Stanovisko Európskeho hospodárskeho a sociálneho výboru na tému „Návrh nariadenia Európskeho parlamentu a Rady o Európskej agentúre pre bezpečnosť sietí a informácií (ENISA)“

[KOM(2010) 521 v konečnom znení]

(2011/C 107/12)

Spravodajca: **pán MORGAN**

Rada sa 19. októbra 2010 rozhodla podľa článku 114 Zmluvy o fungovaní Európskej únie prekonzultovať s Európskym hospodárskym a sociálnym výborom

„*Návrh nariadenia Európskeho parlamentu a Rady o Európskej agentúre pre bezpečnosť sietí a informácií (ENISA)*“

KOM(2010) 521 v konečnom znení.

Odborná sekcia pre dopravu, energetiku, infraštruktúru a informačnú spoločnosť poverená vypracovaním návrhu stanoviska výboru v danej veci prijala svoje stanovisko 2. februára 2011.

Európsky hospodársky a sociálny výbor na svojom 469. plenárnom zasadnutí 16. a 17. februára 2011 (schôdza zo 17. februára) prijal 173 hlasmi za, pričom nikto nehlasoval proti a 5 členovia sa hlasovania zdržali, nasledujúce stanovisko:

1. **Závery a odporúčania**

1.1 EHSV si veľmi dobre uvedomuje mieru, do akej je v súčasnej dobe občianska spoločnosť závislá od služieb poskytovaných cez internet. Výbor tiež znepokojuje relatívna neinformovanosť občianskej spoločnosti vo veciach jej vlastnej počítačovej bezpečnosti. EHSV zastáva názor, že Európska agentúra pre bezpečnosť sietí a informácií (ENISA) je agentúrou zodpovednou za pomoc členským štátom a poskytovateľom služieb pri zvyšovaní všeobecných bezpečnostných noriem s tým cieľom, aby všetci užívatelia internetu urobili potrebné kroky na ich vlastnú osobnú bezpečnosť v oblasti informačných technológií.

1.2 EHSV preto podporuje návrh budovať agentúru ENISA s cieľom prispieť k vysokej úrovni bezpečnosti sietí a informácií v rámci EÚ a s cieľom zvýšiť informovanosť a rozvíjať v spoločnosti kultúru bezpečnosti sietí a informácií v prospech občanov, spotrebiteľov, podnikov a organizácií verejného sektora v Európskej únii, a tým pomôcť k hladkému fungovaniu vnútorného trhu.

1.3 Agentúra ENISA má kľúčovú úlohu z hľadiska bezpečného vývoja sieťovej infraštruktúry verejnej správy, priemyslu, obchodu a občianskej spoločnosti v EÚ. EHSV očakáva od Európskej komisie stanovenie maximálnych výkonnostných noriem pre agentúru ENISA a monitorovanie jej výkonu v kontexte vývoja a vzniku hrozieb v oblasti počítačovej bezpečnosti.

1.4 Všetky stratégie v oblasti informačných technológií, tak ako ich navrhli NATO, Europol a Európska komisia, závisia od účinnej spolupráce s členskými štátmi, ktoré sami disponujú širokou škálou vlastných agentúr zaoberajúcich sa otázkami počítačovej bezpečnosti. Stratégie NATO a Europolu majú byť proaktívne a operatívne. Agentúra ENISA je v rámci stratégie Európskej komisie evidentne dôležitou súčasťou komplexného súboru agentúr a misií zameraných na ochranu kritických informačných infraštruktúr (CIIP). Napriek tomu, že nové nariadenie neobsahuje návrh operatívnej úlohy agentúry ENISA, EHSV ju stále vníma ako agentúru, ktorá je v prvom rade zodpovedná za CIIP v občianskej spoločnosti EÚ.

1.5 Operatívna zodpovednosť za počítačovú bezpečnosť na úrovni členských štátov prináleží členským štátom, ale normy CIIP sú v 27 členských štátoch evidentne nejednotné. Úlohou agentúry ENISA je dostať menej vybavené členské štáty na prijateľnú úroveň. Musí zabezpečiť spoluprácu medzi členskými štátmi a pomáhať im pri uplatňovaní najlepšieho postupu. V kontexte cezhraničných hrozieb musí byť úlohou agentúry ENISA varovanie a prevencia.

1.6 Zároveň je potrebné, aby sa agentúra ENISA podieľala na medzinárodnej spolupráci s mocnosťami mimo EÚ. Takáto spolupráca bude vysoko politická a bude zahŕňať mnoho oblastí EÚ, ale EHSV sa domnieva, že agentúra ENISA si musí nájsť svoje miesto na medzinárodnej politickej scéne.

1.7 Výbor sa domnieva, že agentúra ENISA môže mať veľmi cennú úlohu pri podpore a iniciovaní výskumných projektov v oblasti bezpečnosti.

1.8 EHSV v rámci hodnotenia vplyvu v súčasnosti nepodporí uplatňovanie možností č. 4 a 5 v plnom rozsahu, na základe ktorých by sa ENISA stala operačnou agentúrou. Počítačová bezpečnosť predstavuje taký obrovský problém s dynamicky sa vyvíjajúcimi hrozbami, že si členské štáty musia zachovať schopnosť proaktívne bojovať proti týmto hrozbám. Rozvoj

operačných agentúr na úrovni EÚ sa obyčajne končí stratou schopnosti na strane členských štátov. V oblasti počítačovej bezpečnosti platí opak: členské štáty musia svoje schopnosti zlepšovať.

1.9 EHSV chápe postoj Komisie, podľa ktorého by agentúra ENISA mala mať jasne vymedzené a dobre kontrolované poslanie so zodpovedajúcimi zdrojmi. Rovnako sa však EHSV obáva, že mandát agentúry ENISA časovo ohraničený na 5 rokov môže obmedziť dlhodobé projekty a ohroziť rozvoj ľudského kapitálu a vedomostí v rámci agentúry. Pôjde totiž o pomerne malú agentúru zaoberajúcu sa veľkým a stále narastajúcim problémom. Oblasť a rozsah poslania agentúry ENISA naznačuje, že musí zamestnávať tímy špecialistov. Ich práca bude pozostávať z kombinácie krátkodobých úloh a dlhodobých projektov. Výbor by preto uprednostnil taký mandát agentúry ENISA, ktorý by bol dynamický a časovo neohraničený, pričom by bol potvrdzovaný na priebežnej báze prostredníctvom pravidelných posúdení a hodnotení. Zdroje by bolo následne možné postupne prideľovať tak, ako a kedy budú opodstatnené.

2. **Úvod**

2.1 Toto stanovisko sa týka nariadenia o ďalšom rozvoji agentúry ENISA.

2.2 Komisia predložila svoj prvý návrh politického prístupu k bezpečnosti sietí a informácií v oznámení z roku 2001 [KOM(2001) 298 v konečnom znení]. Pán Retureau vypracoval komplexné stanovisko ([1]) ako odpoveď na oznámenie.

2.3 Komisia následne navrhla nariadenie o zriadení agentúry ENISA [KOM(2003) 63 v konečnom znení]. Stanovisko EHSV ([2]) k tomuto nariadeniu napísal pán Lagerholm. Agentúra bola skutočne zriadená nariadením (ES) č. 460/2004.

2.4 S exponenciálnym nárastom využívania internetu sa bezpečnosť informácií stala predmetom rastúceho znepokojenia. Komisia v roku 2006 vydala oznámenie, v ktorom načrtáva stratégiu pre bezpečnú informačnú spoločnosť [KOM(2006) 251 v konečnom znení]. Autorom stanoviska EHSV ([3]) bol pán Pezzini.

2.5 S rastúcimi obavami o informačnú bezpečnosť prišla Komisia v roku 2009 s návrhom na ochranu kritických informačných infraštruktúr [KOM(2009) 149 v konečnom znení]. Pán McDonogh bol autorom stanoviska ([4]), ktoré bolo prijaté na plenárnom zasadnutí EHSV v decembri 2009.

2.6 V súčasnosti sa navrhuje posilnenie a zlepšenie agentúry ENISA s cieľom prispieť k vysokej úrovni bezpečnosti sietí a informácií v rámci EÚ a zvýšiť informovanosť a rozvíjať v spoločnosti kultúru bezpečnosti sietí a informácií v prospech občanov, spotrebiteľov, podnikov a organizácií verejného sektora v Európskej únii, a tým pomôcť k hladkému fungovaniu vnútorného trhu.

2.7 Agentúra ENISA však nie je jedinou bezpečnostnou agentúrou, ktoré je plánovaná pre kybernetický priestor EÚ. Reakcia na kybernetickú vojnu a kybernetický terorizmus je záležitosťou ozbrojených síl. V tejto oblasti je hlavnou agentúrou NATO. Podľa svojej novej strategickej koncepcie zverejnenej v novembri 2010 v Lisabone (dostupná na internetovej adrese http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf) bude NATO *ďalej rozvíjať svoju schopnosť predchádzať počítačovým útokom, odhaľovať ich, poskytovať ochranu voči nim a zaisťovať nápravu, a to aj prostredníctvom využitia svojho plánovacieho procesu s cieľom zlepšiť a koordinovať schopnosti štátov v oblasti kybernetickej obrany, začlenenia všetkých svojich orgánov pod centralizovanú počítačovú ochranu a lepšej integrácie medzi NATO a členskými štátmi, pokiaľ ide o kybernetickú informovanosť, varovanie a reakcie.*

2.8 Po počítačovom útoku voči Estónsku v roku 2007 bolo 14. mája 2008 oficiálne založené Kooperatívne centrum excelencie kybernetickej obrany (CCD COE) s cieľom zvyšovať kybernetickú obrannú schopnosť NATO. Centrum, ktorého sídlo sa nachádza v estónskom Tallinne, je výrazom medzinárodného úsilia, na ktorom sa v súčasnosti ako sponzorujúce krajiny podieľajú Estónsko, Lotyšsko, Litva, Nemecko, Maďarsko, Taliansko, Slovenská republika a Španielsko.

2.9 Elektronická kriminalita na úrovni EÚ patrí do oblasti pôsobnosti Europolu. Nasleduje úryvok z dokumentu predloženého agentúrou Europol hornej komore britského parlamentu (pozri http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68we05.htm):

Je zrejmé, že agentúry presadzujúce právo potrebujú držať krok s technologickým napredovaním páchateľov trestných činov, aby mohli zabezpečiť, že trestným činom, ktorých sa dopúšťajú, je možné účinne zabrániť alebo ich je možné odhaliť. Vzhľadom na to, že vyspelé technológie nie sú limitované hranicami, musia byť ďalej schopnosti v rámci EÚ na podobne vysokej úrovni, aby nedošlo k vzniku „slabých miest", v ktorých kriminalita založená na vyspelých technológiách môže beztrestne prekvitať. Tieto schopnosti v rámci EÚ zďaleka nie sú homogénne. V skutočnosti ide o zjavne asymetrický vývoj, keď niektoré členské štáty (ČŠ) rýchlo postupujú so značným pokrokom v určitých oblastiach, pričom iné členské štáty z technologického pohľadu zaostávajú. Vytvára to potrebu mať centralizovanú službu, ktorá bude všetkým členským štátom pomáhať pri koordinácii spoločných aktivít, presadzovaní štandardizácie prístupov a noriem kvality a pri identifikácii a výmene osvedčených postupov. Iba týmto spôsobom je možné zabezpečiť homogénne presadzovanie práva EÚ v boji proti kriminalite založenej na vyspelých technológiách.

([1]) Ú. v. ES C 48, 21.2.2002, s. 33.
([2]) Ú. v. EÚ C 220, 16.9.2003, s. 33.
([3]) Ú. v. EÚ C 97, 28.4.2007, s. 21.
([4]) Ú. v. EÚ C 255, 22.9.2010, s. 98.

2.10 V roku 2002 bolo zriadené Stredisko Europolu zamerané na boj proti trestnej činnosti páchanej prostredníctvom moderných technológií (HTCC). Ide o relatívne malý útvar, ale očakáva sa, že bude v budúcnosti rásť a bude ústredným bodom činnosti Europolu v tejto oblasti. HTCC zohráva hlavnú úlohu pri koordinácii, operačnej podpore, strategickej analýze a školeniach. Školiaca funkcia je mimoriadne dôležitá. Europol ďalej zriadil Európsku platformu na boj proti počítačovej kriminalite (ECCP). Zameriava sa na nasledujúce témy:

— on-line systém nahlasovania internetovej kriminality (*The Internet Crime Reporting Online System,* I-CROS),

— analytický pracovný súbor (Cyborg),

— systém *The Internet and Forensic Expertise recipient* (I-FOREX).

2.11 Stratégia počítačovej bezpečnosti EÚ je načrtnutá v Digitálnej agende pre Európu v kapitole s názvom „Dôvera a bezpečnosť". Výzvy sú opísané takto:

„Internet sa doteraz osvedčil ako mimoriadne bezpečný, odolný a stabilný, ale siete IT a terminály konečných používateľov sú naďalej vystavené rozmanitým a vyvíjajúcim sa hrozbám: v uplynulých rokoch narástol objem nevyžiadaných komerčných elektronických správ (spamu) do tej miery, že spôsobujú vážne zápchy v e-mailovom styku – z rozličných odhadov vyplýva, že predstavujú 80 % až 98 % všetkých zasielaných e-mailov – a šíri sa nimi aj veľká škála vírusov a škodlivého softvéru. Rozmáhajú sa aj krádeže totožností a online podvody. Útoky sú čoraz sofistikovanejšie (trójske kone, botnety atď.) a často sú motivované finančným ziskom. Ich motívy sú neraz aj politického rázu, čoho sme boli svedkami pri počítačových útokoch proti Estónsku, Litve a Gruzínsku".

2.12 Záväzné opatrenia prijaté v agende sú:

Kľúčové opatrenie 6: v roku 2010 predostrieť návrhy opatrení zamerané na posilnenie **politiky v oblasti bezpečnosti sietí a informácií vysokej úrovne** vrátane legislatívnych iniciatív, napríklad iniciatívy týkajúcej sa modernizácie agentúry ENISA, ako aj opatrenia umožňujúce rýchlejšie reagovať v prípade počítačových útokov vrátane tímu reakcie na núdzové počítačové situácie (CERT) pre inštitúcie EÚ;

Kľúčové opatrenie 7: predložiť návrh opatrenia vrátane legislatívnych iniciatív na **boj proti počítačovým útokom na informačné systémy** do roku 2010 a súvisiace pravidlá právomoci v kybernetickom priestore na úrovni EÚ a na medzinárodnej úrovni do roku 2013.

2.13 Komisia vo svojom oznámení z novembra 2010 [KOM(2010) 673 v konečnom znení] v rámci presadzovania agendy navrhla stratégiu vnútornej bezpečnosti EÚ. Má päť cieľov, pričom tretím cieľom je zvýšiť úroveň bezpečnosti občanov a podnikov v kybernetickom priestore. V pláne sú tri akčné programy, pričom podrobnosti týkajúce sa týchto opatrení sú načrtnuté v nasledujúcej tabuľke (prevzaté z oznámenia, ktoré je dostupné na internetovej adrese http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf).

CIELE A OPATRENIA	ZODPOVEDNÝ SUBJEKT	ČASOVÝ HARMONOGRAM
CIEĽ 3: Zvýšiť úroveň bezpečnosti občanov a podnikov v kybernetickom priestore		
Opatrenie č. 1: Vybudovať kapacity v oblasti presadzovania práva a súdnictva		
Zriadenie strediska EÚ pre počítačovú kriminalitu	Závisí od výsledkov štúdie uskutočniteľnosti, ktorú KOM vypracuje v roku 2011	2013
Vybudovať kapacity v oblasti vyšetrovania a trestného stíhania počítačovej kriminality	ČŠ s CEPOL, Europol a Eurojust	2013
Opatrenie č. 2: Spolupracovať s priemyslom v záujme posilnenia a ochrany občanov		
Vytvoriť mechanizmy na hlásenie incidentov v oblasti počítačovej kriminality a poskytnúť občanom usmernenia o počítačovej bezpečnosti a počítačovej kriminalite	ČŠ, KOM, Europol, **ENISA** a súkromný sektor	Prebieha
Vypracovať usmernenia o spolupráci pri zaobchádzaní s nelegálnym obsahom na internete	KOM s ČŠ a súkromným sektorom	2011
Opatrenie č. 3: Zlepšiť schopnosť čeliť počítačovým útokom		
Vytvoriť sieť tímov reakcie na núdzové počítačové situácie v každom členskom štáte a jeden pre inštitúcie EÚ, pravidelne vypracúvať národné pohotovostné plány a pravidelne organizovať praktické cvičenia zamerané na reakcie na incidenty a nápravu po katastrofe.	ČŠ a inštitúcie EÚ s agentúrou **ENISA**	2012
Vytvoriť Európsky systém zdieľania informácií a varovania (EISAS)	ČŠ s KOM a agentúrou **ENISA**	2013

2.14 Všetky stratégie v oblasti informačných technológií, tak ako ich navrhli NATO, Europol a Európska komisia, závisia od účinnej spolupráce s členskými štátmi, ktoré sami disponujú širokou škálou vlastných agentúr zaoberajúcich sa otázkami počítačovej bezpečnosti. Stratégie NATO a Europolu majú byť proaktívne a operatívne. Agentúra ENISA je v rámci stratégie Európskej komisie evidentne dôležitou súčasťou komplexného súboru agentúr a misií zameraných na ochranu kritických informačných infraštruktúr (CIIP). Napriek tomu, že nové nariadenie neobsahuje návrh operatívnej úlohy agentúry ENISA, EHSV ju stále vníma ako agentúru, ktorá je v prvom rade zodpovedná za CIIP v občianskej spoločnosti EÚ.

3. **Návrh týkajúci sa agentúry ENISA**

3.1 Problém, ktorým sa má agentúra ENISA zaoberať, je spôsobený siedmimi faktormi:

(1) roztrieštenosť a rôznorodosť vnútroštátnych prístupov;

(2) obmedzená schopnosť európskeho včasného varovania a reakcie;

(3) nedostatok spoľahlivých údajov a obmedzenosť poznatkov o vznikajúcich problémoch;

(4) nedostatočná informovanosť o rizikách a výzvach v oblasti bezpečnosti sietí a informácií;

(5) medzinárodný rozmer problémov týkajúcich sa bezpečnosti sietí a informácií;

(6) potreba modelov spolupráce, ktoré sú určené na vykonávanie politík;

(7) potreba účinnejších opatrení v boji proti počítačovej kriminalite.

3.2 Návrh týkajúci sa agentúry ENISA poskytuje ústredný bod pre existujúce politické ustanovenia aj pre nové iniciatívy načrtnuté v Digitálnej agende pre Európu.

3.3 Existujúce politiky, ktoré má agentúra ENISA podporovať, zahŕňajú:

(i) Európske fórum pre členské štáty (EFMS) zamerané na podporu diskusie a výmenu týkajúcu sa osvedčených postupov v oblasti politiky s cieľom sledovať spoločné politické ciele a priority v oblasti bezpečnosti a odolnosti infraštruktúry IKT;

(ii) Európske verejno-súkromné partnerstvo pre odolnosť (EP3R), ktoré predstavuje flexibilný celoeurópsky riadiaci rámec pre odolnosť infraštruktúry IKT, pôsobiaci prostredníctvom podpory spolupráce medzi verejným a súkromným sektorom v otázkach bezpečnosti a odolnosti;

(iii) Štokholmský program, ktorý Európska rada prijala 11. decembra 2009, podporuje politiky zaisťujúce bezpečnosť sietí a umožňujúce rýchlejšiu reakciu v prípade počítačových útokov v Únii.

3.4 Medzi nové oblasti, ktoré by mala agentúra ENISA podporovať, patrí:

(i) zintenzívnenie činností v rámci Európskeho fóra členských štátov;

(ii) podpora EP3R prostredníctvom prediskutovania inovatívnych opatrení a nástrojov na zlepšenie bezpečnosti a odolnosti;

(iii) zavedenie bezpečnostných požiadaviek uvedených v regulačnom balíku o elektronickej komunikácii do praxe;

(iv) uľahčenie celoeurópskych cvičení zameraných na pripravenosť v oblasti počítačovej bezpečnosti;

(v) vytvorenie CERT pre inštitúcie EÚ;

(vi) mobilizácia a podpora členských štátov pri kompletizácii a v prípade potreby zriaďovaní CERT na vnútroštátnej/vládnej úrovni s cieľom vytvoriť riadne fungujúcu sieť CERT pokrývajúcu celú Európu;

(vii) zvyšovanie informovanosti o výzvach v oblasti bezpečnosti sietí a informácií.

3.5 Pred dopracovaním tohto návrhu do konečnej podoby bolo preskúmaných päť politických možností. Každá možnosť mala svoje zameranie a zodpovedajúce možnosti zdrojov. Bola vybraná tretia možnosť. Zahŕňa rozšírenie úloh, ktoré sú v súčasnosti stanovené pre agentúru ENISA, a začlenenie agentúr v oblasti presadzovania práva a ochrany súkromia ako zainteresovaných strán.

3.6 Modernizovaná agentúra zameraná na bezpečnosť sietí a informácií by v rámci možnosti č. 3 prispela k:

— Zníženiu roztrieštenosti vnútroštátnych prístupov (príčinný faktor č. 1), pribúdaniu politík a rozhodovania (príčinný faktor č. 3), ktoré sú založené na údajoch a poznatkoch, zvýšeniu celkovej informovanosti o rizikách a problémoch sieťovej a informačnej bezpečnosti a ich riešeniu (príčinný faktor č. 4), a to tak, že sa bude podieľať na:

  — účinnejšom zbere dôležitých informácií týkajúcich sa rizík, hrozieb a zraniteľnosti každým jednotlivým členským štátom,

  — zvýšenej dostupnosti informácií o súčasných a budúcich výzvach a rizikách v oblasti bezpečnosti sietí a informácií,

  — vyššej kvalite politických ustanovení týkajúcich sa bezpečnosti sietí a informácií v členských štátoch.

— Zlepšeniu schopnosti európskeho včasného varovania a reakcie (príčinný faktor č. 2) prostredníctvom:

  — pomoci poskytnutej Komisii a členským štátom pri príprave celoeurópskych cvičení, čím sa dosiahnu úspory z rozsahu pri reakcii na celoeurópske incidenty,

  — zjednodušenia fungovania EP3R, ktoré by nakoniec mohlo viesť k väčšiemu množstvu investícií vyvolaných spoločnými politickými cieľmi a normami pre bezpečnosť a odolnosť na úrovni EÚ.

— Presadzovaniu spoločného globálneho prístupu k bezpečnosti sietí a informácií (príčinný faktor č. 5), a to prostredníctvom:

  — zintenzívnenia výmeny informácií a poznatkov medzi krajinami mimo EÚ.

— Účinnejšiemu a efektívnejšiemu boju proti počítačovej kriminalite (príčinný faktor č. 7) prostredníctvom:

  — podieľania sa na neoperatívnych úlohách týkajúcich sa aspektov spolupráce pri presadzovaní práva a súdnej spolupráce v súvislosti s bezpečnosťou sietí a informácií, ako sú obojsmerná výmena informácií a školenia (napr. v spolupráci s Európskou policajnou akadémiou CEPOL).

3.7 Agentúra ENISA by v rámci možnosti č. 3 disponovala všetkými zdrojmi potrebnými na vykonávanie jej činností uspokojivým a dôkladným spôsobom, t. j. tak, aby mali skutočný vplyv. Ak by mala agentúra ENISA k dispozícii viac zdrojov ([5]), mohla by zaujať omnoho proaktívnejšiu úlohu a ujať sa viacerých iniciatív v záujme podnecovania aktívneho zapojenia zainteresovaných strán. Táto nová situácia byť ďalej umožnila väčšiu flexibilitu pri rýchlych reakciách na zmeny v neustále sa meniacom prostredí bezpečnosti sietí a informácií.

3.8 Politická možnosť č. 4 zahŕňa operatívne funkcie v boji proti počítačovým útokom a pri reakciách na počítačové incidenty. Navyše by agentúra mala okrem vyššie uvedených aktivít aj operatívne funkcie, ako je aktívnejšia úloha v rámci CIIP v EÚ, napríklad pri predchádzaní incidentom a pri reakciách, a to konkrétne prijatím úlohy CERT pre bezpečnosť sietí a informácií v rámci EÚ a koordinovaním národných tímov CERT ako krízového centra EÚ v oblasti bezpečnosti sietí a informácií vrátane každodenných riadiacich činností a poskytovania služieb v núdzových situáciách.

3.9 Možnosť č. 4 by na operatívnej úrovni mala väčší účinok, ktorý by dopĺňal účinky dosiahnuté v rámci možnosti č. 3. Agentúra by v úlohe tímu CERT pre bezpečnosť sietí a informácií v rámci EÚ a tiež ako koordinátor vnútroštátnych tímov CERT napríklad prispela k väčším úsporám z rozsahu pri reakciách na celoeurópske incidenty a k nižším operatívnym rizikám pri podnikateľskej činnosti vzhľadom na vyššiu úroveň bezpečnosti a odolnosti. Možnosť č. 4 by vyžadovala podstatné zvýšenie rozpočtu agentúry a ľudských zdrojov, čo vzbudzuje obavy o jej kapacite čerpania a účinnom využívaní rozpočtu vo vzťahu k výhodám, ktoré sa majú dosiahnuť.

3.10 Politická možnosť č. 5 zahŕňa operatívne funkcie pri podpore presadzovania práva a súdnych orgánov v boji proti počítačovej kriminalite. Táto možnosť by agentúre ENISA okrem aktivít uvedených pri možnosti č. 4 umožnila:

— poskytovať podporu súvisiacu s procesným právom (porovnaj dohovor o počítačovej kriminalite): napr. zber údajov týkajúcich sa prenosu, zachytávanie údajov týkajúcich sa obsahu, monitorovanie tokov v prípade útokov týkajúcich sa odmietnutia služby,

— byť expertíznym centrom na vyšetrovanie trestných činov vrátane aspektov bezpečnosti sietí a informácií.

3.11 Možnosť č. 5 by dosiahla vyššiu účinnosť v boji proti počítačovej kriminalite ako možnosti č. 3 a 4, pričom navyše disponuje operatívnymi funkciami pri podpore presadzovania práva a súdnych orgánov.

3.12 Možnosť č. 5 by si vyžadovala značné navýšenie zdrojov agentúry a opäť vzbudzuje obavy týkajúce sa kapacity čerpania a účinného využívania rozpočtu.

3.13 Napriek tomu, že možnosti č. 4 a 5 by mali väčšie pozitívne účinky ako možnosť č. 3, Komisia sa domnieva, že existuje množstvo dôvodov na neuskutočnenie týchto možností:

— pre členské štáty by boli politicky citlivé vo vzťahu k ich úlohám v rámci CIIP (t. j. množstvo členských štátov by nebolo za centralizované operatívne funkcie),

— rozšírením mandátu podľa možností č. 4 a 5 by sa pozícia agentúry stala nejednoznačnou,

— pridanie týchto nových a úplne rozdielnych operatívnych úloh k mandátu agentúry by sa mohlo ukázať v krátkodobom horizonte ako veľmi náročné a existuje značné riziko, že by agentúra nebola schopná splniť tento druh úlohy riadne v primeranom časovom intervale,

— navyše sú náklady na uplatnenie možností č. 4 a 5 príliš vysoké – požadovaný rozpočet by bol štyrikrát alebo päťkrát vyšší ako súčasný rozpočet agentúry ENISA.

([5]) Odvolanie sa na viac zdrojov je podmienené prijatím návrhu týkajúceho sa agentúry ENISA v jeho súčasnej podobe.

4. **Ustanovenia nariadenia**

4.1 Agentúra pomáha Komisii a členským štátom plniť právne a regulačné požiadavky na bezpečnosť sietí a informácií.

4.2 Správna rada vymedzuje všeobecné smerovanie činnosti agentúry.

4.3 Správnu radu tvorí jeden zástupca každého členského štátu, traja zástupcovia vymenovaní Komisiou a jeden zástupca priemyslu informačných a komunikačných technológií, jeden zástupca za skupiny spotrebiteľov a jeden zástupca spomedzi akademických expertov na bezpečnosť sietí a informácií.

4.4 Agentúru riadi nezávislý výkonný riaditeľ, ktorý je zodpovedný za vypracovanie pracovného programu agentúry, ktorý podlieha schváleniu správnej rady.

4.5 Výkonný riaditeľ je zodpovedný aj za vypracovanie ročného rozpočtu na podporu pracovného programu. Správna rada je povinná predložiť rozpočet a pracovný program na schválenie Komisii a členským štátom.

4.6 Správna rada na návrh výkonného riaditeľa zriadi stálu skupinu zainteresovaných strán zloženú z expertov zastupujúcich priemysel informačných a komunikačných technológií, skupiny spotrebiteľov, akademickú obec a orgány pôsobiace v oblasti presadzovania práva a ochrany súkromia.

4.7 Keďže nariadenie je ešte stále vo fáze návrhu, existuje určitá neistota, čo sa týka čísel. V súčasnosti má agentúra 44 až 50 zamestnancov a rozpočet vo výške 8 miliónov EUR. Možnosť č. 3 by koncepčne vyžadovala 99 zamestnancov a rozpočet vo výške 17 miliónov EUR.

4.8 V nariadení sa navrhuje mandát na dobu určitú v dĺžke päť rokov.

V Bruseli 17. februára 2011

Predseda
Európskeho hospodárskeho a sociálneho výboru
Staffan NILSSON