EUROPESE COMMISSIE

Brussel, 30.9.2010
SEC(2010) 1127

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN DE EFFECTBEOORDELING

Begeleidend document bij het

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

inzake het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA)

{COM(2010) 521 definitief}
{SEC(2010) 1126}

SAMENVATTING VAN DE EFFECTBEOORDELING

1. TOEPASSINGSGEBIED EN CONTEXT

1.1. Toepassingsgebied

Deze effectbeoordeling belicht de wijze waarop het beste vorm kan worden gegeven aan een gemoderniseerd agentschap voor netwerk- en informatiebeveiliging, waarvan algemeen wordt erkend dat het een passend en noodzakelijk beleidsinstrument is om uitdagingen op het gebied van netwerk- en informatiebeveiliging aan te pakken, teneinde de organen van de lidstaten en de Commissie te steunen bij het verwezenlijken van beleidsdoelstellingen op het gebied van netwerk- en informatiebeveiliging, na afloop van het mandaat van het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) in maart 2012.

1.2. Context

Tegenwoordig is de goede werking van informatie- en communicatietechnologieën (ICT) van cruciaal belang voor de maatschappij en de economie. Het is dan ook van het allergrootste belang te garanderen dat deze systemen stabiel zijn en dat de gebruikers er vertrouwen in kunnen hebben. De toename van het aantal bedreigingen, aanvallen en malware tegen deze systemen kan de goede werking van de fundamentele netwerk- en informatie-infrastructuur in gevaar brengen. Aangezien deze systemen en netwerken grensoverschrijdend van aard zijn, is ook een Europees antwoord nodig op de uitdagingen op het gebied van netwerk- en informatiebeveiliging.

Om het hoofd te bieden aan deze uitdagingen is in 2004[1] het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) opgericht voor een periode van 5 jaar, teneinde *"te zorgen voor een hoog en doeltreffend niveau van netwerk- en informatiebeveiliging in de Gemeenschap en (…) een cultuur van netwerk- en informatiebeveiliging ten behoeve van de burgers, consumenten, bedrijven en publieke organen in de Europese Unie tot stand te brengen en op die manier bij te dragen tot de goede werking van de interne markt".*

Sindsdien zijn de uitdagingen op het gebied van netwerk- en informatiebeveiliging voortdurend veranderd ten gevolge van technologische en marktontwikkelingen. Daarom is de Commissie, geruime tijd voor de ENISA-verordening in maart 2009 verstreek, samen met relevante belanghebbenden beginnen na te gaan welke beleidsvoorstellen het beste geschikt waren met het oog op de verwezenlijking van de EU-doelstellingen inzake netwerk- en informatiebeveiliging na 2009. Na een tussentijdse evaluatie van het ENISA in 2007[2] en een openbare raadpleging[3] hebben de Raad en het Europees Parlement op 24 september 2008 een verordening vastgesteld waarbij het mandaat van het ENISA met drie jaar wordt verlengd, tot 13 maart 2012[4]. In de overwegingen van deze verordening worden de Raad en het Europees

---

1 Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging.

2 Mededeling van de Commissie aan het Europees Parlement en de Raad inzake de evaluatie van het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) - COM(2007) 285 van 1.6.2007: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:NL:NOT.

3 De raadpleging vond plaats van 13 juni tot 7 september 2007.

4 Verordening (EG) nr. 1007/2008 van het Europees Parlement en de Raad van 24 september 2008 tot wijziging van Verordening (EG) nr. 460/2004 tot oprichting van het Europees Agentschap voor

Parlement opgeroepen tot ***'nader overleg over het Agentschap [en] de route die het Europese streven naar een betere netwerk- en informatiebeveiliging dient te volgen'.***

De Commissie heeft de bespreking vergemakkelijkt door in november 2008 een nieuwe EU-wijde openbare raadpleging op te starten over de mogelijke doelstellingen van een versterkt beleid inzake netwerk- en informatiebeveiliging en over de middelen om die doelstellingen te verwezenlijken[5]. De Commissie heeft in december 2008 ook een workshop met deskundigen van de bevoegde organen van de lidstaten georganiseerd over de instrumenten en mechanismen van een versterkt EU-beleid inzake netwerk- en informatiebeveiliging. Bovendien heeft de Commissie in maart 2009 een mededeling betreffende de bescherming van kritieke informatie-infrastructuur[6] vastgesteld, waarin aan het ENISA een sleutelrol wordt toebedeeld bij het ondersteunen van de EU teneinde de beveiliging, veerkracht en paraatheid te verbeteren. Deze benadering werd bevestigd in een van de conclusies van de ministeriële conferentie inzake kritieke informatie-infrastructuur die op 27 en 28 april 2009 plaatsvond in Tallinn: ***'de nieuwe en langdurige uitdagingen voor de toekomst vereisten dat het mandaat van het Agentschap grondig opnieuw wordt bekeken en geformuleerd, zodat het beter is afgestemd op de prioriteiten en behoeften van de EU,*** *zodat een flexibeler responscapaciteit kan worden opgebouwd, vaardigheden en bekwaamheden kunnen worden ontwikkeld, en algemene impact van het Agentschap kunnen worden versterkt, teneinde ervoor te zorgen dat het Agentschap een permanente aanwinst wordt voor alle lidstaten en voor de Europese Unie in haar geheel.*'

Bovendien heeft de Raad Telecom van 18 december 2009 een resolutie vastgesteld over *'een coöperatieve Europese aanpak met betrekking tot netwerk- en informatiebeveiliging'*[7], waarin onder meer wordt benadrukt dat ***'ENISA, met een herzien mandaat, het centrum van deskundigheid van de EU moet worden in EU-aangelegenheden op het gebied van netwerk- en informatiebeveiliging'***.

De Europese Digitale Agenda, waarin een centrale rol is weggelegd voor netwerk- en informatiebeveiliging, is een van de vlaggenschipinitiatieven van de Europa 2020-strategie voor slimme, duurzame en inclusieve groei[8]. Het **doel van dit beleidsinitiatief van de Europese Digitale Agenda is ervoor te zorgen dat de EU, de lidstaten en belanghebbenden de nodige bekwaamheden en paraatheid ontwikkelen om problemen op het gebied van netwerk- en informatiebeveiliging te voorkomen, op te sporen en aan te pakken**. Dit zal bijdragen tot meer vertrouwen in en een betere beveiliging van de Europese digitale interne markt en zal de concurrentiekracht van het Europese bedrijfsleven verbeteren.

---

netwerk- en informatiebeveiliging, ten aanzien van de looptijd van het Agentschap (PB L 293 van 31.10.2008).

5 Van 7 november 2008 tot en met 9 januari 2009; het verslag kan worden geraadpleegd op: http://ec.europa.eu/information_society/policy/nis/nis_public_consultation/index_en.htm.

6 Mededeling aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's betreffende de bescherming van kritieke informatie-infrastructuur, COM(2009) 149 van 30.3.2009.

7 Resolutie van de Raad van 18 december 2009 over een coöperatieve Europese aanpak met betrekking tot netwerk- en informatiebeveiliging (2009/C 321/01).

8 COM(2010) 2020.

2. OMSCHRIJVING VAN HET PROBLEEM

2.1. Wat is het probleem?

Hierna wordt een overzicht gegeven van de vastgestelde problemen, die tot gevolg hebben dat belanghebbenden kwetsbaar worden voor bedreigingen en incidenten met betrekking tot netwerk- en informatiebeveiliging. Hieruit blijkt dat er behoefte is aan een betrouwbare structuur op EU-niveau om deze problemen op te lossen en om in heel Europa op de hoogte te blijven van de voortdurende veranderende technologische en marktomstandigheden op het gebied van netwerk- en informatiebeveiliging.

- **De diversiteit en versnippering van nationale benaderingen.** Problemen met netwerk- en informatiebeveiliging stoppen niet aan nationale grenzen en kunnen dus ook niet efficiënt worden aangepakt op nationaal niveau alleen. Tegelijk wordt het probleem op uiteenlopende wijze aangepakt door de overheidsautoriteiten in verschillende lidstaten. De vele beveiligingseisen in verschillende lidstaten leiden tot kosten voor bedrijven die in de hele EU actief zijn, tot versnippering van de interne markt en tot een daling van het concurrentievermogen op die markt.

- **Beperkte Europese capaciteit voor vroegtijdige waarschuwing en respons.** De huidige nationale systemen voor vroegtijdige waarschuwing en aanpak van incidenten verschillen van lidstaat tot lidstaat; er bestaat geen EU-systeem. Er is behoefte aan EU-beleidsinstrumenten waarin risico's en zwakke punten met betrekking tot netwerk- en informatiebeveiliging worden geïdentificeerd en passende responsmechanismen worden vastgesteld; bovendien moeten deze instrumenten ervoor zorgen dat de belanghebbenden deze responsmechanismen kennen en toepassen.

- **Gebrek aan betrouwbare Europese gegevens en beperkte kennis over veranderende problemen.** Er is zeer weinig betrouwbare kwantitatieve informatie voorhanden over incidenten op het gebied van netwerk- en informatiebeveiliging en de gevolgen ervan, waardoor beleidmakers moeilijk passende maatregelen kunnen treffen en bedrijven moeilijk beslissingen over investeringen in beveiliging kunnen nemen.

- **Gebrek aan bewustzijn van risico's en uitdagingen met betrekking tot netwerk- en informatiebeveiliging.** De individuele belanghebbenden zijn verantwoordelijk voor netwerk- en informatiebeveiliging; hun verantwoordelijkheid is echter niet altijd duidelijk gedefinieerd en meegedeeld. Enerzijds onderschatten consumenten vaak de risico's in verband met netwerk- en informatiebeveiliging en weten ze niet dat ze zelf verantwoordelijk zijn voor het beveiligen van hun ICT-systemen. Anderzijds zien bedrijven vaak alleen maar de kosten van netwerk- en informatiebeveiliging en niet de potentiële besparingen.

- **De internationale dimensie van problemen met netwerk- en informatiebeveiliging.** Aangezien bedreigingen van netwerk- en informatiebeveiliging en eventuele incidenten internationaal zijn, kan de effectiviteit van EU-maatregelen afnemen als de problemen op internationaal niveau minder adequaat worden aangepakt. We moeten een EU-strategie en een referentiepunt voor netwerk- en informatiebeveiliging ontwikkelen, zodat de internationale positie van de EU verbetert.

- **Behoefte aan samenwerkingsmodellen teneinde adequate tenuitvoerlegging van het beleid te garanderen.** De adequate tenuitvoerlegging van beleid op het gebied van

netwerk- en informatiebeveiliging vereist samenwerkingsmodellen op EU-niveau. Belanghebbenden hebben begeleiding nodig bij het identificeren van bedreigingen voor netwerk- en informatiebeveiliging en bij het ontwikkelen van goede praktijken voor de tenuitvoerlegging van beleidsmaatregelen inzake netwerk- en informatiebeveiliging.

- **Behoefte aan efficiënter optreden tegen cybercriminaliteit.** De inspanningen op het gebied van netwerk- en informatiebeveiliging zijn hoofdzakelijk georganiseerd in het kader van de eerste pijler, d.w.z. kwesties die tussen de instellingen worden besproken. Nu het Lissabonverdrag in werking is getreden, moet evenwel rekening worden gehouden met een breder takenpakket voor een agentschap inzake netwerk- en informatiebeveiliging, dat ook betrekking heeft op kwesties van de 'tweede en derde pijler', d.w.z. kwesties waarover voorheen alleen de Raad besliste.

2.2. Wie ondervindt de meeste gevolgen van het probleem?

Incidenten met netwerk- en informatiebeveiliging kunnen grote gevolgen hebben voor diverse belanghebbenden, waaronder grote en kleine bedrijven, overheden en overheidsinstanties en individuele burgers. Met andere woorden: iedereen heeft belang bij en is verantwoordelijk voor netwerk- en informatiebeveiliging.

Er is weinig of geen objectieve kwantitatieve informatie beschikbaar over het exacte aantal incidenten met netwerk- en informatiebeveiliging en/of de economische gevolgen ervan. In de IDC EMEA-marktstudie[9] wordt wel een indicatie gegeven: 28% van de gezinnen in de EU-27 heeft het voorbije jaar problemen gehad met spam of virussen. Gemiddeld heeft ongeveer 7% van de gebruikers in bedrijven het voorbije jaar te maken gehad met een beveiligingsincident.

3. REDENEN VOOR EU-ACTIE, TOEGEVOEGDE WAARDE VAN EU-ACTIE EN SUBSIDIARITEIT.

Door de verwevenheid van netwerken en informatiesystemen is het voor individuele actoren extreem moeilijk, zoniet onmogelijk, om de mondiale economische en maatschappelijke gevolgen van hun maatregelen ter bescherming tegen incidenten op het gebied van netwerk- en informatiebeveiliging correct in te schatten. Uiteenlopende nationale beleidsmaatregelen en praktijken verstoren de interne markt, zowel door de negatieve externe gevolgen van incidenten op het gebied van netwerk- en informatiebeveiliging (ontoereikende beleidsmaatregelen hebben gevolgen voor markten in andere lidstaten) als door de positieve externe gevolgen van goede praktijken (goede praktijken in een lidstaat verbeteren de netwerk- en informatiebeveiliging in haar geheel, hetgeen een duidelijk voordeel oplevert voor de maatschappij). EU-beleid is dan ook gerechtvaardigd, omdat het echt bijdraagt tot de goede werking van de interne markt. Deze toegevoegde waarde is ook erkend in Verordening (EG) nr. 460/2004 tot oprichting van het ENISA, waarin bepaald is dat de bevoegdheden van het ENISA tot doel hebben bij te dragen tot de goede werking van de interne markt.

Bovendien rechtvaardigt ook het *subsidiariteitsbeginsel* EU-beleid op het gebied van netwerk- en informatiebeveiliging. Zoals ook vermeld in de mededeling over kritieke informatie-infrastructuur staat niet-ingrijpen door de EU in het nationale beleid inzake

[9] IDC EMEA, 'The European Network and Information Security Market, Scenario, Trends and Challenges', april 2009, met verwijzing naar de Eurobarometerenquête over e-communicatie van april 2007.

netwerk- en informatiebeveiliging gelijk met de lidstaten te vragen alleen hun eigen achtertuin te bewaken, zonder rekening te houden met de onderlinge verwevenheid van informatiesystemen. Een passende mate van coördinatie tussen de lidstaten, om te garanderen dat de grensoverschrijdende risico's van netwerk- en informatiebeveiliging goed worden beheerd, is dan ook in overeenstemming met het subsidiariteitsbeginsel. Bovendien zou EU-actie de effectiviteit van de bestaande nationale beleidsmaatregelen verbeteren.

EU-burgers vertrouwen hun gegevens steeds vaker toe aan complexe informatiesystemen (bijv. 'cloud computing'). Een gezamenlijk en coöperatief beleid inzake netwerk- en informatiebeveiliging zal dan ook een positief effect hebben op de effectieve *bescherming van de grondrechten*, en met name het recht op de *bescherming van persoonsgegevens en privacy*. Ook om deze reden is EU-beleid ruimschoots gerechtvaardigd.

4. BELEIDSDOELSTELLINGEN

In deze effectbeoordeling wordt nagegaan hoe een gemoderniseerd agentschap voor netwerk- en informatiebeveiliging, dat algemeen wordt beschouwd als de meest geschikte organisatorische structuur, samen met andere EU-instrumenten het beste kan bijdragen tot de verwezenlijking van de beleidsdoelstellingen.

Het algemene doel is ervoor te zorgen dat de EU, de lidstaten en belanghebbenden de nodige bekwaamheden en paraatheid ontwikkelen om problemen op het gebied van netwerk- en informatiebeveiliging te voorkomen, op te sporen en aan te pakken. Dit zal bijdragen tot meer vertrouwen in en een betere beveiliging van de Europese digitale interne markt en zal de concurrentiekracht van het Europese bedrijfsleven verbeteren.

Deze doelstelling valt uiteen in zeven **specifieke doelen**:

(1) **Coherentie van regelgevende benaderingen** - de Commissie en de lidstaten verstrekken advies en begeleiding met betrekking tot de ontwikkeling en actualisering van een holistisch normatief kader op het gebied van netwerk- en informatiebeveiliging;

(2) **Preventie, detectie en respons** – de paraatheid verbeteren door bij te dragen tot een Europese capaciteit voor vroege waarschuwing en respons op incidenten, pan-Europese noodplannen en oefeningen;

(3) **Ondersteuning van de beleidsvorming** – bijstand en advies verstrekken aan de Commissie en de lidstaten;

(4) **Empowerment van belanghebbenden** – een cultuur van beveiliging en risicobeheer ontwikkelen door informatie-uitwisseling en brede samenwerking tussen actoren uit de publieke en de private sector aan te moedigen, ook rechtstreeks ten behoeve van de burger en het mkb, en door een cultuur van bewustzijn van netwerk- en informatiebeveiliging tot stand te brengen;

(5) **Van Europa een leefbare speler maken in de internationale context** – een hoog niveau van samenwerking met derde landen en internationale organisaties tot stand brengen om een gemeenschappelijke mondiale benadering van netwerk- en informatiebeveiliging te bevorderen en om ervoor te zorgen dat internationale activiteiten op hoog niveau in Europa hun effect niet missen;

(6) **Coöperatieve tenuitvoerlegging** – samenwerking bevorderen bij de tenuitvoerlegging van beleid op het gebied van netwerk- en informatiebeveiliging;

(7) **Cybercriminaliteit bestrijden** – een effectief antwoord bieden op aspecten van cybercriminaliteit die te maken hebben met netwerk- en informatiebeveiliging, via samenwerking met autoriteiten van de (voormalige) tweede en derde pijlers, bijv. met Europol.

5. MOGELIJKE ORGANISATIEVORMEN EN BELEIDSOPTIES

In de effectbeoordeling (hoofdstuk 4 en bijlage 4) worden een aantal mogelijke organisatievormen onderzocht om de bovenvermelde beleidsopties ten uitvoer te leggen, waaronder: (i) een agentschap, (ii) een min of meer formeel publiek-privaat partnerschap (PPP), (iii) een informeel contactnetwerk, (iv) een permanent netwerk van bevoegde organen, en (v) directe integratie in een dienst van de Commissie.

Uit een vergelijking van deze verschillende organisatievormen blijkt dat een agentschap het best geschikt is als beleidsinstrument omdat het voordelen biedt inzake: (1) de rechtszekerheid van de organisatiestructuur en de inhoud, (2) de geschiktheid voor de specifieke kenmerken van een gevoelige sector als netwerk- en informatiebeveiliging (externe deskundigheid, coördinatie van de relaties met belanghebbenden, betrokkenheid/engagement van lidstaten) en (3) de aanvaarding en goede reputatie van ENISA in de gemeenschap die zich bezighoudt met netwerk- en informatiebeveiliging.

Bij de gedetailleerde beoordeling van de volgende beleidsopties is dan ook uitgegaan van een agentschap als organisatievorm.

Beleidsoptie 1: geen beleid

Dit betekent dat het ENISA na maart 2012 ophoudt te bestaan en dat geen enkele andere EU-instelling haar taken of een deel ervan overneemt.

Het sluiten van het ENISA betekent dat alle investeringen die tot dusver zijn gedaan, bijvoorbeeld voor het opzetten van een organisatie die in staat is hooggespecialiseerde mensen aan te trekken, voor het opbouwen van ervaring, voor het tot stand brengen van netwerken met en tussen belanghebbenden en met internationale instellingen, stilvallen op een ogenblik dat het Agentschap op kruissnelheid is gekomen.

Het complexe karakter van netwerk- en informatiebeveiliging in heel Europa vergt een modernisering en versterking van het Agentschap, niet de sluiting ervan. Dit wordt bevestigd door de expliciete rol die aan het ENISA is toegekend, bijvoorbeeld in het hervormde regelgevingskader voor elektronische communicatie[10], en door het feit dat de belanghebbenden expliciet voorstander zijn van een prominentere rol voor een Europees Agentschap inzake netwerk- en informatiebeveiliging.

Beleidsoptie 2: ongewijzigde voortzetting van het huidige beleid

Dit is het 'business as usual'-scenario, d.w.z. een voortzetting van hetzelfde beleidsinstrument in een identieke vorm en met dezelfde middelen. Bij de belanghebbenden heerst een algemene consensus dat het ENISA is uitgegroeid tot een geloofwaardig referentiepunt voor kwesties

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

met betrekking tot netwerk- en informatiebeveiliging en dat het zich heeft ontwikkeld tot een centrum van uitmuntendheid op zijn domein.

Gezien de huidige beperkingen inzake personeel en begroting kan het Agentschap slechts invloed uitoefenen op een zeer beperkt aantal kwesties met betrekking tot netwerk- en informatiebeveiliging. Dit ligt niet in de lijn van de algemene verwachtingen van de belanghebbenden. Als het Agentschap niet de mogelijkheid krijgt zich verder te ontwikkelen en tegemoet te komen aan de toenemende verwachtingen, kan dit uiteindelijk tot een geloofwaardigheidscrisis leiden.

Beleidsoptie 3: de huidige functies van het ENISA uitbreiden en ordehandhavings- en privacybeschermingsautoriteiten aan het ENISA toevoegen als volwaardige belanghebbenden

Dit betekent dat de rol van het Agentschap inzake netwerk- en informatiebeveiliging wordt uitgebreid tot:

- het tot stand brengen en in stand houden van een verbindingsnetwerk tussen belanghebbenden en een kennisnetwerk;
- dienst doen als ondersteuningscentrum voor netwerk- en informatiebeveiliging met het oog op de ontwikkeling en toepassing van het beleid (met name met betrekking tot e-privacy, e-sign, e-ID en aanbestedingsnormen voor netwerk- en informatiebeveiliging);
- het EU-beleid inzake de bescherming van kritieke informatie-infrastructuur en de veerkracht van die infrastructuur ondersteunen (bijv. oefeningen, EP3R[11], Europees informatie-uitwisselings- en waarschuwingssysteem enz.);
- het opzetten van een EU-kader voor het verzamelen van gegevens met betrekking tot netwerk- en informatiebeveiliging, inclusief het ontwikkelen van methoden en praktijken voor wettelijke rapportering en uitwisseling;
- de economische aspecten van netwerk- en informatiebeveiliging bestuderen en er verslag over uitbrengen;
- het stimuleren van samenwerking met derde landen en internationale organisaties om een gemeenschappelijke mondiale benadering van netwerk- en informatiebeveiliging te bevorderen en om ervoor te zorgen dat internationale activiteiten op hoog niveau in Europa hun effect niet missen;
- het uitvoeren van niet-operationele taken met betrekking tot aspecten van netwerk- en informatiebeveiliging die verband houden met ordehandhaving en gerechtelijke samenwerking.

Het Agentschap moet kunnen beschikken over alle nodige middelen om zijn activiteiten zodanig uit te voeren dat ze werkelijk effect hebben. Als het ENISA over meer middelen beschikt, kan het een veel proactievere rol spelen en meer initiatieven nemen om de belanghebbenden aan te moedigen tot actieve participatie. Deze nieuwe situatie zou het ook mogelijk maken flexibeler en sneller te reageren op veranderingen in de voortdurend evoluerende omstandigheden op het gebied van netwerk- en informatiebeveiliging.

[11] Europees publiekprivaat partnerschap voor veerkracht, zie COM(2009) 149.

Beleidsoptie 4: extra taken toekennen op het gebied van de strijd tegen cybercriminaliteit en respons op cyberincidenten

Dit betekent dat het Agentschap, naast de activiteiten die onder optie 3 zijn vermeld, ook operationele taken op zich neemt, zoals het vervullen van een actievere rol in de bescherming van kritieke informatie-infrastructuur in de EU, bijvoorbeeld wat de preventie van en de respons op incidenten betreft, met name door op te treden als het EU-computercalamiteitenteam voor netwerk- en informatiebeveiliging en door de nationale computercalamiteitenteams te coördineren tot een EU-noodcentrum inzake netwerk- en informatiebeveiliging, inclusief dagelijks beheer en nooddiensten.

Deze optie vereist een aanzienlijke toename van de begroting en het personeelsbestand van het Agentschap, hetgeen bezorgdheid doet rijzen over het opnemingsvermogen van het Agentschap en het effectieve gebruik van de begroting in verhouding tot de te behalen voordelen.

Beleidsoptie 5: extra taken toekennen wat de ondersteuning van ordehandhavings- en gerechtelijke autoriteiten bij het bestrijden van cybercriminaliteit betreft

Dit betekent dat het Agentschap, naast de onder optie 4 vermelde activiteiten, ook de volgende taken op zich neemt:

- steun verlenen met betrekking tot procedurele wetgeving (cf. de conventie over cybercriminaliteit): bijv. het verzamelen van verkeersgegevens, het onderscheppen van inhoudgegevens, het volgen van gegevensstromen in het geval van "denial-of-service"-aanvallen;
- optreden als centrum van deskundigheid voor strafrechtelijke onderzoeken die betrekking hebben op aspecten van netwerk- en informatiebeveiliging.

Zoals bij optie 4 zou ook deze optie een aanzienlijke toename van de middelen van het Agentschap vergen en soortgelijke bezorgdheid doen rijzen over het opnemingsvermogen van het Agentschap en het effectieve gebruik van de begroting.

6. VERGELIJKING VAN DE BELEIDSOPTIES EN BEOORDELING VAN DE GEVOLGEN

Uit de analyse van de mogelijke economische, sociale en milieueffecten blijkt dat ***optie 1*** negatieve gevolgen zou hebben op al deze gebieden en zou leiden tot een verslechtering van de situatie.

Ook ***optie 2*** blijkt suboptimaal te zijn omdat het Agentschap niet over de nodige middelen zou beschikken om op passende wijze het hoofd te bieden aan de uitdagingen van de voortdurend veranderende situatie inzake netwerk- en informatiebeveiliging, hetgeen de reputatie van het Agentschap kan aantasten en uiteindelijk tot een geloofwaardigheidscrisis kan leiden.

De in ***optie 3*** voorgestelde modernisering van het Agentschap inzake netwerk- en informatiebeveiliging zou bijdragen tot:

een beperking van de versnippering van de nationale benaderingen (probleem 1), een verbetering van het kennis-/informatiegebaseerd beleid en van de beleidsvorming (probleem 3) en een verhoging van het algemene bewustzijn van en de aanpak van risico's en uitdagingen op het gebied van netwerk- en informatiebeveiliging (probleem 4) door bij te dragen tot:

- efficiëntere verzameling van relevante informatie over risico's, bedreigingen en kwetsbare punten door elke individuele lidstaat;

- grotere beschikbaarheid van informatie over huidige en toekomstige uitdagingen en risico's op het gebied van netwerk- en informatiebeveiliging;

- een verbetering van de kwaliteit van het beleid inzake netwerk- en informatiebeveiliging in de lidstaten;

een verbetering van de Europese capaciteit voor vroegtijdige waarschuwing en incidentenrespons (probleem 2), door:

- de Commissie en de lidstaten te helpen bij het opzetten van pan-Europese diensten, hetgeen schaalvoordelen oplevert bij het reageren op EU-wijde incidenten;

- de werking van EP3R te vergemakkelijken, wat uiteindelijk tot gevolg kan hebben dat gemeenschappelijke beleidsdoelstellingen en EU-wijde normen voor beveiliging en veerkracht leiden tot grotere investeringen;

het stimuleren van een gemeenschappelijke mondiale benadering van netwerk- en informatiebeveiliging (probleem 5), door:

- meer informatie en kennis uit te wisselen met niet-EU-landen;

efficiëntere en effectievere bestrijding van cybercriminaliteit (probleem 7), door:

- deel te nemen aan niet-operationele taken met betrekking tot aspecten van ordehandhaving en gerechtelijke samenwerking die verband houden met netwerk- en informatiebeveiliging, zoals de uitwisseling van informatie en opleidingen in twee richtingen (bijv. in samenwerking met de Europese Politieacademie CEPOL).

Optie 4 zou op operationeel niveau een groter effect hebben dan optie 3. Door op te treden als EU-computercalamiteitenteam inzake netwerk- en informatiebeveiliging en door de nationale computercalamiteitenteams te coördineren zou het Agentschap bijdragen tot grotere schaalvoordelen bij het reageren op EU-wijde incidenten en tot lagere operationele risico's voor het bedrijfsleven door het hogere niveau van beveiliging en veerkracht.

Optie 5 zou leiden tot grotere effectiviteit bij het bestrijden van cybercriminaliteit dan opties 3 en 4 omdat het Agentschap extra taken zou krijgen ter ondersteuning van de ordehandhavings- en gerechtelijke autoriteiten.

Hoewel zowel optie 4 als 5 een groter positief effect zou hebben dan optie 3, liggen deze twee opties politiek gevoelig voor een aantal lidstaten omdat ze er geen voorstander van zijn bevoegdheden inzake de bescherming van kritieke informatie-infrastructuur af te staan aan een centraal agentschap). Bovendien zou de in opties 4 en 5 onderzochte uitbreiding van het mandaat het Agentschap in een ambigue positie brengen. Ten slotte kan de toevoeging van deze nieuwe en volledig verschillende operationele taken aan het mandaat van het Agentschap op korte termijn een grote uitdaging vormen, met een reëel risico dat het Agentschap niet in staat zou zijn deze taken goed uit te voeren binnen een redelijke termijn. Ten slotte zijn de

kosten van de tenuitvoerlegging van opties 4 en 5 veel te hoog - dit zou een vervier- of vervijfvoudiging van de huidige begroting van het ENISA vergen.

Bij het vergelijken van het effect van de vijf beleidsopties voor de organisatievorm van een gemoderniseerd Agentschap inzake netwerk- en informatiebeveiliging, moeten opties 1 en 2 worden afgewezen omdat geen van beide het mogelijk maakt deze complexe materie adequaat aan te pakken op EU-niveau. Opties 3, 4 en 5 zouden het daarentegen wel mogelijk maken de toekomstige opties van het beleid inzake netwerk- en informatiebeveiliging op passende wijze aan te pakken. Opties 4 en 5 lijken voorlopig te ambitieus, zowel wegens de politieke gevoeligheid van de meerderheid van de lidstaten als wegens de gevolgen voor de begroting. Daarom ***lijkt optie 3 de beste optie om de zeven vastgestelde problemen op het gebied van netwerk- en informatiebeveiliging zo efficiënt mogelijk aan te pakken***.

7. MONITORING EN EVALUATIE: HOE KUNNEN DE WERKELIJKE KOSTEN EN BATEN EN DE MATE WAARIN DE GEWENSTE EFFECTEN ZIJN BEREIKT, WORDEN GEMETEN?

Dit beleidsinitiatief voorziet in periodieke evaluaties die door de Commissie naar het Europees Parlement en de Raad worden gestuurd en openbaar worden gemaakt. In deze evaluaties wordt rekening gehouden met de standpunten van alle relevante belanghebbenden, op basis van het referentiekader dat met de raad van bestuur van het Agentschap is overeengekomen, en wordt beoordeeld of het Agentschap zijn doelstellingen effectief heeft bereikt, of het Agentschap nog steeds een effectief instrument is en of wijzigingen moeten worden aangebracht aan het mandaat van het Agentschap en/of aan andere punten van de oprichtingsverordening. Na afloop van een evaluatie verstrekt de raad van bestuur van het Agentschap aanbevelingen aan de Commissie over passende wijzigingen van de verordening. De raad van bestuur en de uitvoerend directeur van het Agentschap houden rekening met de resultaten van de evaluaties in de meerjarenplanning van het Agentschap.

De activiteiten van het Agentschap staan onder het toezicht van de Ombudsman, overeenkomstig artikel 228 van het Verdrag.