RÅDET FOR DEN EUROPÆISKE UNION

Bruxelles, den 1. oktober 2010 (06.10)
(OR. en)

14358/10
ADD 2

Interinstitutionel sag:
2010/0275 (COD)

TELECOM 99
MI 346
DATAPROTECT 70
JAI 794
CAB 16
INST 361
CODEC 943

FØLGESKRIVELSE

fra:	Jordi AYET PUIGARNAU, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget den:	1. oktober 2010
til:	Pierre de BOISSIEU, generalsekretær for Rådet for Den Europæiske Union
Vedr.:	Arbejdsdokument fra Kommissionens tjenestegrene - Ledsagedokument til forslag til Europa-Parlamentets og Rådets forordning om Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA)

Hermed følger til delegationerne Kommissionens dokument - SEK(2010) 1127.

Bilag: SEK(2010) 1127

EUROPA-KOMMISSIONEN

Bruxelles, den 30.9.2010
SEK(2010) 1127

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

RESUMÉ AF KONSEKVENSANALYSEN

Ledsagedokument til

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA)

{KOM(2010) 521 endelig}
{SEK(2010) 1126}

RESUMÉ AF KONSEKVENSANALYSEN

1. ANVENDELSESOMRÅDE OG BAGGRUND

1.1. Anvendelsesområde

I denne konsekvensanalyse fokuseres der på, hvordan et moderne agentur for net- og informationssikkerhed, som i vide kredse anses for at være et velegnet og nødvendigt politikinstrument til håndtering af problemer inden for net- og informationssikkerhed, bedst kan udformes, så det understøtter medlemsstaternes organers og Kommissionens bestræbelser på at virkeliggøre målene på dette område, når Det Europæiske Agentur for Net- og Informationssikkerheds (ENISA) mandat udløber i marts 2012.

1.2. Baggrund

Som verden ser ud i dag, er samfundet og økonomien helt afhængige af, at informations- og kommunikationsteknologi (ikt) fungerer. Det har derfor afgørende betydning, at man sikrer, både at systemerne er stabile, og at brugerne stoler på dem. Med den stigende mængde af trusler, angreb og malware, som systemerne udsættes for, er der en vis risiko for, at den grundlæggende net- og informationsinfrastruktur ikke kan fungere som tilsigtet. Eftersom systemer og net er tværnationale, er der behov for et europæisk svar på problemerne med at bevare net- og informationssikkerheden.

Som reaktion på disse spørgsmål blev Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) oprettet i 2004[1] for en periode på fem år for "*at sikre et højt og effektivt net- og informationssikkerhedsniveau i Fællesskabet og for at udvikle en net- og informationssikkerhedskultur til gavn for borgerne, forbrugerne, virksomhederne og den offentlige sektors organisationer i Den Europæiske Union og dermed bidrage til et velfungerende indre marked*".

Siden da har problemerne med net- og informationssikkerhed hele tiden ændret sig i takt med den teknologiske og markedsmæssige udvikling. Derfor påbegyndte Kommissionen i god tid, inden ENISA-forordningen udløb i marts 2009, sammen med de relevante interessenter en undersøgelse af, hvilke politikker der bedst ville tilgodese EU's net- og informationssikkerhedsmål fra 2009 og frem. Efter en midtvejsevaluering af ENISA[2] og en offentlig høring[3] i 2007 vedtog Europa-Parlamentet og Rådet den 24. september 2008 en forordning om at forlænge ENISA's mandat uændret i tre år indtil den 13. marts 2012[4]. I forordningens betragtninger opfordrede Rådet og Europa-Parlamentet til "***yderligere drøftelser om agenturet [og] om den generelle retning for EU's bestræbelser hen imod et udvidet net- og informationssamfund***".

---

1 Europa-Parlamentets og Rådets forordning (EF) nr. 460/2004 af 10. marts 2004 om oprettelse af et europæisk agentur for net- og informationssikkerhed

2 Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om evaluering af Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA), KOM(2007) 285 af 1.6.2007. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:DA:NOT.

3 Den offentlige høring blev gennemført fra den 13. juni til den 7. september 2007.

4 Europa-Parlamentets og Rådets forordning (EF) nr. 1007/2008 af 24. september 2008 om ændring af forordning (EF) nr. 460/2004 om oprettelse af et europæisk agentur for net- og informationssikkerhed for så vidt angår agenturets mandatperiode (EUT L 293 af 31.10.2008).

Kommissionen satte fart i drøftelserne ved i november 2008 at igangsætte endnu en EU-dækkende offentlig høring om, hvilke mål man kunne sætte for en skærpet net- og informationssikkerhedspolitik, og hvordan sådanne mål kunne nås[5]. Kommissionen afholdt tillige i december 2008 en workshop med eksperter fra de kompetente organer i medlemsstaterne inden for net- og informationssikkerhed. Emnet var instrumenter og mekanismer i en skærpet EU-politik for net- og informationssikkerhed. Endvidere vedtog Kommissionen i marts 2009 en meddelelse om beskyttelse af kritisk informationsinfrastruktur[6], hvori ENISA får tildelt den centrale rolle at støtte EU's forøgelse af sikkerhed, robusthed og beredskab. Den tilgang vandt tilslutning på ministerkonferencen om beskyttelse af kritisk informationsinfrastruktur, der blev holdt den 27.-28. april 2009 i Tallinn, og hvor man konkluderede, at "***de nye og vedvarende udfordringer, der ligger forude, kræver omhyggelig revurdering og omformulering af agenturets mandat med det formål i højere grad at rette fokus mod EU's prioriteter og behov,*** *opnå en mere fleksibel reaktionsevne, udvikle europæiske færdigheder og kompetencer og forbedre agenturets operationelle effektivitet og dets samlede gennemslagskraft. På denne måde kan ENISA gøres til et permanent aktiv for de enkelte medlemsstater og for EU som helhed*".

Den 18. december 2009 vedtog Rådet en resolution om en samordnet europæisk strategi for net- og informationssikkerhed[7], hvori det bl.a. understreges, at "***ENISA under et revideret mandat bør udgøre EU's ekspertisecenter i spørgsmål, der vedrører net- og informationssikkerhed i EU***."

I Kommissionens Europa 2020-strategi for intelligent, bæredygtig og inklusiv vækst[8] er et af de flagskibsinitiativer, der skal føre Europa 2020-strategien ud i livet, en digital agenda for Europa, hvori net- og informationssikkerhed indtager en central plads. **Målet for det foreliggende politikinitiativ til fremme af tillid og sikkerhed inden for den digitale dagsorden for Europa er at sætte EU, medlemsstaterne og interessenterne i stand til at udvikle et avanceret beredskab med henblik på at forebygge, opdage og reagere bedre på net- og informationssikkerhedsproblemer**. Det vil medvirke til større tillid og sikkerhed på Europas digitale indre marked og bedre konkurrenceevne i de europæiske virksomheder.

2. PROBLEMSTILLING

2.1. Hvad er problemet?

Der er påvist en række problemkilder, som øger interessenternes sårbarhed over for trusler mod og svagheder i net- og informationssikkerheden. Alle viser de, at der er behov for en pålidelig struktur på EU-plan, således at der kan tages fat på problemet og man i hele Europa holder sig på omgangshøjde med de evigt skiftende teknologi- og markedsforhold omkring net- og informationssikkerheden.

---

5 Fra den 7. november 2008 til den 9. januar 2009; rapporten kan læses på: http://ec.europa.eu/information_society/policy/nis/nis_public_consultation/index_en.htm.

6 Meddelelse fra Kommissionen til Rådet og Europa-Parlamentet om beskyttelse af kritisk informationsinfrastruktur, KOM(2009) 149 af 30.3.2009.

7 Rådets resolution af 18. december 2009 om en samordnet europæisk strategi for net- og informationssikkerhed (2009/C 321/01).

8 KOM(2010) 2020.

- **Mange forskellige nationale tilgange.** Net- og informationssikkerhedsproblemer holder sig ikke inden for de nationale grænser og kan derfor ikke løses effektivt på nationalt plan alene. Og desuden håndterer de offentlige myndigheder i de forskellige medlemsstater problemet på mange forskellige måder. Mange forskellige sikkerhedskrav i forskellige medlemsstater lægger en omkostningsbyrde på de virksomheder, der opererer på EU-plan, hvilket fører til opsplitning og forringelse af konkurrenceevnen på EU's indre marked.

- **Begrænset europæisk forvarslings- og beredskabssystem.** Der er store forskelle mellem de nuværende nationale forvarslings- og beredskabssystemer, og der findes ikke noget EU-system. Der er behov for EU-politikinstrumenter, som kan kortlægge risici og svage punkter i net- og informationssikkerheden, etablere passende beredskabssystemer og sikre, at interessenterne kender og anvender disse systemer.

- **Mangel på pålidelige data og begrænset viden om nye problemer, der er ved at opstå.** Der foreligger meget få pålidelige kvantitative oplysninger om virkningerne af net- og informationssikkerhedshændelser, for ikke at tale om deres hyppighed, og det gør det vanskeligt for politikplanlæggere at træffe passende politiske foranstaltninger og for virksomhederne at træffe beslutning om at investere i sikkerhed.

- **Utilstrækkelig bevidsthed om net- og informationssikkerhedsrisici og –udfordringer.** Ansvaret for net- og informationssikkerheden ligger hos de enkelte interessenter, men er ikke altid klart defineret og kommunikeret. På den ene side er der forbrugerne, der ofte undervurderer net- og informationssikkerhedsrisici og ikke vil påtage sig deres personlige ansvar for sikring af deres ikt-systemer. På den anden side er der virksomhederne, der ofte lægger mest mærke til omkostningerne til net- og informationssikkerhed, men ikke de potentielle besparelser derved.

- **Den internationale dimension af net- og informationssikkerhedsproblemer.** Trusler mod net- og informationssikkerheden og deraf følgende hændelser er af natur internationale, så EU-tiltag kan blive mindre effektive, hvis net- og informationssikkerhedsproblemer ikke samtidig tages op internationalt. Vi må lægge en EU-strategi og nogle referencepunkter for net- og informationssikkerhed, således at EU bliver stillet bedre i international sammenhæng.

- **Behov for samarbejdsmodeller, der sikrer, at politikkerne bliver fulgt.** At net- og informationssikkerhedspolitikkerne bliver fulgt, kræver modeller for samarbejde på EU-niveau. Interessenterne har brug for vejledning i, hvordan net- og informationssikkerhedstrusler påvises, og hvordan de oparbejder god praksis for gennemførelse af de fastlagte net- og informationssikkerhedspolitikker.

- **Behov for en mere effektiv indsats mod internetkriminalitet.** Indsatsen for net- og informationssikkerhed er overvejende ydet under den tidligere første søjle, dvs. drøftet mellem institutionerne. Nu hvor Lissabontraktaten er trådt i kraft, er det imidlertid påkrævet at overveje en bredere vifte af opgaver for et net- og informationssikkerhedsagentur, som også omfatter områder under "anden og tredje søjle", dvs. emner, der tidligere blev truffet beslutning om af Rådet alene.

2.2. Hvem berøres mest af problemet?

Net- og informationssikkerhedshændelser kan få voldsomme virkninger for de forskellige berørte parter, dvs. såvel store som små virksomheder, offentlige myndigheder og

enkeltpersoner. Det vil med andre ord sige, at alle bliver berørt af og må tage ansvar for net- og informationssikkerhed.

Der findes kun få eller slet ingen kvantitative oplysninger om hyppigheden af net- og informationssikkerhedshændelser og/eller deres økonomiske følgevirkninger. IDC EMEA's markedsundersøgelse[9] giver et fingerpeg herom, idet den viste, at 28 % af husstandene i EU-27 havde haft problemer med spam eller virus inden for det foregående år. I gennemsnit har ca. 7 % af alle erhvervsbrugere været ude for en sikkerhedshændelse inden for det seneste år.

3. BEGRUNDELSE FOR EU-TILTAG, EU-MERVÆRDI OG SUBSIDIARITET

At net og informationssystemer er indbyrdes afhængige, gør det meget vanskeligt, måske endda umuligt, for den enkelte interessent at danne sig et korrekt indtryk af, hvilke økonomiske og samfundsmæssige virkninger vedkommendes beskyttelsesforanstaltninger mod net- og informationssikkerhedshændelser har globalt. Når nationale politikker og praksis er forskellige, bliver det indre marked brudt op, både på grund af de negative eksternaliteter ved net- og informationssikkerhedshændelser (utilstrækkelige politikker påvirker markederne i de andre medlemsstater) og positive eksternaliteter ved god net- og informationssikkerhedspraksis (god praksis i én medlemsstat giver samlet set en bedre net- og informationssikkerhed og bliver dermed et klart samfundsmæssigt gode). Politisk indgriben på EU-plan er således berettiget, fordi den medfører reel merværdi i form af et bedre fungerende indre marked. Denne merværdi er også erkendt i forordning (EF) nr. 460/2004 om oprettelse af ENISA, hvori det hedder, at ENISA's arbejdsopgaver skal bidrage til et velfungerende indre marked.

Endvidere er EU's indtræden i net- og informationssikkerhedspolitikken berettiget ifølge subsidiaritetsprincippet. Som det bemærkes i meddelelsen om beskyttelse af kritisk informationsinfrastruktur, svarer en EU-strategi, hvor der slet ikke gribes ind i de nationale net- og informationssikkerhedspolitikker, nærmest til at bede medlemsstaterne om blot at feje for egen dør, uanset at informationssystemerne hænger indbyrdes sammen. En vis koordinering mellem medlemsstaterne, som sikrer, at de grænseoverskridende aspekter af net- og informationssikkerheden kan håndteres, er derfor helt i overensstemmelse med subsidiaritetsprincippet. Desuden vil et EU-tiltag gøre enhver national politik mere effektiv.

EU's borgere overlader i stigende omfang deres data i komplekse informationssystemers varetægt (fx ved cloud computing). En samordnet og samarbejdsorienteret net- og informationssikkerhedspolitik kan derfor styrke en reel *beskyttelse af grundlæggende rettigheder*, især retten til *beskyttelse af personoplysninger og privatlivets fred*. Også dette begrunder rigeligt en videreførelse af EU's politiske engagement.

4. POLITISKE MÅLSÆTNINGER

I denne konsekvensanalyse ses der på, i hvilket omfang et mere moderne agentur for net- og informationssikkerhed, som generelt anses for at være den bedst egnede organisationsstruktur,

---

[9] IDC EMEA, The European Network and Information Security Market, Scenario, Trends and Challenges, April 2009, hvori der henvises til Eurobarometers undersøgelse af elektronisk kommunikation fra april 2007.

bedst kan formes, så det sammen med de øvrige EU-instrumenter kan medvirke til, at de politiske målsætninger bliver nået.

Det overordnede mål er at sætte EU, medlemsstaterne og interessenterne i stand til at udvikle et avanceret beredskab med henblik på at forebygge, opdage og reagere bedre på net- og informationssikkerhedsproblemer. Det vil medvirke til større tillid og sikkerhed på Europas digitale indre marked og bedre konkurrenceevne i de europæiske virksomheder.

Dette mål kan opdeles i følgende syv **specifikke mål**:

(1) **Sammenhængende lovgivningsstrategier** – at vejlede og rådgive Kommissionen og medlemsstaterne med henblik på udvikling og ajourføring af et helhedsorienteret sæt normative rammer for net- og informationssikkerhed.

(2) **Forebyggelse, opdagelse og indsats** – at styrke beredskabet ved at bidrage til et europæisk forvarslings- og beredskabssystem samt fælleseuropæiske katastrofeplaner og -øvelser.

(3) **Støtte til politikudformning** – at yde bistand og rådgivning til Kommissionen og medlemsstaterne.

(4) **Ansvarliggørelse af de berørte parter** – at udvikle en sikkerheds- og risikostyringskultur ved at fremme informationsformidling og samarbejde mellem aktører fra den offentlige og den private sektor, hvilket også direkte vil gavne borgerne og de små og mellemstore virksomheder, og ved at skabe øget bevidsthed om net- og informationssikkerhed.

(5) **Europa som en levedygtig aktør i international sammenhæng** – at etablere et tæt samarbejde med tredjelande og internationale organisationer for at fremme en fælles verdensomspændende strategi for net- og informationssikkerhed og sikre, at initiativer på højt internationalt plan får virkning i Europa.

(6) **Samordnet gennemførelse** – at fremme samarbejdet om gennemførelsen af politikker for net- og informationssikkerhed.

(7) **Bekæmpelse af internetkriminalitet** – at udvikle en virkningsfuld reaktion på net- og informationssikkerhedsaspekterne af internetkriminalitet gennem samarbejde med myndigheder under (tidligere) anden og tredje søjle, f.eks. Europol.

5. ORGANISATIONSMÆSSIGE MULIGHEDER OG POLITIKMULIGHEDER

I konsekvensanalysen gennemgås flere måder, hvorpå politikmulighederne kan føres ud i livet rent organisatorisk (kapitel 4 og bilag 4), nemlig: i) et agentur; ii) et mere eller mindre formaliseret offentlig-privat partnerskab (PPP); iii) et uformelt kontaktnetværk; iv) et fast netværk af kompetente organer; v) direkte integration i en af Kommissionens tjenestegrene.

Ved en sammenligning af disse organisationsmåder synes agenturet at være bedst egnet som politikinstrument, idet det indebærer følgende fordele: 1) det giver juridisk sikkerhed i kraft af sin organisationsstruktur og substans; 2) det er velegnet i specifikke problemstillinger i en så følsom sektor som net- og informationssikkerhed (organ med ekstern ekspertise, koordinering

af forholdet til interessenterne, inddragelse/engagement af medlemsstaterne); 3) accept af ENISA og ENISA's omdømme i net- og informationssikkerhedskredse.

Følgelig er nedenstående politikmuligheder opstillet og detailvurderet på baggrund af agentur-organisationsmåden.

Valgmulighed 1: Ingen politik

I tilfældet af "ingen politik" antages det, at ENISA ikke længere eksisterer efter marts 2012, og at ingen af ENISA's aktuelle aktiviteter overtages af en anden EU-institution, hverken helt eller delvis.

Nedlæggelse af ENISA vil betyde, at alle hidtidige investeringer, fx i etablering af en organisation, der kan tiltrække højt specialiserede folk, og i opbygning af dels ekspertise, dels netværk med og mellem de berørte parter og med internationale institutioner, vil gå tabt på et tidspunkt, hvor det eksisterende agentur er kommet op i arbejdstempo.

Net- og informationssikkerhedsproblemet har i hele Europa en så kompleks karakter, at der er behov for et moderne og stærkt agentur, ikke lukning af et eksisterende agentur. Det bekræftes af, at ENISA har fået tildelt en eksplicit rolle i fx de ændrede rammebestemmelser for elektronisk kommunikation[10], og at der blandt interessenterne er generel støtte til, at et europæisk agentur for net- og informationssikkerhed får en vigtigere rolle.

Valgmulighed 2: Fortsætte som hidtil

Valgmulighed 2 er business as usual-scenariet, dvs. at det samme politikinstrument fortsætter i uændret form og med samme ressourcer. Blandt interesseparterne er der generel enighed om, at ENISA har udviklet sig til et troværdigt referencepunkt i net- og informationssikkerhedsspørgsmål og et ekspertisecenter på sit område.

Med de nuværende personale- og budgetbegrænsninger vil agenturet kun være i stand til at gøre sin indflydelse gældende i ganske få net- og informationssikkerhedsspørgsmål. Det står imidlertid i skærende kontrast til interessenternes generelle forventninger. Får agenturet ikke mulighed for at udvikle sig yderligere og leve op til disse stigende forventninger, kan der i sidste ende opstå en troværdighedskrise.

Valgmulighed 3: Udvide de funktioner, der i dag er defineret for agenturet, og lade myndigheder med ansvar for retshåndhævelse og beskyttelse af privatlivets fred blive fuldgyldige interessenter

I dette tilfælde vil et agentur for net- og informationssikkerhed få en større rolle med fokus på:

- at opbygge og vedligeholde et kontaktnetværk mellem interessenter samt et videnetværk
- at fungere som et center for støtte til udvikling og gennemførelse af net- og informationssikkerhedspolitikken (særlig mht. privatlivsbeskyttelse i forbindelse med elektronisk kommunikation, e-signatur, e-id og offentlige indkøb)

[10] Se http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2009:337:SOM:DA:HTML.

- at yde støtte til EU's politik for beskyttelse af kritisk informationsinfrastruktur og robusthed (øvelser, EP3R[11], europæisk informationsudvekslings- og varslingssystem mv.)

- at skabe en EU-ramme for indsamling af data om net- og informationssikkerhed, herunder udvikle metoder og praksis for indberetning og udveksling af data i overensstemmelse med lovgivningen

- at undersøge de økonomiske aspekter af net- og informationssikkerhed

- at fremme samarbejdet med tredjelande og internationale organisationer for at fremme en fælles verdensomspændende strategi for net- og informationssikkerhed og sikre, at initiativer på højt internationalt plan får virkning i Europa

- at udføre ikke-operationelle opgaver i forbindelse med net- og informationssikkerheds-aspekterne af retshåndhævelse og retligt samarbejde.

Agenturet vil 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 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.

Valgmulighed 4: Tilføje operationelle funktioner i bekæmpelsen af internetangreb og andre trusler mod internettets sikkerhed

Her vil agenturet, ud over de aktiviteter, der er opregnet under valgmulighed 3, få tildelt operationelle funktioner, såsom en mere aktiv rolle i EU's beskyttelse af kritisk informationsinfrastruktur, eksempelvis forebyggelse og reaktion på hændelser, nærmere bestemt ved at fungere dels som EU's it-beredskabsenhed (CERT) inden for net- og informationssikkerhed, dels EU's "Storm Centre", der koordinerer nationale CERT'er, med hensyn til både den daglige forvaltning og håndteringen af udrykningstjenester.

Dette 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.

Valgmulighed 5: Tilføje operationelle funktioner i støtten til retshåndhævende og retlige myndigheder i kampen mod internetkriminalitet

Her skal agenturet, ud over de aktiviteter, der er opregnet under valgmulighed 4, udøve funktioner i forbindelse med, at det

- yder støtte til procesret (jf. konventionen om it-kriminalitet), dvs. fx indsamle trafikdata, opfange dataindhold og overvåge datastrømme i tilfælde af denial of service-angreb

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

[11] Europæisk offentlig-privat partnerskab for en robust infrastruktur, se KOM(2009) 149.

Dette vil ligesom valgmulighed 4 kræve en betydelig forøgelse af agenturets budget og afføder tilsvarende usikkerhed om agenturets absorptionskapacitet og effektive udnyttelse af budgettet.

6. SAMMENLIGNING AF POLITIKMULIGHEDER OG VURDERING AF DERES INDVIRKNING

En analyse af de mulige økonomiske, samfundsmæssige og miljømæssige virkninger har vist, at ***valgmulighed 1*** vil få negative virkninger i alle henseender, og at situationen vil blive forværret.

Valgmulighed 2 har vist sig at være suboptimal, da agenturet ikke vil have de nødvendige ressourcer til at tage ordentligt fat om de udfordringer, det evigt skiftende net- og informationssikkerhedslandskab byder på. Det kan bringe agenturets renommé i fare og i den sidste ende føre til en troværdighedskrise.

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

- 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
- 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 i

kampen mod internetkriminalitet, såsom gensidig udveksling af information og uddannelse (fx i samarbejde med European Police College, CEPOL).

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 (CERT) inden for net- og informationssikkerhed og koordinere de nationale CERT'er 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.

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.

Selv om både valgmulighed 4 og 5 vil få større positive virkninger end valgmulighed 3, er begge disse muligheder 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). Ydermere kan en udvidelse af mandatet som beskrevet under valgmulighed 4 og 5 gøre agenturets stilling tvetydig. Desuden vil tilføjelse af disse nye og helt anderledes operationelle opgaver til agenturets mandat 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.

I en sammenligning af virkningerne af alle fem politikmuligheder ved organiseringen af et mere moderne agentur for net- og informationssikkerhed må valgmulighed 1 og 2 forkastes, da ingen af dem vil give mulighed for at tage ordentligt fat om det komplekse net- og informationssikkerhedsproblem på EU-plan. Valgmulighed 3, 4 og 5 vil derimod sætte EU i stand til virkelig at tage fat om de fremtidige politiske valg inden for net- og informationssikkerhed. Valgmulighed 4 og 5 synes i dag at være for ambitiøse, både med hensyn til den politiske følsomhed i størsteparten af medlemsstaterne og med hensyn til budgetvirkningerne. Således ***anses valgmulighed 3 for at være den, der mest effektivt kan føre til løsning af de syv opregnede net- og informationssikkerhedsproblemer***.

7. OVERVÅGNING OG EVALUERING: HVORDAN SKAL DE FAKTISKE OMKOSTNINGER OG FORDELE OG OPNÅELSEN AF DE ØNSKEDE VIRKNINGER MÅLES?

Under dette politiske initiativ påregnes der periodiske evalueringer, som Kommissionen sender til Europa-Parlamentet og Rådet, og som offentliggøres. I evalueringerne vil der blive taget højde for alle relevante interessenters synspunkter på baggrund af et kommissorium, der fastlægges med agenturbestyrelsens samtykke. Evalueringerne kommer til at indeholde en vurdering af, om agenturet på effektiv måde har nået sine mål, om agenturet stadig er et effektivt instrument, og om der bør ændres på agenturets mandat og/eller andre aspekter af den forordning, hvorved det er oprettet. Efter en evaluering fremsætter agenturets bestyrelse henstillinger til Kommissionen om eventuelt påkrævede ændringer af forordningen. Bestyrelsen og den administrerende direktør tager hensyn til resultaterne af evalueringen i agenturets flerårige planlægning.

Agenturets virke er underlagt ombudsmandens tilsyn i overensstemmelse med traktatens artikel 228.