Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii

COM(2013) 48 final – 2013/0027 (COD)

(2013/C 271/25)

Sprawozdawca: **Thomas McDONOGH**

Rada, w dniu 21 lutego 2013 r., oraz Parlament Europejski, w dniu 15 kwietnia 2013 r., działając na podstawie art. 114 Traktatu o funkcjonowaniu Unii Europejskiej, postanowiły zasięgnąć opinii Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie

wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii

COM(2013) 48 final – 2013/0027 (COD).

Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego, której powierzono przygotowanie prac Komitetu w tej sprawie, przyjęła swoją opinię 30 kwietnia 2013 r.

Na 490. sesji plenarnej w dniach 22–23 maja 2013 r. (posiedzenie z 22 maja) Europejski Komitet Ekonomiczno-Społeczny stosunkiem głosów 163 do 1 – 5 osób wstrzymało się od głosu – przyjął następującą opinię:

1. **i zalecenia**

1.1 Komitet odnotowuje proponowaną dyrektywę, którą należy postrzegać w szerszym kontekście opublikowanej niedawno strategii bezpieczeństwa cybernetycznego ([1]). W strategii tej nakreślono całościową wizję bezpieczeństwa sieci i informacji (NIS), by zapewnić bezpieczny wzrost gospodarki cyfrowej, szerząc jednocześnie europejskie wartości, jakimi są wolność i demokracja.

1.2 EKES przyjmuje z zadowoleniem wniosek dotyczący dyrektywy, który ma zapewnić wspólny wysoki poziom NIS w całej UE. Harmonizacja NIS i zarządzanie nim na szczeblu europejskim mają kluczowe znaczenie dla urzeczywistnienia jednolitego rynku cyfrowego i dla sprawnego funkcjonowania całego rynku wewnętrznego. Komitet podziela obawy Komisji, że niepowodzenie NIS może przynieść wielkie szkody gospodarce i dobrobytowi obywateli. Niemniej proponowana dyrektywa nie spełnia jego oczekiwań, jeżeli chodzi o zdecydowane działania legislacyjne w tej kluczowej sprawie.

1.3 Komitet wyraża rozczarowanie, że wiele państw członkowskich nie poczyniło postępów na drodze do wdrożenia skutecznego NIS na szczeblu krajowym. Ubolewa nad zwiększonym ryzykiem dla obywateli, które wiąże się z tym niedopatrzeniem, a także nad jego negatywnym wpływem na urzeczywistnienie jednolitego rynku cyfrowego. Wszystkie państwa członkowskie powinny bezzwłocznie przystąpić do wywiązania się z niespełnionych zobowiązań w zakresie NIS.

1.4 Brak postępów powoduje kolejną przepaść cyfrową między elitarną grupą o bardzo zaawansowanym NIS a mniej zaawansowanymi państwami członkowskimi. Przepaść ta wpływa niekorzystnie na zaufanie i współpracę w dziedzinie NIS na szczeblu UE i jeżeli kwestia ta nie zostanie pilnie rozwiązana, może spowodować niedoskonałości rynku wewnętrznego wynikające z różnic w potencjale państw członkowskich.

1.5 Zgodnie ze swymi zaleceniami zawartymi we wcześniejszych opiniach ([2]) EKES uważa, że nieśmiałe, dobrowolne działania są nieskuteczne i że należy nałożyć na państwa członkowskie zdecydowane zobowiązania regulacyjne, by zapewnić harmonizację, zarządzanie i egzekwowanie w zakresie europejskiego NIS. Niestety EKES jest zdania, że wniosek dotyczący dyrektywy nie zapewnia potrzebnych jasnych i zdecydowanych przepisów. Uważa, że rozporządzenie – wraz z dokładnie określonymi wiążącymi zobowiązaniami dla państw członkowskich – byłoby skuteczniejsze niż dyrektywa w zapewnieniu niezbędnego wspólnego wysokiego poziomu NIS.

1.6 Pomimo zamiaru przyjęcia przez Komisję Europejską aktów wykonawczych w celu zapewnienia jednolitych warunków wdrażania części dyrektywy, Komitet dostrzega brak standardów, jasnych definicji i kategorycznych zobowiązań w proponowanym akcie, co tym samym daje państwom członkowskim zbyt dużą swobodę interpretacji i transpozycji zasadniczych elementów. Komitet wyraża życzenie, by jaśniej określono w dokumencie standardy, wymogi i procedury dla państw członkowskich, władz publicznych, podmiotów rynkowych i dostawców kluczowych usług internetowych.

([1]) „Otwarta i bezpieczna cyberprzestrzeń", JOIN(2013) 1.

([2]) Opinia EKES-u „Ochrona krytycznej infrastruktury informatycznej", Dz.U. C 255 z 22.9.2010, s. 98 oraz opinia EKES-u „Dyrektywa w sprawie ataków na systemy informatyczne", Dz.U. C 218 z 23.7.2011, s. 130.

1.7 By zapewnić opracowanie i realizację zdecydowanej polityki w dziedzinie NIS w UE, Komitet zaleca stworzenie unijnego organu ds. NIS, analogicznego do głównego organu przemysłu lotniczego (EASA) ([3]). Organ ten ustalałby standardy i monitorowałby egzekwowanie wszystkich aspektów NIS w całej UE: od certyfikacji bezpiecznych urządzeń końcowych i ich zastosowania po bezpieczeństwo sieci i danych.

1.8 EKES ma świadomość zwiększonego zagrożenia bezpieczeństwa cybernetycznego i ochrony danych, które wynika z wprowadzenia chmury obliczeniowej ([4]) w Europie. Wyraża życzenie, by w proponowanym dokumencie wyraźnie uwzględniono szczególne, dodatkowe wymogi i zobowiązania w zakresie bezpieczeństwa, jeżeli chodzi o świadczenie usług w chmurze obliczeniowej i korzystanie z nich.

1.9 By odpowiednio rozliczano się za NIS, w dokumencie trzeba jasno zaznaczyć, że podmioty mające zobowiązania wynikające z proponowanej dyrektywy miałyby prawo obciążyć odpowiedzialnością dostawców oprogramowania i sprzętu komputerowego za jakiekolwiek defekty ich produktów lub usług, które przyczyniły się bezpośrednio do incydentów w zakresie NIS.

1.10 EKES wzywa państwa członkowskie do szczególnej dbałości o rozwój wiedzy na temat NIS i umiejętności w zakresie bezpieczeństwa cybernetycznego w małych i średnich przedsiębiorstwach (MŚP). Zwraca również uwagę Komisji na popularność zawodów hakerskich w USA ([5]) i niektórych państwach członkowskich ([6]), na podniesienie świadomości na temat bezpieczeństwa cybernetycznego i na wykształcenie następnego pokolenia specjalistów w dziedzinie NIS.

1.11 Zważywszy na znaczenie przestrzegania we wszystkich państwach członkowskich zasad bezpieczeństwa sieci i informacji całej UE, EKES zwraca się do Komisji o rozważenie, jaką część wieloletnich ram finansowych można by przeznaczyć na zapewnienie zgodności w dziedzinie NIS, by pomóc państwom członkowskim potrzebującym wsparcia finansowego.

1.12 Wydatki na działalność badawczą, rozwojową i innowacyjną w dziedzinie technologii NIS powinny być priorytetem w programie ramowym w zakresie badań naukowych i innowacji „Horyzont 2020", tak by Europa mogła dotrzymać kroku szybko zmieniającej się sytuacji związanej z zagrożeniami cybernetycznymi.

1.13 By pomóc w wyjaśnieniu, które podmioty ponoszą odpowiedzialność prawną na mocy proponowanego dokumentu, EKES proponuje, by każde państwo członkowskie było zobowiązane do opublikowania internetowego spisu wszystkich podmiotów objętych wymogami dyrektywy w zakresie zarządzania ryzykiem i sprawozdawczości. Tego rodzaju przejrzystość i rozliczalność publiczna przyczyniłyby się do budowania zaufania i sprzyjałyby zgodności.

1.14 Komitet zwraca uwagę Komisji na wiele swoich wcześniejszych opinii, w których omówił kwestię bezpieczeństwa sieci i informacji oraz potrzebę bezpiecznego społeczeństwa informacyjnego i ochrony infrastruktury krytycznej ([7]).

2. **Streszczenie wniosku Komisji**

2.1 Proponowaną dyrektywę NIS opublikowano wraz z europejską strategią bezpieczeństwa cybernetycznego, której celem jest zwiększenie odporności systemów informacyjnych, ograniczenie cyberprzestępczości, wzmocnienie międzynarodowej polityki UE w zakresie bezpieczeństwa cybernetycznego i cyberobrony, a także rozwinięcie zasobów przemysłowych i technologicznych na rzecz bezpieczeństwa cybernetycznego, przy jednoczesnym propagowaniu praw podstawowych i innych podstawowych wartości UE.

2.2 NIS dotyczy ochrony internetu i innych sieci, systemów informacyjnych i powiązanych z nimi usług, które wspierają funkcjonowanie naszego społeczeństwa. Ma kluczowe znaczenie dla sprawnego działania rynku wewnętrznego.

2.3 Stosowane dotychczas przez UE całkowicie dobrowolne podejście do NIS nie zapewnia odpowiedniej ochrony przed zagrożeniami dla NIS. Zdolności w zakresie NIS są niewystarczające, by dotrzymać kroku szybko zmieniającym się zagrożeniom i zapewnić wspólny, wysoki poziom ochrony we wszystkich państwach członkowskich.

([3]) Europejska Agencja Bezpieczeństwa Lotniczego: http://easa.europa.eu/

([4]) Opinia EKES-u „Chmury obliczeniowe (*cloud computing*) w Europie", Dz.U. C 24 z 28.1.2012, s. 40 oraz opinia EKES-u „Wykorzystanie potencjału chmury obliczeniowej w Europie", Dz.U. C 76 z 14.3.2013, s. 59.

([5]) http://www.nytimes.com/2013/03/25/technology/united-states-wants-to-attract-hackers-to-public-sector.html?pagewanted=all&_r=0

([6]) http://www.bbc.co.uk/news/technology-17333601

([7]) Opinia EKES-u „Strategia na rzecz bezpiecznego społeczeństwa informacyjnego", Dz.U. C 97 z 28.4.2007, s. 21; opinia EKES-u „Ochrona krytycznej infrastruktury informatycznej", Dz.U. C 255 z 22.9.2010, s. 98; opinia EKES-u „Rozporządzenie w sprawie agencji ENISA", Dz.U. C 107 z 6.4.2011, s. 58; opinia EKES-u „Ogólne rozporządzenie o ochronie danych", Dz.U. C 229 z 31.7.2012, s. 90; opinia EKES-u „Ataki na systemy informatyczne", Dz.U. C 218 z 23.7.2011, s. 130; opinia EKES-u „Transakcje elektroniczne na rynku wewnętrznym", Dz.U. C 351 z 15.11.2012, s. 73; opinia EKES-u „Wykorzystanie potencjału chmury obliczeniowej w Europie" Dz.U. C 76 z 14.3.2013, s. 59.

2.4 Państwa członkowskie mają obecnie bardzo różny poziom zdolności i gotowości, czego skutkiem jest fragmentacja podejścia do NIS w całej UE. Zważywszy, że sieci i systemy są wzajemnie połączone, państwa członkowskie nieposiadające odpowiedniego poziomu ochrony osłabiają ogólny NIS w UE. Utrudnia to budowanie zaufania między partnerami, co jest warunkiem niezbędnym do współpracy i wymiany informacji. W rezultacie współpracę prowadzi mniejszość państw członkowskich, posiadających wysoki poziom zdolności.

2.5 Celem dyrektywy proponowanej zgodnie z art. 114 TFUE jest ułatwienie urzeczywistnienia i sprawnego funkcjonowania jednolitego rynku cyfrowego:

— stworzenie minimalnego wspólnego poziomu NIS w państwach członkowskich i tym samym podniesienie ogólnego poziomu gotowości i reagowania na incydenty;

— rozwój współpracy w dziedzinie NIS na szczeblu UE, by zapobiec incydentom i zagrożeniom transgranicznym;

— stworzenie kultury zarządzania ryzykiem i poprawa wymiany informacji między sektorem publicznym i prywatnym.

2.6 W proponowanej dyrektywie ustanawia się wymogi prawne, m.in.:

a) Każde państwo członkowskie musi przyjąć strategię NIS i wyznaczyć właściwe organy krajowe NIS wyposażone w odpowiednie zasoby finansowe i ludzkie, by zapobiegać zagrożeniom i incydentom w zakresie NIS, a także je rozwiązywać i na nie reagować.

b) Stworzenie mechanizmu współpracy między państwami członkowskimi i Komisją w celu przekazywania wczesnych ostrzeżeń w sprawie zagrożeń i incydentów, a także prowadzenia współpracy i organizowania regularnych ocen wzajemnych.

c) Zobowiązanie konkretnych podmiotów w całej UE do przyjęcia praktyk zarządzania ryzykiem oraz do zgłaszania właściwym organom krajowym poważnych incydentów zagrażających bezpieczeństwu, które zaszły w ramach ich podstawowych usług. Do podmiotów objętych tymi wymogami należą: operatorzy krytycznej infrastruktury teleinformatycznej w niektórych sektorach (usługi finansowe, transport, energetyka, opieka zdrowotna), dostawcy usług społeczeństwa informacyjnego (zwłaszcza chmur obliczeniowych, platform handlu elektronicznego, internetowych portali płatniczych, wyszukiwarek, sklepów z aplikacjami i portali społecznościowych) oraz organy administracji publicznej.

2.7 Państwa członkowskie będą musiały wdrożyć dyrektywę w ciągu 18 miesięcy od jej przyjęcia przez Radę i Parlament Europejski (czego można oczekiwać w 2014 r.).

3. **Uwagi ogólne**

3.1 Rozwój internetu i społeczeństwa cyfrowego wywiera głęboki wpływ na życie codzienne. Jednak w miarę wzrostu zależności od internetu, wolność, dobrobyt i jakość życia są coraz bardziej zależne od zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji (NIS). Jeżeli internet nie działa i w nagłym przypadku nie można uzyskać dostępu do dokumentacji medycznej, może to mieć skutek śmiertelny. Tymczasem bezpieczeństwo europejskiej kluczowej infrastruktury teleinformatycznej jest coraz bardziej zagrożone, a nasz poziom NIS nie jest wystarczająco wysoki.

3.2 Dyrektor Europolu stwierdził w zeszłym roku, że jest „bardzo zaniepokojony nieuzasadnioną wiarą w absolutną niezawodność internetu" ([8]). Często słyszymy o nowych atakach cybernetycznych przestępców, terrorystów i obcych rządów na podstawową infrastrukturę. Ofiary nie zgłaszają większości ataków, by nie narazić na szwank swojej reputacji, jednak w ostatnich tygodniach przeprowadzono tak destrukcyjne ataki na europejską infrastrukturę internetową ([9]) i systemy bankowe ([10]), że nie dało się tego ukryć. W jednym ze sprawozdań ([11]) oszacowano, że w 2011 r. Holandia stała się celem 92 mln cyberataków, a Niemcy – 82 mln. Rząd Wielkiej Brytanii szacuje, że w 2011 r. przypuszczono na nią 44 mln ataków cybernetycznych, co kosztowało gospodarkę do 30 mld euro ([12]).

3.3 W 2007 r. Rada UE poruszyła europejski problem w zakresie NIS ([13]). Stosowane od tamtej pory podejście polityczne ([14]) polegało przede wszystkim na dobrowolnych działaniach państw członkowskich, z których jedynie mniejszość przedsięwzięła skuteczne środki. Komitet odnotowuje, że wiele państw członkowskich ani nie opublikowało krajowej strategii bezpieczeństwa cybernetycznego, ani nie opracowało krajowego planu postępowania awaryjnego na wypadek incydentu cybernetycznego, a niektóre nie powołały jeszcze zespołu reagowania na incydenty komputerowe (CERT). Jednocześnie kilka państw członkowskich nie ratyfikowało dotąd konwencji Rady Europy w sprawie cyberprzestępczości ([15]).

([8]) http://forumblog.org/2012/05/what-if-the-internet-collapsed/
([9]) http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?pagewanted=all&_r=0
([10]) http://www.dutchnews.nl/news/archives/2013/04/online_retailers_demand_banks.php
([11]) http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011
([12]) Strategia bezpieczeństwa cybernetycznego Wielkiej Brytanii, „Landscape Review", http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf
([13]) Rezolucja Rady 2007/C 68/01.
([14]) COM(2006) 251 i COM(2009) 149.
([15]) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

3.4 Dziesięć państw członkowskich bardzo zaawansowanych pod względem NIS stworzyło europejską rządową grupę roboczą CERT (EGC) w celu ściślejszej współpracy nad NIS i reagowania na incydenty. Obecnie członkowstwo w EGC jest zamknięte: pozostałe, mniej zaawansowane 17 państw członkowskich oraz nowo utworzony CERT-UE ([16]) są aktualnie wykluczone z tej elitarnej grupy. Powstaje nowa przepaść cyfrowa między państwami członkowskimi zaawansowanymi pod względem NIS a resztą. Jeśli rozłam ten nie zostanie zlikwidowany, przepaść w zakresie NIS zagrozi jednolitemu rynkowi cyfrowemu, ograniczając rozwój zaufania, harmonizacji i interoperacyjności. Ponadto bez zdecydowanych działań rozziew ten prawdopodobnie się powiększy, a wraz z nim pogłębią się niedoskonałości rynku wewnętrznego związane z różnicami w potencjale państw członkowskich.

3.5 Sukces strategii bezpieczeństwa cybernetycznego i skuteczność proponowanej dyrektywy w sprawie NIS będą zależeć od silnego sektora NIS w Europie i wystarczającej liczby pracowników posiadających specjalistyczne umiejętności w zakresie NIS. EKES z zadowoleniem przyjmuje uwzględnienie w proponowanej dyrektywie wzmianki o konieczności inwestowania przez państwa członkowskie w edukację, wiedzę i szkolenia w dziedzinie NIS. Komitet chciałby też, by każde państwo członkowskie poczyniło szczególne starania na rzecz informowania, kształcenia i wspierania sektora MŚP w zakresie bezpieczeństwa cybernetycznego. Duże przedsiębiorstwa mogą z łatwością zdobyć potrzebną wiedzę, lecz MŚP potrzebują wsparcia.

3.6 EKES cieszy się na współpracę z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji (ENISA) na rzecz propagowania NIS podczas „miesiąca bezpieczeństwa cybernetycznego", który będzie miał miejsce w tym roku. Jeżeli chodzi o cel strategii bezpieczeństwa cybernetycznego i dyrektywy w sprawie NIS, dotyczący rozwoju kultury dbałości o bezpieczeństwo w całej UE oraz zwiększenia poziomu umiejętności w zakresie NIS, Komitet zwraca uwagę Komisji na „konkursy hakerskie" dla młodzieży, które okazały się bardzo skuteczne w podnoszeniu świadomości w niektórych państwach członkowskich i w USA.

3.7 Komitet przyjmuje również z zadowoleniem zobowiązanie w strategii bezpieczeństwa cybernetycznego do wydatkowania środków w ramach badań, rozwoju i innowacji na technologię NIS.

3.8 Rozwój przetwarzania w chmurze stwarza nowe zagrożenia dla bezpieczeństwa cybernetycznego. Przykładowo, ogromna moc obliczeniowa jest obecnie dostępna stosunkowo małym kosztem dla cyberprzestępców, zaś dane tysięcy przedsiębiorstw znajdują się aktualnie w scentralizowanych magazynach danych narażonych na skoncentrowane ataki. EKES wezwał do zwiększenia odporności cybernetycznej dla chmur obliczeniowych ([17]).

([16]) CERT-UE to stały zespół reagowania na incydenty komputerowe w instytucjach, agencjach i organach UE.

([17]) Opinia EKES-u „Chmury obliczeniowe (*cloud computing*) w Europie", Dz.U. C 24 z 28.1.2012, s. 40 oraz opinia EKES-u „Wykorzystanie potencjału chmury obliczeniowej w Europie", Dz.U. C 76 z 14.3.2013, s. 59.

3.9 Komitet wzywał już wcześniej do wprowadzenia dobrowolnego unijnego programu identyfikacji elektronicznej dla transakcji on-line w uzupełnieniu do istniejących programów krajowych. Program ten zapewniłby wyższy poziom ochrony przed oszustwami, lepszy klimat zaufania między podmiotami gospodarczymi, niższe koszty świadczenia usług oraz wyższą jakość usług i ochrony obywateli.

4. **Uwagi szczegółowe**

4.1 Niestety wniosek Komisji w sprawie dyrektywy o bezpieczeństwie sieci i informacji ma charakter zbyt niezdecydowany, brakuje mu wystarczającej jasności i w zbyt dużym stopniu opiera się na samoregulacji państw członkowskich. Brak standardów, jasnych definicji i zdecydowanych zobowiązań, zwłaszcza w rozdziale IV dyrektywy, umożliwia państwom członkowskim zbyt dużą swobodę interpretacji i transpozycji najważniejszych elementów tego aktu. Rozporządzenie, z dobrze określonymi wiążącymi zobowiązaniami prawnymi dla państw członkowskich, byłoby skuteczniejsze niż dyrektywa.

4.2 Komitet odnotowuje, że art. 6 dyrektywy wymaga od każdego państwa członkowskiego wyznaczenia „właściwego organu" w celu monitorowania i zapewnienia spójnego stosowania dyrektywy w całej UE. EKES zwraca także uwagę, że w art. 8 ustanawia się sieć współpracy, która dzięki przyznanym jej uprawnieniom oraz kompetencjom Komisji zapewni ogólnoeuropejskie przywództwo i monitorowanie, a w razie potrzeby również egzekwowanie na szczeblu państw członkowskich. Zdaniem EKES-u podczas rozwoju tej sieci zarządzania UE powinna rozważyć utworzenie na szczeblu UE organu ds. bezpieczeństwa sieci i informacji na wzór Europejskiej Agencji Bezpieczeństwa Lotniczego (EASA), która ustanawia standardy i zarządza egzekwowaniem bezpieczeństwa i zgodności w przypadku samolotów, lotnisk i działań linii lotniczych.

4.3 Unijny organ ds. bezpieczeństwa informacji i sieci zaproponowany przez Komitet w punkcie 4.2 powyżej może zostać utworzony na bazie prac sieci bezpieczeństwa cybernetycznego prowadzonych przez ENISA, Europejski Komitet Normalizacyjny (CEN), CERT, europejską rządową grupę roboczą CERT (EGC) i inne. Taki organ ustalałby standardy i monitorowałby egzekwowanie wszystkich aspektów NIS, od certyfikacji bezpiecznych urządzeń końcowych i ich zastosowania po bezpieczeństwo sieci i danych.

4.4 Zważywszy na wysoką współzależność państw członkowskich w zapewnianiu NIS w całej UE oraz na potencjalnie bardzo wysoki koszt niewłaściwego funkcjonowania systemu ponoszony przez wszystkie zainteresowane strony, EKES pragnie, by w przepisach uwzględniono wyraźne i proporcjonalne sankcje za brak zgodności, zharmonizowane tak, aby odzwierciedlały ogólnoeuropejski wymiar odpowiedzialności i skalę potencjalnych szkód, nie tylko na rynku krajowym, lecz także w całej UE. Art. 17 aktu prawnego dotyczący sankcji jest ogólny i umożliwia państwom członkowskim zbyt dużą swobodę nakładania sankcji. Nie zapewnia też wystarczających wytycznych pozwalających uwzględnić skutki transgraniczne i ogólnoeuropejskie.

4.5 Obecnie rządy i dostawcy podstawowych usług nie informują, jeśli nie muszą, o błędach w zakresie bezpieczeństwa i odporności. To nieujawnianie informacji naraża na szwank zdolność Europy do szybkiego i skutecznego reagowania na zagrożenia cybernetyczne oraz do poprawy ogólnego NIS dzięki uczeniu się od siebie nawzajem. Komitet przyjmuje z zadowoleniem decyzję Komisji dotyczącą ustanowienia na mocy dyrektywy obowiązku powiadamiania o wszystkich istotniejszych incydentach w zakresie NIS. EKES nie sądzi, by dobrowolne zgłaszanie incydentów miało dobrze funkcjonować, ponieważ obawy o reputację i odpowiedzialność prawną skłaniają do zatajania takich zdarzeń.

4.6 Jednakże w art. 14 dyrektywy dotyczącym sprawozdawczości nie definiuje się, co mogłoby stanowić zdarzenie o „znaczących skutkach" dla bezpieczeństwa. Artykuł ten stwarza też odpowiednim organom i państwom członkowskim zbyt dużą swobodę podejmowania decyzji o zgłaszaniu bądź nie incydentów w zakresie NIS. Dla zapewnienia skuteczności przepisów potrzebne są jednoznaczne wymogi. Jako że proponowana dyrektywa jest zbyt ogólna co do zasadniczej definicji wymogów, niemożliwe jest nałożenie na strony odpowiedzialności za nieprzestrzeganie przepisów, zgodnie z art. 17 dyrektywy.

4.7 Jako że zapewnianie NIS leży przede wszystkim w gestii sektora prywatnego, ważne jest wspieranie wysokiego poziomu zaufania i współpracy z udziałem wszystkich firm odpowiedzialnych za podstawową infrastrukturę i usługi informacyjne. Należy z zadowoleniem przyjąć inicjatywę dotyczącą utworzenia europejskiego partnerstwa publiczno-prywatnego na rzecz odporności (EP3R), zainicjowaną przez Komisję w 2009 r. oraz zachęcać do brania w niej udziału. Komitet uważa, że inicjatywę tę należy wzmocnić i wspierać za pomocą zobowiązań regulacyjnych w akcie dotyczącym NIS, aby zapewnić współpracę kluczowych podmiotów, które odpowiednio się w nią nie angażują.

4.8 Każde państwo członkowskie powinno opublikować w odniesieniu do swej jurysdykcji internetowy spis wszystkich podmiotów objętych wymogami bezpieczeństwa i zgłaszania incydentów na mocy art. 14 proponowanej dyrektywy. Oprócz objaśnienia, w jaki sposób każde państwo członkowskie zdecyduje się stosować definicje w art. 3 aktu, przejrzystość ta umożliwiłaby budowę zaufania i kultury zarządzania ryzykiem wśród obywateli.

4.9 EKES odnotowuje, że twórcy oprogramowania i producenci sprzętu komputerowego są wyraźnie wyłączeni z wymogów dyrektywy, ponieważ nie świadczą oni usług społeczeństwa informacyjnego. Komitet uważa jednak, że w zaproponowanym akcie powinno się stwierdzić, że podmioty mające obowiązki na mocy dyrektywy mogłyby odwołać się do dostawców oprogramowania i sprzętu komputerowego w przypadku wszelkich niedoskonałości ich produktów lub usług, które przyczyniają się bezpośrednio do incydentów w zakresie NIS.

4.10 Choć Komisja szacuje koszty wdrożenia proponowanej dyrektywy w sprawie NIS na ok. 2 mld euro rocznie, podzielone między sektor publiczny i prywatny w Europie, Komitet zauważa, że niektóre państwa członkowskie pod presją finansową będą miały trudności w znalezieniu inwestycji niezbędnych do przestrzegania przepisów. Należy rozważyć, w jaki sposób można zapewnić wsparcie w ramach WRF dla zgodności NIS, za pomocą różnych instrumentów, w tym Europejskiego Funduszu Rozwoju Regionalnego (EFRR) i ewentualnie Funduszu Bezpieczeństwa Wewnętrznego.

Bruksela, 22 maja 2013 r.

Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego
Henri MALOSSE