Opinia Komitetu Regionów: „Strategia bezpieczeństwa cybernetycznego”

(2013/C 280/05)

KOMITET REGIONÓW

— Z zadowoleniem przyjmuje przedstawioną przez Komisję strategię bezpieczeństwa cybernetycznego oraz dyrektywę w sprawie bezpieczeństwa sieci i informacji, a także popiera cel strategii, którym jest zapewnienie otwartej, bezpiecznej i chronionej cyberprzestrzeni i uczynienie unijnego środowiska internetowego najbezpieczniejszym na świecie.

— Jest zdania, że pilnie potrzebny jest pakiet, który łączyłby prowadzone już i proponowane działania w tej dziedzinie i który pomógłby zapewnić skoordynowaną i strategiczną wizję dla Europy. Pakiet jest pożądany, ponieważ pomoże zapewnić koordynację, zachęci do współpracy, przyczyni się do podjęcia jasnych, zdecydowanych działań, osiągnięcia wspólnego poziomu ochrony cybernetycznej, zwiększy odporność systemów i sieci IT na nowe i wyłaniające się zagrożenia cybernetyczne oraz zmniejszy fragmentację w UE.

— Zaleca opublikowanie przez Komisję planu działania, by wyjaśnić, w jaki sposób ambitne cele wyznaczone w pakiecie będą realizowane w praktyce. W planie działania trzeba też uwzględnić wytyczne pozwalające na ocenę i mierzenie efektów strategii, aby upewnić się, czy doszło do współpracy i czy osiągnięto postępy.

— Podkreśla, że nowy pakiet powinien pomóc w zapobieganiu incydentom w cyberprzestrzeni, wykrywaniu ich i reagowaniu na nie oraz służyć lepszemu dzieleniu się informacjami i lepszej koordynacji między państwami członkowskimi a Komisją w dziedzinie przeciwdziałania poważnym incydentom. Aby to osiągnąć, potrzeba faktycznych partnerskich stosunków obejmujących państwa członkowskie, instytucje unijne, władze lokalne i regionalne, sektor prywatny i społeczeństwo obywatelskie.

Sprawozdawca	Robert BRIGHT (UK/PSE), członek Rady Miasta Newport
Dokumenty źródłowe	Wspólny komunikat „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej" JOIN(2013) 1 final Wniosek dotyczący dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii COM(2013) 48 final

I. ZALECENIA POLITYCZNE

KOMITET REGIONÓW

1. Z zadowoleniem przyjmuje przedstawioną przez Komisję strategię bezpieczeństwa cybernetycznego oraz dyrektywę w sprawie bezpieczeństwa sieci i informacji, a także popiera cel strategii, którym jest zapewnienie otwartej, bezpiecznej i chronionej cyberprzestrzeni i uczynienie unijnego środowiska internetowego najbezpieczniejszym na świecie.

2. Oczekuje, że nowy pakiet „Bezpieczeństwo cybernetyczne" (obejmujący strategię i dyrektywę) podniesie poprzeczkę i wniesie istotny wkład w opracowywanie norm w tej dziedzinie w całej Unii, zmniejszając niepewność prawa, zwiększając zaufanie do usług online, ograniczając niepotrzebne koszty i obciążenia administracyjne, jak też wspierając jednolity rynek cyfrowy i cele strategii „Europa 2020".

3. Jest zdania, że pilnie potrzebny jest pakiet, który łączyłby prowadzone już i proponowane działania w tej dziedzinie i który pomógłby zapewnić skoordynowaną i strategiczną wizję dla Europy. Pakiet jest pożądany, ponieważ pomoże zapewnić koordynację, zachęci do współpracy, przyczyni się do podjęcia jasnych, zdecydowanych działań, osiągnięcia wspólnego poziomu ochrony cybernetycznej, zwiększy odporność systemów i sieci IT na nowe i wyłaniające się zagrożenia cybernetyczne oraz zmniejszy fragmentację w UE.

4. Zaleca, by organizacje, w tym władze publiczne, uznały, iż zwalczanie cyberprzestępczości wymaga nieustających wysiłków oraz uszeregowały zagrożenia stwarzane przez zakłócenia i ataki w cyberprzestrzeni według ważności, wskazując słabe punkty, a także rozwinęły zdolności organizacyjne w celu zarządzania przypadkami naruszeń. Internet staje się coraz bardziej nieodłączną częścią życia; równolegle jednak rosną i rozprzestrzeniają się zagrożenia spowodowane cyberprzestępczością. Cyberprzestępczość, we wszystkich swoich formach, gwałtowanie wzrasta i stanowi coraz bardziej wyrafinowane nowe zagrożenie dla państw członkowskich, organizacji i obywateli UE w XXI wieku; jest coraz powszechniejsza, bardziej złożona i nie zna granic.

5. Odnotowuje najważniejsze postępy UE w dziedzinie lepszej ochrony obywateli przed przestępstwami w sieci, obejmujące m.in. projekty prawodawstwa dotyczącego ataków na systemy informatyczne oraz światowy sojusz przeciwko niegodziwemu traktowaniu dzieci w internecie w celach seksualnych. W pakiecie należy rozwinąć wcześniejsze inicjatywy, w tym działania wskazane w europejskiej strategii cyfrowej z 2010 r. ([1]), oraz dążyć do opracowania solidnej europejskiej polityki cyberobrony. W tym celu wzywa współlegislatorów, którzy obecnie dyskutują nad wnioskiem Komisji Europejskiej dotyczącym dyrektywy w sprawie ataków na systemy informatyczne ([2]), by szybko osiągnęli porozumienie w sprawie tego wniosku.

6. Popiera ambitny kierunek wytyczony w strategii, obejmujący nie tylko ujednolicenie zdolności państw członkowskich w obszarze bezpieczeństwa cybernetycznego oraz powiązanie różnych bieżących i proponowanych działań w celu ustanowienia wspólnych norm i równych warunków, lecz także koordynację i zapewnienie spójności w trzech obszarach politycznych, a mianowicie egzekwowania prawa, agendy cyfrowej oraz polityki obrony, bezpieczeństwa i polityki zagranicznej – kompetencje ich dotyczące były dotychczas rozdzielone.

7. Sugeruje, że użyteczne dla pakietu mogłoby być zbieranie dowodów przez rządy krajowe i że należałoby zaproponować zbiór zharmonizowanych norm dotyczących bezpieczeństwa sieci i informacji.

8. Z zadowoleniem przyjmuje przyjęte w pakiecie podejście do kształtowania polityki uwzględniające wiele zainteresowanych stron. W pakiecie uznaje się znaczenie współpracy publiczno-prywatnej i osiągnięcia faktycznego partnerstwa przy wykorzystaniu odpowiednich zasobów. Aspiruje się także do ukończenia jednolitego rynku cyfrowego oraz stworzenia bezpiecznego, chronionego i prosperującego środowiska cyfrowego online dla przedsiębiorstw, rządów i obywateli.

([1]) COM(2010) 245, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:PL:HTML.

([2]) COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:PL:PDF.

9. Z zadowoleniem przyjmuje środki zaproponowane w dyrektywie, w tym zalecenie, aby państwa członkowskie przyjęły krajowe strategie w zakresie bezpieczeństwa sieci i informacji, powołały zespoły reagowania na incydenty komputerowe (CERT), współpracujące z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji (ENISA), i utworzyły jasny mechanizm współpracy między państwami członkowskimi i Komisją w celu dzielenia się wczesnymi ostrzeżeniami dotyczącymi zagrożeń i incydentów za pośrednictwem bezpiecznej infrastruktury. Te środki i podejście regulacyjne zastosowane w dyrektywie powinny posłużyć poprawie spójności, ustanowieniu wspólnego minimalnego poziomu gotowości na szczeblu krajowym oraz wzmocnieniu cyberobrony w całej Unii.

10. Zachęca Parlament Europejski i Radę do szybkiego przyjęcia wniosku dotyczącego dyrektywy w sprawie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii.

11. Jest zdania, że pakiet skorzystałby na dalszym wyjaśnieniu kwestii sprawozdawczości i zbierania danych z zakresu cyberprzestępczości przez państwa członkowskie, jak też sposobów wdrażania środków. Wspólne systemy sprawozdawczości oraz dalsze wyjaśnienie obowiązku powiadamiania będą miały kluczowe znaczenie dla uniknięcia niepewności i niespójności w odniesieniu do określania i mierzenia przez właściwe krajowe organy odpowiedzialne za bezpieczeństwo informacji i sieci incydentów w cyberprzestrzeni mających „znaczące konsekwencje". Absolutnie niezbędne jest także, aby, powołując krajowe organy ds. bezpieczeństwa informacji i sieci, uwzględniono podział kompetencji w państwach członkowskich, szczególnie tych o wysoce sfederalizowanej lub zdecentralizowanej strukturze.

12. Wyraża wobec tego niejakie obawy w związku z niektórymi aspektami regulacyjnymi i prawnymi pakietu, zwłaszcza w odniesieniu do niejasności co do kryteriów, które państwo członkowskie musi spełnić, aby mogło uczestniczyć w bezpiecznym systemie wymiany informacji, co do dokładniejszego określenia zdarzeń uruchamiających system wczesnego ostrzegania oraz co do okoliczności, w których podmioty gospodarcze i organy administracji publicznej są zobowiązane do zgłaszania incydentów. Brak wyraźnie określonych zasad dotyczących tych zagadnień nie sprzyja pewności prawa.

13. Wyraża obawy, że dyrektywa może nałożyć niepotrzebne obciążenia regulacyjne na przedsiębiorstwa i organy publiczne. Trzeba poczynić wszelkie wysiłki celem uniknięcia powielania przepisów i dopilnowania, by wszelkie dodatkowe przepisy były zgodne z zasadą proporcjonalności. Będzie to miało szczególne znaczenie dla tych organizacji, na których może już spoczywać obowiązek powiadamiania, w zasadzie przypominający proponowane tu rozwiązania.

14. Zaleca opublikowanie przez Komisję planu działania, by wyjaśnić, w jaki sposób ambitne cele wyznaczone w pakiecie będą realizowane w praktyce. W planie działania trzeba też uwzględnić wytyczne pozwalające na ocenę i mierzenie efektów strategii, aby upewnić się, czy doszło do współpracy i czy osiągnięto postępy.

15. Wzywa wszystkie państwa członkowskie do opracowania krajowych strategii bezpieczeństwa cybernetycznego (do 2012 r. uczyniło to jedynie 10 państw), które uzupełnią nową strategię UE. Komplementarność strategii krajowych ze strategią UE ma istotne znaczenie dla zapewnienia spójności. Ważne jest również, by działania UE uzupełniały istniejące struktury i sprawdzone rozwiązania w państwach członkowskich.

16. Z zadowoleniem przyjmuje planowane rozwinięcie przez Komisję zdolności UE w zakresie bezpieczeństwa cybernetycznego, w tym rozpoczęcie projektu pilotażowego w celu zwalczania botnetów i złośliwego oprogramowania, zobowiązanie do nasilenia współpracy między krajowymi zespołami reagowania na incydenty komputerowe, ENISA i nowym Europejskim Centrum ds. Walki z Cyberprzestępczością, rozwinięcie sieci krajowych centrów doskonałości ds. walki z cyberprzestępczością, a także zainicjowanie platformy publiczno-prywatnej w celu poszukiwania rozwiązań kwestii związanych z bezpieczeństwem informacji i sieci, które zachęcą do przyjmowania bezpiecznych rozwiązań ICT. Należy również przyjąć z zadowoleniem cel strategii, jakim jest zebranie wszystkich zainteresowanych stron, by ocenić postępy poczynione w ciągu 12 miesięcy.

17. Podkreśla, że skuteczna strategia w zakresie bezpieczeństwa cybernetycznego zależy od ścisłej współpracy organów odpowiedzialnych za bezpieczeństwo sieci i informacji oraz organów egzekwowania prawa. Niezbędne w tym celu jest systematyczne zgłaszanie organom ścigania incydentów, które mogą mieć charakter poważnych przestępstw.

Zaangażowanie władz lokalnych i regionalnych

18. Sądzi, że priorytety nakreślone w pakiecie są właściwie wyważone i stosowne. Priorytety te, dotyczące ochrony praw podstawowych, danych osobowych i prywatności, skutecznego wspólnego zarządzania przez wiele zainteresowanych stron oraz wspólnej odpowiedzialności za zapewnienie bezpieczeństwa, są obszarami, w których władze lokalne i regionalne powinny odgrywać centralną rolę jako podmioty dysponujące informacjami sektora publicznego.

19. Proponuje, by uznać regiony, obok państw członkowskich, za główne motory ściślejszej współpracy między użytkownikami i producentami innowacji ICT w różnych dziedzinach, którymi zajmują się rządy i administracja, w tym w dziedzinie bezpieczeństwa cybernetycznego i ochrony danych.

20. Podkreśla, że nowy pakiet powinien pomóc w zapobieganiu incydentom w cyberprzestrzeni, wykrywaniu ich i reagowaniu na nie oraz służyć lepszemu dzieleniu się informacjami i lepszej koordynacji między państwami członkowskimi a Komisją w dziedzinie przeciwdziałania poważnym incydentom. Aby to osiągnąć, potrzeba faktycznych partnerskich stosunków obejmujących państwa członkowskie, instytucje unijne, władze lokalne i regionalne, sektor prywatny i społeczeństwo obywatelskie.

21. Przyznaje, że zwalczanie zagrożeń sieciowych będzie wymagać większych zasobów, zwiększenia świadomości zagrożeń spowodowanych cyberprzestępczością oraz skutecznego i adekwatnego systemu bezpieczeństwa cybernetycznego. Odnośnie do wielopoziomowego sprawowania rządów, solidne podejście do bezpieczeństwa cybernetycznego musi uwzględniać władze lokalne i regionalne, które należy w pełni i skutecznie włączyć w zarządzanie inicjatywami związanymi z ICT.

22. Mając na względzie, iż naruszenie bezpieczeństwa zagraża usługom użyteczności publicznej, np. lokalnemu zaopatrywaniu w wodę i energię, i z uwagi na to, że władze lokalne i regionalne wykorzystują i posiadają wiele produktów i usług cyfrowych, sądzi, że samorządy mają do odegrania kluczową rolę w zwalczaniu cyberprzestępczości, gromadzeniu danych na ten temat i zapewnianiu bezpieczeństwa danych. Na władzach samorządowych spoczywa coraz większa odpowiedzialność za dostarczenie obywatelom i społecznościom np. usług cyfrowych oraz zapewnienie w szkołach kształcenia z zakresu bezpieczeństwa informacji i sieci. Rządy, w tym samorządy lokalne i regionalne odpowiadają za zagwarantowanie dostępu i otwartości, poszanowanie i ochronę praw podstawowych w sieci oraz utrzymanie wiarygodności i interoperacyjności internetu.

23. Sugeruje, by – w celu zapewnienia lepszego stanowienia prawa i mając na uwadze kompetencje władz samorządowych i ich centralną rolę w planowaniu i wdrażaniu wszelkich działań w obszarze ICT (szczególnie odnośnie do prywatności, ochrony danych i bezpieczeństwa cybernetycznego) – instytucje UE i państwa członkowskie regularnie zasięgały opinii władz lokalnych i regionalnych na etapie opracowywania i realizacji środków służących urzeczywistnieniu europejskiej agendy cyfrowej. W rzeczy samej należy ubolewać, iż nie poczyniono żadnych specjalnych wysiłków, by wysłuchać stanowiska władz lokalnych i regionalnych w fazie przygotowywania wniosku dotyczącego dyrektywy. KR jasno stwierdził, że jest gotów wesprzeć Komisję w konsultacjach poprzedzających proces ustawodawczy, co potwierdzono w protokole o współpracy między KR-em a Komisją ([3]).

24. Zaleca uwzględnienie środków odnoszących się do władz samorządowych w art. 14 ust. 1 dyrektywy. Środki te mogą obejmować ustanowienie procesu oceny ryzyka i zarządzania ryzykiem, egzekwowanie polityki w dziedzinie bezpieczeństwa informacji, a także podnoszenie świadomości zagadnień związanych z bezpieczeństwem cybernetycznym i poprawę umiejętności cyfrowych.

25. Zaznacza, że na poziomie niższym niż krajowy należy zachęcać do nawiązywania partnerstw i rozwijać je między wszystkimi zainteresowanymi podmiotami, aby koordynować działania w zakresie bezpieczeństwa cybernetycznego i wnosić wkład w podejmowane na szczeblu krajowym i unijnym działania w tym obszarze w celu zwalczania przestępczości w sieci i minimalizacji skutków bezpośredniej kradzieży własności finansowej lub intelektualnej, przerwania komunikacji lub zniszczenia danych o kluczowym znaczeniu dla przedsiębiorstw.

([3]) Protokół o współpracy między Komisją Europejską a Komitetem Regionów podpisany 16 lutego 2012 r., R/CdR 39/2012 pkt 7.

Pomocniczość i proporcjonalność

26. Odnotowuje, że ogólnie wydają się spełnione dwa warunki związane z przestrzeganiem zasady pomocniczości, a mianowicie niezbędny charakter działań UE i ich wartość dodana. Zaproponowane działania są konieczne, gdyż obejmują ponadnarodowe aspekty, których państwa członkowskie i/lub władze samorządowe nie są w stanie same regulować. Przyniosą one też prawdopodobnie wyraźne korzyści w porównaniu z jednostkowym działaniem na poziomie krajowym, regionalnym bądź lokalnym, ponieważ np. dane osobowe są coraz częściej przekazywane ponad granicami – i to zarówno wewnętrznymi, jak zewnętrznymi. Ponadto wymogi prawne na poziomie pomogą stworzyć równe warunki działania i usunąć luki prawne.

27. Z zadowoleniem przyjmuje fakt, że dyrektywa zasadniczo odpowiada zasadom pomocniczości i proporcjonalności. Z uwagi na transgraniczny aspekt incydentów i zagrożeń w dziedzinie bezpieczeństwa informacji i sieci, cele wytyczone w dyrektywie zostaną lepiej zrealizowane na poziomie UE, zgodnie z zasadą pomocniczości. Badania wykazały, że obywatele UE ufają takim instytucjom jak Komisja w związku z ochroną danych osobowych ([4]). Uwzględnia się też zasadniczo zasadę proporcjonalności, dbając o to, by proponowana dyrektywa nie wykraczała poza to, co jest konieczne do osiągnięcia wyznaczonych celów. Kwestia przestrzegania zasady proporcjonalności i poszanowania wewnętrznych struktur sprawowania rządów w państwach członkowskich budzi jednak wątpliwości, gdyż dla każdego państwa członkowskiego przewiduje się tylko jeden właściwy organ lub zespół CERT.

28. Mimo że podstawą prawną pakietu są art. 26 i art. 114 TFUE, to proponowane działania wykraczają poza te artykuły, gdyż wniosek obejmuje wszystkie systemy informacyjne administracji publicznej, w tym wewnętrzne systemy informacyjne, jak np. intranet.

Karta praw podstawowych

29. Z zadowoleniem przyjmuje fakt, że dyrektywa odnosi się do zasad Karty praw podstawowych Unii Europejskiej. Te same normy, zasady i wartości, których Unia broni w świecie realnym, powinny mieć również zastosowanie w sieci. Technologie informacyjno-komunikacyjne (ICT) powinny uwzględniać potrzeby wszystkich członków społeczeństwa, w tym osób narażonych na wykluczenie społeczne. Wszyscy użytkownicy internetu mają prawo oczekiwać przestrzegania minimalnych norm w odniesieniu do szerokiego spektrum potrzeb, w tym wiarygodności, bezpieczeństwa, przejrzystości, prostoty, interoperacyjności oraz ograniczenia ryzyka i odpowiedzialności. W interesie skutecznej ochrony praw podstawowych, pewności prawnej i zachowania zastrzeżenia parlamentarnego zaleca się zawarcie w samej dyrektywie konkretniejszych zapisów określających normy bezpieczeństwa sieci i informacji pod

([4]) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

względem materialnoprawnym. Należałoby przy tym sformułować wymogi dotyczące bezpieczeństwa sieci i informacji z punktu widzenia praw podstawowych i prawa dotyczącego ochrony danych i bezpieczeństwa danych.

30. Podkreśla, że ochrona obywateli w sieci musi zostać odpowiednio wyważona w stosunku do praw, swobód i wartości przysługujących obywatelom na mocy Karty. Z zadowoleniem należy przyjąć znaczenie nadane kształtowaniu polityki w dziedzinie cyberbezpieczeństwa z poszanowaniem podstawowych wartości UE. Jak stwierdzono w poprzednich opiniach ([5]), należy „spełnić wszystkie wymogi bezpieczeństwa i zagwarantować odpowiedni poziom ochrony prywatności i danych osobowych oraz zapobiec nieupoważnionemu śledzeniu wszelkiego rodzaju informacji osobowych i profilowaniu użytkowników".

31. Mimo że prywatni operatorzy są w coraz większym stopniu odpowiedzialni za krytyczną infrastrukturę i usługi online i pomimo potrzeby uznania kluczowej roli sektora prywatnego, Komitet zaznacza, że w ostatecznym rozrachunku to na państwie musi spoczywać odpowiedzialność za zachowanie swobód i ochronę bezpieczeństwa obywateli w sieci.

Uproszczenie

32. Podkreśla, że stosowanie w całej Europie zasady jednorazowej rejestracji danych dotyczących osób i przedmiotów, bez potrzeby wielokrotnego wypełniania różnych formularzy, znacznie przyczyni się do usunięcia niepotrzebnych obciążeń biurokratycznych spoczywających na obywatelach i obniżenia nakładów na administrację publiczną. Trzeba przy tym zadbać o właściwe przestrzeganie wymogów z zakresu ochrony danych.

Szkolenie

33. Podkreśla, że skuteczna cyberobrona wymaga szkolenia i podnoszenia umiejętności pracowników, w tym pracowników władz lokalnych i regionalnych. Należy zapewnić szeroko zakrojone programy szkoleniowe dla wszystkich pracowników, szczególnie wyspecjalizowanego personelu technicznego, pracowników bezpośrednio zaangażowanych w procedury ochrony wykorzystujące różne technologie oraz pracowników ogólnie lub pośrednio zajmujących się innowacjami i modernizacją w obszarze zaufania i bezpieczeństwa. Kształcenie ustawiczne ma duże znaczenie dla skutecznego funkcjonowania lokalnej administracji elektronicznej, a władze lokalne i regionalne odgrywają coraz ważniejszą rolę w informowaniu obywateli i doradzaniu im na tematy związane z odpowiednim korzystaniem z systemów i rozpoznawaniem zagrożeń sieciowych ([6]).

34. Podkreśla, że zaangażowanie szczebla kierowniczego jest bardzo ważnym czynnikiem sukcesu. Z tego względu konieczne jest ukierunkowane szkolenie osób na stanowiskach nadzorczych i kierowniczych, aby zwiększyć ich wiedzę i zapewnić odpowiednie podstawy do rozwoju kultury bezpieczeństwa w ich organizacjach.

35. Przyjmuje do wiadomości usprawnienia w kształceniu i szkoleniu poprzez wprowadzenie kształcenia z zakresu bezpieczeństwa informacji i sieci oraz organizację konkursu na temat bezpieczeństwa cybernetycznego w 2014 r. Należy tu uwzględnić odbywające się już w państwach członkowskich wydarzenia i zachęcać do wymiany najlepszych rozwiązań. Z zadowoleniem przyjmuje dążenie do tego, by za pośrednictwem tej strategii wprowadzić w szkołach zajęcia z bezpieczeństwa informacji i sieci, niemniej ze względu na to, że edukacja leży w kompetencjach państw członkowskich, zwraca uwagę, że realizacja tego zamiaru do 2014 r. będzie wymagała znacznych środków i planowania.

Wspieranie przedsiębiorstw, innowacji i rozwiązań technicznych

36. Zwraca uwagę, że zapewnienie ochrony prywatności zależy od określonych czynników: struktury organów sektora publicznego (w większości działających na szczeblu lokalnym), konwergencji przepisów UE, wspierania kultury innowacyjności – wśród pracowników administracji publicznej, także poprzez stosowanie wspólnego kodeksu etyki, oraz wśród obywateli, dzięki określaniu przysługujących im praw konsumentów w świecie cyfrowym i podnoszeniu ich świadomości w tym zakresie – a także zarządzania aplikacjami opartymi na ICT.

37. Sądzi, że dalsze działania powinny mieć na celu stymulowanie i wspieranie rozwoju i zastosowania rozwiązań technicznych służących zwalczaniu niezgodnych z prawem treści i szkodliwych zachowań w środowisku online oraz promowanie współpracy i wymiany sprawdzonych rozwiązań między wieloma różnymi zainteresowanymi stronami na szczeblu lokalnym, regionalnym, europejskim i międzynarodowym. W tym kontekście pierwszorzędne znaczenie mają telefony zaufania dla dzieci, rodziców i opiekunów, gorące linie służące zgłaszaniu przypadków molestowania, oprogramowanie umożliwiające lepszą identyfikację niewłaściwych treści oraz łatwe i szybkie składanie sprawozdań.

38. Zaleca poczynienie wszelkich możliwych wysiłków w celu podwyższenia niewielkiego odsetka przedsiębiorstw w UE (26 % w styczniu 2012 r.) posiadających formalnie określoną politykę bezpieczeństwa ICT ([7]). Należy zachęcać wszystkie przedsiębiorstwa, niezależnie od ich wielkości, do inwestowania w bezpieczeństwo cybernetyczne; można to wykorzystać jako narzędzie marketingu w odniesieniu do potencjalnych klientów, a przy tym złagodzić katastrofalne skutki cyberprzestępczości. Przedsiębiorstwa powinny rozważyć podparte technologią biznesowe podejście do bezpieczeństwa cybernetycznego. Muszą przy tym ustalić hierarchię swoich najważniejszych aktywów bądź procesów.

([5]) CdR 104/2010 fin.

([6]) http://www.enisa.europa.eu/publications/archive/scandinavian-approaches-survey.

([7]) http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises.

Potencjał gospodarczy ICT

39. Podkreśla, że z uwagi na duże znaczenie gospodarcze ICT dla gospodarki europejskiej (obecnie to prawie 6 % PKB Unii ([8])) trzeba podjąć już teraz konkretne działania, aby przeciwdziałać coraz częstszemu zjawisku cyberprzestępczości i przywrócić zaufanie obywateli i przedsiębiorstw do bezpieczeństwa internetu (zmniejszając jednocześnie liczbę użytkowników internetu w UE zaniepokojonych kwestią bezpieczeństwa np. płatności online ([9])).

40. Utrzymuje, że w celu zmniejszenia olbrzymich kosztów cyberprzestępczości i zwiększenia zaufania konsumentów potrzeba pilnych środków na poziomie lokalnym, regionalnym, krajowym i unijnym przeciwdziałających temu procederowi.

41. Jest zdania, że strategia skorzystałaby na wyjaśnieniu sposobów ochrony i dalszego rozwoju chmury obliczeniowej, która ma olbrzymi potencjał gospodarczy. Gwałtowny wzrost liczby użytkowników mobilnych urządzeń elektronicznych nie wykazuje żadnych oznak spowolnienia. Gartner w swoim raporcie twierdzi, że do 2016 r. co najmniej 50% użytkowników poczty elektronicznej w przedsiębiorstwach będzie polegać na klientach mobilnych ([10]). Należy przyjrzeć się nowym problemom i szansom związanym ze stosowaniem mobilnych urządzeń elektronicznych i przetwarzaniem w chmurze. Ponadto technologia chmury obliczeniowej potrzebuje odpowiednich struktur, by osiągnąć maksymalne poziomy bezpieczeństwa ([11]). Komitet wyraził już obawy co do tego, że w niedawno opublikowanym komunikacie w sprawie chmury obliczeniowej Komisja nie dość dogłębnie analizuje związki miedzy zaproponowaną strategią a innymi kwestiami, takimi jak bezpieczne przetwarzanie danych, przepisy dotyczące praw autorskich oraz prace nad dostępnością i przenoszeniem danych ([12]).

Współpraca międzynarodowa

42. Jest zdania, iż z uwagi na globalne, wzajemnie powiązane i transgraniczne zagrożenia ze strony cyberprzestępczości należy zachęcać do współpracy międzynarodowej i dialogu ponad granicami UE, aby zapewnić prawdziwie światowe, skoordynowane podejście do bezpieczeństwa cybernetycznego. W tym kontekście trzeba zachęcać wszystkie państwa do przestrzegania międzynarodowej Konwencji o cyberprzestępczości (konwencji z Budapesztu) ([13]). Istotna jest również ciągła współpraca zarówno na poziomie dwustronnym, zwłaszcza ze Stanami Zjednoczonymi, jak i wielostronnym, z różnymi organizacjami międzynarodowymi.

Powiązania z unijnymi programami finansowania i ramami budżetowymi

43. Podkreśla znaczenie poprawy koordynacji z bieżącymi i przyszłymi instrumentami finansowania, takimi jak program „Horyzont 2020", europejskie ramy współpracy oraz Fundusz Bezpieczeństwa Wewnętrznego, celem zapewnienia bardziej skoordynowanego podejścia do inwestycji związanych z cyberprzestrzenią.

44. Wątpi, czy alokacja budżetowa w wysokości 1,25 mln euro wystarczy do zbudowania solidnej i odpowiedniej infrastruktury bezpieczeństwa informacji i sieci. Wyraża rozczarowanie zmniejszeniem środków przeznaczonych na instrument „Łącząc Europę", które zapisano w porozumieniu w sprawie wieloletnich ram finansowych na lata 2014–2020 na posiedzeniu Rady 8 lutego. Solidny i większy budżet jest potrzebny z punktu widzenia wsparcia kluczowej infrastruktury ICT, powiązania zdolności państw członkowskich w dziedzinie bezpieczeństwa informacji i sieci i tym samym ułatwienia współpracy w Unii Europejskiej.

II. ZALECANE POPRAWKI

Poprawka 1

Motyw (4) preambuły

Tekst zaproponowany przez Komisję	Poprawka KR-u
Na poziomie Unii należy ustanowić mechanizm współpracy, który umożliwi wymianę informacji i podejmowanie skoordynowanych działań w zakresie wykrywania i reagowania w odniesieniu do bezpieczeństwa sieci i informacji. Aby mechanizm ten był skuteczny i dostępny dla wszystkich, konieczne jest, by wszystkie państwa członkowskie posiadały minimalne zdolności i strategię zapewniające wysoki poziom bezpieczeństwa sieci i informacji na ich terytorium. Aby promować kulturę wspierającą przeciwdziałanie zagrożeniom i zapewnić zgłaszanie najpoważniejszych incydentów, należy wprowadzić minimalne wymogi w zakresie bezpieczeństwa również w odniesieniu do organów administracji publicznej i operatorów krytycznej infrastruktury teleinformatycznej.	Na poziomie Unii należy ustanowić mechanizm współpracy, który umożliwi wymianę informacji i podejmowanie skoordynowanych działań w zakresie wykrywania i reagowania w odniesieniu do bezpieczeństwa sieci i informacji. Aby mechanizm ten był skuteczny i dostępny dla wszystkich, konieczne jest, by wszystkie państwa członkowskie posiadały minimalne zdolności i strategię zapewniające wysoki poziom bezpieczeństwa sieci i informacji na ich terytorium. Aby promować kulturę wspierającą przeciwdziałanie zagrożeniom i zapewnić zgłaszanie najpoważniejszych incydentów, należy wprowadzić minimalne wymogi w zakresie bezpieczeństwa również w odniesieniu do organów administracji publicznej, **w tym do władz lokalnych i regionalnych oraz** ~~i~~ operatorów krytycznej infrastruktury teleinformatycznej.

([8]) http://europa.eu/rapid/press-release_MEMO-13-71_en.htm.
([9]) http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf.
([10]) http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf.
([11]) http://www.mcafee.com/hk/resources/reports/rp-sda-cyber-security.pdf.
([12]) CdR 1673/2012.
([13]) http://conventions.coe.int/Treaty/EN/Treaties/PDF/Polish/185-Polish.pdf.

Poprawka 2

Motyw (9) preambuły

Tekst zaproponowany przez Komisję	Poprawka KR-u
W celu osiągnięcia i utrzymania wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych każde państwo członkowskie powinno posiadać krajową strategię w zakresie bezpieczeństwa sieci i informacji określającą cele strategiczne i konkretne działania, które należy wdrożyć. Na poziome krajowym należy opracować spełniające zasadnicze wymagania plany współpracy w zakresie bezpieczeństwa sieci i informacji, tak aby osiągnąć poziom zdolności reagowania umożliwiający skuteczną i sprawną współpracę na poziomach krajowym i unijnym w przypadku wystąpienia incydentów.	W celu osiągnięcia i utrzymania wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych każde państwo członkowskie powinno posiadać krajową strategię w zakresie bezpieczeństwa sieci i informacji określającą cele strategiczne i konkretne działania, które należy wdrożyć. Na poziome krajowym, **z pełnym zaangażowaniem władz lokalnych i regionalnych**, należy opracować spełniające zasadnicze wymagania plany współpracy w zakresie bezpieczeństwa sieci i informacji, tak aby osiągnąć poziom zdolności reagowania umożliwiający skuteczną i sprawną współpracę na poziomach krajowym i unijnym w przypadku wystąpienia incydentów.

Poprawka 3

Motyw (35) preambuły

Tekst zaproponowany przez Komisję	Poprawka KR-u
Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów. Przygotowując i opracowując akty delegowane, Komisja powinna zapewnić jednoczesne, terminowe i odpowiednie przekazywanie stosownych dokumentów Parlamentowi Europejskiemu i Radzie.	Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów. Przygotowując i opracowując akty delegowane, **z myślą o uzupełnieniu lub zmianie innych niż istotne elementów aktu podstawowego**, Komisja powinna zapewnić jednoczesne, terminowe i odpowiednie przekazywanie stosownych dokumentów Parlamentowi Europejskiemu i Radzie.

Poprawka 4

Rozdział IV

Artykuł 14 ust. 1

Tekst zaproponowany przez Komisję	Poprawka KR-u
Wymogi w zakresie bezpieczeństwa i zgłaszanie incydentów 1. Państwa członkowskie zapewniają zastosowanie przez organy administracji publicznej i podmioty gospodarcze właściwych środków technicznych i organizacyjnych w celu przeciwdziałania zagrożeniom, na jakie narażone są kontrolowane i wykorzystywane przez nie sieci i systemy informatyczne. Uwzględniając aktualny stan wiedzy i technologii, środki te zapewniają poziom bezpieczeństwa stosowny do istniejącego zagrożenia. W szczególności należy podjąć środki zapobiegające incydentom dotyczącym sieci i systemów informatycznych organów administracji publicznej i podmiotów gospodarczych oraz minimalizujące wpływ tych incydentów na świadczone przez nie podstawowe usługi, zapewniając tym samym ciągłość usług opartych na tych sieciach i systemach informatycznych.	Wymogi w zakresie bezpieczeństwa i zgłaszanie incydentów 1. Państwa członkowskie zapewniają zastosowanie przez organy administracji publicznej i podmioty gospodarcze właściwych środków technicznych i organizacyjnych w celu przeciwdziałania zagrożeniom, na jakie narażone są kontrolowane i wykorzystywane przez nie sieci i systemy informatyczne. **Środki te mogą obejmować – na poziomie lokalnym i regionalnym – ustanowienie procesu oceny ryzyka i zarządzania ryzykiem, egzekwowanie polityki w dziedzinie bezpieczeństwa informacji, a także podnoszenie świadomości zagadnień związanych z bezpieczeństwem cybernetycznym i poprawę umiejętności cyfrowych.** Uwzględniając aktualny stan wiedzy i technologii, środki te zapewniają poziom bezpieczeństwa stosowny do istniejącego zagrożenia. W szczególności należy podjąć środki zapobiegające incydentom dotyczącym sieci i systemów informatycznych organów administracji publicznej i podmiotów gospodarczych oraz minimalizujące wpływ tych incydentów na świadczone przez nie podstawowe usługi, zapewniając tym samym ciągłość usług opartych na tych sieciach i systemach informatycznych.

Uzasadnienie

Rola władz lokalnych i regionalnych w walce z cyberprzestępczością ma kluczowe znaczenie i powinna zostać w pełni uznana.

Poprawka 5

Rozdział IV

Artykuł 16

Tekst zaproponowany przez Komisję	Poprawka KR-u
Normalizacja	Normalizacja
1. W celu zapewnienia spójnego wdrażania art. 14 ust. 1 państwa członkowskie wspierają stosowanie norm lub specyfikacji mających znaczenie dla bezpieczeństwa sieci i informacji.	1. W celu zapewnienia spójnego wdrażania art. 14 ust. 1 państwa członkowskie wspierają stosowanie **zharmonizowanych** norm lub specyfikacji mających znaczenie dla bezpieczeństwa sieci i informacji.
2. Komisja sporządza – w drodze aktów wykonawczych – wykaz norm, o których mowa w ust. 1. Wykaz ten zostaje opublikowany w Dzienniku Urzędowym Unii Europejskiej.	2. Komisja sporządza – w drodze aktów wykonawczych – wykaz norm, o których mowa w ust. 1. Wykaz ten zostaje opublikowany w Dzienniku Urzędowym Unii Europejskiej.

Uzasadnienie

Komisja Europejska przyznaje, że stosowanie odmiennych norm przez poszczególne państwa członkowskie jest poważnym wyzwaniem. Wobec tego do zapewnienia wspólnego poziomu bezpieczeństwa sieci i informacji w całej UE niezbędna jest harmonizacja norm.

Bruksela, 3 lipca 2013 r.

Przewodniczący
Komitetu Regionów
Ramón Luis VALCÁRCEL SISO