Mnenje Evropskega ekonomsko-socialnega odbora o predlogu uredbe Evropskega parlamenta in Sveta o Evropski agenciji za varnost omrežij in informacij (ENISA)

COM(2010) 521 konč.

(2011/C 107/12)

Poročevalec: **g. MORGAN**

Svet je 19. oktobra 2010 sklenil, da v skladu s členom 114 Pogodbe o delovanju Evropske unije Evropski ekonomsko-socialni odbor zaprosi za mnenje o naslednjem dokumentu:

Predlog uredbe Evropskega parlamenta in Sveta o Evropski agenciji za varnost omrežij in informacij (ENISA)

COM(2010) 521 konč.

Strokovna skupina za promet, energijo, infrastrukturo in informacijsko družbo, zadolžena za pripravo dela Odbora na tem področju, je mnenje sprejela 2. februarja 2011.

Evropski ekonomsko-socialni odbor je mnenje sprejel na 469. plenarnem zasedanju 16. in 17. februarja 2011 (seja z dne 17. februarja) s 173 glasovi za in 5 vzdržanimi glasovi.

1. **Sklepi in priporočila**

1.1 EESO se zaveda stopnje odvisnosti civilne družbe od storitev, ki se zagotavljajo prek spleta. Prav tako ga skrbi sorazmerno nezanimanje civilne družbe za lastno kibernetsko varnost. EESO meni, da je Evropska agencija za varnost omrežij in informacij (ENISA) odgovorna za pomoč državam članicam in ponudnikom storitev pri izboljšanju splošnih standardov varnosti, tako da bodo vsi internetni uporabniki izvajali ustrezne ukrepe za zagotovitev svoje osebne kibernetske varnosti.

1.2 Zato EESO podpira predlog za razvoj agencije ENISA, ki naj bi prispevala k visoki ravni varnosti omrežij in informacij v Uniji, ozaveščala ter razvijala kulturo varnosti omrežij in informacij v družbi v korist državljanov, potrošnikov, podjetij in organizacij javnega sektorja Unije ter tako prispevala k nemotenemu delovanju notranjega trga.

1.3 Naloga ENISA je ključna za varen razvoj omrežne infrastrukture vlade, industrije, trgovine in civilne družbe v EU. EESO pričakuje, da bo Evropska komisija določila najvišje standarde uspešnosti za ENISA ter spremljala njeno delovanje v okviru razvijajočih se in nastajajočih groženj kibernetski varnosti.

1.4 Vse kibernetske strategije, ki so jih predstavili NATO, Europol in Evropska komisija, so odvisne od učinkovitega sodelovanja z državami članicami, ki že same razpolagajo z množico notranjih agencij, ki se ukvarjajo z vprašanji kibernetske varnosti. Strategije organizacije NATO in Europola so proaktivne in operativne. V okviru strategije Evropske komisije je agencija ENISA pomemben del sestavljanke agencij in misij za zaščito kritične informacijske infrastrukture. Nova uredba agenciji ENISA ne daje operativne vloge, vendar EESO še vedno meni, da ima ENISA glavno odgovornost za zaščito kritične informacijske infrastrukture v civilni družbi EU.

1.5 Operativna odgovornost za kibernetsko varnost na ravni držav članic pripada državam članicam, vendar se standardi glede zaščite kritične informacijske infrastrukture v 27 državah članicah jasno razlikujejo. Naloga agencije ENISA je, da tudi slabše opremljene države članice dosežejo sprejemljivo raven. ENISA mora zagotoviti sodelovanje med državami članicami ter jim pomagati pri uporabi najboljše prakse. Kar zadeva čezmejne grožnje, mora biti naloga ENISA opozarjanje in preprečevanje.

1.6 Prav tako bo morala biti ENISA vključena v mednarodno sodelovanje s silami zunaj EU. Takšno sodelovanje je zelo politično in vključuje številna področja EU, vendar EESO meni, da mora ENISA najti svoj prostor na mednarodnem prizorišču.

1.7 Odbor je prepričan, da lahko agencija ENISA s prispevanjem k raziskovalnim projektom na področju varnosti in z dajanjem pobud zanje ima zelo pomembno vlogo.

1.8 V okviru ocene učinka EESO trenutno ne bo podprl polnega obsega izvajanja četrte in pete možnosti, na podlagi katerih bi ENISA postala operativna agencija. Kibernetska varnost je ob dinamičnem razvoju groženj tako velik problem, da morajo države članice ohraniti sposobnost proaktivnega boja proti tem grožnjam. Razvoj operativnih agencij EU

običajno privede do zmanjšanja strokovne usposobljenosti držav članic. Na področju kibernetske varnosti velja nasprotno; države članice morajo pridobiti dodatna strokovna znanja.

1.9 EESO razume stališče Komisije, da bi morala imeti ENISA natančno opredeljeno in dobro nadzorovano nalogo z ustreznimi viri. Kljub temu pa EESO izraža zaskrbljenost, da bi lahko dokončen petletni mandat agencije ENISA omejil dolgoročne projekte ter ogrozil razvoj človeškega kapitala in znanja v agenciji. To bo dokaj majhna agencija, ki se bo ukvarjala z velikim in nenehno rastočim problemom. Agencija ENISA bo zaradi obsega in pomembnosti svoje naloge morala zaposlovati skupine strokovnjakov. Njeno delo bo mešano: kratkoročne naloge in dolgoročni projekti. Zato se EESO zavzema za dinamičen in nedoločen čas trajanja mandata agencije ENISA, ki bi se sproti potrjeval z rednimi ocenjevanji in vrednotenji. Tako bi se sredstva lahko dodeljevala postopoma in glede na upravičenost.

2. **Uvod**

2.1 To mnenje obravnava uredbo za nadaljnji razvoj ENISA.

2.2 Komisija je svoj prvi predlog za politični pristop k varnosti omrežja in informacij predstavila v svojem sporočilu iz leta 2001 (COM(2001) 298 konč.). G. Retureau je v odgovor na to sporočilo pripravil obsežno mnenje ([1]).

2.3 Komisija je nato predlagala uredbo o ustanovitvi agencije ENISA (COM(2003) 63 konč.). Mnenje EESO ([2]) o tej uredbi je pripravil g. Lagerholm. Agencija je bila dejansko ustanovljena z Uredbo ES št. 460/2004.

2.4 Varnost informacij je z nadaljnjo izjemno hitro rastjo uporabe interneta zbujala vse večjo zaskrbljenost. Leta 2006 je Komisija objavila sporočilo, v katerem je predstavila strategijo za varno informacijsko družbo (COM(2006) 251 konč.). Mnenje EESO ([3]) je pripravil g. Pezzini.

2.5 Zaradi vse večje zaskrbljenosti glede varnosti informacij je Komisija leta 2009 predložila predlog o zaščiti kritične informacijske infrastrukture (COM(2009) 149 konč.). Mnenje ([4]), ki ga je EESO sprejel na plenarnem zasedanju decembra 2009, je pripravil g. McDonogh.

2.6 Zdaj se predlaga krepitev in izboljšanje delovanja agencije ENISA, ki naj bi prispevala k visoki ravni varnosti omrežij in informacij v Uniji, ozaveščala ter razvila kulturo varnosti omrežij in informacij v družbi v korist državljanov, potrošnikov, podjetij in organizacij javnega sektorja Unije ter tako prispevala k nemotenemu delovanju notranjega trga.

2.7 Vendar pa agencija ENISA ni edina agencija, predvidena za zagotavljanje varnosti kibernetskega prostora EU. Odzivanje na kibernetske vojne in kibernetski terorizem je dolžnost vojske. Na tem področju ima glavno vlogo NATO. V skladu s svojim novim strateškim konceptom, objavljenim v Lizboni novembra 2010 (na voljo na spletni strani http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf), bo NATO nadalje razvijal svojo sposobnost preprečevanja in odkrivanja kibernetskih napadov, obrambe pred njimi ter okrevanja po njih, tudi z uporabo svojega postopka načrtovanja, da bi tako okrepil in uskladil nacionalne zmogljivosti za kibernetsko obrambo, pri tem pa vsem organom organizacije NATO zagotovil centralizirano kibernetsko zaščito in bolje povezal orodja organizacije NATO za ozaveščanje o kibernetski nevarnosti ter opozarjanje in odzivanje nanjo v državah članicah.

2.8 Po kibernetskem napadu na Estonijo leta 2007 je bil 14. maja 2008 uradno ustanovljen Center odličnosti za sodelovanje pri kibernetski obrambi (CCD COE), ki naj bi okrepil zmogljivost organizacije NATO za kibernetsko obrambo. Center s sedežem v Talinu v Estoniji je plod mednarodnega prizadevanja, ki ga trenutno podpirajo Estonija, Latvija, Litva, Nemčija, Madžarska, Italija, Slovaška in Španija.

2.9 Za boj proti elektronskemu kriminalu na ravni EU je odgovoren Europol. Sledi izvleček iz pisnega dokazila, ki ga je Europol posredoval zgornjemu domu britanskega parlamenta (glej http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68we05.htm):

Jasno je, da morajo organi pregona iti v korak s tehnološkim razvojem storilcev kaznivih dejanj in tako zagotoviti učinkovito preprečevanje ali odkrivanje takšnih dejanj. Glede na to, da se visoka tehnologija ne meni za državne meje, mora biti tudi standard zmogljivosti enako visok po vsej EU, da se prepreči nastanek „šibkih točk", kjer bi se visokotehnološki kriminal lahko nekaznovano razvijal. Ta zmogljivost v EU še zdaleč ni enotna. Razvoj je namreč izrazito asimetričen; nekatere države članice prednjačijo z zelo naprednimi dosežki na določenih področjih, medtem ko ostale z vidika tehnologije zaostajajo. Zato nastaja potreba po centralizirani službi, ki bi vsem državam članicam pomagala usklajevati skupne dejavnosti, spodbujala standardizacijo pristopov in standarde kakovosti ter prepoznavala in izmenjevala najboljše prakse; samo na ta način je mogoče zagotoviti enotno izvrševanje zakonodaje EU v boju proti visokotehnološkemu kriminalu.

([1]) UL C 48, 21.2.2002, str. 33.
([2]) UL C 220, 16.9.2003, str. 33.
([3]) UL C 97, 28.4.2007, str. 21.
([4]) UL C 255, 22.9.2010, str. 98.

2.10 Leta 2002 je bil pri Europolu ustanovljen Center za kriminaliteto visokih tehnologij (HTCC). Ta sorazmerno majhna enota se bo v prihodnje kot osrednji del Europolovih prizadevanj na tem področju predvidoma povečala. HTCC ima pomembno vlogo pri usklajevanju, operativni podpori, strateški analizi in usposabljanju. Funkcija usposabljanja je še posebno pomembna. Europol je ustanovil tudi Evropsko platformo za kibernetsko kriminaliteto, ECCP. Slednja se osredotoča na naslednje tematike:

— spletni sistem za poročanje o internetnem kriminalu (I-CROS);

— analitična delovna datoteka (Cyborg);

— portal za internetno forenziko (I-FOREX).

2.11 Strategija EU za kibernetsko varnost je predstavljena v poglavju „Zaupanje in varnost" sporočila Evropska digitalna agenda. Izzivi so navedeni kot sledi:

Zaenkrat se je internet izkazal kot izredno varen, odporen in stabilen, vendar pa omrežja IT in končne postaje končnih uporabnikov ostajajo ranljivi za številne nove grožnje: v zadnjih letih je obseg neželene elektronske pošte narasel toliko, da je močno zgostil promet z elektronsko pošto (različne ocene se gibajo med 80 % in 98 % vse elektronske pošte, ki kroži), s tako pošto pa se tudi širi široka paleta virusov in škodljivih programov. Nastaja prava epidemija kraj identitete in spletnih prevar. Napadi so vedno bolj prefinjeni (trojanci, botneti itd.) in imajo pogosto finančen motiv. Lahko pa so tudi politično motivirani, kot kažejo nedavni kibernetski napadi na Estonijo, Litvo in Gruzijo.

2.12 Komisija je v Agendi napovedala naslednja ukrepa:

ključni ukrep št. 6: v letu 2010 bo predstavila ukrepe, katerih cilj je **okrepljena politika varnosti omrežij in informacij na visoki ravni**, vključno z zakonodajnimi pobudami, kot je posodobljena ENISA, ter ukrepi, ki omogočajo hitrejše odzivanje na kibernetske napade, vključno s skupino za odzivanje na računalniške grožnje (CERT) za institucije EU;

ključni ukrep št. 7: do leta 2010 bo predstavila ukrepe, vključno z zakonodajnimi pobudami, za **boj proti kibernetskim napadom na informacijske sisteme** ter do leta 2013 še s tem povezana pravila o pristojnostih v kibernetskem prostoru na evropski in mednarodni ravni.

2.13 V sporočilu iz novembra 2010 (COM(2010) 673 konč.) je Komisija nadalje razvila Agendo z opredelitvijo strategije notranje varnosti EU. Ta ima pet ciljev, od katerih je tretji zvišanje ravni varnosti v kibernetskem prostoru za državljane in podjetja. Predvideni so trije ukrepi, podrobnosti o teh ukrepih pa so opredeljene v naslednji preglednici (vzeti iz sporočila, ki je na voljo na spletni strani http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf).

CILJI IN UKREPI	PRISTOJNOST	ČASOVNI NAČRT
CILJ 3: Zvišanje ravni varnosti v kibernetskem prostoru za državljane in podjetja		
Ukrep 1: Vzpostavljanje zmogljivosti na področju kazenskega pregona in sodstva		
Ustanovitev centra EU za kibernetsko kriminaliteto	Ob upoštevanju študije KOM o izvedljivosti, končane leta 2011	2013
Razvoj zmogljivosti za preiskovanje in pregon kibernetskih kaznivih dejanj	DČ s CEPOL, Europolom in Eurojustom	2013
Ukrep 2: Sodelovanje z industrijo za vključevanje in zaščito državljanov		
Vzpostavitev zmogljivosti za obveščanje o kibernetskih kaznivih dejanjih ter navodila državljanom o kibernetski varnosti in kibernetskih kaznivih dejanjih	DČ, KOM, Europol, **ENISA** in zasebni sektor	v teku
Smernice za sodelovanje pri ukrepanju proti nezakonitim internetnim vsebinam	KOM z DČ in zasebnim sektorjem	2011
Ukrep 3: Izboljšanje sposobnosti reagiranja na kibernetske napade		
Vzpostavitev omrežja skupin za odzivanje na računalniške grožnje z eno skupino v vsaki DČ in eno za institucije EU, redni nacionalni načrti ukrepov ter vaje za odzivanje na incidente in odpravo posledic	DČ in institucije EU ter **ENISA**	2012
Vzpostavitev evropskega sistema za izmenjavo informacij in opozarjanje (EISAS)	DČ s KOM in **ENISA**	2013

2.14 Vse kibernetske strategije, ki so jih predstavili NATO, Europol in Evropska komisija, so odvisne od učinkovitega sodelovanja z državami članicami, ki že same razpolagajo z množico notranjih agencij, ki se ukvarjajo z vprašanji kibernetske varnosti. Strategije organizacije NATO in Europola so proaktivne in operativne. V okviru strategije Evropske komisije predstavlja agencija ENISA pomemben del zapletene sestavljanke agencij in misij za zaščito kritične informacijske infrastrukture (CIIP). Nova uredba agenciji ENISA ne daje operativne vloge, vendar EESO še vedno meni, da ima ENISA glavno odgovornost za zaščito kritične informacijske infrastrukture v civilni družbi EU.

3. **Predlog uredbe o Evropski agenciji za varnost omrežij in informacij (ENISA)**

3.1 Težava, ki jo mora obravnavati ENISA, je pogojena s sedmimi dejavniki:

(1) razdrobljeni in raznoliki nacionalni pristopi,

(2) omejena evropska sposobnost za zgodnje opozarjanje in odzivanje,

(3) premalo zanesljivih podatkov in omejeno znanje o nastajajočih težavah,

(4) premalo ozaveščenosti o tveganjih in izzivih varnosti omrežij in informacij,

(5) mednarodna razsežnost težav na področju varnosti omrežij in informacij,

(6) potreba po modelih sodelovanja, s katerimi bi se zagotovilo ustrezno izvajanje politike,

(7) potreba po učinkovitejših ukrepih za preprečevanje kibernetskega kriminala.

3.2 Predlog uredbe o ENISA zagotavlja izhodišče tako za veljavne določbe politike kot za nove pobude iz Evropske digitalne agende.

3.3 Obstoječe politike, ki naj bi jih podpirala ENISA, vključujejo:

(i) Evropski forum za države članice (EFMS), ki naj bi pospešil razpravo o dobrih praksah in njihovo izmenjavo, s čimer naj bi se na področju varnosti in odpornosti infrastrukture IKT določili skupni cilji politik in prednostne naloge;

(ii) evropsko javno-zasebno partnerstvo za odpornost (EP3R) kot prožen evropski upravni okvir za odpornost infrastrukture IKT, ki spodbuja sodelovanje med javnim in zasebnim sektorjem pri vprašanjih varnosti in odpornosti;

(iii) stockholmski program, ki ga je 11. decembra 2009 sprejel Evropski svet in podpira ukrepe, ki zagotavljajo varnost omrežij ter pri kibernetskih napadih v Uniji omogočajo hitrejše ukrepanje.

3.4 Novosti, ki naj bi jih podpirala ENISA, vključujejo:

(i) krepitev dejavnosti Evropskega foruma za države članice (EFMS);

(ii) podpiranje evropskega javno-zasebnega partnerstva za odpornost (EP3R) z razpravami o inovativnih ukrepih in instrumentih za izboljšanje varnosti in odpornosti;

(iii) uporabo varnostnih zahtev regulativnega paketa o elektronskih komunikacijah v praksi;

(iv) podpiranje pripravljalnih vaj za kibernetsko varnost po vsej EU;

(v) ustanovitev skupine CERT za institucije EU;

(vi) mobiliziranje in podpiranje držav članic pri izpopolnitvi in po potrebi pri ustanovitvi nacionalnih/vladnih CERT, da se vzpostavi dobro delujoča mreža CERT, ki bo pokrivala vso Evropo;

(vii) ozaveščanje o izzivih na področju varnosti omrežij in informacij.

3.5 Pred dokončanjem tega predloga je bilo preučenih pet možnosti politike. Vsaka možnost je vključevala poslanstvo in možnosti glede sredstev v povezavi z njo. Izbrana je bila tretja možnost. Ta vključuje razširitev trenutnih nalog ENISA ter vključitev organov pregona in organov za zaščito zasebnosti kot akterjev.

3.6 Pri tretji možnosti bi posodobljena agencija za varnost omrežij in informacij prispevala k:

— manjši razdrobljenosti nacionalnih pristopov (težava št. 1), razširitvi politike in sprejemanju odločitev na podlagi znanja in informacij (težava št. 3) ter boljši splošni ozaveščenosti o tveganjih in izzivih varnosti omrežij in informacij ter njihovem reševanju (težava št. 4) tako, da bi prispevala k:

  — učinkovitejšemu zbiranju ustreznih informacij o tveganjih, nevarnostih in dovzetnostih v posameznih državah članicah;

  — večji razpoložljivosti informacij o trenutnih in prihodnjih izzivih in tveganjih varnosti omrežij in informacij;

  — kakovostnejšim določbam politike varnosti omrežij in informacij v državah članicah.

— izboljšanju evropske zmogljivosti za zgodnje opozarjanje in odzivanje (težava št. 2) tako, da bi:

  — Komisiji in državam članicam pomagala pri pripravi vseevropskih vaj, s čimer bi pri evropskih incidentih dosegli ekonomijo obsega;

  — olajšala delovanje EP3R, kar bi zaradi skupnih ciljev politike in evropskih standardov za varnost in odpornost lahko zagotovilo več naložb;

— spodbujanju skupnega globalnega pristopa do varnosti omrežij in informacij (težava št. 5) tako, da bi:

  — spodbujala izmenjavo informacij in znanja z državami nečlanicami EU;

— učinkovitejšemu in uspešnejšemu boju proti kibernetskemu kriminalu (težava št. 7) tako, da bi:

  — se pri pregonu in sodelovanju na področju pravosodja vključila v neoperativne naloge v zvezi z vidiki varnosti omrežij in informacij, npr. v medsebojno izmenjavo informacij in usposabljanja (npr. v sodelovanju z Evropsko policijsko akademijo CEPOL).

3.7 V skladu s tretjo možnostjo bi agencija ENISA razpolagala z vsemi sredstvi, ki jih potrebuje, da bi zadostno in temeljito opravljala naloge ter imela dejanski vpliv. Z več sredstvi ([5]) ima lahko agencija ENISA veliko proaktivnejšo vlogo ter lahko predlaga več pobud, s katerimi bi spodbujala aktivno udeležbo zainteresiranih strani. Poleg tega bi s tem novim položajem pridobila več prožnosti in se hitro odzivala na spremembe v stalno spreminjajočem se okolju varnosti omrežij in informacij.

3.8 Četrta možnost vključuje operativni nalogi v zvezi s preprečevanjem kibernetskih napadov in odzivanjem na kibernetske incidente. Poleg zgoraj omenjenih dejavnosti bi agencija prevzela tudi operativne naloge, tj. zavzela aktivnejšo vlogo pri zaščiti kritične informacijske infrastrukture v EU, npr. pri preprečevanju incidentov in odzivanju nanje, zlasti tako, da bi delovala kot evropska skupina za odzivanje na računalniške grožnje (CERT) ter kot krizni center EU za varnost omrežij in informacij usklajevala nacionalne CERT pri vsakdanjih dejavnostih upravljanja kot tudi v izrednih primerih.

3.9 Četrta možnost bi poleg učinkov, predvidenih pri tretji možnosti, imela večji učinek tudi na operativni ravni. V vlogi evropskega CERT za varnost omrežij in informacij in z usklajevanjem nacionalnih CERT bi agencija pri evropskih incidentih prispevala k večjim ekonomijam obsega ter z večjo varnostjo in odpornostjo npr. zmanjšala operativna tveganja za podjetja. Pri četrti možnosti bi bilo treba znatno povečati proračunska sredstva in človeške vire agencije, kar vzbuja pomisleke glede njene sposobnosti absorpcije in učinkovite uporabe proračunskih sredstev v primerjavi s pridobljenimi prednostmi.

3.10 Peta možnost vključuje kot operativno nalogo pomoč organom pregona in pravosodnim organom pri preprečevanju kibernetskega kriminala. Poleg dejavnosti, predvidenih pri četrti možnosti, bi ta agenciji ENISA omogočila:

— zagotavljati podporo pri vprašanjih, ki se nanašajo na procesno pravo (prim. Konvencijo o kibernetskem kriminalu): npr. zbiranje podatkov o prometu, prestrezanje podatkov o vsebini, spremljanje podatkovnih tokov pri napadih z ohromitvijo storitev;

— biti center odličnosti pri preiskavi kriminalnih dejanj, vključno z vidiki varnosti omrežij in informacij.

3.11 Peta možnost bi zaradi novih operativnih nalog, h katerim spadajo zagotavljanje pomoči organom pregona in pravosodnim organom, zagotovila večjo učinkovitost v boju proti kibernetskemu kriminalu kot tretja in četrta možnost.

3.12 Pri peti možnosti bi bilo treba znatno povečati sredstva agencije, kar bi ponovno vzbudilo pomisleke glede njene sposobnosti absorpcije in učinkovite uporabe proračunskih sredstev.

3.13 Medtem ko bi četrta in peta možnost imeli večji pozitivni učinek kot tretja možnost, Komisija meni, da obstajajo številni razlogi proti tema možnostma:

— bili bi politično občutljivi za države članice zaradi njihovih pristojnosti na področju zaščite kritične informacijske infrastrukture (npr. nekatere države članice ne bi podprle njenih centraliziranih operativnih nalog);

— razširitev mandata, ki je predvidena pri četrti in peti možnosti, bi lahko povzročila nejasnosti glede položaja agencije;

— te nove in popolnoma drugačne operativne naloge, ki bi se dodale mandatu agencije, bi se lahko kratkoročno izkazale za zelo zahtevne, poleg tega pa obstaja tudi nevarnost, da agencija takšnih nalog ne bi mogla opraviti uspešno v razumnem časovnem obdobju;

— navsezadnje so tudi stroški izvajanja pri četrti in peti možnosti bistveno višji – potrebno bi bilo štiri- do petkrat več sredstev, kot jih ima ENISA trenutno.

([5]) Sklicevanje na več sredstev je pogojeno s sprejetjem predloga uredbe o agenciji ENISA v sedanji obliki.

4. **Določbe uredbe**

4.1 Agencija pri izpolnjevanju pravnih in regulativnih zahtev, ki se nanašajo na varnost omrežij in informacij, pomaga Komisiji in državam članicam.

4.2 Upravni odbor določi splošno usmeritev delovanja agencije.

4.3 Upravni odbor sestavljajo po en predstavnik vsake države članice, trije predstavniki, ki jih imenuje Komisija, ter po en predstavnik stroke informacijskih in komunikacijskih tehnologij, skupin potrošnikov in znanstvenih strokovnjakov s področja IT.

4.4 Agencijo vodi neodvisni izvršni direktor, ki je odgovoren za pripravo programa dela agencije, ki ga sprejme upravni odbor.

4.5 Izvršni direktor je odgovoren za pripravo letnega proračuna, ki podpira delovni program. Upravni odbor mora proračun in delovni program predložiti v potrditev Komisiji in državam članicam.

4.6 Po nasvetu izvršnega direktorja upravni odbor ustanovi stalno skupino zainteresiranih strani, ki jo sestavljajo strokovnjaki iz panoge informacijskih in komunikacijskih tehnologij, skupin potrošnikov, akademskih krogov, organov pregona in organov za zaščito zasebnosti.

4.7 Ker je uredba še v fazi predloga, so številke še negotove. Trenutno šteje agencija 44-50 zaposlenih, njen proračun pa znaša 8 milijonov eurov. V tem smislu bi tretja možnost vključevala 99 zaposlenih in proračun v višini 17 milijonov eurov.

4.8 Uredba predlaga mandat za določen čas petih let.

V Bruslju, 17. februarja 2011

Predsednik
Evropskega ekonomsko-socialnega odbora
Staffan NILSSON