 4 – litera b

Tekst proponowany przez Komisję

- b) wspomaganie organów publicznych, branż po stronie popytu i innych użytkowników w przyjmowaniu i wdrażaniu **najnowszych rozwiązań** w dziedzinie cyberbezpieczeństwa;

Poprawka

- b) wspomaganie organów publicznych, branż po stronie popytu i innych użytkowników w **zwiększaniu odporności dzięki** przyjmowaniu i wdrażaniu **najnowocześniejszych produktów i procesów** w dziedzinie cyberbezpieczeństwa;



Środa, 13 marca 2019 r.

### Poprawka 75

#### Wniosek dotyczący rozporządzenia

#### Artykuł 4 – akapit 1 – punkt 4 – litera c

Tekst proponowany przez Komisję

- c) wspieranie w szczególności organów publicznych w organizacji udzielania zamówień publicznych lub przeprowadzanie zamówień na **nowoczesne** produkty i **rozwiązania** w dziedzinie cyberbezpieczeństwa w imieniu organów publicznych;

Poprawka

- c) wspieranie w szczególności organów publicznych w organizacji udzielania zamówień publicznych lub przeprowadzanie zamówień na **najnowocześniejsze** produkty i **procesy** w dziedzinie cyberbezpieczeństwa w imieniu organów publicznych, **w tym przez zapewnianie wsparcia na potrzeby zamówień, aby zwiększyć bezpieczeństwo inwestycji publicznych i płynących z nich korzyści;**

### Poprawka 76

#### Wniosek dotyczący rozporządzenia

#### Artykuł 4 – akapit 1 – punkt 4 – litera d

Tekst proponowany przez Komisję

- d) zapewnianie wsparcia finansowego i pomocy technicznej przedsiębiorstwom typu start-up oraz **MŚP** w dziedzinie cyberbezpieczeństwa w **celu** ich **połączenia** z potencjalnymi rynkami i **przyciągnięcia inwestycji;**

Poprawka

- d) zapewnianie wsparcia finansowego i pomocy technicznej przedsiębiorstwom typu start-up i **MŚP, mikroprzedsiębiorstwom, indywidualnym ekspertom, projektem dotyczącym powszechnie wykorzystywanego wolnego i otwartego oprogramowania** oraz **obywatelskim projektem technicznym** w dziedzinie cyberbezpieczeństwa, **aby poszerzać wiedzę fachową w dziedzinie cyberbezpieczeństwa, połączyć ich z potencjalnymi rynkami i możliwościami wdrażania, a także aby przyciągać inwestycje;**

### Poprawka 77

#### Wniosek dotyczący rozporządzenia

#### Artykuł 4 – akapit 1 – punkt 5 – wprowadzenie

Tekst proponowany przez Komisję

5. poprawa zrozumienia kwestii cyberbezpieczeństwa i wnoszenie wkładu w ograniczanie niedoborów kwalifikacji w zakresie cyberbezpieczeństwa w Unii dzięki realizacji następujących zadań:

Poprawka

5. poprawa zrozumienia kwestii cyberbezpieczeństwa i wnoszenie wkładu w ograniczanie niedoborów kwalifikacji **oraz wzmocnienie poziomu kwalifikacji** w zakresie cyberbezpieczeństwa w Unii dzięki realizacji następujących zadań:

Środa, 13 marca 2019 r.

## Poprawka 78

## Wniosek dotyczący rozporządzenia

## Artykuł 4 – akapit 1 – punkt 5 – litera -a (nowa)

Tekst proponowany przez Komisję

Poprawka

- a) *wspieranie, w stosownych przypadkach, realizacji celu szczegółowego 4 – zaawansowane umiejętności cyfrowe – programu „Cyfrowa Europa” we współpracy z europejskimi centrami innowacji cyfrowych;*

## Poprawka 79

## Wniosek dotyczący rozporządzenia

## Artykuł 4 – akapit 1 – punkt 5 – litera a

Tekst proponowany przez Komisję

Poprawka

- a) wspieranie dalszego rozwoju umiejętności w dziedzinie cyberbezpieczeństwa, w stosownych przypadkach z **udziałem odpowiednich agencji i organów** UE, w tym **Agencji** Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji;

- a) wspieranie dalszego rozwoju, **łączenia i wymiany** umiejętności **i kompetencji** w dziedzinie cyberbezpieczeństwa **na wszystkich odpowiednich poziomach kształcenia, wspieranie celu polegającego na osiągnięciu równowagi płci, ułatwianie osiągnięcia wspólnego wysokiego poziomu wiedzy w zakresie cyberbezpieczeństwa oraz przyczynianie się do budowania odporności użytkowników i infrastruktury w całej Unii w koordynacji z siecią oraz, w stosownych przypadkach, we współpracy z odpowiednimi agencjami i organami** UE, w tym **Agencją** Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji **ENISA**;

## Poprawka 80

## Wniosek dotyczący rozporządzenia

## Artykuł 4 – akapit 1 – punkt 6 – litera a

Tekst proponowany przez Komisję

Poprawka

- a) zapewnianie wsparcia finansowego na wysiłki badawcze w dziedzinie cyberbezpieczeństwa, których podstawą jest wspólny, stale oceniany i ulepszany wieloletni **program** dotyczący strategii, przemysłu, technologii i badań naukowych;

- a) zapewnianie wsparcia finansowego na wysiłki badawcze w dziedzinie cyberbezpieczeństwa, których podstawą jest wspólny, stale oceniany i ulepszany wieloletni **plan** dotyczący strategii, przemysłu, technologii i badań naukowych, **o którym mowa w art. 13**;

Środa, 13 marca 2019 r.

### Poprawka 81

#### Wniosek dotyczący rozporządzenia

#### Artykuł 4 – akapit 1 – punkt 6 – litera b

Tekst proponowany przez Komisję

- b) wspieranie dużych projektów badawczych i demonstracyjnych dotyczących możliwości technologicznych nowej generacji w dziedzinie cyberbezpieczeństwa we współpracy z przemysłem i siecią;

Poprawka

- b) wspieranie dużych projektów badawczych i demonstracyjnych dotyczących możliwości technologicznych nowej generacji w dziedzinie cyberbezpieczeństwa we współpracy z przemysłem, **społecznością akademicką i naukową, sektorem publicznym i organami publicznymi, w tym z siecią i środowiskiem;**

### Poprawka 82

#### Wniosek dotyczący rozporządzenia

#### Artykuł 4 – akapit 1 – punkt 6 – litera b a (nowa)

Tekst proponowany przez Komisję

Poprawka

- ba) **zapewnianie poszanowania praw podstawowych i etycznego postępowania w projektach badań naukowych w dziedzinie cyberbezpieczeństwa finansowanych przez Centrum Kompetencji;**

### Poprawka 83

#### Wniosek dotyczący rozporządzenia

#### Artykuł 4 – akapit 1 – punkt 6 – litera b b (nowa)

Tekst proponowany przez Komisję

Poprawka

- bb) **monitorowanie zgłoszeń o lukach w zabezpieczeniach wykrytych przez środowisko i ułatwianie ujawniania luk, opracowywania łat, poprawek i rozwiązań oraz ich dystrybucja;**

Środa, 13 marca 2019 r.

**Poprawka 84****Wniosek dotyczący rozporządzenia****Artykuł 4 – akapit 1 – punkt 6 – litera b c (nowa)**

---

*Tekst proponowany przez Komisję*

---

*Poprawka*

*bc) monitorowanie we współpracy z ENISA wyników badań w zakresie algorytmów samouczących się stosowanych w szkodliwych działaniach w cyberprzestrzeni oraz wspieranie wdrażania dyrektywy (UE) 2016/1148;*

**Poprawka 85****Wniosek dotyczący rozporządzenia****Artykuł 4 – akapit 1 – punkt 6 – litera b d (nowa)**

---

*Tekst proponowany przez Komisję*

---

*Poprawka*

*bd) wspieranie badań naukowych w dziedzinie cyberprzestępczości;*

**Poprawka 86****Wniosek dotyczący rozporządzenia****Artykuł 4 – akapit 1 – punkt 6 – litera b e (nowa)**

---

*Tekst proponowany przez Komisję*

---

*Poprawka*

*be) wspieranie badań naukowych i opracowania produktów i procesów, które można swobodnie analizować i wykorzystywać oraz którymi można się dzielić, zwłaszcza w dziedzinie zweryfikowanego i dającego się zweryfikować sprzętu i oprogramowania, w ściślejszej współpracy z przemysłem, siecią i środowiskiem;*

Środa, 13 marca 2019 r.

### Poprawka 87

#### Wniosek dotyczący rozporządzenia

#### Artykuł 4 – akapit 1 – punkt 6 – litera c

Tekst proponowany przez Komisję

c) wspieranie badań naukowych i innowacji w celu standaryzacji technologii cyberbezpieczeństwa;

Poprawka

c) wspieranie badań naukowych i innowacji w celu **formalnej i nieformalnej** standaryzacji i **certyfikacji** technologii cyberbezpieczeństwa, **w połączeniu z istniejącymi pracami i w stosownych przypadkach w ścisłej współpracy z europejskimi organizacjami normalizacyjnymi, jednostkami certyfikującymi i ENISA;**

### Poprawka 88

#### Wniosek dotyczący rozporządzenia

#### Artykuł 4 – akapit 1 – punkt 6 – litera c a (nowa)

Tekst proponowany przez Komisję

ca) **zapewnienie specjalnego wsparcia dla MŚP poprzez ułatwienie im dostępu do wiedzy i szkoleń dzięki dostosowanemu do potrzeb dostępowi do rezultatów prac badawczo-rozwojowych wzmocnianych przez Centrum Kompetencji i sieć w celu zwiększenia konkurencyjności;**

### Poprawka 184

#### Wniosek dotyczący rozporządzenia

#### Artykuł 4 – akapit 1 – punkt 7 – wprowadzenie

Tekst proponowany przez Komisję

7. zacieśnienie współpracy między kręgami cywilnymi i kręgami obronnymi w odniesieniu do technologii i aplikacji podwójnego zastosowania w dziedzinie cyberbezpieczeństwa dzięki wykonywaniu następujących zadań:

Poprawka

7. zacieśnienie współpracy między kręgami cywilnymi i kręgami obronnymi w odniesieniu do technologii i aplikacji podwójnego zastosowania w dziedzinie cyberbezpieczeństwa dzięki wykonywaniu następujących zadań, **reaktywnych i defensywnych technologii, aplikacji i usług cyberobrony;**

Środa, 13 marca 2019 r.

**Poprawka 185****Wniosek dotyczący rozporządzenia****Artykuł 4 – akapit 1 – punkt 8 – wprowadzenie***Tekst proponowany przez Komisję*

8. zwiększanie synergii między wymiarem cywilnym i wymiarem obronnym cyberbezpieczeństwa w odniesieniu do Europejskiego Funduszu Obronnego dzięki wykonywaniu następujących zadań:

*Poprawka*

8. zwiększanie synergii między wymiarem cywilnym i wymiarem obronnym cyberbezpieczeństwa w odniesieniu do Europejskiego Funduszu Obronnego dzięki wykonywaniu następujących zadań, **reaktywnych i defensywnych technologii, aplikacji i usług cyberobrony**:

**Poprawka 89****Wniosek dotyczący rozporządzenia****Artykuł 4 – akapit 1 – punkt 8 – litera b a (nowa)***Tekst proponowany przez Komisję*

*ba) pomaganie i doradzanie Komisji w związku z wdrażaniem rozporządzenia (UE) 2019/XXX [przekształcenie rozporządzenia (WE) nr 428/2009 zgodnie z wnioskiem COM(2016)0616].*

*Poprawka***Poprawka 90****Wniosek dotyczący rozporządzenia****Artykuł 4 – akapit 1 – punkt 8 a (nowy)***Tekst proponowany przez Komisję*

**8a. zapewnianie wkładu w wysiłki Unii mające na celu wzmocnienie współpracy międzynarodowej w zakresie cyberbezpieczeństwa przez:**

- a) ułatwianie udziału Centrum Kompetencji w konferencjach międzynarodowych i organizacjach rządowych, jak również udziału w pracach międzynarodowych organizacji normalizacyjnych;
- b) współpracę z państwami trzecimi i organizacjami międzynarodowymi w odpowiednich ramach współpracy międzynarodowej.

*Poprawka*

Środa, 13 marca 2019 r.

### Poprawka 91

#### Wniosek dotyczący rozporządzenia

##### Artykuł 5 – nagłówek

Tekst proponowany przez Komisję

Inwestowanie w infrastrukturę, możliwości, produkty lub **rozwiązania** oraz ich wykorzystanie

Poprawka

Inwestowanie w infrastrukturę, możliwości, produkty lub **procesy** oraz ich wykorzystanie

### Poprawka 92

#### Wniosek dotyczący rozporządzenia

##### Artykuł 5 – ustęp 1 – wprowadzenie

Tekst proponowany przez Komisję

1. W przypadku gdy Centrum Kompetencji zapewnia finansowanie infrastruktury, możliwości, produktów lub **rozwiązań** zgodnie z art. 4 ust. 3 i 4 w formie dotacji lub nagrody, w planie prac Centrum Kompetencji mogą być określone w szczególności:

Poprawka

1. W przypadku gdy Centrum Kompetencji zapewnia finansowanie infrastruktury, możliwości, produktów lub **procesów** zgodnie z art. 4 ust. 3 i 4 w formie **zamówień**, dotacji lub nagrody, w planie prac Centrum Kompetencji mogą być określone w szczególności:

### Poprawka 93

#### Wniosek dotyczący rozporządzenia

##### Artykuł 5 – ustęp 1 – litera a

Tekst proponowany przez Komisję

a) zasady dotyczące funkcjonowania infrastruktury lub możliwości, w tym w stosownych przypadkach dotyczące powierzenia obsługi podmiotowi zajmującemu się hostingiem, w oparciu o kryteria, które określa Centrum Kompetencji;

Poprawka

a) **szczegółowe** zasady dotyczące funkcjonowania infrastruktury lub możliwości, w tym w stosownych przypadkach dotyczące powierzenia obsługi podmiotowi zajmującemu się hostingiem, w oparciu o kryteria, które określa Centrum Kompetencji;

### Poprawka 94

#### Wniosek dotyczący rozporządzenia

##### Artykuł 5 – ustęp 1 – litera b a (nowa)

Tekst proponowany przez Komisję

Poprawka

**ba) szczegółowe przepisy regulujące różne fazy wdrażania;**

Środa, 13 marca 2019 r.

## Poprawka 95

## Wniosek dotyczący rozporządzenia

## Artykuł 5 – ustęp 1 – litera b b (nowa)

Tekst proponowany przez Komisję

Poprawka

*bb) zasada, aby w wyniku wkładu Unii dostęp był otwarty w największym możliwym zakresie, a zamknięty tylko w koniecznym i aby możliwe było ponowne wykorzystanie.*

## Poprawka 96

## Wniosek dotyczący rozporządzenia

## Artykuł 5 – ustęp 2

Tekst proponowany przez Komisję

Poprawka

2. Centrum Kompetencji może być odpowiedzialne za ogólne wykonanie odpowiednich działań związanych ze wspólnym udzielaniem zamówień, w tym za przedkomercyjne zamówienia publiczne w imieniu członków sieci, **członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa lub innych osób trzecich reprezentujących użytkowników produktów i rozwiązań w dziedzinie cyberbezpieczeństwa**. W tym celu Centrum Kompetencji może być wspierane przez co najmniej jeden krajowy ośrodek koordynacji **lub** członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa.

2. Centrum Kompetencji może być odpowiedzialne za ogólne wykonanie odpowiednich działań związanych ze wspólnym udzielaniem zamówień, w tym za przedkomercyjne zamówienia publiczne w imieniu członków sieci. W tym celu Centrum Kompetencji może być wspierane przez co najmniej jeden krajowy ośrodek koordynacji, członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa **lub odpowiednie europejskie centra innowacji cyfrowych**.

## Poprawka 97

## Wniosek dotyczący rozporządzenia

## Artykuł 6 – ustęp - 1 (nowy)

Tekst proponowany przez Komisję

Poprawka

**-1. W każdym państwie członkowskim ustanawia się jeden krajowy ośrodek koordynacji.**



Środa, 13 marca 2019 r.

### Poprawka 98

#### Wniosek dotyczący rozporządzenia

##### Artykuł 6 – ustęp 4

Tekst proponowany przez Komisję

4. Wyznaczony krajowy ośrodek koordynacji posiada możliwość wspierania Centrum Kompetencji oraz sieci w wypełnianiu ich misji określonej w art. 3 niniejszego rozporządzenia. Ośrodki dysponują techniczną wiedzą fachową w dziedzinie cyberbezpieczeństwa lub bezpośrednim dostępem do niej oraz mają możliwość skutecznego angażowania przemysłu, sektora publicznego i społeczności badawczej i współpracy z nimi.

Poprawka

4. Wyznaczony krajowy ośrodek koordynacji posiada możliwość wspierania Centrum Kompetencji oraz sieci w wypełnianiu ich misji określonej w art. 3 niniejszego rozporządzenia. Ośrodki dysponują techniczną wiedzą fachową w dziedzinie cyberbezpieczeństwa lub bezpośrednim dostępem do niej oraz mają możliwość skutecznego angażowania przemysłu, sektora publicznego, **środowiska akademickiego** i społeczności badawczej **oraz obywateli** i współpracy z nimi. **Komisja wydaje wytyczne zawierające informacje szczegółowe na temat procedury oceny i wyjaśniające zastosowanie kryteriów.**

### Poprawka 99

#### Wniosek dotyczący rozporządzenia

##### Artykuł 6 – ustęp 5

Tekst proponowany przez Komisję

5. Relacje między Centrum Kompetencji i krajowymi ośrodkami koordynacji opierają się na umowach podpisanych między Centrum Kompetencji i każdym z krajowych ośrodków koordynacji. **W umowie określa** się reguły dotyczące relacji między Centrum Kompetencji i każdym z krajowych ośrodków koordynacji oraz podziału zadań między nimi.

Poprawka

5. Relacje między Centrum Kompetencji i krajowymi ośrodkami koordynacji opierają się na **standardowych** umowach podpisanych między Centrum Kompetencji i każdym z krajowych ośrodków koordynacji. **Umowa zawiera ten sam zestaw zharmonizowanych ogólnych warunków określających** reguły dotyczące relacji między Centrum Kompetencji i każdym z krajowych ośrodków koordynacji oraz podziału zadań między nimi, **a także warunki szczególne dostosowane do specyfiki danego krajowego ośrodka koordynacji.**

### Poprawka 100

#### Wniosek dotyczący rozporządzenia

##### Artykuł 6 – ustęp 5 a (nowy)

Tekst proponowany przez Komisję

Poprawka

5a. **Komisja przyjmuje, zgodnie z art. 45a, akty delegowane w celu uzupełnienia niniejszego rozporządzenia przez ustanowienie zharmonizowanych ogólnych warunków umownych, o których mowa w ust. 5 niniejszego artykułu, w tym ich formatu.**

Środa, 13 marca 2019 r.

**Poprawka 101****Wniosek dotyczący rozporządzenia****Artykuł 7 – ustęp 1 – litera a**

---

*Tekst proponowany przez Komisję*

- a) wspieranie Centrum Kompetencji w osiągnięciu jego celów, a w szczególności w koordynowaniu działań środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa;

---

*Poprawka*

- a) wspieranie Centrum Kompetencji w osiągnięciu jego celów, a w szczególności w **ustanawianiu i** koordynowaniu działań środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa;

**Poprawka 102****Wniosek dotyczący rozporządzenia****Artykuł 7 – ustęp 1 – litera b**

---

*Tekst proponowany przez Komisję*

- b) ułatwianie przemysłowi i innym podmiotom na szczeblu państwa członkowskiego udziału w projektach transgranicznych;

---

*Poprawka*

- b) ułatwianie **społeczeństwu obywatelskiemu**, przemysłowi, **w szczególności przedsiębiorstwom typu start-up i MŚP, społeczności akademickiej i badawczej oraz** innym podmiotom na szczeblu państwa członkowskiego udziału w projektach transgranicznych **oraz promowanie go i zachęcanie do niego**;

**Poprawka 103****Wniosek dotyczący rozporządzenia****Artykuł 7 – ustęp 1 – litera b a (nowa)**

---

*Tekst proponowany przez Komisję*

---

*Poprawka*

- ba) **funkcjonowanie – we współpracy z innymi podmiotami realizującymi podobne zadania – jako punkt kompleksowej obsługi w zakresie produktów i procesów w dziedzinie cyberbezpieczeństwa finansowanych w ramach innych programów unijnych, takich jak InvestEU lub program na rzecz jednolitego rynku, w szczególności w przypadku MŚP;**

Środa, 13 marca 2019 r.

**Poprawka 104****Wniosek dotyczący rozporządzenia****Artykuł 7 – ustęp 1 – litera c***Tekst proponowany przez Komisję*

c) udział wspólnie z Centrum Kompetencji w określaniu i eliminowaniu **stojących przed przemysłem** wyzwań w dziedzinie cyberbezpieczeństwa, które dotyczą konkretnych sektorów;

*Poprawka*

c) udział wspólnie z Centrum Kompetencji w określaniu i eliminowaniu wyzwań w dziedzinie cyberbezpieczeństwa, które dotyczą konkretnych sektorów;

**Poprawka 105****Wniosek dotyczący rozporządzenia****Artykuł 7 – ustęp 1 – litera c a (nowa)***Tekst proponowany przez Komisję**Poprawka*

ca) **przewodzenie ścisłej współpracy z krajowymi organizacjami normalizacyjnymi w celu wsparcia absorpcji istniejących norm i zaangażowania wszystkich zainteresowanych stron, w szczególności MŚP, w ustalanie nowych norm;**

**Poprawka 106****Wniosek dotyczący rozporządzenia****Artykuł 7 – ustęp 1 – litera e***Tekst proponowany przez Komisję**Poprawka*

e) dążenie do tworzenia synergii z odpowiednimi działaniami na szczeblu krajowym **i** regionalnym;

e) dążenie do tworzenia synergii z odpowiednimi działaniami na szczeblu krajowym, regionalnym **i lokalnym;**

**Poprawka 107****Wniosek dotyczący rozporządzenia****Artykuł 7 – ustęp 1 – litera f a (nowa)***Tekst proponowany przez Komisję**Poprawka*

fa) **promowanie i rozpowszechnianie wspólnych minimalnych programów nauczania w dziedzinie cyberbezpieczeństwa we współpracy z właściwymi organami w państwach członkowskich;**

Środa, 13 marca 2019 r.

**Poprawka 108****Wniosek dotyczący rozporządzenia****Artykuł 7 – ustęp 1 – litera g**

---

*Tekst proponowany przez Komisję*

g) promowanie i rozpowszechnianie przez sieć, środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa i Centrum Kompetencji odpowiednich wyników prac na szczeblu krajowym **i** regionalnym;

---

*Poprawka*

g) promowanie i rozpowszechnianie przez sieć, środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa i Centrum Kompetencji odpowiednich wyników prac na szczeblu krajowym, regionalnym **lub lokalnym**;

**Poprawka 109****Wniosek dotyczący rozporządzenia****Artykuł 7 – ustęp 1 – litera h**

---

*Tekst proponowany przez Komisję*

h) ocena wniosków o włączenie do środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa składanych przez podmioty mające siedzibę w tym samym państwie członkowskim co ośrodek koordynacji.

---

*Poprawka*

h) ocena wniosków o włączenie do środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa składanych przez podmioty **i osoby fizyczne** mające siedzibę **lub zamieszkałe** w tym samym państwie członkowskim co ośrodek koordynacji.

**Poprawka 110****Wniosek dotyczący rozporządzenia****Artykuł 7 – ustęp 4**

---

*Tekst proponowany przez Komisję*

4. W stosownych przypadkach krajowe ośrodki koordynacji współpracują za pośrednictwem sieci w celu realizacji zadań, o których mowa w ust. 1 **lit. a), b), c), e) i g)**.

---

*Poprawka*

4. W stosownych przypadkach krajowe ośrodki koordynacji współpracują w ramach sieci **i z właściwymi europejskimi centrami innowacji cyfrowych** w celu realizacji zadań, o których mowa w ust. 1.

Środa, 13 marca 2019 r.

**Poprawka 111**  
**Wniosek dotyczący rozporządzenia**  
**Artykuł 8 – ustęp 1**

*Tekst proponowany przez Komisję*

1. Środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa wnosi swój wkład w misję Centrum Kompetencji, jak określono w art. 3, oraz wzmacnia i rozpowszechnia wiedzę fachową z zakresu cyberbezpieczeństwa w całej Unii.

*Poprawka*

1. Środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa wnosi swój wkład w misję Centrum Kompetencji, jak określono w art. 3, oraz wzmacnia, **gromadzi, udostępnia** i rozpowszechnia wiedzę fachową z zakresu cyberbezpieczeństwa w całej Unii, **a także zapewnia techniczną wiedzę fachową.**

**Poprawka 112**  
**Wniosek dotyczący rozporządzenia**  
**Artykuł 8 – ustęp 2**

*Tekst proponowany przez Komisję*

2. W skład środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa wchodzi **organizacje** przemysłowe, akademickie i **organizacje** naukowe **non-profit, a także stowarzyszenia** oraz podmioty publiczne i inne podmioty zajmujące się kwestiami operacyjnymi i technicznymi. Środowisko to skupia główne zainteresowane strony, jeżeli chodzi o technologiczne i **przemysłowe** zdolności w dziedzinie cyberbezpieczeństwa w Unii. W jego skład wchodzi krajowe ośrodki koordynacji, a także unijne instytucje i organy posiadające odpowiednią wiedzę fachową.

*Poprawka*

2. W skład środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa wchodzi **społeczeństwo obywatelskie, środowisko** przemysłowe **po stronie zarówno popytu, jak i podaży, w tym MŚP, środowisko** akademickie i naukowe, **stowarzyszenia użytkowników, indywidualni eksperci, właściwe europejskie organizacje normalizacyjne** oraz **inne stowarzyszenia, a także** podmioty publiczne i inne podmioty zajmujące się kwestiami operacyjnymi i technicznymi **w obszarze cyberbezpieczeństwa.** Środowisko to skupia główne zainteresowane strony, jeżeli chodzi o technologiczne, **przemysłowe, akademickie i naukowe oraz społeczne** zdolności **i możliwości** w dziedzinie cyberbezpieczeństwa w Unii, **a** w jego skład wchodzi krajowe ośrodki koordynacji, **europejskie centra innowacji cyfrowych,** a także unijne instytucje i organy posiadające odpowiednią wiedzę fachową, **zgodnie z art. 10 niniejszego rozporządzenia.**

Środa, 13 marca 2019 r.

**Poprawka 113****Wniosek dotyczący rozporządzenia****Artykuł 8 – ustęp 3 – wprowadzenie**

---

*Tekst proponowany przez Komisję*

3. Jako członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa można akredytować jedynie podmioty, które mają siedzibę w Unii. **Podmioty te** muszą wykazać, że **dysponują wiedzą** fachową z zakresu cyberbezpieczeństwa w co najmniej jednej z następujących dziedzin:

---

*Poprawka*

3. Jako członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa można akredytować jedynie podmioty **i osoby fizyczne**, które mają siedzibę **lub miejsce zamieszkania** w Unii, **na terenie Europejskiego Obszaru Gospodarczego (EOG) lub Europejskiego Stowarzyszenia Wolnego Handlu**. **Wnioskodawcy** muszą wykazać, że **mogą zapewnić wiedzę** fachową z zakresu cyberbezpieczeństwa w co najmniej jednej z następujących dziedzin:

**Poprawka 114****Wniosek dotyczący rozporządzenia****Artykuł 8 – ustęp 3 – litera a**

---

*Tekst proponowany przez Komisję*

a) **badania** naukowe;

---

*Poprawka*

a) **środowisko akademickie lub badania** naukowe;

**Poprawka 115****Wniosek dotyczący rozporządzenia****Artykuł 8 – ustęp 3 – litera c a (nowa)**

---

*Tekst proponowany przez Komisję*

---

*Poprawka*

**ca) etyka;**

Środa, 13 marca 2019 r.

**Poprawka 116****Wniosek dotyczący rozporządzenia****Artykuł 8 – ustęp 3 – litera c b (nowa)**

Tekst proponowany przez Komisję

Poprawka

*cb) formalna i techniczna standaryzacja oraz specyfikacje.***Poprawka 117****Wniosek dotyczący rozporządzenia****Artykuł 8 – ustęp 4**

Tekst proponowany przez Komisję

Poprawka

4. Centrum Kompetencji akredytuje podmioty ustanowione na mocy prawa krajowego jako członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa po przeprowadzeniu przez krajowy ośrodek koordynacji państwa członkowskiego, w którym ma siedzibę dany podmiot, oceny, czy podmiot ten spełnia kryteria określone w ust. 3. Akredytacja nie jest ograniczona czasowo, ale Centrum Kompetencji może ją w każdym momencie cofnąć, jeżeli samo Centrum lub właściwy krajowy ośrodek koordynacji uzna, że podmiot nie spełnia kryteriów określonych w ust. 3 lub podlega odpowiednim przepisom określonym w art. 136 rozporządzenia XXX [nowe rozporządzenie finansowe].

4. Centrum Kompetencji akredytuje podmioty ustanowione na mocy prawa krajowego **lub osoby fizyczne** jako członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa po przeprowadzeniu przez **Centrum Kompetencji**, krajowy ośrodek koordynacji państwa członkowskiego, w którym ma siedzibę dany podmiot **lub w którym zamieszkuje osoba fizyczna, zharmonizowanej** oceny, czy podmiot ten spełnia kryteria określone w ust. 3. Akredytacja nie jest ograniczona czasowo, ale Centrum Kompetencji może ją w każdym momencie cofnąć, jeżeli samo Centrum lub właściwy krajowy ośrodek koordynacji uzna, że podmiot **lub osoba fizyczna** nie spełnia kryteriów określonych w ust. 3 lub podlega odpowiednim przepisom określonym w art. 136 rozporządzenia XXX [nowe rozporządzenie finansowe]. **Krajowe ośrodki koordynacji państw członkowskich dążą do osiągnięcia równoważonej reprezentacji zainteresowanych stron w środowisku, aktywnie stymulując uczestnictwo w niewystarczająco reprezentowanych kategoriach, szczególnie MŚP, i grupach osób fizycznych.**

**Poprawka 118****Wniosek dotyczący rozporządzenia****Artykuł 8 – ustęp 4 a (nowy)**

Tekst proponowany przez Komisję

Poprawka

**4a. Komisja przyjmuje akty delegowane zgodnie z art. 45a, aby uzupełnić niniejsze rozporządzenie dzięki dokładniejszemu określeniu kryteriów, o których mowa w ust. 3 niniejszego artykułu i na podstawie których wnioskodawcy są wybierani, oraz procedury oceny i akredytacji jednostek, które spełniają kryteria określone w ust. 4 niniejszego artykułu.**

Środa, 13 marca 2019 r.

## Poprawka 119

## Wniosek dotyczący rozporządzenia

## Artykuł 9 – akapit 1 – punkt 5 a (nowy)

Tekst proponowany przez Komisję

Poprawka

5a) *wspierają Centrum Kompetencji dzięki zgłaszaniu i ujawnianiu luk w zabezpieczeniach, pomocy w ich łagodzeniu i doradzaniu w zakresie eliminowania takich słabych punktów, w tym poprzez certyfikację w ramach systemów przyjętych zgodnie z rozporządzeniem (UE) 2019/XXX [akt ws. cyberbezpieczeństwa].*

## Poprawka 120

## Wniosek dotyczący rozporządzenia

## Artykuł 10 – ustęp 1

Tekst proponowany przez Komisję

Poprawka

1. Centrum Kompetencji współpracuje z odpowiednimi instytucjami, organami, urzędami i agencjami Unii, w tym z **Agencją Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji**, z zespołem reagowania na incydenty komputerowe (CERT-UE), Europejską Służbą Działań Zewnętrznych, ze Wspólnym Centrum Badawczym Komisji, Agencją Wykonawczą ds. Badań Naukowych, Agencją Wykonawczą ds. Innowacyjności i Sieci, Europejskim Centrum ds. Walki z Cyberprzestępczością w Europolu oraz z Europejską Agencją Obrony.

1. ***W celu zapewnienia spójności i komplementarności*** Centrum Kompetencji współpracuje z odpowiednimi instytucjami, organami, urzędami i agencjami Unii, w tym **ENISA**, z zespołem reagowania na incydenty komputerowe (CERT-UE), Europejską Służbą Działań Zewnętrznych, ze Wspólnym Centrum Badawczym Komisji, Agencją Wykonawczą ds. Badań Naukowych, Agencją Wykonawczą ds. Innowacyjności i Sieci, **odpowiednimi europejskimi centrami innowacji cyfrowych**, Europejskim Centrum ds. Walki z Cyberprzestępczością w Europolu oraz z Europejską Agencją Obrony **w odniesieniu do projektów, usług i kompetencji podwójnego zastosowania.**

## Poprawka 121

## Wniosek dotyczący rozporządzenia

## Artykuł 10 – ustęp 2

Tekst proponowany przez Komisję

Poprawka

2. Taka współpraca ma miejsce w ramach uzgodnień roboczych. Uzgodnienia te **należy uprzednio przedłożyć do zatwierdzenia** przez Komisję.

2. Taka współpraca ma miejsce w ramach uzgodnień roboczych. Uzgodnienia te **przyjmuje Rada Zarządzająca po uprzednim zatwierdzeniu** przez Komisję.



Środa, 13 marca 2019 r.

### Poprawka 122

#### Wniosek dotyczący rozporządzenia

##### Artykuł 12 – ustęp 1

Tekst proponowany przez Komisję

1. W skład Rady Zarządzającej wchodzi po jednym przedstawicielu każdego państwa członkowskiego oraz **pięciu** przedstawicieli Komisji w imieniu Unii.

Poprawka

1. W skład Rady Zarządzającej wchodzi po jednym przedstawicielu każdego państwa członkowskiego, **jeden przedstawiciel wyznaczony przez Parlament Europejski do roli obserwatora** oraz **czterech** przedstawicieli Komisji w imieniu Unii, **przy czym dąży się do zachowania równowagi płci wśród członków Rady i ich zastępców.**

### Poprawka 123

#### Wniosek dotyczący rozporządzenia

##### Artykuł 12 – ustęp 3

Tekst proponowany przez Komisję

3. Członków Rady Zarządzającej i ich zastępców powołuje się, biorąc pod uwagę ich wiedzę z dziedziny **technologii**, a także odpowiednie umiejętności kierownicze, administracyjne i w zakresie zarządzania budżetem. Komisja oraz państwa członkowskie dokładają starań, aby ograniczyć rotację swoich przedstawicieli w Radzie Zarządzającej w celu zapewnienia ciągłości pracy Rady. Komisja oraz państwa członkowskie mają na celu osiągnięcie zrównoważonej reprezentacji mężczyzn i kobiet w Radzie Zarządzającej.

Poprawka

3. Członków Rady Zarządzającej i ich zastępców powołuje się, biorąc pod uwagę ich wiedzę z dziedziny **cyberbezpieczeństwa**, a także odpowiednie umiejętności kierownicze, administracyjne i w zakresie zarządzania budżetem. Komisja oraz państwa członkowskie dokładają starań, aby ograniczyć rotację swoich przedstawicieli w Radzie Zarządzającej w celu zapewnienia ciągłości pracy Rady. Komisja oraz państwa członkowskie mają na celu osiągnięcie zrównoważonej reprezentacji mężczyzn i kobiet w Radzie Zarządzającej.

### Poprawka 124

#### Wniosek dotyczący rozporządzenia

##### Artykuł 12 – ustęp 6

Tekst proponowany przez Komisję

6. **Komisja** może, w stosownych przypadkach, zapraszać obserwatorów, w tym przedstawicieli odpowiednich unijnych organów, urzędów i agencji, do udziału w posiedzeniach Rady Zarządzającej.

Poprawka

6. **Rada Zarządzająca** może, w stosownych przypadkach, zapraszać obserwatorów, w tym przedstawicieli odpowiednich unijnych organów, urzędów i agencji, **a także członków środowiska**, do udziału w posiedzeniach Rady Zarządzającej.

Środa, 13 marca 2019 r.

**Poprawka 125****Wniosek dotyczący rozporządzenia****Artykuł 12 – ustęp 7**

Tekst proponowany przez Komisję

7. **Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) jest stałym obserwatorem** w Radzie Zarządzającej.

Poprawka

7. ENISA oraz Rada Konsultacyjna ds. Przemysłowych i Naukowych są stałymi obserwatorami w Radzie Zarządzającej, zapewniając doradztwo bez prawa głosu. Rada Zarządzająca w najwyższym stopniu uwzględnia opinie wyrażone przez stałych obserwatorów.

**Poprawka 126****Wniosek dotyczący rozporządzenia****Artykuł 13 – ustęp 3 – litera a**

Tekst proponowany przez Komisję

a) przyjmuje wieloletni plan strategiczny obejmujący zestawienie głównych priorytetów oraz planowanych inicjatyw Centrum Kompetencji, w tym oszacowanie potrzeb finansowych i źródeł finansowania;

Poprawka

a) przyjmuje wieloletni plan strategiczny obejmujący zestawienie głównych priorytetów oraz planowanych inicjatyw Centrum Kompetencji, w tym oszacowanie potrzeb finansowych i źródeł finansowania, **uwzględniając doradztwo ENISA;**

**Poprawka 127****Wniosek dotyczący rozporządzenia****Artykuł 13 – ustęp 3 – litera b**

Tekst proponowany przez Komisję

b) na podstawie wniosku dyrektora wykonawczego przyjmuje plan prac Centrum Kompetencji, roczne sprawozdanie finansowe i bilans oraz roczne sprawozdanie z działalności;

Poprawka

b) na podstawie wniosku dyrektora wykonawczego przyjmuje plan prac Centrum Kompetencji, roczne sprawozdanie finansowe i bilans oraz roczne sprawozdanie z działalności, **uwzględniając doradztwo ENISA;**

**Poprawka 128****Wniosek dotyczący rozporządzenia****Artykuł 13 – ustęp 3 – litera e**

Tekst proponowany przez Komisję

e) przyjmuje **kryteria i** procedury oceny i akredytacji podmiotów jako członków środowiska **posiadającego kompetencje w dziedzinie cyberbezpieczeństwa;**

Poprawka

e) przyjmuje procedury oceny i akredytacji podmiotów jako członków środowiska;

Środa, 13 marca 2019 r.

**Poprawka 129**

**Wniosek dotyczący rozporządzenia  
Artykuł 13 – ustęp 3 – litera e a (nowa)**

Tekst proponowany przez Komisję

Poprawka

*ea) przyjmuje uzgodnienia robocze, o których mowa w art. 10 ust. 2;*

**Poprawka 130**

**Wniosek dotyczący rozporządzenia  
Artykuł 13 – ustęp 3 – litera g a (nowa)**

Tekst proponowany przez Komisję

Poprawka

*ga) przyjmuje dla Centrum Kompetencji przepisy dotyczące przejrzystości;*

**Poprawka 131**

**Wniosek dotyczący rozporządzenia  
Artykuł 13 – ustęp 3 – litera i**

Tekst proponowany przez Komisję

Poprawka

*i) ustanawia grupy robocze złożone z członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa;*

*i) ustanawia grupy robocze złożone z członków środowiska, uwzględniając doradztwo stałych obserwatorów;*

**Poprawka 132**

**Wniosek dotyczący rozporządzenia  
Artykuł 13 – ustęp 3 – litera l**

Tekst proponowany przez Komisję

Poprawka

*l) promuje Centrum Kompetencji w skali globalnej, aby zwiększyć jego atrakcyjność i uczynić z niego światowej klasy podmiot doskonałości w dziedzinie cyberbezpieczeństwa;*

*l) promuje współpracę Centrum Kompetencji z globalnymi podmiotami;*

Środa, 13 marca 2019 r.

## Poprawka 133

## Wniosek dotyczący rozporządzenia

## Artykuł 13 – ustęp 3 – litera r

Tekst proponowany przez Komisję

- r) przyjmuje strategię zwalczania nadużyć finansowych, **która jest proporcjonalna** do istniejących w tym zakresie zagrożeń, **uwzględniając analizę** kosztów i **korzyści w odniesieniu do** środków, które mają zostać wdrożone;

Poprawka

- r) przyjmuje strategię zwalczania nadużyć finansowych i **korupcji, proporcjonalną** do istniejących w tym zakresie zagrożeń, z **uwzględnieniem analizy** kosztów i **korzyści** środków, które mają zostać wdrożone, **jak również przyjmuje kompleksowe środki ochrony osób zgłaszających przypadki naruszenia prawa Unii zgodnie z mającym zastosowanie ustawodawstwem Unii;**

## Poprawka 134

## Wniosek dotyczący rozporządzenia

## Artykuł 13 – ustęp 3 – litera s

Tekst proponowany przez Komisję

- s) przyjmuje metodę obliczania **wkładu finansowego** państw członkowskich;

Poprawka

- s) przyjmuje **wyczerpującą definicję wkładów finansowych państw członkowskich oraz** metodę obliczania **kwoty dobrowolnych wkładów** państw członkowskich, **które mogą być rozliczane jako wkłady finansowe zgodnie z tą definicją; takie obliczenia przeprowadza się na koniec każdego roku budżetowego;**

## Poprawka 135

## Wniosek dotyczący rozporządzenia

## Artykuł 14 – ustęp 1

Tekst proponowany przez Komisję

1. Rada Zarządzająca wybiera na okres dwóch lat przewodniczącego i zastępcę przewodniczącego spośród tych członków, którzy mają prawo głosu. Kadencję przewodniczącego i zastępcy przewodniczącego można jednokrotnie przedłużyć na podstawie decyzji Rady Zarządzającej. Jeżeli jednak w dowolnym momencie swojej kadencji stracą oni status członka Rady Zarządzającej, kadencja ich kończy się automatycznie w tym samym dniu. Zastępca przewodniczącego zastępuje z urzędu przewodniczącego, jeżeli przewodniczący nie jest w stanie pełnić swoich obowiązków. Przewodniczący bierze udział w głosowaniu.

Poprawka

1. Rada Zarządzająca, **starając się zachować równowagę płci,** wybiera na okres dwóch lat przewodniczącego i zastępcę przewodniczącego spośród tych członków, którzy mają prawo głosu. Kadencję przewodniczącego i zastępcy przewodniczącego można jednokrotnie przedłużyć na podstawie decyzji Rady Zarządzającej. Jeżeli jednak w dowolnym momencie swojej kadencji stracą oni status członka Rady Zarządzającej, kadencja ich kończy się automatycznie w tym samym dniu. Zastępca przewodniczącego zastępuje z urzędu przewodniczącego, jeżeli przewodniczący nie jest w stanie pełnić swoich obowiązków. Przewodniczący bierze udział w głosowaniu.

Środa, 13 marca 2019 r.

### Poprawka 136

#### Wniosek dotyczący rozporządzenia

##### Artykuł 14 – ustęp 3

Tekst proponowany przez Komisję

3. Dyrektor wykonawczy ma prawo uczestniczenia w obradach, o ile Rada Zarządzająca nie postanowi inaczej, lecz bez prawa głosu. **Rada Zarządzająca może zapraszać na poszczególne posiedzenia również inne osoby w charakterze obserwatorów.**

Poprawka

3. Dyrektor wykonawczy ma prawo uczestniczenia w obradach, o ile Rada Zarządzająca nie postanowi inaczej, lecz bez prawa głosu.

### Poprawka 137

#### Wniosek dotyczący rozporządzenia

##### Artykuł 14 – ustęp 4

Tekst proponowany przez Komisję

4. Członkowie Rady Konsultacyjnej ds. Przemysłowych i Naukowych mogą brać udział w posiedzeniach Rady Zarządzającej, na zaproszenie przewodniczącego, bez prawa głosu.

Poprawka

skreśla się

### Poprawka 138

#### Wniosek dotyczący rozporządzenia

##### Artykuł 15

Tekst proponowany przez Komisję

##### Artykuł 15

#### Zasady głosowania Rady Zarządzającej

1. Unia posiada 50 % praw głosu. Głosy Unii są niepodzielne.

2. Każde uczestniczące państwo członkowskie posiada jeden głos.

3. Rada Zarządzająca podejmuje decyzje większością co najmniej 75 % wszystkich głosów, w tym głosów członków nieobecnych, reprezentujących co najmniej 75 % całkowitych wkładów finansowych na rzecz Centrum Kompetencji. Wkład finansowy oblicza się na podstawie zaproponowanych przez państwa członkowskie szacowanych wydatków, o których mowa w art. 17 ust. 2 lit. c), oraz na podstawie sprawozdania na temat wartości wkładów uczestniczących państw członkowskich, o którym mowa w art. 22 ust. 5.

Poprawka

skreśla się

Środa, 13 marca 2019 r.

Tekst proponowany przez Komisję

Poprawka

4. *Jedynie przedstawiciele Komisji i przedstawiciele uczestniczących państw członkowskich posiadają prawo głosu.*

5. *Przewodniczący bierze udział w głosowaniu.*

### Poprawka 139

#### Wniosek dotyczący rozporządzenia

#### Artykuł 15 a (nowy)

Tekst proponowany przez Komisję

Poprawka

#### Artykuł 15a

##### Zasady głosowania Rady Zarządzającej

1. *Decyzje poddawane pod głosowanie mogą dotyczyć:*
  - a) *zarządzania i organizacji Centrum Kompetencji i sieci;*
  - b) *przydziału środków budżetowych na rzecz Centrum Kompetencji i sieci;*
  - c) *wspólnych działań szeregu państw członkowskich, z ewentualnym wkładem z budżetu Unii zgodnie z decyzją o przydziale, o której mowa w lit. b).*
2. *Rada Zarządzająca podejmuje decyzje większością co najmniej 75 % głosów wszystkich członków. Głosy Unii, która reprezentowana jest przez Komisję, są niepodzielne.*
3. *W przypadku decyzji, o których mowa w ust. 1 lit. a), każde państwo członkowskie jest reprezentowane i posiada takie same równe prawa głosu. Jeżeli chodzi o pozostałe głosy (w obrębie puli 100 %), Unia powinna posiadać co najmniej 50 % praw głosu odpowiadających jej wkładowi finansowemu.*
4. *W przypadku decyzji wchodzących w zakres ust. 1 lit. b) lub c) lub jakiegokolwiek innej decyzji nienależącej do żadnej innej kategorii wymienionej w ust. 1 Unia posiada co najmniej 50 % praw głosu odpowiadających jej wkładowi finansowemu. Tylko finansujące państwa członkowskie mają prawo głosu odpowiadające wkładowi finansowemu danego państwa.*
5. *Jeżeli przewodniczący został wybrany spośród przedstawicieli państw członkowskich, przewodniczący bierze udział w głosowaniu jako przedstawiciel swojego państwa członkowskiego.*

Środa, 13 marca 2019 r.

### Poprawka 140

#### Wniosek dotyczący rozporządzenia

##### Artykuł 16 – ustęp 3

Tekst proponowany przez Komisję

3. Rada Zarządzająca w ramach otwartej i **przejrzystej** procedury wyboru mianuje dyrektora wykonawczego z listy kandydatów zaproponowanych przez Komisję.

Poprawka

3. Rada Zarządzająca w ramach otwartej, **przejrzystej** i **niedyskryminującej** procedury wyboru mianuje dyrektora wykonawczego z listy kandydatów zaproponowanych przez Komisję **oraz kandydatur z państw członkowskich zgłoszonych z myślą o zachowaniu równości płci.**

### Poprawka 141

#### Wniosek dotyczący rozporządzenia

##### Artykuł 16 – ustęp 5

Tekst proponowany przez Komisję

5. Kadencja dyrektora wykonawczego trwa **cztery lata**. Przed upływem tego okresu Komisja przeprowadza ocenę, w której uwzględnia ocenę wykonywania zadań przez dyrektora wykonawczego oraz przyszłe zadania i wyzwania Centrum Kompetencji.

Poprawka

5. Kadencja dyrektora wykonawczego trwa **pięć lat**. Przed upływem tego okresu Komisja przeprowadza ocenę, w której uwzględnia ocenę wykonywania zadań przez dyrektora wykonawczego oraz przyszłe zadania i wyzwania Centrum Kompetencji.

### Poprawka 142

#### Wniosek dotyczący rozporządzenia

##### Artykuł 16 – ustęp 6

Tekst proponowany przez Komisję

6. Rada Zarządzająca, działając na wniosek Komisji, w którym uwzględniono ocenę, o której mowa w ust. 5, może przedłużyć kadencję dyrektora wykonawczego jednokrotnie na okres nie dłuższy niż **cztery lata**.

Poprawka

6. Rada Zarządzająca, działając na wniosek Komisji, w którym uwzględniono ocenę, o której mowa w ust. 5, może przedłużyć kadencję dyrektora wykonawczego jednokrotnie na okres nie dłuższy niż **pięć lat**.

Środa, 13 marca 2019 r.

**Poprawka 143****Wniosek dotyczący rozporządzenia****Artykuł 16 – ustęp 8***Tekst proponowany przez Komisję*

8. Dyrektor wykonawczy zostaje odwołany ze stanowiska jedynie na mocy decyzji Rady Zarządzającej działającej na wniosek Komisji.

*Poprawka*

8. Dyrektor wykonawczy zostaje odwołany ze stanowiska jedynie na mocy decyzji Rady Zarządzającej działającej na wniosek **swoich członków lub na wniosek** Komisji.

**Poprawka 144****Wniosek dotyczący rozporządzenia****Artykuł 17 – ustęp 2 – litera c***Tekst proponowany przez Komisję*

c) przygotowuje i przedkłada Radzie Zarządzającej do przyjęcia, po konsultacjach z Radą Zarządzającą i Komisją, projekt wieloletniego planu strategicznego oraz projekt rocznego planu prac Centrum Kompetencji, uwzględniając zakres zaproszeń do składania wniosków, zaproszeń do wyrażenia zainteresowania i zaproszeń do składania ofert potrzebnych do celów realizacji planu prac oraz powiązane szacunki wydatków proponowane przez państwa członkowskie i Komisję;

*Poprawka*

c) przygotowuje i przedkłada Radzie Zarządzającej do przyjęcia, po konsultacjach z Radą Zarządzającą, **Radą Konsultacyjną ds. Przemysłowych i Naukowych, ENISA i** Komisją, projekt wieloletniego planu strategicznego oraz projekt rocznego planu prac Centrum Kompetencji, uwzględniając zakres zaproszeń do składania wniosków, zaproszeń do wyrażenia zainteresowania i zaproszeń do składania ofert potrzebnych do celów realizacji planu prac oraz powiązane szacunki wydatków proponowane przez państwa członkowskie i Komisję;

**Poprawka 145****Wniosek dotyczący rozporządzenia****Artykuł 17 – ustęp 2 – litera h***Tekst proponowany przez Komisję*

h) przygotowuje plan działania w następstwie wniosków z ocen retrospektywnych oraz przedkłada Komisji co dwa lata sprawozdania z postępów;

*Poprawka*

h) przygotowuje plan działania w następstwie wniosków z ocen retrospektywnych oraz przedkłada Komisji **i Parlamentowi Europejskiemu** co dwa lata sprawozdania z postępów;



Środa, 13 marca 2019 r.

### Poprawka 146

#### Wniosek dotyczący rozporządzenia

##### Artykuł 17 – ustęp 2 – litera l

Tekst proponowany przez Komisję

- l) zatwierdza wykaz działań wybranych do finansowania w oparciu o listę rankingową ustaloną przez zespół niezależnych ekspertów;

Poprawka

- l) zatwierdza, **po zasięgnięciu opinii Rady Konsultacyjnej ds. Przemysłowych i Naukowych i ENISA**, wykaz działań wybranych do finansowania w oparciu o listę rankingową ustaloną przez zespół niezależnych ekspertów;

### Poprawka 147

#### Wniosek dotyczący rozporządzenia

##### Artykuł 17 – ustęp 2 – litera s

Tekst proponowany przez Komisję

- s) przygotowuje plan działania na podstawie wniosków ze sprawozdań z kontroli wewnętrznej lub zewnętrznej, a także z dochodzeń przeprowadzanych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF), oraz składa sprawozdania z postępów prac dwa razy w roku Komisji i regularnie Radzie Zarządzającej;

Poprawka

- s) przygotowuje plan działania na podstawie wniosków ze sprawozdań z kontroli wewnętrznej lub zewnętrznej, a także z dochodzeń przeprowadzanych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF), oraz składa sprawozdania z postępów prac dwa razy w roku Komisji i **Parlamentowi Europejskiemu oraz** regularnie Radzie Zarządzającej;

### Poprawka 148

#### Wniosek dotyczący rozporządzenia

##### Artykuł 17 – ustęp 2 – litera v

Tekst proponowany przez Komisję

- v) zapewni skuteczną komunikację z instytucjami Unii;

Poprawka

- v) zapewni skuteczną komunikację z instytucjami Unii **oraz przedstawia sprawozdanie Parlamentowi Europejskiemu i Radzie na wniosek;**

Środa, 13 marca 2019 r.

## Poprawka 149

## Wniosek dotyczący rozporządzenia

## Artykuł 18 – ustęp 1

Tekst proponowany przez Komisję

1. Rada Konsultacyjna ds. Przemysłowych i Naukowych liczy nie więcej niż **16** członków. Członków mianuje Rada Zarządzająca spośród przedstawicieli podmiotów będących częścią środowiska **posiadającego kompetencje w dziedzinie cyberbezpieczeństwa**.

Poprawka

1. Rada Konsultacyjna ds. Przemysłowych i Naukowych liczy nie więcej niż **25** członków. Członków mianuje Rada Zarządzająca spośród przedstawicieli podmiotów będących częścią środowiska **lub poszczególnych członków. Kwalifikują się jedynie przedstawiciele podmiotów, które nie są kontrolowane przez państwo trzecie lub podmioty z państw trzecich, z wyjątkiem państw EOG i EFTA. Mianowanie odbywa się zgodnie z otwartą, przejrzystą i niedyskryminacyjną procedurą. W składzie Rady dąży się do osiągnięcia równowagi płci i zapewnia zrównoważoną reprezentację grup zainteresowanych stron reprezentujących przemysł, środowisko akademickie i społeczeństwo obywatelskie.**

## Poprawka 150

## Wniosek dotyczący rozporządzenia

## Artykuł 18 – ustęp 2

Tekst proponowany przez Komisję

2. Członkowie Rady Konsultacyjnej ds. Przemysłowych i Naukowych posiadają wiedzę fachową albo w dziedzinach badań nad cyberbezpieczeństwem, rozwoju przemysłu, **zawodów regulowanych albo we wdrażaniu rozwiązań w tych obszarach**. Rada Zarządzająca szczegółowo określa wymogi dotyczące takiej wiedzy fachowej.

Poprawka

2. Członkowie Rady Konsultacyjnej ds. Przemysłowych i Naukowych posiadają wiedzę fachową albo w dziedzinach badań nad cyberbezpieczeństwem, rozwoju przemysłu **albo oferowaniu, realizowaniu lub wdrażaniu usług świadczonych w ramach zawodów regulowanych lub produktów z tym związanych**. Rada Zarządzająca szczegółowo określa wymogi dotyczące takiej wiedzy fachowej.

## Poprawka 151

## Wniosek dotyczący rozporządzenia

## Artykuł 18 – ustęp 5

Tekst proponowany przez Komisję

5. Przedstawiciele Komisji oraz **Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji mogą brać udział** w pracach Rady Konsultacyjnej ds. Przemysłowych i Naukowych i **zapewniać im** wsparcie.

Poprawka

5. Przedstawiciele Komisji oraz **ENISA są zapraszani do udziału** w pracach Rady Konsultacyjnej ds. Przemysłowych i Naukowych i **zapewniają jej** wsparcie. **W indywidualnych przypadkach Rada może zaprosić dodatkowych przedstawicieli ze środowiska w charakterze obserwatora, doradców lub ekspertów.**

Środa, 13 marca 2019 r.

### Poprawka 152

#### Wniosek dotyczący rozporządzenia

##### Artykuł 19 – ustęp 1

Tekst proponowany przez Komisję

1. Posiedzenia Rady Konsultacyjnej ds. Przemysłowych i Naukowych odbywają się co najmniej **dwa** razy w roku.

Poprawka

1. Posiedzenia Rady Konsultacyjnej ds. Przemysłowych i Naukowych odbywają się co najmniej **trzy** razy w roku.

### Poprawka 153

#### Wniosek dotyczący rozporządzenia

##### Artykuł 19 – ustęp 2

Tekst proponowany przez Komisję

2. Rada Konsultacyjna ds. Przemysłowych i Naukowych **może doradzać** Radzie Zarządzającej w sprawie tworzenia, w razie potrzeby, grup roboczych ds. konkretnych kwestii istotnych dla pracy Centrum Kompetencji **koordynowanych całościowo** przez co najmniej jednego członka Rady Konsultacyjnej ds. Przemysłowych i Naukowych.

Poprawka

2. Rada Konsultacyjna ds. Przemysłowych i Naukowych **przedstawia wskazówki** Radzie Zarządzającej w sprawie tworzenia, w razie potrzeby, grup roboczych ds. konkretnych kwestii istotnych dla pracy Centrum Kompetencji, **w przypadkach gdy kwestie te wchodzi w zakres zadań i obszarów kompetencji określonych w art. 20 i gdy są konieczne z uwagi na ogólną koordynację** przez co najmniej jednego członka Rady Konsultacyjnej ds. Przemysłowych i Naukowych.

### Poprawka 154

#### Wniosek dotyczący rozporządzenia

##### Artykuł 20 – akapit 1 – wprowadzenie

Tekst proponowany przez Komisję

Rada Konsultacyjna ds. Przemysłowych i Naukowych doradza Centrum Kompetencji w kwestiach dotyczących prowadzenia jego działalności i wykonuje następujące zadania:

Poprawka

Rada Konsultacyjna ds. Przemysłowych i Naukowych **regularnie** doradza Centrum Kompetencji w kwestiach dotyczących prowadzenia jego działalności i wykonuje następujące zadania:

Środa, 13 marca 2019 r.

**Poprawka 155****Wniosek dotyczący rozporządzenia****Artykuł 20 – akapit 1 – punkt 1**

---

*Tekst proponowany przez Komisję*

- 1) zapewnia dyrektorowi wykonawczemu i Radzie Zarządzającej doradztwo strategiczne i **uwagi dotyczące przygotowania** planu prac i wieloletniego planu strategicznego w terminach ustalonych przez Radę Zarządzającą;

---

*Poprawka*

- 1) zapewnia dyrektorowi wykonawczemu i Radzie Zarządzającej doradztwo strategiczne i **wkład we wdrażanie planów przez Centrum Kompetencji, jego ukierunkowanie i działalność w obszarach przemysłu i nauki, a także w przygotowanie** planu prac i wieloletniego planu strategicznego w terminach ustalonych przez Radę Zarządzającą;

**Poprawka 156****Wniosek dotyczący rozporządzenia****Artykuł 20 – akapit 1 – punkt 1 a (nowy)**

---

*Tekst proponowany przez Komisję*

- 1a ) zapewnia doradztwo na rzecz Rady Zarządzającej w zakresie tworzenia grup roboczych zajmujących się szczególnymi kwestiami związanymi z pracą Centrum Kompetencji;**

---

*Poprawka***Poprawka 157****Wniosek dotyczący rozporządzenia****Artykuł 20 – akapit 1 – punkt 3**

---

*Tekst proponowany przez Komisję*

- 3) promuje przesyłanie informacji zwrotnych na temat planu prac i wieloletniego planu strategicznego Centrum Kompetencji oraz je gromadzi.

---

*Poprawka*

- 3) promuje przesyłanie informacji zwrotnych na temat planu prac i wieloletniego planu strategicznego Centrum Kompetencji oraz je gromadzi, **a także doradza Radzie Zarządzającej na temat możliwości poprawy strategicznego ukierunkowania i działania Centrum Kompetencji.**

Środa, 13 marca 2019 r.

### Poprawka 158

#### Wniosek dotyczący rozporządzenia

##### Artykuł 21 – ustęp 1 – litera a

Tekst proponowany przez Komisję

- a) **1 981 668 000** EUR z programu „Cyfrowa Europa”, w tym do wysokości 23 746 000 EUR na pokrycie kosztów administracyjnych;

Poprawka

- a) **1 780 954 875** EUR w cenach z 2018 r. (**1 998 696 000** EUR w cenach bieżących) z programu „Cyfrowa Europa”, w tym do wysokości **21 385 465** EUR w cenach z 2018 r. (23 746 000 EUR w cenach bieżących) na pokrycie kosztów administracyjnych;

### Poprawka 159

#### Wniosek dotyczący rozporządzenia

##### Artykuł 21 – ustęp 1 – litera b a (nowa)

Tekst proponowany przez Komisję

- ba) kwotę pochodzącą z Europejskiego Funduszu Obronnego na działania Centrum Kompetencji związane z obronnością, w tym na koszty administracyjne, takie jak koszty, jakie może ponieść Centrum Kompetencji, gdy występuje w charakterze kierownika projektu w przypadku działań prowadzonych w ramach Europejskiego Funduszu Obronnego.

Poprawka

### Poprawka 160

#### Wniosek dotyczący rozporządzenia

##### Artykuł 21 – ustęp 2

Tekst proponowany przez Komisję

2. Maksymalny wkład Unii wypłaca się ze środków w budżecie ogólnym Unii przeznaczonych na [program „Cyfrowa Europa”] **i na** program szczegółowy służący realizacji programu „Horyzont Europa”, ustanowiony decyzją XXX.

Poprawka

2. Maksymalny wkład Unii wypłaca się ze środków w budżecie ogólnym Unii przeznaczonych na [program „Cyfrowa Europa”], program szczegółowy służący realizacji programu „Horyzont Europa”, ustanowiony decyzją XXX, **Europejski Fundusz Obronny oraz na inne programy i projekty wchodzące w zakres Centrum Kompetencji i sieci.**

Środa, 13 marca 2019 r.

**Poprawka 161****Wniosek dotyczący rozporządzenia****Artykuł 21 – ustęp 4**

---

*Tekst proponowany przez Komisję*

4. Wkład finansowy Unii nie pokrywa zadań, o których mowa w art. 4 ust. 8 lit. b).

---

*Poprawka*

4. Wkład finansowy Unii z **programu „Cyfrowa Europa” i programu „Horyzont Europa”** nie pokrywa zadań, o których mowa w art. 4 ust. 8 lit. b). **Zadania te realizowane są ze środków pochodzących z Europejskiego Funduszu Obronnego.**

**Poprawka 162****Wniosek dotyczący rozporządzenia****Artykuł 22 – ustęp 4**

---

*Tekst proponowany przez Komisję*

4. Komisja może zakończyć, w proporcjonalnym stopniu ograniczyć lub zawiesić wypłacanie wkładu finansowego Unii na rzecz Centrum Kompetencji, jeżeli uczestniczące państwa członkowskie nie wnoszą swojego wkładu, o którym mowa w ust. 1, wnoszą go jedynie częściowo lub **spóźniają się z jego wniesieniem.**

---

*Poprawka*

4. Komisja może zakończyć, w proporcjonalnym stopniu ograniczyć lub zawiesić wypłacanie wkładu finansowego Unii na rzecz Centrum Kompetencji, jeżeli uczestniczące państwa członkowskie nie wnoszą swojego wkładu, o którym mowa w ust. 1, **lub** wnoszą go jedynie częściowo. **Zakończenie, ograniczenie lub zawieszenie przez Komisję wypłacania wkładu finansowego Unii jest proporcjonalne pod względem kwoty i czasu do ograniczenia, zakończenia lub zawieszenia wypłacania wkładów państw członkowskich.**

**Poprawka 163****Wniosek dotyczący rozporządzenia****Artykuł 23 – ustęp 4 – litera a**

---

*Tekst proponowany przez Komisję*

a) wkłady finansowe uczestniczących państw członkowskich na pokrycie kosztów administracyjnych;

---

*Poprawka*

a) wkłady finansowe **Unii i** uczestniczących państw członkowskich na pokrycie kosztów administracyjnych;

Środa, 13 marca 2019 r.

### Poprawka 164

#### Wniosek dotyczący rozporządzenia

##### Artykuł 23 – ustęp 4 – litera b

Tekst proponowany przez Komisję

b) wkłady finansowe uczestniczących państw członkowskich na pokrycie kosztów operacyjnych;

Poprawka

b) wkłady finansowe **Unii i** uczestniczących państw członkowskich na pokrycie kosztów operacyjnych;

### Poprawka 165

#### Wniosek dotyczący rozporządzenia

##### Artykuł 23 – ustęp 8 a (nowy)

Tekst proponowany przez Komisję

Poprawka

**8a. Centrum Kompetencji współpracuje ściśle z innymi instytucjami, agencjami i organami Unii w celu wykorzystania synergii i w odpowiednich przypadkach zmniejszenia kosztów administracyjnych.**

### Poprawka 166

#### Wniosek dotyczący rozporządzenia

##### Artykuł 30 – ustęp 1

Tekst proponowany przez Komisję

1. W trakcie realizacji działań finansowanych na podstawie niniejszego rozporządzenia Centrum Kompetencji stosuje odpowiednie środki w celu zapewnienia ochrony interesów finansowych Unii przeciw nadużyciom finansowym, korupcji i wszelkim innym nielegalnym działaniom, w drodze skutecznych kontroli oraz, w razie wykrycia nieprawidłowości, w drodze odzyskiwania kwot nienależnie wypłaconych, a także, w stosownych przypadkach, skutecznych, proporcjonalnych i odstraszających sankcji administracyjnych.

Poprawka

1. W trakcie realizacji działań finansowanych na podstawie niniejszego rozporządzenia Centrum Kompetencji stosuje odpowiednie środki w celu zapewnienia ochrony interesów finansowych Unii przeciw nadużyciom finansowym, korupcji i wszelkim innym nielegalnym działaniom, w drodze **regularnych i** skutecznych kontroli oraz, w razie wykrycia nieprawidłowości, w drodze odzyskiwania kwot nienależnie wypłaconych, a także, w stosownych przypadkach, skutecznych, proporcjonalnych i odstraszających sankcji administracyjnych.

Środa, 13 marca 2019 r.

## Poprawka 167

## Wniosek dotyczący rozporządzenia

## Artykuł 31 – ustęp 7

Tekst proponowany przez Komisję

7. **Personel Centrum Kompetencji składa się z personelu zatrudnionego** na czas określony **i personelu kontraktowego.**

Poprawka

7. **Centrum Kompetencji dąży do osiągnięcia równowagi płci wśród swojego personelu. W skład personelu wchodzi personel zatrudniony** na czas określony **i personel kontraktowy.**

## Poprawka 168

## Wniosek dotyczący rozporządzenia

## Artykuł 34 – ustęp 2 – litera c a (nowa)

Tekst proponowany przez Komisję

Poprawka

ca) Art. 22 [Własność wyników], art. 23 [Własność wyników] i art. 30 [Stosowanie zasad dotyczących informacji niejawnych] rozporządzenia (UE) 2019/XXX [Europejski Fundusz Obronny] stosuje się do udziału Centrum Kompetencji we wszystkich działaniach związanych z obronnością, o ile zostało to przewidziane w planie prac, a przyznawanie licencji niewyłącznych ogranicza się do osób trzecich z siedzibą w państwach członkowskich lub uznanych za prowadzących działalność w państwach członkowskich i kontrolowanych przez państwa członkowskie lub obywateli państw członkowskich.

## Poprawka 169

## Wniosek dotyczący rozporządzenia

## Artykuł 35 – ustęp 1

Tekst proponowany przez Komisję

1. Centrum Kompetencji wykonuje swoje działania przy zachowaniu **wysokiego** stopnia przejrzystości.

Poprawka

1. Centrum Kompetencji wykonuje swoje działania przy zachowaniu **najwyższego** stopnia przejrzystości.



Środa, 13 marca 2019 r.

### Poprawka 170

#### Wniosek dotyczący rozporządzenia

##### Artykuł 35 – akapit 2

Tekst proponowany przez Komisję

2. Centrum Kompetencji **zapewnia**, aby **społeczeństwo** i wszelkie inne zainteresowane strony otrzymywały odpowiednie, obiektywne, wiarygodne i łatwo dostępne informacje, w szczególności dotyczące wyników **jej pracy**. Centrum Kompetencji podaje również do wiadomości publicznej deklaracje interesów złożone zgodnie z art. 41.

Poprawka

2. Centrum Kompetencji **dopilnowuje**, aby **opinia publiczna** i wszelkie inne zainteresowane strony otrzymywały **w terminie wyczerpujące**, odpowiednie, obiektywne, wiarygodne i łatwo dostępne informacje, w szczególności dotyczące wyników **pracy Centrum Kompetencji, sieci, Rady Konsultacyjnej ds. Przemysłowych i Naukowych oraz środowiska**. Centrum Kompetencji podaje również do wiadomości publicznej deklaracje interesów złożone zgodnie z art. 42.

### Poprawka 171

#### Wniosek dotyczący rozporządzenia

##### Artykuł 38 – ustęp 3

Tekst proponowany przez Komisję

3. Ocena, o której mowa w ust. 2, obejmuje ocenę rezultatów osiągniętych przez Centrum Kompetencji z uwzględnieniem jego celów, mandatu i zadań. Jeżeli Komisja uzna, że kontynuacja prac Centrum Kompetencji jest uzasadniona pod względem jego założonych celów, mandatu i zadań, może zaproponować przedłużenie mandatu Centrum Kompetencji określonego w art. 46.

Poprawka

3. Ocena, o której mowa w ust. 2, obejmuje ocenę rezultatów osiągniętych przez Centrum Kompetencji z uwzględnieniem jego celów, mandatu i zadań, **skuteczności i wydajności**. Jeżeli Komisja uzna, że kontynuacja prac Centrum Kompetencji jest uzasadniona pod względem jego założonych celów, mandatu i zadań, może zaproponować przedłużenie mandatu Centrum Kompetencji określonego w art. 46.

### Poprawka 172

#### Wniosek dotyczący rozporządzenia

##### Artykuł 38 a (nowy)

Tekst proponowany przez Komisję

Poprawka

##### Artykuł 38a

###### Osobowość prawna Centrum Kompetencji

1. Centrum Kompetencji posiada osobowość prawną.
2. We wszystkich państwach członkowskich Centrum Kompetencji ma zdolność prawną o najszerszym zakresie przyznawanym osobom prawnym zgodnie z ustawodawstwem danego państwa członkowskiego. Może ono zwłaszcza nabywać i zbywać nieruchomości i ruchomości oraz być stroną w postępowaniach sądowych.

Środa, 13 marca 2019 r.

**Poprawka 173****Wniosek dotyczący rozporządzenia****Artykuł 42 – akapit 1**

---

*Tekst proponowany przez Komisję*

Rada Zarządzająca Centrum Kompetencji przyjmuje zasady, których celem jest zapobieganie konfliktom interesów i **zarządzanie nimi** w odniesieniu do członków, organów i **personelu Centrum Kompetencji**. **Zasady te zawierają przepisy służące unikaniu konfliktów interesów przez przedstawicieli członków pełniących obowiązki w Radzie Zarządzającej oraz w Radzie Konsultacyjnej ds. Przemysłowych i Naukowych zgodnie z rozporządzeniem XXX [nowe rozporządzenie finansowe].**

---

*Poprawka*

Rada Zarządzająca Centrum Kompetencji przyjmuje zasady, których celem jest zapobieganie konfliktom interesów **oraz ich identyfikacja i eliminowanie** w odniesieniu do członków, organów i **personelu, w tym dyrektora wykonawczego, Rady Zarządzającej, a także Rady Konsultacyjnej ds. Przemysłowych i Naukowych oraz środowiska.**

**Poprawka 174****Wniosek dotyczący rozporządzenia****Artykuł 42 – akapit 1 a (nowy)**

---

*Tekst proponowany przez Komisję*

---

*Poprawka*

**Państwa członkowskie zapewniają zapobieganie konfliktom interesów oraz ich identyfikację i eliminowanie w odniesieniu do krajowych ośrodków koordynacji.**

**Poprawka 175****Wniosek dotyczący rozporządzenia****Artykuł 42 – akapit 1 b (nowy)**

---

*Tekst proponowany przez Komisję*

---

*Poprawka*

**Zasady, o których mowa w akapicie pierwszym, są zgodne z rozporządzeniem (UE, Euratom) 2018/1046.**

**Poprawka 176****Wniosek dotyczący rozporządzenia****Artykuł 44 – nagłówek**

---

*Tekst proponowany przez Komisję*

---

*Poprawka*

Wsparcie ze strony przyjmującego państwa członkowskiego

**Siedziba i** wsparcie ze strony przyjmującego państwa członkowskiego

Środa, 13 marca 2019 r.

### Poprawka 177

#### Wniosek dotyczący rozporządzenia

##### Artykuł 44 – akapit - 1 (nowy)

Tekst proponowany przez Komisję

Poprawka

*Siedzibę Centrum Kompetencji określa się w drodze procedury podlegającej demokratycznej kontroli, na podstawie przejrzystych kryteriów i zgodnie z prawem Unii.*

### Poprawka 178

#### Wniosek dotyczący rozporządzenia

##### Artykuł 44 – akapit - 1 a (nowy)

Tekst proponowany przez Komisję

Poprawka

*Przyjmujące państwo członkowskie zapewnia możliwie najlepsze warunki dla zagwarantowania właściwego funkcjonowania Centrum Kompetencji, w tym jedną lokalizację, a także dodatkowe warunki takie jak dostępność odpowiedniej infrastruktury szkolnej dla dzieci członków personelu, odpowiedni dostęp do rynku pracy, zabezpieczenie społeczne i opiekę zdrowotną zarówno dla dzieci, jak i dla partnerów.*

### Poprawka 179

#### Wniosek dotyczący rozporządzenia

##### Artykuł 44 – akapit 1

Tekst proponowany przez Komisję

Poprawka

Centrum Kompetencji i państwo członkowskie [Belgia], w którym znajduje się jego siedziba, **mogą dokonać** ustaleń administracyjnych w sprawie przywilejów i immunitetów oraz innego wsparcia udzielanego Centrum Kompetencji przez to państwo członkowskie.

Centrum Kompetencji i **przyjmujące** państwo członkowskie, w którym znajduje się jego siedziba, **dokonują** ustaleń administracyjnych w sprawie przywilejów i immunitetów oraz innego wsparcia udzielanego Centrum Kompetencji przez to państwo członkowskie.

Środa, 13 marca 2019 r.

**Poprawka 180**  
**Wniosek dotyczący rozporządzenia**  
**Artykuł 45 a (nowy)**

Tekst proponowany przez Komisję

Poprawka

**Artykuł 45a**

**Wykonywanie przekazanych uprawnień**

1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.
2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 6 ust. 5a i art. 8 ust. 4b, powierza się Komisji na czas nieokreślony od ... [data wejścia w życie rozporządzenia].
3. Przekazanie uprawnień, o którym mowa w art. 6 ust. 5a i art. 8 ust. 4b, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.
4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r.
5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.
6. Akt delegowany przyjęty na podstawie art. 6 ust. 5a i art. 8 ust. 4b wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.