Det Europæiske Økonomiske og Sociale Udvalgs udtalelse om forslag til Europa-Parlamentets og Rådets forordning om Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA)

KOM(2010) 521 endelig

(2011/C 107/12)

Ordfører: **Peter MORGAN**

Rådet for Den Europæiske Union besluttede den 19. oktober 2010 under henvisning til artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF) at anmode om Det Europæiske Økonomiske og Sociale Udvalgs udtalelse om:

Forslag til Europa-Parlamentets og Rådets forordning om Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA)

KOM(2010) 521 endelig.

Det forberedende arbejde henvistes til Den Faglige Sektion for Transport, Energi, Infrastruktur og Informationssamfundet, som vedtog sin udtalelse den 2. februar 2011.

Det Europæiske Økonomiske og Sociale Udvalg vedtog på sin 469. plenarforsamling den 16.-17. februar 2011, mødet den 17. februar 2011, følgende udtalelse med 173 stemmer for og 5 stemmer hverken for eller imod:

1. **Konklusioner og henstillinger**

1.1 EØSU er meget bevidst om, hvor afhængigt civilsamfundet nu er af tjenester, der leveres gennem internettet. Udvalget er også bekymret over, at civilsamfundet er relativt uvidende om sin egen internetsikkerhed. EØSU mener, at Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) har ansvaret for at hjælpe medlemsstater og tjenesteleverandører med at øge deres egne almindelige sikkerhedskrav, så alle internetbrugere tager de nødvendige skridt til at sikre deres egen personlige internetsikkerhed.

1.2 Derfor støtter EØSU forslaget om at udvikle ENISA med det sigte at bidrage til et højt niveau af net- og informationssikkerhed i Unionen og for at hæve oplysningsniveauet og udvikle en net- og informationssikkerhedskultur i samfundet til gavn for borgerne, forbrugerne, virksomhederne og den offentlige sektors organisationer i Den Europæiske Union og således bidrage til et velfungerende indre marked.

1.3 ENISA's rolle er en forudsætning for en sikker udvikling af netinfrastrukturen i EU's forvaltning, industri, handel og civilsamfund. EØSU forventer, at Kommissionen fastsætter de højeste krav til, hvad ENISA skal yde, og at den overvåger ENISA's præstation i lyset af de nye og stigende trusler for internetsikkerheden.

1.4 De internetstrategier, som NATO, Europol og Kommission har fremsat, forudsætter alle et effektivt samarbejde med medlemsstaterne, som selv har en bred vifte af nationale agenturer, der beskæftiger sig med spørgsmål om internetsikkerhed. NATO's og Europols strategier er bestemt til at være proaktive og operationelle. Inden for rammerne af Kommissionens strategi er ENISA helt klart en vigtig brik i det komplekse puslespil af agenturer og opgaver på området beskyttelse af kritisk informationsinfrastruktur. Selv om forslaget til den nye forordning ikke tildeler ENISA en operationel rolle, mener EØSU, at ENISA er det agentur, der har hovedansvaret for beskyttelse af kritisk informationsinfrastruktur i EU's civilsamfund.

1.5 Medlemsstaterne har det operationelle ansvar for internetsikkerhed på medlemsstatsniveau, men de 27 medlemsstater har meget forskellige standarder for beskyttelse af kritisk informationsinfrastruktur. Det er ENISA's opgave at bringe de dårligst udstyrede medlemsstater op på et acceptabelt niveau. Agenturet skal sikre et samarbejde mellem medlemsstaterne og hjælpe dem med anvendelsen af bedste praksis. Når der er grænseoverskridende trusler, er det ENISA's rolle at advare og forebygge.

1.6 ENISA skal også deltage i det internationale samarbejde med lande uden for EU. Dette samarbejde vil være meget politisk og inddrage mange dele af EU, men EØSU mener, at ENISA er nødt til at finde sin plads på den internationale scene.

1.7 EØSU mener, at ENISA kan spille en meget værdifuld rolle ved at bidrage til og iværksætte forskningsprojekter på sikkerhedsområdet.

1.8 I betragtning af konsekvensanalysen kan EØSU ikke på nuværende tidspunkt støtte den fulde gennemførelse af mulighed 4 og 5, der ville gøre ENISA til et operationelt agentur. Internetsikkerhed er et så stort problem og et område, hvor trusselbilledet er i konstant udvikling, at medlemsstaterne skal opretholde evnen til at bekæmpe trusler proaktivt.

Oprettelsen af operationelle EU-agenturer ender normalt med at nedkvalificere medlemsstaterne. På internetsikkerhedsområdet er der behov for det modsatte. Medlemsstaterne skal opkvalificeres.

1.9 EØSU forstår Kommissionens ønske om, at ENISA skal have en fastlagt rolle, som underlægges nøje kontrol, og at det skal have passende ressourcer. EØSU er ikke desto mindre bekymret for, at begrænsningen af ENISA's mandatperiode til 5 år kan lægge en dæmper på langsigtede projekter og sætte en kæp i hjulet på udviklingen af agenturets menneskelige kapital og viden. Det vil være et meget lille agentur, der beskæftiger sig med et stort og voksende problem. Rækkevidden og omfanget af ENISA's opgaver kræver, at der ansættes hold af specialister. Det vil få blandede arbejdsopgaver: både kortsigtede opgaver og langsigtede projekter. Derfor ville EØSU foretrække, at ENISA fik et dynamisk og tidsubegrænset mandat, som løbende blev bekræftet gennem regelmæssige vurderinger og evalueringer. Det kunne således løbende blive tildelt ressourcer, når og hvis der er begrundet behov for det.

2. **Indledning**

2.1 Udtalelsen vedrører en forordning, der tager sigte på at udvikle ENISA yderligere.

2.2 Kommissionen fremsatte sit første forslag til en politisk strategi for net- og informationssikkerhed i en meddelelse fra 2001 (KOM(2001) 298 endelig). Daniel Retureau har udarbejdet en omfattende udtalelse [1] om denne meddelelse.

2.3 Kommissionen fremsatte derefter forslag til en forordning om oprettelse af et europæisk agentur for net- og informationssikkerhed (KOM(2003) 63 endelig). EØSU's udtalelse [2] om denne forordning blev udarbejdet af Göran Lagerholm. Agenturet blev reelt oprettet med forordning (EF) nr. 460/2004.

2.4 Da brugen af internettet blev ved med at stige eksponentielt, blev internetsikkerhed en kilde til voksende bekymring. I 2006 offentliggjorde Kommissionen en meddelelse om en strategi for et sikkert internetsamfund (KOM(2006) 251 endelig). Antonello Pezzini udarbejdede EØSU's udtalelse [3].

2.5 Som en følge af den voksende bekymring over internetsikkerhed fremsatte Kommissionen i 2009 et forslag om beskyttelse af kritisk informationsinfrastruktur (KOM(2009) 149 endelig). Thomas McDonogh udarbejdede EØSU's udtalelse [4], som blev vedtaget på plenarforsamlingen i december 2009.

2.6 Det foreslås nu at styrke og forbedre ENISA med det sigte at bidrage til et højt niveau af net- og informationssikkerhed i EU og for at hæve oplysningsniveauet og udvikle en net- og informationssikkerhedskultur i samfundet til gavn for borgerne, forbrugerne, virksomhederne og den offentlige sektors organisationer i Den Europæiske Union og således bidrage til et velfungerende indre marked.

2.7 ENISA er dog ikke det eneste planlagte sikkerhedsagentur for EU's cyberspace. Militæret har ansvaret for at reagere på cyberkrig og cyberterrorisme. NATO er hovedagenturet på dette område. Ifølge NATO's nye strategikoncept, som blev offentliggjort i Lissabon i november 2010 (tilgængeligt på engelsk på http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf), vil NATO *yderligere styrke sin evne til at forebygge, afsløre, forsvare sig mod og overvinde cyberangreb, bl.a. ved at bruge NATO's planlægningsproces til at styrke og koordinere nationale cyberforsvarskapaciteter, samle alle NATO's organer under en centraliseret cyberbeskyttelse og ved bedre at samordne cyberovervågning, varslinger og reaktioner med medlemsstaterne*.

2.8 Efter cyberangrebet mod Estland i 2007 blev cyberforsvarscentret »Cooperative Cyber Defence Centre of Excellence (CCD COE)« formelt oprettet den 14. maj 2008 for at øge NATO's cyberforsvarskapacitet. Centeret, som har adresse i Tallinn i Estland, er en international indsats, der i øjeblikket omfatter Estland, Letland, Litauen, Tyskland, Ungarn, Italien, Slovakiet og Spanien som sponsorlande.

2.9 Elektronisk kriminalitet på EU-niveau er Europols ansvarsområde. Følgende er et uddrag af en skriftlig henvendelse fra Europol til det britiske overhus (jf. http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68we05.htm):

Det er klart, at de retshåndhævende myndigheder skal holde trit med den teknologiske udvikling hos de kriminelle for at sikre, at de forbrydelser, de begår, kan forebygges eller afsløres effektivt. Højteknologiens grænseløse natur stiller også krav om, at kapaciteten i hele EU skal være på samme høje niveau, så der ikke udvikles »svage punkter«, hvor højteknologisk kriminalitet kan florere ustraffet. Denne kapacitet er langt fra homogen i EU. Faktisk er der en klar asymmetrisk udvikling. Nogle medlemsstater kæmper en brav kamp og gør store fremskridt på nogle områder, mens andre medlemsstater sakker bagud på teknologiområdet. Dette skaber et behov for en centraliseret tjeneste, der kan hjælpe alle medlemsstater med at koordinere fælles aktiviteter, lette standardisering af tilgange og kvalitetsstandarder samt indkredse og udveksle bedste praksis. Kun på denne måde kan der sikres en homogen EU-retshåndhævende indsats for bekæmpelse af højteknologisk kriminalitet.

[1] EFT C 48 af 21.2.2002, s. 33.
[2] EUT C 220 af 16.9.2003, s. 33.
[3] EUT C 97 af 28.4.2007, s. 21.
[4] EUT C 255 af 22.9.2010, s. 98.

2.10 Centeret for højteknologisk kriminalitet (High Tech Crime Centre (HTCC)) blev oprettet i Europol i 2002. Det er en relativt lille enhed, som forventes at vokse i fremtiden som kernen i Europols arbejde på dette område. Centeret spiller en stor rolle for koordination, operationel støtte, strategisk analyse og uddannelse. Uddannelsesfunktionen er særlig vigtig. Derudover har Europol oprettet en europæisk platform for cyberkriminalitet (European Cyber Crime Platform (ECCP)). Den har fokus på følgende spørgsmål:

— Onlinesystemet for rapportering af internetkriminalitet (Internet Crime Reporting Online System (I-CROS));

— Analysedatabase (Cyborg);

— Portalen for internet- og retsvidenskabelig ekspertise (Internet and Forensic Expertise recipient (I-FOREX)).

2.11 EU's strategi for internetsikkerhed fremgår af kapitlet »Tillid og sikkerhed« i den digitale dagsorden for Europa. Udfordringerne formuleres således:

Hidtil har internettet vist sig bemærkelsesværdigt sikkert, robust og stabilt, men it-nettene og slutbrugernes terminaler er fortsat sårbare over for en lang række trusler i stadig udvikling: i de seneste år er mængden af spammail vokset i den grad, at den hæmmer e-mail-trafikken på internettet betydeligt – diverse skøn tyder på, at spam udgør mellem 80 % og 98 % af al elektronisk post – og samtidig er spam med til at sprede et væld af virusser og andre former for skadelig software. Identitetstyveri og internetbedrageri er en voksende plage. Angrebene bliver mere og mere raffinerede (trojanske heste, botnet, mm.) og har ofte et økonomisk motiv. Der kan også ligge politiske motiver bag, sådan som det var tilfældet med de internetangreb, der blev rettet mod Estland, Litauen og Georgien for nylig.

2.12 Dagsordenen omfatter følgende tiltag:

Nøgletiltag 6: i 2010 forelægge initiativer, der sigter mod en **styrket og højt profileret net- og informationssikkerhedspolitik**, herunder lovgivningsforslag om et moderniseret ENISA, og foranstaltninger, der skal gøre det muligt at gribe hurtigere ind i tilfælde af angreb på internettet, bl.a. en it-beredskabsenhed for EU-institutionerne.

Nøgletiltag 7: forelægge initiativer, herunder lovgivningsforslag, til **bekæmpelse af angreb på informationssystemer** inden udgangen af 2010 og regler for retsmyndighed i internetverdenen på europæisk og internationalt plan senest i 2013.

2.13 I en meddelelse fra november 2010 (KOM(2010) 673 endelig) satte Kommissionen skub i dagsordenen ved at formulere strategien for EU's indre sikkerhed. Den har fem mål, hvoraf det tredje er at øge sikkerhedsniveauet for borgere og virksomheder i cyberspace. Der planlægges tre handlingsprogrammer, som er beskrevet i nedenstående tabel (kopieret fra meddelelsen og tilgængelig på engelsk på: http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf).

MÅLSÆTNINGER OG FORANSTALTNINGER	ANSVARLIGE	FRIST
MÅLSÆTNING 3: Øge sikkerhedsniveauet for borgere og virksomheder i cyberspace		
Foranstaltning 1: Opbygge kapacitet inden for retshåndhævelse og retsvæsenet		
Oprettelse af et EU-center for it-kriminalitet	Genstand for KOM's feasibility-undersøgelse i 2011	2013
Udvikling af kapaciteten til at efterforske og retsforfølge it-kriminalitet	MS sammen med CEPOL, Europol og Eurojust	2013
Foranstaltning 2: Arbejde sammen med erhvervslivet for at aktivere og beskytte borgerne		
Indførelse af ordninger for rapportering af tilfælde af it-kriminalitet og rådgivning til borgerne om internetsikkerhed og it-kriminalitet	MS, KOM, Europol, **ENISA** og den private sektor	Iværksat
Retningslinjer for samarbejdet om tackling af problemet med ulovligt indhold på internettet	KOM med MS og den private sektor	2011
Foranstaltning 3: Forbedre kapaciteten til at tackle internetangreb		
Oprettelse af et netværk af it-udrykningshold (Computer Emergency Response Teams (CERT)) i hver medlemsstat og et for EU-institutionerne samt udarbejdelse af nationale beredskabsplaner og regelmæssige øvelser til afværgelse af it-angreb og datagendannelse.	MS og EU-institutionerne sammen med **ENISA**	2012
Oprettelse af et europæisk informationsudvekslings- og varslingssystem (EISAS)	MS sammen med COM og **ENISA**	2013

2.14 De internetstrategier, som NATO, Europol og Kommission har fremsat, forudsætter alle et effektivt samarbejde med medlemsstaterne, som selv har en bred vifte af nationale agenturer, der beskæftiger sig med spørgsmål om internetsikkerhed. NATO's og Europols strategier er bestemt til at være proaktive og operationelle. Inden for rammerne af Kommissionens strategi er ENISA helt klart en vigtig brik i det komplekse puslespil af agenturer og opgaver på området beskyttelse af kritisk informationsinfrastruktur. Selv om forslaget til den nye forordning ikke tildeler ENISA en operationel rolle, mener EØSU, at ENISA er det agentur, der har hovedansvaret for beskyttelse af kritisk informationsinfrastruktur i EU's civilsamfund.

3. **ENISA-forslaget**

3.1 Det problem, som ENISA skal tage sig af, har syv problemkilder:

(1) Mange forskellige nationale tilgange;

(2) Begrænset europæisk forvarslings- og reaktionsevne;

(3) Mangel på pålidelige data og begrænset viden om nye problemer, der udvikler sig;

(4) Utilstrækkelig bevidsthed om net- og informationssikkerhedsrisici og -udfordringer;

(5) Den internationale dimension af net- og informationssikkerhedsproblemer;

(6) Behov for samarbejdsmodeller, der sikrer, at politikkerne bliver fulgt;

(7) Behov for en mere effektiv indsats mod internetkriminalitet.

3.2 ENISA-forslaget skaber et kontaktpunkt for både eksisterende politiske bestemmelser og de nye initiativer i den digitale dagsorden for Europa.

3.3 De eksisterende politikker, som ENISA skal støtte, omfatter:

(i) Et europæisk forum for medlemsstaterne (EFMS), der skal fremme debat og udveksling af god forvaltningspraksis med det formål at nå frem til fælles mål og prioriteter for sikkerhed og robusthed i ikt-infrastrukturen;

(ii) Et europæisk offentlig-privat partnerskab for en robust ikt-infrastruktur (EP3R), som er en fleksibel fælleseuropæisk forvaltningsramme, der skal fremme samarbejdet mellem den offentlige og den private sektor om sikkerheds- og robusthedsspørgsmål;

(iii) Stockholmprogrammet, der blev vedtaget af Rådet den 11. december 2009, støtter politikker, der går ud på at styrke netsikkerheden og sætte EU i stand til at reagere hurtigere på internetangreb.

3.4 Nye udviklinger, som ENISA skal støtte, omfatter:

(i) Intensivering af EFMS's aktiviteter;

(ii) Det europæiske offentlig-private partnerskab (EP3R) ved at drøfte innovative tiltag og midler til at forbedre sikkerheden og robustheden;

(iii) Den praktiske gennemførelse af sikkerhedskravene i regelsættet for elektronisk kommunikation;

(iv) Fremme af EU-dækkende internetsikkerheds- og beredskabsøvelser;

(v) Etablering af en it-beredskabsenhed for EU-institutionerne;

(vi) Mobilisering af og støtte til medlemsstaterne i indsatsen for at oprette nationale/statslige it-beredskabsenheder, så der kan etableres et velfungerende net af sådanne enheder, der dækker hele Europa;

(vii) Tiltag for at skabe øget bevidsthed om net- og informationssikkerhedsproblemer.

3.5 Fem forskellige politiske valgmuligheder blev undersøgt, før dette forslag blev færdiggjort. Hver enkelt valgmulighed blev vurderet i forhold til opgaver og ressourcer. Den tredje mulighed blev valgt. Denne omfatter udvidelse af de funktioner, der i øjeblikket er fastlagt for ENISA, samt tilføjelse af myndigheder med ansvar for retshåndhævelse og beskyttelse af privatlivets fred som interessenter.

3.6 Ved valgmulighed 3 kommer et moderniseret net- og informationssikkerhedsagentur til at bidrage til:

— at reducere forskellene mellem de nationale tilgange (problemkilde 1), i højere grad at få udformet politikker og truffet beslutninger på grundlag af data og viden/information (problemkilde 3) og at øge den generelle bevidsthed om net- og informationssikkerhedsrisici og –udfordringer og, hvordan de kan tages op, (problemkilde 4), ved at medvirke til at skabe

  — større effektivitet i medlemsstaternes indsamling af relevante oplysninger om risici, trusler og sårbarheder;

  — rådighed over mere information om de nuværende og fremtidige udfordringer og risici på området net- og informationssikkerhed;

  — højere kvalitet i medlemsstaternes politiske bestemmelser vedrørende net- og informationssikkerhed.

— at forbedre det europæiske forvarslings- og beredskabssystem (problemkilde 2) ved at

  — bistå Kommissionen og medlemsstaterne med at arrangere fælleseuropæiske øvelser, så man ved at reagere på sikkerhedsrelaterede hændelser på EU-plan kan opnå stordriftsfordele;

  — hjælpe med til, at EP3R kommer til at fungere, hvilket i sidste ende kan betyde, at de fælles politiske mål og EU-dækkende standarder for sikkerhed og robusthed tiltrækker flere investeringer.

— at fremme en fælles global tilgang til net- og informationssikkerhed (problemkilde 5) ved at

  — øge udvekslingen af information og viden med tredjelande.

— at bekæmpe internetkriminalitet mere effektivt og virkningsfuldt (problemkilde 7) ved at

  — blive inddraget i ikke-operationelle opgaver i forbindelse med net- og informationssikkerhedsaspekterne af retshåndhævelse og retligt samarbejde, såsom gensidig udveksling af information og uddannelse (f.eks. i samarbejde med European Police College (CEPOL)).

3.7 Ved valgmulighed 3 vil ENISA få alle de ressourcer til rådighed, som er nødvendige for, at det kan udøve sin virksomhed på tilfredsstillende og grundig måde, dvs. virkelig få indflydelse. Med flere ressourcer til rådighed ([5]) vil ENISA kunne indtage en mere proaktiv rolle og tage flere initiativer til aktiv deltagelse fra interessenternes side. En sådan ny situation vil give større fleksibilitet til at reagere hurtigt på ændringer i det stadigt skiftende net- og informationssikkerhedsmiljø.

3.8 Valgmulighed 4 omfatter operationelle funktioner til bekæmpelse af internetangreb og andre trusler mod internettets sikkerhed. Her vil agenturet, ud over de ovennævnte aktiviteter, få tildelt operationelle funktioner, såsom en mere aktiv rolle i EU's beskyttelse af kritisk infrastruktur, eksempelvis forebyggelse af og reaktion på hændelser, nærmere bestemt ved at fungere dels som EU's it-beredskabsenhed inden for net- og informationssikkerhed, dels EU's »Storm Centre«, der koordinerer nationale it-beredskabsenheder, med hensyn til både den daglige forvaltning og håndteringen af udrykningstjenester.

3.9 Valgmulighed 4 vil ud over de virkninger, valgmulighed 3 afstedkommer, få større indvirkning på det operationelle plan. Ved at fungere som EU's it-beredskabsenhed inden for net- og informationssikkerhed og koordinere de nationale it-beredskabsenheder vil agenturet eksempelvis medvirke til stordriftsfordele ved at reagere på sikkerhedsrelaterede hændelser på EU-plan og lavere driftsrisici for virksomhederne som følge af øget sikkerhed og robusthed. Valgmulighed 4 vil kræve en betydelig forøgelse af agenturets budget og personale, hvilket sætter spørgsmålstegn ved, om agenturets absorptionskapacitet og effektive udnyttelse af budgettet modsvarer de opnåede fordele.

3.10 Valgmulighed 5 omfatter operationelle funktioner i støtten til retshåndhævende og retlige myndigheder i kampen mod internetkriminalitet. Ud over de aktiviteter, der nævnes under valgmulighed 4, vil dette gøre ENISA i stand til at

— yde støtte til procesret (jf. konventionen om it-kriminalitet), dvs. f.eks. indsamle trafikdata, opfange dataindhold og overvåge datastrømme i tilfælde af »denial of service«-angreb;

— udgøre et ekspertisecenter i strafferetlige undersøgelser, herunder net- og informationssikkerhedsaspekterne.

3.11 Med valgmulighed 5 vil tilføjelsen af operationelle funktioner i støtten til retshåndhævende og retlige myndigheder gøre bekæmpelsen af internetkriminalitet mere effektiv end under valgmulighed 3 og 4.

3.12 Valgmulighed 5 vil kræve en betydelig forøgelse af agenturets budget og afføde usikkerhed om agenturets absorptionskapacitet og effektive udnyttelse af budgettet.

3.13 Selv om både valgmulighed 4 og 5 vil give større positive virkninger end valgmulighed 3, mener Kommissionen, at der er en række grunde til ikke at gå videre med disse valgmuligheder:

— Begge muligheder vil være politisk følsomme for medlemsstaterne, hvad angår deres ansvar for beskyttelse af kritisk informationsinfrastruktur (dvs. at flere af medlemsstaterne ikke vil gå ind for centraliserede operationelle funktioner);

— En udvidelse af mandatet som beskrevet under valgmulighed 4 og 5 kan gøre agenturets stilling tvetydig;

— En tilføjelse af disse nye og helt anderledes operationelle opgaver til agenturets mandat vil måske vise sig at være en større udfordring på kort sigt, og der er en vis risiko for, at agenturet ikke vil være i stand til at udføre denne type opgaver tilfredsstillende inden for en rimelig tidshorisont;

— Sidst, men ikke mindst, er omkostningerne til valgmulighed 4 og 5 særdeles høje, idet der vil kræves et budget, der er 4-5 gange ENISA's nuværende budget.

([5]) Henvisningen til flere ressourcer er betinget af, at den nuværende udgave af ENISA-forslaget vedtages.

4. **Bestemmelser i forordningen**

4.1 Agenturet skal hjælpe Kommissionen og medlemsstaterne med at opfylde de retlige og reguleringsmæssige krav vedrørende net- og informationssikkerhed.

4.2 Bestyrelsen fastlægger de overordnede retningslinjer for agenturets drift.

4.3 Bestyrelsen består af en repræsentant for hver medlemsstat, tre repræsentanter, der udnævnes af Kommissionen, og en repræsentant for henholdsvis ikt-industrien, forbrugergrupper og akademiske it-eksperter.

4.4 Agenturet ledes af en administrerende direktør, der vil være ansvarlig for at udarbejde agenturets arbejdsprogram, som godkendes af bestyrelsen.

4.5 Den administrerende direktør vil også være ansvarlig for at udarbejde et årligt budget til støtte for arbejdsprogrammet. Bestyrelsen skal både fremsætte budgettet og arbejdsprogrammet, som godkendes af Kommissionen og medlemsstaterne.

4.6 Bestyrelsen nedsætter, på forslag fra den administrerende direktør, en stående gruppe af interessenter, som består af eksperter fra ikt-industrien, forbrugergrupper, universitetsverdenen samt myndigheder med ansvar for retshåndhævelse og beskyttelse af privatlivets fred.

4.7 Da forordningen stadig er på forslagsstadiet, er der en vis usikkerhed om de forskellige tal. I øjeblikket har agenturet 44-50 personer ansat og et budget på 8 mio. euro. Valgmulighed 3 vil sandsynligvis indebære et personale på 99 ansatte og et budget på 17 mio. euro.

4.8 I forordningen foreslås en tidsbegrænset mandatperiode på fem år.

Bruxelles, den 17. februar 2011

Staffan NILSSON

Formand

for Det Europæiske Økonomiske og Sociale Udvalg