Komisja Spraw Zagranicznych

2010/0273(COD)

28.11.2011

OPINIA

Komisji Spraw Zagranicznych

dla Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady 2005/222/WSiSW
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Sprawozdawczyni komisji opiniodawczej: Kristiina Ojuland

PA_Legam

ZWIĘZŁE UZASADNIENIE

W opinii stanowczo opowiedziano się za koniecznością zapewnienia lepszej wymiany informacji związanych z bezpieczeństwem cybernetycznym między państwami członkowskim w obliczu narastających obaw dotyczących ewentualnych ataków cybernetycznych. Należy niezwłocznie zająć się kwestią bezpieczeństwa cybernetycznego na szczeblu UE i w drodze skoordynowanych działań państw członkowskich.

W opinii podkreślono rolę Komisji w ułatwianiu propagowania i koordynowania obecnie realizowanych inicjatyw.

Komisja Spraw Zagranicznych wraz z Podkomisją Bezpieczeństwa i Obrony uważają, że ogromne znaczenie ma pilne podjęcie działań i lepsze koordynowanie reakcji, inicjatyw i programów na szczeblu UE. Należy wspierać rozwój zdolności i zacieśniać współpracę w celu zwiększenia poziomu bezpieczeństwa informacji.

W opinii wyrażono poparcie dla koncepcji powołania koordynatora ds. bezpieczeństwa cybernetycznego UE, aby ułatwić integrację i koordynację różnych europejskich działań i inicjatyw podejmowanych na szczeblu UE i przez poszczególne instytucje unijne.

POPRAWKI

Komisja Spraw Zagranicznych zwraca się do Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, jako do komisji przedmiotowo właściwej, o naniesienie w swoim sprawozdaniu następujących poprawek:

Poprawka 1

Wniosek dotyczący dyrektywy
Punkt 1 preambuły

Tekst proponowany przez Komisję	*Poprawka*
(1) Niniejsza dyrektywa ma na celu zbliżenie przepisów prawa karnego w państwach członkowskich w dziedzinie ataków na systemy informatyczne oraz poprawę współpracy między organami sądowymi i innymi właściwymi organami, w tym policją i pozostałymi wyspecjalizowanymi organami ścigania państw członkowskich.	(1) Niniejsza dyrektywa ma na celu zbliżenie przepisów prawa karnego w państwach członkowskich w dziedzinie ataków na systemy informatyczne oraz poprawę współpracy między organami sądowymi i innymi właściwymi organami, w tym policją i pozostałymi wyspecjalizowanymi organami ścigania państw członkowskich ***i Unii; cel ten jest zgodny z ogólną strategią Unii w***

	dziedzinie zwalczania przestępczości zorganizowanej, zwiększenia odporności sieci komputerowych, ochrony krytycznej infrastruktury informatycznej oraz ochrony danych.

Poprawka 2

Wniosek dotyczący dyrektywy
Punkt 1 a preambuły (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(1a) Systemy informatyczne są kluczowym elementem współpracy politycznej, społecznej i gospodarczej w Unii. Zależność społeczeństwa od systemów informatycznych jest coraz większa. Jednocześnie jednak, choć systemy informatyczne mają wiele zalet, to powodują także szereg zagrożeń dla naszego bezpieczeństwa z uwagi na swą złożoność i podatność na różnego rodzaju cyberataki. Z tego powodu bezpieczeństwo systemów informatycznych powinno być przedmiotem stałej troski i wymaga skutecznych reakcji ze strony państw członkowskich i Unii.

Poprawka 3

Wniosek dotyczący dyrektywy
Punkt 2 preambuły

Tekst proponowany przez Komisję	*Poprawka*
(2) Ataki na systemy informatyczne***, w szczególności ze względu na zagrożenie ze strony przestępczości zorganizowanej,*** są coraz bardziej niebezpieczne, narastają również obawy o możliwość ataków o charakterze terrorystycznym lub mających podłoże polityczne ukierunkowanych na systemy informatyczne stanowiące element infrastruktury krytycznej państw członkowskich i Unii. Zagraża to dążeniom	(2) Ataki na systemy informatyczne są coraz bardziej niebezpieczne***. Mogą wynikać z terroryzmu lub zorganizowanej przestępczości i mogą być dokonywane przez państwa lub jednostki.*** Narastają obawy o możliwość ataków mających charakter terrorystyczny lub podłoże polityczne ukierunkowanych na systemy informatyczne stanowiące element infrastruktury krytycznej państw

do zapewnienia bezpieczniejszego społeczeństwa informacyjnego oraz przestrzeni wolności, bezpieczeństwa i sprawiedliwości, dlatego też wymaga reakcji na szczeblu Unii Europejskiej.	członkowskich i Unii. ***Charakter transgraniczny pewnych przestępstw i stosunkowo niskie ryzyko i koszt dla przestępców w połączeniu ze znacznymi korzyściami, jakie mogą uzyskać i szkodami, jakie mogą wyrządzić takie ataki poważnie zwiększa poziom zagrożenia.*** Zagraża to dążeniom do zapewnienia bezpieczniejszego społeczeństwa informacyjnego oraz przestrzeni wolności, bezpieczeństwa i sprawiedliwości, dlatego też wymaga reakcji ***nie tylko*** na szczeblu Unii Europejskiej***, ale także ze strony społeczności międzynarodowej***.

Poprawka 4

Wniosek dotyczący dyrektywy
Punkt 3 preambuły

Tekst proponowany przez Komisję	*Poprawka*
(3) Istnieją dowody wskazujące na tendencję do coraz bardziej niebezpiecznych i ponawianych ataków na wielką skalę przeprowadzanych na systemy informatyczne o zasadniczym znaczeniu dla państw lub poszczególnych funkcji w sektorze publicznym lub prywatnym. Tendencji tej towarzyszy w coraz szerszym stopniu tworzenie coraz bardziej wyrafinowanych narzędzi, z których przestępcy mogą korzystać do przeprowadzania różnego rodzaju cyberataków.	(3) Istnieją dowody wskazujące na tendencję do coraz bardziej niebezpiecznych i ponawianych ataków na wielką skalę przeprowadzanych na systemy informatyczne o zasadniczym znaczeniu dla państw ***członkowskich, Unii*** lub poszczególnych funkcji w sektorze publicznym lub prywatnym***, a także na szczeblu UE***. Tendencji tej towarzyszy w coraz szerszym stopniu ***szybkie*** tworzenie ***technologii informatycznych, a co za tym idzie*** coraz bardziej wyrafinowanych narzędzi, z których przestępcy mogą korzystać do przeprowadzania różnego rodzaju cyberataków***, niekiedy posiadających wielki potencjał powodowania szkód gospodarczych i społecznych***.

Poprawka 5

Wniosek dotyczący dyrektywy
Punkt 4 a preambuły (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4a) Należy przeprowadzić dokładną, wiarygodną i niezależną ocenę ogólnego poziomu zagrożenia atakami na systemy informatyczne. Instytucje unijne powinny odpowiednio dostosować swoje poziomy bezpieczeństwa informacji.

Poprawka 6

Wniosek dotyczący dyrektywy
Punkt 4 b preambuły (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4b) Istnieje potrzeba koordynacji na szczeblu Unii, aby przyczynić się do zintegrowania różnorakich inicjatyw, programów i działań.

Poprawka 7

Wniosek dotyczący dyrektywy
Punkt 6 preambuły

Tekst proponowany przez Komisję	*Poprawka*
(6) Państwa członkowskie powinny przewidzieć kary za ataki na systemy informatyczne. Przewidziane kary powinny być skuteczne, proporcjonalne i odstraszające.	(6) Państwa członkowskie powinny przewidzieć kary za ataki na systemy informatyczne***, które powinny się wpisywać w szersze strategie krajowe na rzecz zapobiegania tego rodzaju atakom i ich zwalczania***. Przewidziane kary powinny być skuteczne, proporcjonalne i odstraszające. ***Z uwagi na międzynarodowy charakter zagrożeń niezbędne jest dostosowanie sankcji i kar nakładanych w państwach członkowskich, a tym samym zmniejszenie różnic między państwami członkowskimi podczas zajmowania się popełnianymi w Unii przestępstwami.***

Poprawka 8

Wniosek dotyczący dyrektywy
Punkt 8 a preambuły (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(8a) Rada i Komisja powinny wezwać te państwa członkowskie, które nie ratyfikowały jeszcze konwencji Rady Europy o cyberprzestępczości, do jej niezwłocznej ratyfikacji.

Poprawka 9

Wniosek dotyczący dyrektywy
Punkt 11 a preambuły (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(11a) Współpraca władz publicznych z sektorem prywatnym i ze społeczeństwem obywatelskim ma wielkie znaczenie w zapobieganiu atakom na systemy informatyczne i zwalczaniu ich. Należy nawiązać stały dialog z tym sektorem z uwagi na szerokie korzystanie przez niego z systemów informatycznych i wspólną odpowiedzialność, która wymaga stabilności i prawidłowego funkcjonowania systemów. Większa świadomość zagrożeń u wszystkich podmiotów korzystających z systemów informatycznych wytworzy kulturę dbania o bezpieczeństwo informatyczne.

Poprawka 10

Wniosek dotyczący dyrektywy
Punkt 11 b preambuły (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(11b) Należy zachęcać do wdrażania inicjatyw i projektów związanych z obroną

	przed atakami cybernetycznymi, na przykład takich, jakie niedawno były realizowane w ramach Europejskiej Agencji Obrony (EAO), aby wspierać zdolności obronne państw członkowskich. Należy przewidzieć ściślejszą współpracę zarówno z EAO, jak i z Centrum Doskonałości NATO ds. Współpracy w Dziedzinie Obrony przed Cyberatakami (CCDCOE), w szczególności w obszarze budowania potencjału oraz szkoleń.

Poprawka 11

Wniosek dotyczący dyrektywy
Punkt 12 preambuły

Tekst proponowany przez Komisję	*Poprawka*
(12) Zachodzi potrzeba gromadzenia danych o przestępstwach, o których mowa w niniejszej dyrektywie, w celu uzyskania bardziej kompletnego obrazu problemu na szczeblu Unii, a tym samym przyczynienia się do opracowania skuteczniejszych środków zaradczych. Dane te pomogą ponadto wyspecjalizowanym agencjom, takim jak Europol i Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji, lepiej ocenić zakres zjawiska cyberprzestępczości oraz stan bezpieczeństwa sieci i informacji w Europie.	(12) Zachodzi potrzeba gromadzenia danych o przestępstwach, o których mowa w niniejszej dyrektywie, w celu uzyskania bardziej kompletnego obrazu problemu na szczeblu Unii, a tym samym przyczynienia się do opracowania skuteczniejszych środków zaradczych. ***Państwa członkowskie powinny zwiększyć wymianę informacji na temat ataków na systemy informatyczne przy wsparciu Komisji i Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji.*** Dane te pomogą ponadto wyspecjalizowanym agencjom, takim jak Europol i Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji, lepiej ocenić zakres ***i skutki*** zjawiska cyberprzestępczości oraz stan bezpieczeństwa sieci i informacji w Europie. ***Lepsza znajomość aktualnych i przyszłych zagrożeń umożliwi podejmowanie decyzji skuteczniej zapobiegających atakom na systemy informatyczne i zwalczającym je oraz zmniejszającym powodowane przez nie szkody.***

Poprawka 12

Wniosek dotyczący dyrektywy
Punkt 12 a preambuły (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(12a) Wymiana informacji oraz partnerstwa publiczno-prywatne (PPP) odgrywają istotną rolę w poprawie bezpieczeństwa cybernetycznego. Dlatego Komisja powinna zbadać, czy możliwe jest zapewnienie ram lub instrumentów wspomagających wzajemną współpracę PPP na szczeblu krajowym i unijnym, w celu wdrażania standardów jakości informacji w odniesieniu do interoperacyjności oraz zagwarantowania poszanowania praw podstawowych, rozdziału władz i nadzoru demokratycznego.

Poprawka 13

Wniosek dotyczący dyrektywy
Punkt 13 preambuły

Tekst proponowany przez Komisję	*Poprawka*
(13) Znaczące luki i różnice w przepisach państw członkowskich w dziedzinie ataków na systemy informatyczne mogą utrudniać walkę z przestępczością zorganizowaną i terroryzmem oraz komplikować skuteczną współpracę sądową i policyjną w tej dziedzinie. Międzynarodowy i transgraniczny charakter współczesnych systemów informatycznych nadaje atakom na takie systemy wymiar transgraniczny, przez co jeszcze pilniejsza staje się potrzeba dalszych działań na rzecz zbliżenia przepisów prawnokarnych w tej dziedzinie. Ponadto koordynacja ścigania przypadków ataków na systemy informatyczne powinna zostać ułatwiona dzięki przyjęciu decyzji ramowej Rady 2009/948/WSiSW w	(13) Znaczące luki i różnice w przepisach państw członkowskich w dziedzinie ataków na systemy informatyczne mogą utrudniać walkę z przestępczością zorganizowaną i terroryzmem oraz komplikować skuteczną współpracę sądową i policyjną w tej dziedzinie. Międzynarodowy i transgraniczny charakter współczesnych systemów informatycznych nadaje atakom na takie systemy wymiar transgraniczny, przez co jeszcze pilniejsza staje się potrzeba dalszych działań na rzecz zbliżenia przepisów prawnokarnych w tej dziedzinie ***w całej Unii***. ***Ponadto na szczeblu Unii należy dążyć do ściślejszej współpracy międzynarodowej w dziedzinie bezpieczeństwa sieci i systemów***

sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów.	***informatycznych blisko współpracując z innymi organizacjami posiadającymi kompetencje w tym zakresie, takimi jak Organizacja Narodów Zjednoczonych, NATO, Rada Europy lub OBWE i angażując inne odnośne podmioty międzynarodowe.*** Ponadto koordynacja ścigania przypadków ataków na systemy informatyczne powinna zostać ułatwiona dzięki przyjęciu decyzji ramowej Rady 2009/948/WSiSW w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów.

Poprawka 14

Wniosek dotyczący dyrektywy
Punkt 16 preambuły

Tekst proponowany przez Komisję	*Poprawka*
(16) Niniejsza dyrektywa ***respektuje*** prawa podstawowe oraz ***jest zgodna z*** zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej, w tym z zasadami ochrony danych osobowych, swobody wypowiedzi i informacji, prawem do rzetelnego procesu, domniemaniem niewinności i prawem do obrony, jak również zasadami legalizmu i proporcjonalności przestępstw i kar kryminalnych. W szczególności niniejsza dyrektywa zmierza do pełnego zagwarantowania poszanowania tych praw i zasad oraz musi być odpowiednio do tego wdrażana.	(16) Niniejsza dyrektywa ***i wszelkie jej praktyczne zastosowania respektują*** prawa podstawowe***, w szczególności prawo do prywatności,*** oraz ***są zgodne*** z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej, w tym z zasadami ochrony danych osobowych, swobody wypowiedzi i informacji, prawem do rzetelnego procesu, domniemaniem niewinności i prawem do obrony, jak również zasadami legalizmu i proporcjonalności przestępstw i kar kryminalnych. W szczególności niniejsza dyrektywa zmierza do pełnego zagwarantowania poszanowania tych praw i zasad oraz musi być odpowiednio do tego wdrażana. ***Niniejsza dyrektywa nie narusza wolnego i otwartego charakteru internetu.***

Poprawka 15

Wniosek dotyczący dyrektywy
Punkt 16 a preambuły (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(16a) Rada i Komisja powinny w negocjacjach i podczas współpracy z krajami trzecimi nalegać na ustanowienie minimalnych wymogów w zakresie zapobiegania i zwalczania cyberprzestępczości i cyberataków, jak również minimalnych standardów bezpieczeństwa systemów informatycznych.

Poprawka 16

Wniosek dotyczący dyrektywy
Punkt 16 b preambuły (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(16b) Komisja powinna rozważyć możliwości wspomożenia krajów trzecich w ich działaniach na rzecz rozwoju ich potencjału w zakresie cyberbezpieczeństwa i cyberobrony.

Poprawka 17

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 2a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	2a. Komisja pomaga państwom członkowskim w promowaniu odporności i stabilności internetu oraz podejmuje inne działania służące zapewnieniu bezpieczeństwa informacji.

Poprawka 18

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 2b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	2b. Rada objaśnia rolę Komitetu Politycznego i Bezpieczeństwa oraz innych jego organów w kontekście obrony przed potencjalnymi atakami cybernetycznymi.

Poprawka 19

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 2c (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	2c. Państwa członkowskie usprawniają wymianę informacji związanych z bezpieczeństwem cybernetycznym. Korzystając ze wsparcia Komisji, państwa członkowskie powinny dążyć do nawiązania stosunków z państwami trzecimi, zwłaszcza z tymi, z których najczęściej przeprowadzane są ataki.

Poprawka 20

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Państwa członkowskie przekazują Komisji dane zgromadzone zgodnie z niniejszym artykułem. Państwa członkowskie ***zapewniają*** również ***publikację skonsolidowanego*** zestawienia tych sprawozdań statystycznych.	3. Państwa członkowskie przekazują Komisji dane zgromadzone zgodnie z niniejszym artykułem. Państwa członkowskie ***dbają*** również ***o to, by skonsolidowane*** zestawienia tych sprawozdań statystycznych ***były przedkładane Parlamentowi Europejskiemu i publikowane***.

Poprawka 21

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 3a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	3a. Koordynator Unii ds. cyberbezpieczeństwa jest powoływany w celu ułatwienia integracji i koordynacji unijnych inicjatyw, programów i działań podejmowanych przez instytucje Unii.

PROCEDURA

Tytuł	Ataki na systemy informatyczne i uchylenie decyzji ramowej Rady 2005/222/WSiSW
Odsyłacze	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)
Komisja(e) przedmiotowo właściwa(e) Data ogłoszenia na posiedzeniu	LIBE 7.10.2010
Komisja(e) wyznaczona(e) do wydania opinii Data ogłoszenia na posiedzeniu	AFET 7.4.2011
Sprawozdawca(y) Data powołania	Kristiina Ojuland 29.3.2011
Data przyjęcia	22.11.2011
Wynik głosowania końcowego	+: 38 –: 8 0: 0
Posłowie obecni podczas głosowania końcowego	Sir Robert Atkins, Frieda Brepoels, Elmar Brok, Marietta Giannakou, Andrzej Grzyb, Takis Hadjigeorgiou, Anna Ibrisagic, Othmar Karas, Ioannis Kasoulides, Tunne Kelam, Evgeni Kirilov, Andrey Kovatchev, Eduard Kukan, Krzysztof Lisek, Sabine Lösing, Ulrike Lunacek, Barry Madlener, Francisco José Millán Mon, Annemie Neyts-Uyttebroeck, Raimon Obiols, Justas Vincas Paleckis, Ioan Mircea Paşcu, Cristian Dan Preda, Libor Rouček, José Ignacio Salafranca Sánchez-Neyra, Jacek Saryusz-Wolski, Werner Schulz, Marek Siwiec, Charles Tannock, Inese Vaidere, Kristian Vigenin, Sir Graham Watson
Zastępca(y) obecny(i) podczas głosowania końcowego	Laima Liucija Andrikienė, Elena Băsescu, Tanja Fajon, Diogo Feio, Monica Luisa Macovei, Emilio Menéndez del Valle, György Schöpflin, Traian Ungureanu, Ivo Vajgl, Renate Weber, Janusz Władysław Zemke
Zastępca(y) (art. 187 ust. 2) obecny(i) podczas głosowania końcowego	Luís Paulo Alves, Sylvie Guillaume, Vladimir Urutchev