Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie komunikatu Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Strategia na rzecz bezpiecznego społeczeństwa informacyjnego — Dialog, partnerstwo i przejmowanie inicjatywy

COM (2006) 251 wersja ostateczna

(2007/C 97/09)

Dnia 31 maja 2006 r. Komisja, działając na podstawie art. 262 Traktatu ustanawiającego Wspólnotę Europejską, postanowiła zasięgnąć opinii Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie wspomnianej powyżej.

Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego, której powierzono przygotowanie prac Komitetu w tej sprawie, przyjęła swoją opinię 11 stycznia 2007 r. Sprawozdawcą był Antonello PEZZINI.

Na 433. sesji plenarnej w dniu 16 lutego 2007 r. Europejski Komitet Ekonomiczno-Społeczny 132 głosami za — 2 osoby wstrzymały się od głosu — przyjął następującą opinię:

1. **Wnioski i zalecenia**

1.1 Komitet jest przekonany, że problem bezpieczeństwa informatycznego posiada coraz większe znaczenie dla przedsiębiorstw, jednostek administracji publicznej, instytucji publicznych i prywatnych oraz dla użytkowników indywidualnych.

1.2 Komitet podziela w zasadzie analizy i argumenty wskazujące na konieczność nowej strategii na rzecz zwiększenia bezpieczeństwa sieci i informacji przeciwko atakom i ingerencjom, które zdarzają się bez względu na granice geograficzne.

1.3 Komitet uważa, że Komisja powinna podejmować dalsze starania w celu realizacji innowacyjnej i rozbudowanej strategii, biorąc pod uwagę wielkość zjawiska oraz jego konsekwencje dla gospodarki i życia prywatnego.

1.3.1 Komitet podkreśla również, że Komisja przyjęła ostatnio nowy komunikat w sprawie bezpieczeństwa informatycznego i że w niedługim czasie powinien zostać wydany kolejny dokument na ten sam temat. Komitet rezerwuje sobie prawo wyrażenia, w przyszłości, bardziej rozbudowanej opinii biorącej pod uwagę ogół komunikatów.

1.4 Komitet podkreśla, że bezpieczeństwo informatyczne nie może w żaden sposób być traktowane rozdzielnie od kwestii wzmocnienia ochrony danych osobowych i zachowania wolności, które są prawami gwarantowanymi przez europejską Konwencję o ochronie praw człowieka i podstawowych wartości.

1.5 EKES zastanawia się, jaka będzie w obecnym stanie wartość dodana wniosku w odniesieniu do zintegrowanego podejścia przyjętego w 2001 r., którego cel był równoznaczny z celem obecnie omawianego komunikatu ([1]).

1.5.1 Dokument dotyczący oceny oddziaływania ([2]), dołączony do wniosku, zawiera parę interesujących zmian w stosunku do stanowiska z 2001 r., ale został opublikowany tylko w jednym języku, co czyni go nieprzystępnym dla wielu obywateli europejskich, którzy wyrabiają sobie opinię w oparciu o oficjalny dokument zredagowany we wszystkich językach Wspólnoty.

1.6 Komitet przypomina końcowe wnioski przyjęte na Światowym Szczycie Społeczeństwa Informacyjnego w Tunisie w 2005 r. i przyjęte przez Zgromadzenie ONZ-u 27 marca 2006 r.:

— zasada równego dostępu,

— promowanie technologii informatyczno-komunikacyjnych (TIK) jako instrumentu wspierania pokoju,

— ustanowienie narzędzi umacniających demokrację, spójność i dobre zarządzanie,

— zapobieganie nadużyciom, w poszanowaniu praw człowieka ([3]).

1.7 Komitet podkreśla, że wspólnotowa strategia, dynamiczna i zintegrowana, powinna móc wziąć pod uwagę nie tylko dialog, partnerstwo i przejmowanie inicjatywy, ale także następujące tematy:

— działania prewencyjne,

— przejście od bezpieczeństwa do „ubezpieczenia" informatycznego ([4]),

— ustanowienie pewnych i uznanych unijnych ram prawno-regulacyjnych oraz ram karnych,

— ulepszenie normalizacji technicznej,

([1]) Por. Opinia EKES-u w sprawie komunikatu Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie „Bezpieczeństwo sieci i bezpieczeństwo informacji: propozycja strategicznego podejścia europejskiego", Dz.U. C 48 z 21.2.2002, str. 33.

([2]) „Dokument dotyczący oceny oddziaływania" nie ma tej samej rangi co „dokument strategiczny".

([3]) ONZ 27.3.2006 r. Zalecenia nr 57 i 58. Końcowy dokument z Tunisu nr 15.

([4]) Por. „Emerging technologies in the context of security" Wspólne Centrum Badawcze — Instytut ochrony i bezpieczeństwa obywateli, zeszyt badań strategicznych, wrzesień 2005 r., Komisja Europejska http://serac.jrc.it.

— cyfrowa identyfikacja użytkowników,

— rozpoczęcie europejskich badań analityczno-perspektywicznych (Foresight) nad bezpieczeństwem informatycznym, w kontekście multimodalnych konwergencji technologicznych,

— wzmocnienie mechanizmów oceny zagrożeń na szczeblu europejskim i krajowym,

— działania skierowane na unikanie powstawania monokultur informatycznych,

— wzmocnienie wspólnotowej koordynacji na szczeblu europejskim i międzynarodowym,

— ustanowienie wspólnego dla Dyrekcji Generalnych punktu kontaktowego „Bezpieczeństwo TIK" (ICT Security Focal Point),

— utworzenie europejskiej sieci na rzecz bezpieczeństwa sieci i informacji (European Network and Information Security Network),

— optymalizacja roli europejskich badań naukowych w dziedzinie bezpieczeństwa informatycznego,

— organizacja „Europejskiego Dnia Bezpiecznego Komputera",

— organizowanie wspólnotowych projektów pilotażowych na tematy związane z bezpieczeństwem informatycznym przeprowadzane w szkołach wszelkiego typu i szczebla.

1.8 EKES uważa wreszcie, że aby zapewnić dynamiczną i zintegrowaną strategię wspólnotową należy przewidzieć odpowiednie środki w budżecie oraz wzmocnione inicjatywy i działania koordynujące na poziomie wspólnotowym, dzięki którym Europa wypowiadałaby się jednym głosem na forum światowym.

2. **Uzasadnienie**

2.1 Budowanie zaufania do sieci i usług komunikacyjnych oraz do ich niezawodności, które są podstawowymi czynnikami rozwoju gospodarki i społeczeństwa, jest głównym wyzwaniem z zakresu bezpieczeństwa społeczeństwa informacyjnego.

2.2 Aby utrzymać zdolność konkurencyjną i handlową, zapewnić integralność i trwałość łączności elektronicznej, zapobiec nadużyciom i zagwarantować prawną ochronę życia prywatnego należy zapewnić ochronę sieci oraz systemów informatycznych.

2.3 Łączność elektroniczna i usługi z nią związane stanowią największą część sektora telekomunikacyjnego: w 2004 r. około 90 % przedsiębiorstw europejskich korzystało w sposób aktywny z internetu, w tym 65 % stworzyło własną stronę internetową. Według obliczeń około połowa obywateli europejskich korzysta regularnie z internetu, a 25 % rodzin korzysta w sposób stały z szerokopasmowego łącza dostępu ([5]).

([5]) *i2010: Strategia na rzecz bezpiecznego społeczeństwa informacyjnego*. DG Społeczeństwo informacyjne i media;„Factsheet 8" (czerwiec 2006 r.) http://ec.europa.eu/information_society/doc/factsheets/001-dg-glance-it.pdf.

2.4 Wobec przyspieszonego rozwoju inwestycji wysokość wydatków na bezpieczeństwo stanowi zaledwie od 5 do 13 % całości inwestycji w technologie informacyjne. Tak więc procent ten jest stanowczo za niski. Niedawne badania pokazały, że „ze średnio 30 protokołów posiadających te same struktury klucza, 23 stanowią łatwy cel ataków wieloprotokołowych" ([6]). Ponadto ilość codziennie przekazywanych wiadomości elektronicznych *spam* ([7]) ocenia się średnio na 25 mln, dlatego Komitet z zadowoleniem przyjmuje ostatnio przedstawiony wniosek Komisji na ten temat.

2.5 W zakresie wirusów komputerowych ([8]), szybkie rozprzestrzenianie się i to na dużą skalę „robaków internetowych" (worm) ([9]) i oprogramowania typu „spyware" ([10]) szło w parze z rosnącym rozwojem systemów i sieci łączności elektronicznej. Stały się one coraz bardziej złożone i podatne na ataki i nawet w przypadku konwergencji multimediów i telefonii komórkowej czy systemów *GRID infoware* ([11]) przypadki wyłudzenia, ataki typu *DDos* (Distributed Denials of Sernice), kradzież tożsamości w sieci, *phishing* ([12]), piractwo ([13]), itd. są zagrożeniem dla społeczeństwa informacyjnego. Wspólnota Europejska zajęła się już tym problemem w swoim komunikacie z 2001 r. ([14]), na temat którego Komitet miał już okazję się wypowiedzieć ([15]), proponując strategię opartą na trzech liniach działania:

— szczególne środki związane z bezpieczeństwem sieci i informacji,

([6]) Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06) — Volume 00 ARES 2006 Editore: IEEE Computer Society.

([7]) Spam — niezamówione informacje reklamowe przekazywane drogą elektroniczną. Pierwotne znaczenie tego wyrażenia oznaczało „spiced pork and ham", mielonkę wieprzową, bardzo popularną w czasie drugiej wojny światowej, kiedy była podstawowym środkiem żywnościowym dla żołnierzy amerykańskich i dla angielskiej ludności cywilnej, gdyż nie była reglamentowana. Po latach stosowania takiej diety pojęcie nabrało negatywnego znaczenia.

([8]) Wirus komputerowy — szczególne oprogramowanie należące do kategorii *malware*, które jest w stanie, po uruchomieniu go, zarazić pliki w sposób samopowielający, zazwyczaj nie będąc zauważonym przez użytkownika. Wirusy mogą być mniej lub bardziej szkodliwe dla systemu operacyjnego w którym się znajdują, ale nawet w najmniej poważnym przypadku są marnotrawstwem pamięci RAM, CPU i miejsca na twardym dysku (www.wikipedia.org/wiki/Virus_informatico).

([9]) *Robak internetowy (worm)* — szkodliwe oprogramowanie zdolne do samopowielania: „e-mail worm" jest niszczącym atakiem przeciwko sieci, polegającym na zebraniu wszystkich adresów e-mail znajdujących się w lokalnym programie (np. w MS Outlook) i wysłaniu na nie setek e-maili zawierających *robaka* w niewidocznym załączniku.

([10]) *Spyware* — oprogramowanie szpiegujące działania użytkownika w internecie, instalujące się bez jego wiedzy, zgody ani kontroli.

([11]) GRID *infoware* — umożliwia podział, wybór i grupowanie szerokiej gamy rozproszonych geograficznie zasobów komputerowych (na przykład superkomputer, klaster serwerów, systemy przechowywania danych, bazy danych, narzędzi, zasobów ludzkich) przedstawiając je jako jedyny, jednolity środek do wykonania bardzo skomplikowanych obliczeń i stosowania informatycznych programów użytkowych o dużej przepustowości danych.

([12]) *Phishing (łowienie haseł)* — w kontekście informatycznym *phishing* oznacza technikę łamania zabezpieczeń (*cracking*) używaną do pozyskania osobistych i poufnych informacji w celu kradzieży tożsamości, poprzez wysyłanie fałszywych wiadomości elektronicznych przypominających do złudzenia autentyczne.

([13]) Piractwo — termin używany przez „piratów" komputerowych do określenia oprogramowania, z którego zdjęto zabezpieczenie przed kopiowaniem i udostępniono w internecie skąd może być ściągnięte.

([14]) COM (2001) 298 końcowy.

([15]) Por. przypis 1.

— ramy regulacyjne dla łączności elektronicznej (w tym zagadnienia dotyczące ochrony prywatności i ochrony danych),

— zwalczanie przestępczości internetowej.

2.6 Wykaz ataków komputerowych i ich rozpoznanie i zapobieganie im, w kontekście systemu w sieci stanowią wyzwanie, jeśli chodzi o poszukiwanie odpowiednich rozwiązań, biorąc pod uwagę ciągłe zmiany konfiguracji, różnorodność protokołów w sieci i mnogość oferowanych i rozwiniętych usług, a także ogromna złożoność asynchronicznych sposobów ataku ([16]).

2.7 Jednakże niewielka widoczność zwrotu z inwestycji w rozwiązania w zakresie bezpieczeństwa oraz niedostateczna świadomość ponoszonej odpowiedzialności ze strony indywidualnych użytkowników doprowadziły do zaniżenia oceny ryzyka i co za tym idzie, zmniejszenia uwagi poświęconej rozwojowi kultury bezpieczeństwa.

3. **Propozycje Komisji**

3.1 Publikując komunikat w sprawie strategii na rzecz bezpiecznego społeczeństwa informacyjnego ([17]) Komisja zmierza do poprawy bezpieczeństwa informatycznego poprzez wdrożenie dynamicznej i zintegrowanej strategii opartej na:

a) intensyfikacji dialogu Komisji z władzami publicznymi, poprzez analizę porównawczą krajowych polityk i określenie najlepszych rozwiązań w dziedzinie łączności elektronicznej w bezpiecznym otoczeniu;

b) szerszym informowaniu obywateli i MŚP o skutecznych systemach bezpieczeństwa, przy aktywnej i stymulującej roli Komisji i większym zaangażowaniu Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA);

c) dialogu na temat narzędzi i instrumentów regulacyjnych w celu uzyskania odpowiedniej równowagi między bezpieczeństwem a ochroną podstawowych praw, w tym prawa do prywatności.

3.2 Ponadto komunikat przewiduje, w perspektywie rozwoju odpowiednich ram dla gromadzenia danych na temat incydentów związanych z bezpieczeństwem, na temat poziomu zaufania konsumentów i rozwoju branży zajmującej się bezpieczeństwem informatycznym, wypracowanie przez ENISA opartego na zaufaniu partnerstwa z:

a) państwami członkowskimi,

b) konsumentami i użytkownikami,

c) branżą zajmującą się bezpieczeństwem informatycznym,

d) sektorem prywatnym,

poprzez utworzenie wielojęzycznego wspólnotowego portalu informującego i ostrzegającego o zagrożeniach w celach zapewnienia strategicznego partnerstwa między sektorem prywatnym, państwami członkowskimi i naukowcami.

3.2.1 Komunikat przewiduje ponadto zwiększenie świadomości zainteresowanych stron na temat potrzeb i zagrożeń w dziedzinie bezpieczeństwa.

3.2.2 Co się tyczy współpracy międzynarodowej i współpracy z krajami trzecimi, „globalny wymiar bezpieczeństwa sieci i informacji stanowi dla Komisji ważne wyzwanie, zarówno na poziomie międzynarodowym, jak i w przypadku współpracy z państwami członkowskimi, do zwiększenia wysiłków we wspieraniu globalnej współpracy nad bezpieczeństwem sieci i informacji" ([18]), ale wskazanie to nie jest uwzględniane w działaniach związanych z dialogiem, partnerstwem i przejmowaniem inicjatywy.

4. **Uwagi**

4.1 Komitet podziela przeprowadzoną analizę i argumenty uzasadniające tworzenie europejskiej zintegrowanej i dynamicznej strategii na rzecz bezpieczeństwa sieci i informacji, uznając, że kwestia bezpieczeństwa ma zasadnicze znaczenie dla kształtowania bardziej pozytywnego nastawienia do aplikacji IT i zwiększania zaufania do nich. Stanowisko EKES-u zostało już zresztą przedstawione w licznych opiniach ([19]).

4.1.1 Komitet powtarza ([20]), że „sieć internetowa i nowe technologie komunikacji w sieci (na przykład dynamicznie upowszechniające się telefony komórkowe i urządzenia typu palmtop zawierające funkcje multimedialne) są w oczach Komitetu podstawowymi instrumentami rozwoju gospodarki opartej na wiedzy oraz gospodarki i administracji elektronicznej".

([16]) Multivariate Statistical Analysis for Network Attacks Detection. Guangzhi Qu, Salim Hariri* — 2005 USA, Arizona — Internet Technology Laboratory, ECE Department, The University of Arizona,http://www.ece.arizona.edu/~hpdc Mazin Yousif, Intel Corporation, USA — Prace sfinansowane po części przez Intel Corporation IT R&D Council.

([17]) COM(251) 2006 z 31.5.2006 r.

([18]) Por. COM 251/2006 przedostatni ustęp rozdz. 3.

([19]) Por. następujące dokumenty:
- Opinia EKES-u w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie zatrzymywania przetwarzanych danych w związku ze świadczeniem publicznych usług łączności elektronicznej (2002 r.), zmieniającej dyrektywę 2002/58/WE, Dz.U. C 69 z 21.3.2006, str. 16
- Opinia EKES-u w sprawie komunikatu Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „i2010 Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia", Dz.U. C 110 z 9.5.2006, str. 83
- Opinia EKES-u w sprawie wniosku dotyczącego decyzji Parlamentu Europejskiego i Rady ustanawiającej wieloletni wspólnotowy program promocji bezpieczniejszego korzystania z Internetu i nowoczesnych technologii w sieci, Dz.U. C 157, z 28.6.2005, str. 136
- Opinia EKES-u w sprawie komunikatu Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Bezpieczeństwo sieci i bezpieczeństwo informacji: propozycja strategicznego podejścia europejskiego", Dz.U. C 48, z 21.2.2002, str. 33.

([20]) Por. przypis 19, ust. 3.

4.2 *Na rzecz wzmocnienia wniosków Komisji*

4.2.1 W każdym razie Komitet uznaje, że podejście zaproponowane przez Komisję, polegające na oparciu takiej strategii, zintegrowanej i dynamicznej, na dialogu otwartym, łączącym wszystkie zainteresowane strony, a w szczególności użytkowników, obejmującym wzmocnione partnerstwo i przejmowanie inicjatywy, mogłoby zostać rozszerzone w przyszłości.

4.2.2 Stanowisko to zostało już podkreślone w poprzednich opiniach: „Jeśli walka ta ma przynieść skutek, powinna bezpośrednio objąć wszystkich użytkowników internetu: należy ich szkolić i informować o niezbędnych środkach ostrożności umożliwiających zabezpieczenie się przed otrzymywaniem niebezpiecznych lub niepożądanych treści oraz uniemożliwiających innym wykorzystanie ich do przekazywania takich treści. Zdaniem Komitetu w części planu działania dotyczącej informacji i szkolenia pierwszeństwo należy przyznać mobilizacji użytkowników" ([21]).

4.2.3 Zdaniem Komitetu mobilizacja użytkowników i obywateli powinna zatem nastąpić w taki sposób, by pogodzić niezbędną ochronę informacji i sieci z wolnościami obywatelskimi oraz prawem użytkowników do korzystania z bezpiecznego dostępu po ograniczonych kosztach.

4.2.4 Należy zauważyć, że badania nad bezpieczeństwem informatycznym stanowią koszt dla użytkownika również z punktu widzenia czasu poświęconego na usunięcie lub ominięcie przeszkód. Według Komitetu byłoby konieczne ustanowienie obowiązku automatycznego instalowania systemów ochrony antywirusowej w każdym komputerze, który użytkownik mógłby aktywować lub nie, ale który istniałby od początku w produkcie.

4.3 *Na rzecz bardziej dynamicznej i innowacyjnej strategii wspólnotowej*

4.3.1 Ponadto, zdaniem Komitetu Unia powinna sobie wyznaczyć bardziej ambitne cele i wprowadzić w życie innowacyjną, zintegrowaną i dynamiczną strategię, w oparciu o nowe inicjatywy. Jak na przykład:

— mechanizmy pozwalające na cyfrową identyfikację poszczególnych użytkowników, od których zbyt często żąda się podawania danych osobowych;

— działania, prowadzone w ramach ETSI ([22]), dla ustalenia wymogów bezpiecznego użytkowania TIK, mogące przynieść dokładne i szybkie rozwiązania, dzięki ustanowieniu wspólnego progu bezpieczeństwa w całej Unii;

— działania zapobiegawcze poprzez wprowadzenie do systemów informatycznych i sieciowych minimalnych wymogów bezpieczeństwa oraz zainicjowanie działań pilotażowych w postaci kursów na temat bezpieczeństwa w szkołach wszelkiego typu i szczebla;

— utworzenie pewnych i uznanych ram prawno-regulacyjnych na szczeblu europejskim. Takie ramy, stosowane w przypadku informatyki i sieci, umożliwiłyby przejście od bezpieczeństwa informatycznego do „ubezpieczenia" informatycznego;

— wzmocnienie krajowych i europejskich mechanizmów oceny ryzyka i zwiększenie zdolności do egzekwowania przepisów prawnych i regulacyjnych w celu zwalczania przestępstw informatycznych naruszających prawo do prywatności i ochronę baz danych;

— działania zapobiegające powstawaniu monokultur informatycznych oferujących produkty i rozwiązania łatwiejsze do „przeniknięcia". Wsparcie dla zróżnicowanych innowacji wielokulturowych mających na celu stworzenie Jednolitej Europejskiej Przestrzeni Informacyjnej (SEIS, Single European Information Space).

4.3.2 Według EKES-u należałoby utworzyć punkt kontaktowy „Bezpieczeństwo TIK" (ICT-Security Focal Point) wspólny dla różnych DG ([23]). Taki punkt pozwoliłoby na działanie:

— na szczeblu służb Komisji;

— na szczeblu poszczególnych państw członkowskich przy pomocy rozwiązań horyzontalnych dla aspektów, takich jak interoperatywność, zarządzanie tożsamością, ochrona prywatności, swoboda dostępu do informacji i usług, minimalne wymogi bezpieczeństwa;

— na szczeblu międzynarodowym dla zapewnienia jednolitego stanowiska europejskiego na różnych forach międzynarodowych, takich jak ONZ, G8, OECD, ISO.

4.4 *Na rzecz wzmocnienia działań europejskich z zakresu odpowiedzialnej koordynacji*

4.4.1 EKES przypisuje równie duże znaczenie utworzeniu europejskiej sieci na rzecz bezpieczeństwa sieci i informacji (European Network and Information Security Network) pomocnej przy prowadzeniu sondaży, badań i studiów nad mechanizmami bezpieczeństwa i ich interoperacyjnością, zaawansowaną kryptografią i ochroną prywatności.

4.4.2 EKES uważa, że w tym szczególnie wrażliwym sektorze należałoby zoptymalizować rolę badań europejskich poprzez odpowiednią syntezę zawartości:

— Europejskiego Programu Badań nad Bezpieczeństwem (ESRP) ([24]) włączonego do Siódmego Programu Ramowego Badań i Rozwoju technologicznego;

([21]) Por. przypis 19, ust. 3.

([22]) ETSI, *European Telecomunications Standards Institute*, por. w szczególności seminarium z 16, 17 stycznia 2006 r. ETSI opracowało między innymi specyfikacje dotyczące bezprawnego przechwytywania informacji (TS 102 232, 102 233; 102 234), dostępu do internetu Lan Wireless (TR 102 519), podpisów elektronicznych oraz opracowało algorytmy bezpieczeństwa dla GSM, GPRS i UMTS.

([23]) Taki Punkt Kontaktowy między różnymi DG mógłby być finansowany w ramach priorytetów IST programu szczegółowego Współpraca programu ramowego FP7-RTD lub w ramach Europejskiego Programu Badań nad Bezpieczeństwem ESRP.

([24]) Por. VII PR — Program Ramowy Badań, Rozwoju Technologicznego i Demonstracji WE, Program szczegółowy Współpraca; Priorytet tematyczny Security Research (badania nad bezpieczeństwem) z budżetem 1,35 mld EUR na okres 2007-2013.

— Programu Safer internet plus;

— I Europejskiego programu ochrony infrastruktur krytycznych (EPCIP) ([25]).

4.4.3 Do tych zaleceń należałoby dodać zorganizowanie „Europejskiego dnia bezpiecznego komputera" wspartego przez krajowe kampanie edukacyjne w szkołach oraz kampanie informacyjne skierowane do konsumentów na temat procedur ochrony informacji przy pomocy PC. Oprócz, oczywiście, wszelkich informacji odnoszących się do postępów w obszernej i wciąż zmieniającej się dziedzinie technologii komputerowej.

4.4.4 Komitet wielokrotnie podkreślał, że „również przedsiębiorstwa uzależniają zastosowanie TIK w działalności od swojej oceny bezpieczeństwa elektronicznych relacji gospodarczych. W podobny sposób gotowość użytkowników do ujawniania danych dotyczących własnych kart kredytowych za pośrednictwem strony internetowej jest ściśle powiązana z ich oceną bezpieczeństwa tej transakcji" ([26]).

4.4.5 Komitet jest przekonany, że ze względu na ogromny potencjał rozwoju tego sektora niezbędne jest wprowadzenie w życie konkretnej polityki i dostosowanie aktualnych działań do zachodzących postępów. Należy powiązać inicjatywy europejskie w zakresie bezpieczeństwa informacyjnego ze zintegrowaną strategią, obalając granice sektorowe i zapewniając jednolite i bezpieczne rozpowszechnienie TIK w społeczeństwie.

4.4.6 Według Komitetu niektóre ważne strategie, takie jak obecnie analizowana, posuwają się do przodu w zbyt wolnym tempie — spowodowane jest to trudnościami biurokratycznymi i kulturowymi, jakie państwa członkowskie piętrzą przed decyzjami, które powinny być podejmowane na poziomie wspólnotowym.

4.4.7 Komitet jest również zdania, że środki wspólnotowe nie wystarczą do realizacji licznych i pilnych projektów, które mogłyby przynieść konkretne odpowiedzi na nowe problemy globalizacji, jedynie wtedy, gdyby były realizowane na poziomie wspólnotowym.

4.5 *Na rzecz zwiększonej gwarancji wspólnotowej ochrony konsumentów*

4.5.1 Komitet jest świadomy, że państwa członkowskie wprowadziły środki technologiczne na rzecz bezpieczeństwa oraz procedury zarządzania bezpieczeństwem zgodne z własnymi potrzebami i raczej koncentrują się na odmiennych aspektach. Również z tego powodu trudno jest udzielić jednoznacznej, skutecznej odpowiedzi na problemy bezpieczeństwa. Za wyjątkiem niektórych sieci administracyjnych państwa członkowskie nie prowadzą systematycznej współpracy transgranicznej, chociaż kwestie bezpieczeństwa trudno jest rozwiązać każdemu państwu z osobna.

4.5.2 Ponadto Komitet stwierdza, że Rada decyzją ramową 2005/222/WSiSW zatwierdziła ramy współpracy władz sądowych i innych właściwych władz w celu zapewnienia spójnego podejścia państw członkowskich, poprzez zbliżenie ich przepisów karnych, do problemu ataków na systemy informatyczne, w zakresie:

— nielegalnego dostępu do systemu informatycznego,

— nielegalnej ingerencji, jeśli chodzi o systemy, poprzez umyślne działanie mające na celu poważne zakłócenie lub przerwanie pracy systemu informatycznego,

— nielegalnej ingerencji w dane poprzez umyślne działanie mające na celu wymazanie, zniszczenie uszkodzenie, zniekształcenie, usunięcie lub zablokowanie danych informatycznych w systemie informatycznym,

— podżegania, pomagania lub współudziału odnośnie do ww. przestępstw.

4.5.3 Poza tym decyzja wskazuje na kryteria pozwalające ustalić odpowiedzialność osób prawnych oraz ewentualne sankcje, jakie można zastosować w wyniku stwierdzenia takiej odpowiedzialności ([27]).

4.5.4 W ramach dialogu z władzami publicznymi państw członkowskich Komitet popiera wniosek Komisji, by władze te rozpoczęły proces oceny porównawczej własnej polityki krajowej w sprawie bezpieczeństwa sieci oraz systemów informatycznych łącznie z polityką dotyczącą sektora publicznego. Taki wniosek zawarto w opinii EKES-u z 2001 r.

4.6 *Na rzecz szerzej rozpowszechnionej kultury bezpieczeństwa*

4.6.1 Co się tyczy zaangażowania branży zajmującej się bezpieczeństwem informatycznym, powinna ona zapewnić w praktyce, w celu ochrony prawa do prywatności i poufności danych osobowych, systemy nadzoru materialnego swoich instalacji i kodowania komunikatów zgodnie z postępem rozwoju techniki ([28]).

([25]) COM(2005) 576 z 17.11.2005 r.
([26]) Por. przypis 19, ust. 2.
([27]) Por. przypis 19, ust. 4.
([28]) Por. dyrektywa 97/66/WE w sprawie przetwarzania danych osobowych w sektorze telekomunikacyjnym (Dz.U. L 24 z 30.1.1998).

4.6.2 Komitet uważa, że w zakresie działań na rzecz podnoszenia świadomości publicznej niezbędne jest stworzenie prawdziwej „kultury bezpieczeństwa" pojmowanej w sposób nienaruszający swobody dostępu do informacji, swobody komunikacji i wypowiedzi. Z drugiej strony przypomina to, że wielu użytkowników nie jest świadomych wszystkich zagrożeń związanych z piractwem komputerowym, podczas gdy wielu operatorów, sprzedawców czy dostawców usług nie jest w stanie ocenić, które aspekty są wrażliwe i w jakim zakresie.

4.6.3 Jeżeli celami priorytetowymi są ochrona prywatności i danych osobowych, to konsumenci mają również prawo do naprawdę skutecznej ochrony przed bezprawnym tworzeniem profili osobowych przy pomocy oprogramowania „szpiegującego" (*spyware* lub *web bug*) czy innych metod. Należałoby również zahamować tzw. *spamming* ([29]) (masowe rozsyłanie niepożądanych wiadomości) będący często wynikiem tego typu bezprawnych działań. Ofiary ponoszą rzeczywiście koszty wskutek takich ingerencji ([30]).

4.7 *Na rzecz silniejszej i bardziej aktywnej roli Agencji UE*

4.7.1 Komitet z zadowoleniem przyjmuje bardziej wyrazistą i wzmocnioną rolę Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA), tak w działaniach na rzecz podniesienia świadomości publicznej, jak i przede wszystkim w działaniach informacyjnych i szkoleniowych dla operatorów i użytkowników, jak zresztą wspominał on w jednej z niedawnych opinii ([31]) na temat dostawy publicznych usług łączności elektronicznej.

4.7.2 Co się tyczy działań proponowanych w zakresie przejmowania inicjatywy przez każdą grupę zainteresowanych podmiotów, wydają się one skierowane na ścisłe przestrzeganie zasady pomocniczości. Pozostawione są bowiem w gestii państw członkowskich i sektora prywatnego, zgodnie z właściwymi kompetencjami.

4.7.3 ENISA powinna korzystać z wkładu oferowanego przez europejską sieć na rzecz bezpieczeństwa sieci i informacji (*European Network and Information Security Network),* aby organizować wspólne przedsięwzięcia, takie jak wielojęzyczny wspólnotowy portal informujący i ostrzegający o zagrożeniach bezpieczeństwa informatycznego, aby dostarczać interaktywnych i dostosowanych do użytkownika informacji, napisanych językiem zrozumiałym zwłaszcza dla klientów indywidualnych w różnym wieku oraz dla małych i średnich przedsiębiorstw.

Bruksela, 16 lutego 2007 r.

Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego
Dimitris DIMITRIADIS

([29]) Po francusku „pollupostage".
([30]) Por. Opinie EKES-u w sprawie Sieci komunikacji elektronicznej (Dz.U. C 123 z 25.4.2001, str. 50, Handel elektroniczny (Dz.U. C 169 z 6.6.1999, str. 36 i *Oddziaływanie handlu elektronicznego na jednolity rynek* (Dz.U. C 123 z 25.4.2001, str. 1).
([31]) Por. przypis 19, ust. 1.