Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego"

[COM(2016) 410 final]

(2017/C 075/21)

Sprawozdawca: **Thomas McDONOGH**

Wniosek o konsultację	Komisja Europejska, 18.8.2016
Podstawa prawna	Art. 304 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego
Data przyjęcia przez sekcję	15.11.2016
Data przyjęcia na sesji plenarnej	14.12.2016
Sesja plenarna nr	521
Wynik głosowania (za/przeciw/wstrzymało się)	148/0/1

1. **Wnioski i zalecenia**

1.1. Komitet z zadowoleniem przyjmuje komunikat Komisji w sprawie wzmocnienia europejskiego systemu odporności cybernetycznej oraz wspierania konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego. Komitet podziela obawy Komisji w kwestii utrzymującej się wrażliwości Europy na ataki cybernetyczne, stwierdzając, że co najmniej 80 % europejskich przedsiębiorstw doświadczyło przynajmniej raz w ciągu ostatniego roku incydentu cybernetycznego, a liczba incydentów w zakresie bezpieczeństwa we wszystkich branżach na całym świecie wzrosła w 2015 r. o 38 % (The Global State of Information Security Survey, 2016 r., PWC). Zgadzamy się z Komisją, że do wzmocnienia europejskiego systemu odporności cybernetycznej i do wspierania konkurencyjności i innowacyjności sektora bezpieczeństwa cybernetycznego w Europie niezbędny jest szeroki wachlarz środków.

1.2. Komitet ze szczególnym zadowoleniem przyjmuje omawiany wniosek w kontekście niedawno przyjętej dyrektywy w sprawie bezpieczeństwa sieci i informacji ([1]), poprzez którą dąży się do ujednolicenia podejścia do bezpieczeństwa cybernetycznego w Unii Europejskiej, oraz szerszej strategii bezpieczeństwa cybernetycznego ([2]), w której nakreślono obecną wizję tego, w jaki sposób można najskuteczniej zapobiegać atakom w sieci oraz reagować na nie, propagować europejskie wartości, takie jak wolność i demokracja, oraz zapewnić bezpieczny wzrost gospodarki cyfrowej.

1.3. EKES zgadza się, że konieczne są szeroko zakrojone działania na rzecz dalszej ochrony europejskiej infrastruktury i usług o kluczowym znaczeniu przed zagrożeniami dla bezpieczeństwa, i wyraża zadowolenie z faktu, że proponowane obecnie środki stanowią duży krok w kierunku wdrożenia licznych zaleceń Komitetu zawartych w wielu wcześniejszych opiniach ([3]) w sprawie zwiększania bezpieczeństwa cybernetycznego w całej Unii.

([1]) Dz.U. L 194 z 19.7.2016, s. 1.
([2]) JOIN(2013) 1.
([3]) Dz.U. C 97 z 28.4.2007, s. 21;
Dz.U. C 175 z 28.7. 2009, s. 92;
Dz.U. C 255 z 22.9. 2010, s. 98;
Dz.U. C 54 z 19.2. 2011, s. 58;
Dz.U. C 107 z 6.4. 2011, s. 58;
Dz.U. C 229 z 31.7. 2012, s. 90;
Dz.U. C 218 z 23.7. 2011, s. 130;
Dz.U. C 24 z 28.1. 2012, s. 40;
Dz.U. C 229 z 31.7. 2012, s. 1;
Dz.U. C 351 z 15.11. 2012, s. 73;
Dz.U. C 76 z 14.3. 2013, s. 59;
Dz.U. C 271 z 19.9. 2013, s. 127;
Dz.U. C 271 z 19.9. 2013, s. 133;
Dz.U. C 451 z 16.12 2014, s. 31.

1.4. EKES wyraża zadowolenie, że Komisja podpisała umowne partnerstwo publiczno-prywatne (PPP) na rzecz bezpieczeństwa cybernetycznego, które ma uruchomić inwestycje w wysokości 1,8 mld EUR w przemyśle bezpieczeństwa cybernetycznego w UE z myślą o rozwijaniu współpracy na wczesnym etapie procesu badań i innowacji oraz o tworzeniu rozwiązań w zakresie bezpieczeństwa cybernetycznego w różnych sektorach, takich jak sektory energii, zdrowia, transportu i finansów. Komitet jest szczególnie zainteresowany tym, by to PPP wykorzystano do wsparcia rozwoju przedsiębiorstw sektora bezpieczeństwa cybernetycznego w całej Unii, znajdujących się na wczesnym etapie rozwoju.

1.5. Komitet z zadowoleniem przyjmuje zamiar Komisji, aby ocenić, czy należy zmienić lub rozszerzyć mandat Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) do końca 2017 r., i oczekuje, że Komisja zwróci się w tej sprawie do niego o konsultacje. EKES uważa, że wszelkie przedłużanie mandatu agencji ENISA powinno obejmować zwiększenie roli operacyjnej tej agencji, tak aby skuteczniej podnieść świadomość zagrożenia atakami cybernetycznymi i usprawnić reagowanie na nie w całej Unii, jak również poszerzyć zakres bezpośredniej odpowiedzialności za kształcenie i programy upowszechniania wiedzy w zakresie bezpieczeństwa cybernetycznego skierowane w szczególności do obywateli oraz małych i średnich przedsiębiorstw (MŚP).

1.6. Aby zapewnić silne przywództwo i integrację na poziomie UE konieczne do zajęcia się złożonym wdrażaniem skutecznej polityki bezpieczeństwa cybernetycznego na szczeblu europejskim, Komitet zwraca się do Komisji o dokonanie oceny możliwości zmiany statusu agencji ENISA na unijny organ ds. bezpieczeństwa cybernetycznego, na podobieństwo centralnego organu w lotnictwie, jakim jest Europejska Agencja Bezpieczeństwa Lotniczego (EASA). Jeśli taka zmiana mandatu agencji ENISA jest niewykonalna, wówczas EKES opowiada się za utworzeniem takiego organu od zera.

1.7. EKES zwraca się do Komisji, by rozważyła opracowanie krajowego modelu rozwoju i systemu oceny bezpieczeństwa cybernetycznego analogicznie do modelu oceny procesu wytwórczego (CMM) w przemyśle IT, tak by obiektywnie oszacować odporność każdego państwa członkowskiego pod względem bezpieczeństwa cybernetycznego.

1.8. Komitet odnotowuje, że Komisja zamierza rozważyć potrzebę aktualizacji strategii bezpieczeństwa cybernetycznego UE z 2013 r. w najbliższej przyszłości i liczy na to, że w odpowiednim czasie się z nim w tej sprawie skonsultuje.

1.9. Biorąc pod uwagę znaczenie bezpieczeństwa cybernetycznego i zwiększające się zagrożenie cyberprzestępczością, EKES wzywa do przeznaczenia odpowiedniego finansowania i zasobów Europejskiemu Centrum ds. Walki z Cyberprzestępczością przy Europolu i Europejskiej Agencji Obrony.

1.10. Zważywszy na duże znaczenie ochrony danych osobowych obywateli, przechowywanych przez instytucje i agencje administracji publicznej, Komitet apeluje o przeprowadzenie specjalnych szkoleń na temat zarządzania informacją, ochrony danych osobowych i bezpieczeństwa cybernetycznego dla pracowników administracji publicznej.

1.11. EKES uważa, że jeśli chcemy kompleksowo zająć się ochroną UE przed cyberprzestępczością i atakami cybernetycznymi, jak również doprowadzić do rozwoju silnego sektora bezpieczeństwa cybernetycznego w Europie, polityka UE w zakresie bezpieczeństwa cybernetycznego musi w szczególności skupić się na wynikach w następujących dziedzinach: silne przywództwo UE; polityka bezpieczeństwa cybernetycznego, która podnosi bezpieczeństwo przy jednoczesnej ochronie prywatności oraz innych praw podstawowych; podnoszenie świadomości wśród obywateli i wspieranie ochrony proaktywnej; kompleksowe sprawowanie rządów w państwach członkowskich; świadome i odpowiedzialne działania przedsiębiorstw; ścisłe partnerstwo między władzami, sektorem prywatnym i obywatelami; odpowiedni poziom inwestycji; wysokie standardy techniczne i wystarczające inwestycje w B+R+I, a także zaangażowanie międzynarodowe.

2. **Streszczenie dokumentu Komisji**

2.1. W komunikacie przedstawiono środki mające na celu wzmocnienie europejskiej odporności na zagrożenia cybernetyczne oraz wspieranie konkurencyjności i innowacyjności przemysłu bezpieczeństwa cybernetycznego w Europie, jak zapowiedziano w strategii UE w zakresie bezpieczeństwa cybernetycznego i w strategii jednolitego rynku cyfrowego.

2.2. Aby osiągnąć ten cel, środki zaproponowane przez Komisję wykorzystują przepisy dyrektywy w sprawie bezpieczeństwa sieci i informacji w celu wzmocnienia współpracy w dziedzinie bezpieczeństwa cybernetycznego, wymiany informacji oraz organizacji szkoleń i bezpieczeństwa w całej Unii. Komisja ukończy także ocenę agencji ENISA do końca 2017 r. i rozważy potrzebę zmiany lub rozszerzenia jej mandatu.

2.2.1. Komisja będzie ściśle współpracować z państwami członkowskimi, agencją ENISA, ESDZ oraz innymi właściwymi organami UE w celu ustanowienia platformy szkoleń o cyberprzestępczości.

2.2.2. Proponuje się liczne środki w celu zmniejszenia zależności między sektorami zwiększenia odporności kluczowej publicznej infrastruktury sieciowej, w tym rozwijanie europejskich ośrodków wymiany informacji i analizy sektorowej oraz ich współpracę z CSIRT. Komisja proponuje również, aby organy krajowe mogły zwracać się CSIRT o przeprowadzanie regularnych kontroli kluczowej infrastruktury sieciowej.

2.3. Środki proponowane przez Komisję będą również dotyczyły konieczności zwiększenia wsparcia dla wzrostu i rozwoju silnego europejskiego przemysłu bezpieczeństwa cybernetycznego łącznie ze szkoleniem, inwestycjami, wymogami jednolitego rynku oraz utworzeniem nowego partnerstwa publiczno-prywatnego w zakresie bezpieczeństwa cybernetycznego, które ma stymulować inwestycje o wartości 1,8 mld EUR do roku 2020.

2.3.1. Proponuje się również opracowanie wniosku dotyczącego europejskich ram certyfikacji bezpieczeństwa ICT, który miałby być przedstawiony do końca 2017 r., oraz dokonanie oceny wykonalności i skutków lekkich europejskich ram etykietowania w zakresie bezpieczeństwa cybernetycznego.

2.3.2. Aby zwiększyć inwestycje w bezpieczeństwo cybernetyczne w Europie i wesprzeć MŚP, Komisja będzie w środowisku związanym z bezpieczeństwem cybernetycznym podnosiła świadomość na temat istniejących mechanizmów finansowania; będzie zwiększała wykorzystanie narzędzi i instrumentów UE do wspierania innowacyjnych MŚP w poszukiwaniu synergii pomiędzy cywilnymi i obronnymi rynkami bezpieczeństwa (na przykład Europejska Sieć Przedsiębiorczości i Europejska Sieć Regionów Związanych z Obronnością stworzy regionom nowe szanse zbadania możliwości współpracy transgranicznej w dziedzinie produktów podwójnego zastosowania, w tym w dziedzinie bezpieczeństwa cybernetycznego, a MŚP – możliwość zaangażowania w działania matchmakingowe); będzie badała możliwość ułatwienia inwestycji za pomocą specjalnej platformy inwestycji w bezpieczeństwo cybernetyczne oraz innych narzędzi; oraz stworzy platformę inteligentnej specjalizacji w zakresie bezpieczeństwa cybernetycznego, która wesprze państwa członkowskie i regiony zainteresowane inwestycjami w sektorze bezpieczeństwa cybernetycznego (RIS3).

2.3.3. Ponadto, aby stymulować i wesprzeć europejski sektor bezpieczeństwa cybernetycznego poprzez innowacje, Komisja podpisze z tym sektorem umowne partnerstwo publiczno-prawne w zakresie bezpieczeństwa cybernetycznego; zainicjuje zaproszenia do składania wniosków związanych z umownym PPP w ramach programu „Horyzont 2020" oraz zapewni koordynację tego partnerstwa z odpowiednimi strategiami sektorowymi, instrumentami programu „Horyzont 2020" i sektorowymi PPP.

3. **Uwagi ogólne**

3.1. Gospodarka internetowa wytwarza ponad jedną piątą wzrostu PKB w UE, a każdego roku większość Europejczyków robi zakupy w Internecie. Jesteśmy zależni od Internetu i związanych z nim technologii cyfrowych, dzięki którym funkcjonują kluczowe usługi energetyczne, zdrowotne, administracji państwowej i finansowe. Jednakże najważniejsza infrastruktura i usługi cyfrowe, które odgrywają tak istotną rolę w naszym życiu gospodarczym i społecznym, są narażone na rosnące zagrożenie cyberprzestępczością i atakami cybernetycznymi zagrażającymi naszemu dobrobytowi i jakości życia.

3.2. Wiele danych osobowych dotyczących wszystkich obywateli przechowywanych jest obecnie w formie elektronicznej przez rządy, a także instytucje i agencje publiczne. Dlatego też dobre zarządzanie informacjami, bezpieczeństwo cybernetyczne i ochrona danych osobowych mają kluczowe znaczenie dla obywateli w całej Unii, których należy zapewnić, że ich dane osobowe i prywatność są chronione zgodnie z dyrektywami i przepisami UE. Dotyczy to zwłaszcza danych odnoszących się do kwestii zdrowotnych, finansowych, prawnych itd., które mogą zostać wykorzystane do kradzieży tożsamości lub nieodpowiednio ujawnione stronom trzecim. Bardzo istotne jest, by wszyscy pracownicy sektora publicznego byli dobrze przeszkoleni w zakresie zarządzania informacjami, bezpieczeństwa cybernetycznego i ochrony danych.

3.3. Uczenie obywateli zasad osobistego bezpieczeństwa cybernetycznego, w tym bezpieczeństwa danych, powinno stanowić zasadniczy element wszystkich programów nauczania umiejętności cyfrowych. Program edukacyjny prowadzony przez UE może wspierać wysiłki mniej aktywnych państw członkowskich, a także zapewnić właściwe rozumienie strategii, co zmniejszy obawy dotyczące prywatności i zwiększy zaufanie do gospodarki cyfrowej. Taki program może zostać zrealizowany z udziałem stowarzyszeń konsumentów i organizacji społeczeństwa obywatelskiego w całej Unii, w tym placówek oświatowych zaspokajających potrzeby starszych obywateli.

3.4. Każde państwo członkowskie powinno upoważnić swe istniejące organizacje rozwoju przemysłowego do informowania, kształcenia i wspierania sektora MŚP w zakresie bezpieczeństwa cybernetycznego. Duże przedsiębiorstwa z łatwością mogą zdobyć potrzebną wiedzę, natomiast MŚP potrzebują jednak wsparcia w tym zakresie.

3.5. Przydatne byłoby opracowanie obiektywnego kryterium oceny poziomu odporności każdego państwa członkowskiego w zakresie bezpieczeństwa cybernetycznego, tak by można wykorzystać porównania do zaradzenia niedociągnięciom i wprowadzenia ulepszeń. Być może można by stworzyć krajowy model rozwoju i system oceny bezpieczeństwa cybernetycznego analogicznie do modelu oceny procesu wytwórczego (CMM) w przemyśle IT, tak by ocenić krajową ochronę i odporność pod względem bezpieczeństwa cybernetycznego.

3.6. Kompleksowa strategia bezpieczeństwa cybernetycznego powinna obejmować następujące działania:

— silne przywództwo UE ustanawiające polityki, prawa i instytucje w celu wspierania wysokiego poziomu bezpieczeństwa cybernetycznego w całej Unii,

— polityki bezpieczeństwa cybernetycznego, które zwiększałyby bezpieczeństwo zbiorowe i indywidualne, przy jednoczesnym zachowaniu prawa obywateli do prywatności i chronieniu innych podstawowych wartości i wolności,

— wysoka świadomość wszystkich obywateli o ryzyku związanym z korzystaniem z Internetu oraz zachęcanie do proaktywnego podejścia do ochrony swoich urządzeń cyfrowych, tożsamości, prywatności i transakcji on-line,

— kompleksowy system zarządzania we wszystkich państwach członkowskich gwarantujący bezpieczeństwo i odporność krytycznej infrastruktury teleinformatycznej,

— przemyślane i odpowiedzialne działania wszystkich przedsiębiorstw w celu zapewnienia, że ich systemy ICT są bezpieczne i odporne, aby chronić ich działalność i interesy klientów,

— proaktywne podejście dostawców usług internetowych do ochrony swoich klientów przed atakami cybernetycznymi,

— podejście do bezpieczeństwa cybernetycznego oparte na ścisłym partnerstwie w całej UE między rządami, sektorem prywatnym i obywatelami, na poziomie strategicznym i operacyjnym,

— oparte na projektowaniu podejście do wbudowanego bezpieczeństwa cybernetycznego przy opracowywaniu technologii i usług internetowych,

— odpowiedni poziom inwestycji w rozwój wiedzy i umiejętności dotyczących bezpieczeństwa cybernetycznego, aby wykształcić silną grupę specjalistów od bezpieczeństwa cybernetycznego,

— dobre normy techniczne bezpieczeństwa cybernetycznego i wystarczające inwestycje w B+R+I, aby wspierać rozwój silnego sektora bezpieczeństwa cybernetycznego oraz tworzenie rozwiązań światowej klasy,

— aktywne zaangażowanie międzynarodowe wraz z państwami spoza UE w prace nad skoordynowaną globalną polityką i systemem reagowania wobec zagrożeń cybernetycznych.

4. **Uwagi szczegółowe**

4.1. Opierając się na ramach zarządzania bezpieczeństwem cybernetycznym, określonych w dyrektywie w sprawie bezpieczeństwa sieci i informacji oraz na innych środkach zawartych w komunikacie, UE powinna rozważyć zaradzenie fragmentarycznemu podejściu do poprawy bezpieczeństwa cybernetycznego w całej Unii za pomocą stworzenia silnego scentralizowanego organu bezpieczeństwa cybernetycznego na wzór Europejskiej Agencji Bezpieczeństwa Lotniczego (EASA) lub Federalnego Głównego Urzędu ds. Bezpieczeństwa Informacji, niedawno utworzonego w Stanach Zjednoczonych (krajowy plan w zakresie bezpieczeństwa cybernetycznego, Biały Dom, dnia 9 lutego 2016 r.), który byłby odpowiedzialny za nadzorowanie wdrażania polityki bezpieczeństwa cybernetycznego na szczeblu UE oraz za połączenie wysiłków różnych agencji działających w tej dziedzinie.

4.2. Komitet jest pod wrażeniem kompetencji agencji ENISA, zdobytych na przestrzeni lat i uważa, że agencja ta w jeszcze większym stopniu może przyczynić się do zwiększenia odporności i bezpieczeństwa Europy w zakresie bezpieczeństwa cybernetycznego. Należy wzmocnić mandat operacyjny agencji ENISA, tak aby skuteczniej zwiększać świadomość zagrożenia atakami cybernetycznymi i usprawniać reagowanie na nie w całej Unii. Należałoby także dokonać przeglądu mandatu, zważywszy na zmianę warunków w zakresie bezpieczeństwa cybernetycznego od momentu ustanowienia agencji ENISA. Na podstawie dyrektywy w sprawie bezpieczeństwa sieci i informacji operacyjnych być może można by rozszerzyć rolę agencji ENISA, tak aby zwiększyć wartość, jaką może ona przynieść UE, państwom członkowskim, obywatelom i przedsiębiorstwom poprzez współdziałanie jej kompetencji i synergii z działaniami innych podmiotów UE i instytucji, agencji i organów państw członkowskich, takich jak CERT-UE, Europejskie Centrum ds. Walki z Cyberprzestępczością oraz Europejska Agencja Obrony. Agencji ENISA należy także przyznać bardziej bezpośrednią odpowiedzialność za kształcenie i programy upowszechniania wiedzy w zakresie bezpieczeństwa cybernetycznego skierowane w szczególności do obywateli i MŚP.

4.3. Gdy w 2013 r. zostało utworzone Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3), dysponowało budżetem operacyjnym w wysokości jedynie 7 mln EUR, co stanowi mniej niż 10 % całkowitego budżetu Europolu (notatka Komisji Europejskiej/13/6 z dnia 9 stycznia 2012 r.). W 2014 r. dyrektor EC3 powiedział, że cięcia bardzo ograniczyły zasoby przydzielone jego działowi i że z trudem próbują oni dotrzymać kroku szybko zmieniającym się zagrożeniom związanym z cyberprzestępczością (Security Magazine, dnia 1 listopada 2014 r.). EKES uważa, że należy znacząco zwiększyć zasoby przydzielone Europolowi na rzecz zwalczania cyberprzestępczości, tak aby możliwe było nadążanie za zmieniającymi się zagrożeniami. Budżet Europolu na rok 2016 nadal wynosi jedynie 100 mln EUR ([4]).

4.4. Komitet z zadowoleniem przyjmuje przepisy dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz działania zaproponowane w komunikacie, których celem jest usprawnienie współpracy między państwami członkowskimi w zakresie bezpieczeństwa cybernetycznego. Aby zapewnić bezpieczeństwo wszystkich obywateli i osiągnąć wysoką odporność cybernetyczną w całej UE, gdzie systemy informacji o kluczowej infrastrukturze są często powiązane ze sobą, ważne jest, aby środki współpracy dotyczyły rosnącej przepaści między krajami z najbardziej zaawansowanymi kompetencjami w zakresie bezpieczeństwa cybernetycznego i innymi krajami członkowskimi o mniej rozwiniętych kompetencjach.

Bruksela, dnia 14 grudnia 2016 r.

Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego
Georges DASSIS

([4]) Dz.U. C 113z 30.3.2016, s. 144.