Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ochrony krytycznej infrastruktury informatycznej: „Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności"

COM(2009) 149 wersja ostateczna

(2010/C 255/18)

Sprawozdawca: **Thomas McDONOGH**

Dnia 30 marca 2009 r. Komisja Europejska, działając na podstawie art. 262 Traktatu ustanawiającego Wspólnotę Europejską, postanowiła zasięgnąć opinii Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie

komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ochrony krytycznej infrastruktury informatycznej „Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności"

COM(2009) 149 wersja ostateczna.

Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego, której powierzono przygotowanie prac Komitetu w tej sprawie, przyjęła swoją opinię 12 listopada 2009 r. Sprawozdawcą był Thomas McDONOGH.

Na 458. sesji plenarnej w dniach 16–17 grudnia 2009 r. (posiedzenie z 16 grudnia) Europejski Komitet Ekonomiczno-Społeczny 179 głosami – 4 osoby wstrzymały się od głosu – przyjął następującą opinię:

1. Wnioski i zalecenia

1.1 Komitet z zadowoleniem przyjmuje komunikat Komisji w sprawie planu działania dotyczącego ochrony krytycznej infrastruktury informatycznej (ang. *critical information infrastructures*, CII) w Europie. Komitet podziela obawy Komisji dotyczące wrażliwości Europy na szeroko zakrojone ataki cybernetyczne, awarie techniczne, ataki dokonywane przez ludzi, katastrofy naturalne oraz ewentualne ogromne szkody dla gospodarki i dobra obywateli europejskich. Zgadzamy się z Komisją, że potrzebne jest pilne działanie w celu zwiększenia koordynacji i współpracy na szczeblu UE, aby rozwiązać ten bardzo poważny problem. Zgadzamy się również, że potrzebne jest szybkie stworzenie całościowych ram politycznych w celu ochrony CII.

1.2 Komitet odnotowuje wnioski konferencji ministrów UE na temat ochrony krytycznej infrastruktury informatycznej i jest bardzo zaniepokojony słabym przygotowaniem Europy do radzenia sobie z zakrojonymi na szeroką skalę atakami lub zakłóceniami cybernetycznymi dotyczącymi CII, ponieważ podejście poszczególnych państw członkowskich do ochrony CII jest często zróżnicowane i niedostatecznie skoordynowane. Zrozumiałe jest, że rozwój internetu oraz brak myślenia o bezpieczeństwie i odporności infrastruktury informatycznej w kategoriach dużych systemów spowodowały poważną sytuację, w której się znajdujemy. Obecnie jednak, kiedy wskazano już konieczność działania, Komitet wzywa Komisję do bezzwłocznego podjęcia zdecydowanych działań w celu rozwiązania problemu.

1.3 Komitet popiera oparty na pięciu filarach plan działania na wysokim szczeblu przedstawiony w komunikacie i pochwala starania, których dołożyła Komisja; wyjątkowo trudno jest opracować zintegrowane, wielostronne i wielopoziomowe podejście do wzmacniania bezpieczeństwa i odporności CII, zwłaszcza w sytuacji, w której istnieje tak różnorodna grupa zainteresowanych podmiotów, a europejską infrastrukturę informatyczną charakteryzuje wysoki stopień złożoności. Komitet uznaje również pomocną rolę Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz jej wkład w osiągnięcie celów komunikatu.

1.4 Komitet zwraca uwagę, że zainteresowane podmioty nie podjęły wystarczających działań w celu wprowadzenia w życie rezolucji Rady 2007/C 68/01, która dotyczy bezpieczeństwa i odporności infrastruktury teleinformatycznej [1]. Trudność w zakresie opracowania skutecznych strategii ochrony najbardziej krytycznej infrastruktury informatycznej Europy jest korzystna dla osób, które chciałyby dokonać ataku na CII z powodów politycznych lub finansowych. W związku z tym Komitet chciałby, aby Komisja z większym zdecydowaniem odgrywała wiodącą rolę, potrzebną do zjednoczenia wszystkich zainteresowanych podmiotów i wprowadzenia w życie skutecznych środków w celu ochrony Europy przed ewentualnymi zagrożeniami dla jej krytycznej infrastruktury informatycznej. Komitet uważa, że określony w komunikacie plan działania nie przyniesie zamierzonych skutków, jeśli odpowiedzialność nie będzie spoczywać na stosownym organie regulacyjnym.

1.5 Komitet zwraca uwagę Komisji na poprzednie opinie EKES-u zawierające uwagi na temat konieczności istnienia bezpiecznego społeczeństwa informacyjnego, troski o bezpieczeństwo internetu i ochrony krytycznej infrastruktury.

[1] COM(2006) 251.

2. **Zalecenia**

2.1 Unia Europejska powinna powierzyć obowiązek wprowadzenia w życie skutecznej ochrony krytycznej infrastruktury informatycznej w UE stosownemu organowi regulacyjnemu, w skład którego wchodzą członkowie Agencji Praw Podstawowych Unii Europejskiej.

2.2 Wszystkie państwa członkowskie powinny opracować krajową strategię, solidną politykę i solidne otoczenie regulacyjne, całościowe krajowe procesy zarządzania ryzykiem oraz stosowne środki i mechanizmy dotyczące gotowości. W tym zakresie każde państwo członkowskie powinno utworzyć zespół ds. reagowania kryzysowego w dziedzinie informatycznej (ang. *Computer Emergency Response Team*, CERT) i powiązać go z Europejską Grupą Rządowych CERT (EGC) ([2]).

2.3 Komisja powinna przyspieszyć prace nad utworzeniem europejskiego partnerstwa publiczno-prywatnego na rzecz odporności (ang. *European Public Private Partnership for Resilience*, EP3R) oraz włączyć je w działania Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) i Europejskiej Grupy Rządowych CERT (EGC).

2.4 W prowadzonej na wszystkich szczeblach polityce w zakresie ochrony krytycznej infrastruktury informatycznej należy wykorzystywać najlepsze praktyki w dziedzinie zarządzania ryzykiem. W szczególności należy ująć liczbowo potencjalne koszty awarii wynikających z braków w zakresie bezpieczeństwa i odporności i podać je do wiadomości odpowiednich zainteresowanych podmiotów.

2.5 Wobec zainteresowanych podmiotów, które nie spełniają swoich obowiązków wynikających z polityki w zakresie ochrony CII, należy stosować kary finansowe i inne, proporcjonalne do ryzyka i kosztów awarii systemów spowodowanych ich zaniedbaniem.

2.6 Odpowiedzialność za bezpieczeństwo i odporność CII powinna w największej mierze spoczywać na dużych podmiotach – rządach, dostawcach infrastruktury i dostawcach technologii – którym nie należy pozwolić na uchylanie się od odpowiedzialności poprzez przenoszenie jej na konsumentów będących przedsiębiorstwami lub osobami fizycznymi.

2.7 Bezpieczeństwo i odporność winny być podstawowymi wymogami konstrukcyjnymi wszystkich wdrażanych w UE systemów opartych na technologiach informacyjno-komunikacyjnych (TIK). Zachęcalibyśmy podmioty prywatne, których dotyczy polityka w zakresie ochrony CII, do podejmowania ciągłych starań w celu dokonania ulepszeń w konkretnych dziedzinach związanych z odpornością, np. w zakresie zarządzania siecią, zarządzania ryzykiem i ciągłości działania.

2.7.1 Wyznaczanie i kontrolowanie najlepszych praktyk i norm powinno być podstawową częścią każdej polityki dotyczącej zapobiegania awariom, środków reagowania na problemy i przywracania sprawności operacyjnej CII.

2.7.2 Jako kwestię o pierwszorzędnym znaczeniu należy potraktować wdrożenie technologii IPv6 (najnowszy protokół adresów internetowych) i DNSSEC (pakiet rozszerzeń zabezpieczeń systemu nazw domen internetowych) w UE, co zwiększyłoby bezpieczeństwo internetu.

2.8 Zachęcamy zainteresowane podmioty publiczne i prywatne do regularnej współpracy w celu sprawdzania własnej gotowości i własnych środków reagowania poprzez ćwiczenia. Całkowicie popieramy zawarte w omawianym komunikacie sugestie Komisji dotyczące zorganizowania do 2010 roku pierwszych ogólnoeuropejskich ćwiczeń.

2.9 Należy wspierać rozwój silnego sektora bezpieczeństwa informatycznego w Europie, aby dorównał on kompetencjom bardzo dobrze finansowanego sektora w Stanach Zjednoczonych. Należy znacznie podwyższyć inwestycje w działalność badawczo-rozwojową związaną z kwestiami ochrony CII.

2.10 W dziedzinie bezpieczeństwa cybernetycznego należy zwiększyć fundusze przeznaczone na rozwój umiejętności oraz programy podnoszenia wiedzy i świadomości.

2.11 W każdym państwie członkowskim powinien działać organ udzielający informacji i wsparcia, którego celem byłoby pomóc MŚP i obywatelom w zrozumieniu i wypełnianiu swoich obowiązków wynikających z polityki ochrony CII.

2.12 Ze względów bezpieczeństwa UE powinna wzmocnić swoją pozycję, jeśli chodzi o przyszłe zarządzanie internetem ([3]), co wymaga wielostronnego podejścia zapewniającego poszanowanie krajowych priorytetów Stanów Zjednoczonych, lecz odzwierciedlającego również interesy Unii Europejskiej. Działania UE w tej dziedzinie powinny uwzględniać pogłębioną refleksję na temat powiązań między bezpieczeństwem cybernetycznym a poszanowaniem swobód osobistych i publicznych.

3. **Kontekst ogólny**

3.1 Zagrożenie zakrojonymi na szeroką skalę atakami cybernetycznymi na krytyczną infrastrukturę informatyczną.

3.1.1 Krytyczna infrastruktura informatyczna (CII) obejmuje technologie informacyjno-komunikacyjne (TIK), które zapewniają bazę informacyjno-komunikacyjną potrzebną do dostarczania podstawowych towarów i świadczenia podstawowych usług, co dotyczy również zasadniczych funkcji niezbędnych w społeczeństwie, takich jak dostawa energii, wody, usługi transportowe, bankowe, usługi ochrony zdrowia i ratownictwa.

3.1.2 CII charakteryzuje wysoki stopień złożoności powiązań systemowych, współzależności z innymi infrastrukturami (np. energetyczną) oraz powiązań transgranicznych. Te złożone infrastruktury są narażone na wiele niebezpieczeństw, które mogłyby spowodować katastrofalną awarię systemów mającą wpływ na podstawowe usługi świadczone na rzecz społeczeństwa w wielu państwach członkowskich. Niebezpieczeństwa te mogą być spowodowane błędem człowieka, awarią techniczną, atakami dokonywanymi przez ludzi (w tym atakami przestępczymi i atakami z pobudek politycznych) oraz katastrofami naturalnymi. Analiza ryzyka ujawnia słabości tych systemów, a jednocześnie pokazuje możliwość przejęcia kontroli za pośrednictwem celowych lub przypadkowych praktyk, które zagrażają swobodom osobistym i publicznym. Komisja ma obowiązek zapewnienia poszanowania praw podstawowych przy opracowywaniu prawa wspólnotowego.

([2]) Zob. http://www.egc-group.org.

([3]) COM(2009) 277 wersja ostateczna.

3.1.3 Rządy i dostawcy kluczowych usług nie podają do publicznej wiadomości informacji o awariach wynikających z braków w zakresie bezpieczeństwa i odporności, jeśli nie są do tego zmuszeni. Mimo to nawet w takiej sytuacji istnieje wiele powszechnie znanych przykładów zagrożenia dla krytycznej infrastruktury, które wynikły z braków w zakresie bezpieczeństwa i odporności CII:

— W latach 2007 i 2008 w Estonii, na Litwie i w Gruzji nastąpiły zakrojone na szeroką skalę ataki cybernetyczne.

— W 2008 r. uszkodzenia podwodnych kabli transkontynentalnych w Morzu Śródziemnym i Zatoce Perskiej zakłóciły ruch internetowy w wielu krajach.

— W kwietniu 2009 r. urzędnicy bezpieczeństwa narodowego Stanów Zjednoczonych poinformowali, że „szpiedzy cybernetyczni" przedostali się do amerykańskiej sieci elektrycznej i pozostawili programy komputerowe, których można użyć do zakłócenia funkcjonowania systemu.

— W lipcu Stany Zjednoczone i Korea Południowa musiały poradzić sobie z powszechnie znanym atakiem typu „odmowa dostępu" (z udziałem 100–200 tys. komputerów „zombie"), który zakłócił działanie wielu rządowych stron internetowych.

3.1.4 Problem w znacznym stopniu zaostrzają złe zamiary grup przestępczych i wojny cybernetyczne prowadzone z pobudek politycznych.

— Dzięki wykorzystaniu słabości systemów operacyjnych zainstalowanych na komputerach osobistych podłączonych do internetu, grupy przestępcze utworzyły botnety – sieci komputerów osobistych połączonych za pomocą złośliwego oprogramowania w pojedynczy wirtualny komputer posłuszny poleceniom przestępców (na podobieństwo „zombie" lub pojazdu bezzałogowego typu „drone"). Botnety te są wykorzystywane do różnorakich działań przestępczych, pomagają też terrorystom i rządom prowadzącym cybernetyczną wojnę i „dzierżawiącym" botnety od przestępców w dokonywaniu zakrojonych na szeroką skalę ataków cybernetycznych. Uważa się, że jeden taki botnet zwany „Confickerem" ma do dyspozycji ponad 5 milionów komputerów osobistych.

3.1.5 Ekonomiczny koszt awarii CII mógłby być niezwykle wysoki. Światowe Forum Ekonomiczne oszacowało, że prawdopodobieństwo poważnej awarii CII w ciągu następnych 10 lat wynosi 10–20 %, a potencjalny globalny koszt to 250 mld dolarów i tysiące istnień ludzkich.

3.2 Problemy gotowości, bezpieczeństwa i odporności

3.2.1 Internet jest podstawową bazą znacznej części europejskiej CII. Struktura internetu opiera się na wzajemnych połączeniach milionów komputerów, a funkcje przetwarzania danych, łączności i kontroli są rozproszone po całym świecie. Ta rozproszona struktura jest kluczem do stabilności i odporności internetu i stanowi o możliwości szybkiego przywrócenia sprawności strumieni ruchu w razie wystąpienia problemu. Jednakże oznacza to również, że każda osoba o złych zamiarach posiadająca podstawową wiedzę może dokonać zakrojonych na szeroką skalę ataków cybernetycznych z brzegowej części sieci przy użyciu np. botnetów.

3.2.2 Globalne sieci łączności i CII są w znacznym stopniu wzajemnie powiązane w wymiarze transgranicznym. Jeżeli zatem w jednym kraju poziom bezpieczeństwa i odporności sieci jest niski, może to mieć niekorzystny wpływ na bezpieczeństwo i odporność CII we wszystkich innych krajach, z którymi jego sieć jest połączona. Ta międzynarodowa współzależność nakłada na UE obowiązek prowadzenia zintegrowanej polityki zarządzania bezpieczeństwem i odpornością CII w całej Unii.

3.2.3 Wśród większości zainteresowanych podmiotów i w wielu państwach członkowskich poziom wiedzy i świadomości zagrożeń dla CII jest niski. Bardzo niewiele krajów posiada całościową politykę dotyczącą radzenia sobie z tymi zagrożeniami.

3.2.4 Proponowane reformy ram regulacyjnych sieci i usług łączności elektronicznej zwiększą zobowiązania operatorów sieci do podjęcia odpowiednich środków w celu identyfikacji zagrożeń, zagwarantowania ciągłości usług i powiadamiania o przypadkach naruszenia bezpieczeństwa ([4]).

3.2.5 Zdecydowana większość technologii wspomagających platformę dla CII jest dostarczana przez sektor prywatny, a zagwarantowanie właściwej współpracy w celu zapewnienia skutecznej ochrony CII w dużej mierze zależy od wysokiego poziomu kompetencji, zaufania, przejrzystości i komunikacji między wszystkimi zainteresowanymi podmiotami – rządami, przedsiębiorstwami i konsumentami.

3.2.6 Istotne znaczenie ma wielostronne, wielopoziomowe, międzynarodowe podejście.

3.3 Plan działania oparty na pięciu filarach

Komisja proponuje plan działania oparty na pięciu filarach w celu rozwiązania wspomnianych problemów:

1) gotowość i zapobieganie: zapewnienie gotowości na wszystkich szczeblach,

2) wykrywanie i reagowanie: zapewnienie odpowiednich mechanizmów wczesnego ostrzegania,

3) łagodzenie skutków i przywracanie sprawności operacyjnej: wzmocnienie unijnych mechanizmów obronnych dla CII,

4) współpraca międzynarodowa: propagowanie priorytetów UE na scenie międzynarodowej,

5) kryteria dla sektora TIK: wspieranie wdrażania dyrektywy w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej ([5]).

([4]) Art. 13a i 13b w komunikacie COM(2007) 697 (wersja ostateczna) dotyczącym proponowanych zmian dyrektywy 2002/21/WE.

([5]) Dyrektywa Rady 2008/114/WE.

W każdym z tych punktów określono szczegółowe cele wraz z terminami ich osiągnięcia – niektóre z nich przypadają aż na koniec 2011 r.

4. **Uwagi**

4.1 Bardzo trudno będzie opracować i wprowadzić w życie skuteczną strategię ochrony CII w ramach podejścia przedstawionego w komunikacie, które w dużej mierze opiera się na konsultacjach, dobrowolnym uczestnictwie i współpracy. Zważywszy na poważny i pilny charakter problemu, Komitet zaleca, aby Komisja zbadała stosowaną w Wielkiej Brytanii i Stanach Zjednoczonych politykę powierzania obowiązków i uprawnień odpowiedniemu organowi regulacyjnemu.

4.2 Komitet zgadza się z apelem zawartym w rezolucji Zgromadzenia Narodowego ONZ 58/199, który dotyczy *tworzenia globalnej kultury bezpieczeństwa cybernetycznego i ochrony krytycznych struktur informatycznych*. Biorąc pod uwagę wzajemne zależności między krajami, jeśli chodzi o bezpieczeństwo i odporność CII („łańcuch jest tak mocny, jak jego najsłabsze ogniwo"), bardzo niepokojący jest fakt, że jak dotąd jedynie 9 państw członkowskich utworzyło zespoły ds. reagowania kryzysowego w dziedzinie informatycznej (CERT) i przystąpiło do Europejskiej Grupy Rządowych CERT (EGC). W programie międzyrządowym należy przypisać większą wagę tworzeniu tych zespołów.

4.3 Podmiotami zainteresowanymi bezpieczeństwem cybernetycznym w UE są wszyscy obywatele, których życie może zależeć od kluczowych usług. Ci sami obywatele są odpowiedzialni za ochronę – w miarę możliwości – swojego połączenia z internetem przed atakami. Jeszcze większą odpowiedzialność ponoszą dostawcy technologii TIK, które są częścią CII, i usługodawcy z tego sektora. Kwestią zasadniczą jest stosowne informowanie wszystkich zainteresowanych podmiotów o bezpieczeństwie cybernetycznym. Istotne jest również, aby Europa posiadała dużą liczbę wykwalifikowanych ekspertów w dziedzinie bezpieczeństwa i odporności TIK.

4.4 Komitet zaleca utworzenie w każdym państwie członkowskim organizacji, której zadaniem byłoby informowanie, kształcenie i wspieranie sektora MŚP w zakresie zagadnień dotyczących bezpieczeństwa cybernetycznego. Duże przedsiębiorstwa mogą łatwo zdobywać potrzebną im wiedzę, lecz MŚP potrzebują wsparcia.

4.5 Jako że dostarczanie CII należy w głównej mierze do sektora prywatnego, istotne jest zwiększanie zaufania i wspieranie ścisłej współpracy ze wszystkimi przedsiębiorstwami odpowiedzialnymi za CII. Należy pochwalać i wspierać inicjatywę EP3R podjętą przez Komisję w czerwcu. Komitet uważa jednak, że inicjatywę tę należy wspomóc prawodawstwem, aby zmusić do współpracy zainteresowane podmioty, które nie angażują się w sposób odpowiedzialny.

4.6 Dyscyplina zarządzania ryzykiem ma pomagać w rozwiązywaniu tego rodzaju problemów, które zostały przedstawione w omawianym dokumencie. Komisja powinna położyć nacisk na to, by w ramach jej planu działania w odpowiednich przypadkach stosowane były najlepsze praktyki zarządzania ryzykiem. W szczególności bardzo korzystne jest liczbowe ujęcie zagrożeń i kosztów wynikających z awarii na wszystkich poziomach CII. Kiedy znane jest prawdopodobieństwo i ewentualne koszty awarii, łatwiej zmotywować zainteresowane podmioty do podjęcia działań. Łatwiej również pociągnąć je do odpowiedzialności finansowej za zaniedbanie obowiązków.

4.7 Duże zainteresowane podmioty usiłują ograniczyć własną odpowiedzialność, wykorzystując siłę rynkową, aby zmusić swoich klientów lub dostawców do przyjęcia warunków, które zwalniają duże przedsiębiorstwo ze spoczywającej na nim odpowiedzialności – dotyczy to np. umów licencyjnych na oprogramowanie komputerowe lub umów o połączeniu sieci dostawców usług internetowych, które ograniczają odpowiedzialność za sprawy bezpieczeństwa. Umowy te powinny być uznawane za niezgodne z prawem, a odpowiedzialność powinien ponosić największy podmiot.

4.8 Bezpieczeństwo i odporność mogą i powinny być częścią konstrukcji każdej sieci teleinformatycznej. Jako sprawę pierwszorzędnej wagi należy potraktować zbadanie topologii struktur sieci w państwach członkowskich oraz w całej UE w celu określenia punktów niedopuszczalnego natężenia ruchu połączeń i punktów o wysokim ryzyku awarii sieci. W szczególności niedopuszczalne zagrożenie stanowi wysokie natężenie ruchu internetowego w bardzo niewielu punktach wymiany ruchu internetowego (IXP) w niektórych państwach członkowskich.

4.9 Komitet odsyła również Komisję do swojej opinii „Udoskonalenie techniki internetowej – Plan działania dotyczący wdrażania protokołu internetowego, wersja 6 (IPv6) w Europie [6]", dotyczącej dokumentu COM(2008) 313 wersja ostateczna, podkreślającej korzyści dla bezpieczeństwa wynikające z przyjęcia w całej UE protokołu IPv6 w internecie. Zalecamy również wdrożenie – w miarę możliwości – technologii DNSSEC w celu zwiększenia bezpieczeństwa internetu.

4.10 Rozpoczynając politykę dotyczącą bezpieczeństwa w przestrzeni cybernetycznej, Stany Zjednoczone ustalają budżet wydatków na bezpieczeństwo cybernetyczne w latach 2009 i 2010 na 40 mld dolarów. Jest to ogromna inwestycja finansowa w sektor bezpieczeństwa, w związku z czym wiele przedsiębiorstw zajmujących się bezpieczeństwem technologii informacyjnych, w tym przedsiębiorstw europejskich, skoncentruje swoją działalność na Stanach Zjednoczonych. Dostarczy to również bodźca amerykańskim przedsiębiorstwom działającym w sektorze bezpieczeństwa, które staną się światowymi liderami. Bardzo pożądane jest, aby Europa miała własny nowoczesny sektor będący równorzędnym konkurentem dla przedsiębiorstw amerykańskich oraz, aby sektor bezpieczeństwa włożył wystarczające wysiłki na potrzeby Europy w zakresie infrastruktury i na nich się skoncentrował. Komitet chciałby, aby Komisja rozważyła sposoby zrównoważenia ogromnego bodźca finansowego, którego dostarczają Stany Zjednoczone.

[6] Dz.U. C 175 z 28.7.2009, s. 92.

4.11 Komitet popiera ostatni komunikat Komisji w sprawie przyszłego zarządzania internetem ([7]). Uważa, że UE musi wywierać bardziej bezpośredni wpływ na politykę i praktyki Internetowej Korporacji ds. Nadawania Nazw i Numerów (*Internet Corporation for Assigned Names and Numbers*, ICANN) i internetowego organu rejestracyjnego IANA (*Internet Assigned Numbers Authority*) oraz że obecny jednostronny nadzór sprawowany przez Stany Zjednoczone należy zastąpić ustaleniami dotyczącymi wielostronnej, międzynarodowej odpowiedzialności.

Bruksela, 16 grudnia 2009 r.

Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego
Mario SEPI

([7]) COM(2009) 277 wersja ostateczna.