RAAD VAN DE EUROPESE UNIE

Brussel, 22 mei 2014 (OR. en)

10097/14

Interinstitutioneel dossier: 2013/0027 (COD)

LIMITE

TELECOM 118
DATAPROTECT 77
CYBER 31
MI 446
CSC 111
CODEC 1338

NOTA

van:	het voorzitterschap
aan:	de delegaties
nr. Comv.:	6342/13 TELECOM 24 DATAPROTECT 14 CYBER 2 MI 104 CODEC 313 + ADD 1 + ADD 2
nr. vorig doc.:	9757/14 TELECOM 111 DATAPROTECT 69 CYBER 27 MI 419 CSC 103 CODEC 1264
Betreft:	Voorstel voor een richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen - Voortgangsverslag

Dit verslag is opgesteld onder de verantwoordelijkheid van het Griekse voorzitterschap. Het geeft een overzicht van de tot dusver verrichte werkzaamheden in de voorbereidende instanties van de Raad, schetst de stand van de besprekingen van het in hoofde genoemde voorstel en reikt oriëntaties en aanpakken aan met het oog op de voorbereiding van een gewijzigde versie van het voorstel en op de onderhandelingen met het EP in een later stadium.

PROCEDURELE ASPECTEN

1. De Commissie heeft haar voorstel voor een richtlijn van het Europees Parlement en de Raad houdende *maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen* (hierna "NIB-richtlijn") op 12 februari 2013 ingediend met artikel 114 VWEU als rechtsgrondslag[1]. Het voorstel maakt deel uit van de "Strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberspace"[2], waarover de Raad op 25 juni 2013 conclusies heeft aangenomen[3]. De Raad TTE heeft in zijn zittingen van 6 juni[4] en 5 december[5] 2013 nota genomen van de voortgang bij de behandeling van het voorstel voor een NIB-richtlijn.

2. Het Europees Economisch en Sociaal Comité en het Comité van de Regio's hebben op respectievelijk 22 mei[6] en 3-4 juli[7] 2013 advies over het voorstel uitgebracht. Het Europees Parlement heeft op 13 maart 2014 in eerste lezing een wetgevingsresolutie aangenomen en een aantal van de 138 amendementen die waren opgesteld door de Commissie interne markt (IMCO), als commissie ten principale, en de Commissie industrie (ITRE) en de Commissie burgerlijke vrijheden (LIBE), als medeverantwoordelijke commissies[8].

1 Document 6342/13.
2 Document 6225/13.
3 Document 11357/13.
4 Document 10076/13 en document 10457/13.
5 Document 16630/13 en document 17341/13.
6 TEN/513.
7 2013/C 280/05.
8 Document 7451/14.

3. Onder het Griekse voorzitterschap heeft de Groep telecommunicatie en informatiemaatschappij het voorstel gedurende zes vergaderingen artikelsgewijs besproken[9]. Op basis van de besprekingen in de Groep, waarvoor het voorzitterschap discussienota's had opgesteld[10], en van schriftelijke opmerkingen van de meeste lidstaten, heeft het Griekse voorzitterschap het onderhavige voortgangsverslag opgesteld, dat de voornaamste aspecten van het voorstel vermeldt en, waar mogelijk, aangeeft ten aanzien van welke punten de lidstaten het in principe eens zijn over de lijn die moet worden gevolgd. Parallel met dit voortgangsverslag en ter illustratie heeft het voorzitterschap een eerste gewijzigde versie van de tekst van het voorstel opgesteld[11], die op 26 mei is voorgelegd aan de Groep en op basis waarvan de werkzaamheden onder het Italiaanse voorzitterschap zouden kunnen worden voortgezet, met het oog op onderhandelingen met het EP in een later stadium.

4. De vraag is opgeworpen of de voorgestelde rechtsgrondslag (artikel 114 VWEU) toereikend is voor het volledige voorstel, gelet op de doelstelling, het toepassingsgebied en de inhoud. In dit verband is verdere studie en bespreking noodzakelijk. De Juridische dienst van de Raad zal een schriftelijk advies uitbrengen.

KERNPUNTEN

Hoofdstuk 1: algemene beginselen (artikelen 1 t/m 3):

5. De delegaties ondersteunen in het algemeen het voorgestelde onderwerp en toepassingsgebied van artikel 1 (onderwerp) en zijn het erover eens dat de voorgestelde richtlijn een essentieel onderdeel van de algehele strategie van de EU voor cyberbeveiliging vormt. Het voorzitterschap is van mening dat een meerderheid van de lidstaten te vinden zal zijn voor een enigszins aangepaste versie van artikel 1, van de volgende strekking:

- *In lid 1 zou het woord "waarborgen" worden vervangen door "verwezenlijken" of "faciliteren" om aan te geven dat de lidstaten noch individueel, noch collectief volledig een waterdicht niveau van netwerk- en informatiebeveiliging kunnen "waarborgen".*

[9] Op 27 februari, 13 en 28 maart, 10 en 28 april en 21 mei 2014.
[10] Document 7404/14.
[11] Document 10061/14.

- *In plaats van een nieuw "mechanisme voor samenwerking" tussen de lidstaten in het leven te roepen, zou in lid 2, punt b), moeten worden voortgebouwd op bestaande regelingen om de lidstaten te "groeperen" met het oog op uitvoering van de richtlijn op strategisch niveau/beleidsniveau. Er kan worden nagedacht over mogelijkheden voor meer concrete operationele samenwerking, bij voorbeeld in het kader van de CERT's[12] en/of de bevoegde instanties.*
- *De lidstaat die getroffen wordt door een incident en/of diens CERT zal moeten beslissen of en in welke mate relevante informatie (mogelijk met inbegrip van persoonsgegevens) moet worden gedeeld, waarbij belangen van nationale veiligheid en relevante wetgeving, met name met betrekking tot de bescherming van persoonsgegevens of aanvallen op informatie-systemen, in aanmerking moeten worden genomen.*
- *Wat betreft de hierboven in punt 4 gewenste verduidelijking op juridisch vlak is eveneens een antwoord vereist op de vraag of en in welke mate "overheden" dienen te worden opgenomen in of uitgesloten van het toepassingsgebied van het voorstel (in het bijzonder van artikel 14).*

6. De delegaties steunen in het algemeen artikel 2 (minimumharmonisatie).

7. Met betrekking tot de "definities" in artikel 3, die in een later stadium van de besprekingen opnieuw moeten worden bezien, denkt het voorzitterschap dat de delegaties zich in het algemeen zullen kunnen vinden in het volgende:

- *Een nieuwe definitie betreffende "essentiële diensten" zou moeten worden opgenomen in de lijst van definities, aangezien dit de mogelijkheid zou bieden te bepalen welke actoren deze "essentiële" diensten aanbieden en te beoordelen welk risico of welke "dreiging" bestaat voor de beveiliging en de continuïteit van deze diensten.*
- *De richtlijn zou moeten refereren aan een lijst van sectoren die gemeenschappelijke kritieke infrastructuur vormen en in criteria moeten voorzien om te bepalen welke exploitanten deel uitmaken van deze infrastructuren.*
- *De standpunten van de lidstaten zijn nog niet uitgekristalliseerd wat betreft de mate van detail waarin de richtlijn (en met name BIJLAGE II) moet voorzien, zoals de vraag of en in welke mate "diensten van de informatiemaatschappij" en "facilitators van internetdiensten" eveneens onder de richtlijn moeten vallen.*
- *Er moet nader worden bestudeerd of er behoefte is aan opneming van bijkomende definities, bijvoorbeeld inzake kritieke IT-diensten, nationaal plan voor risicobeheer, nationale NIB-strategie en nationaal NIB-samenwerkingsplan.*

---

[12] CERT staat voor "Computer Emergency Response Team" ofte wel computercrisisteam. Er is op gewezen dat het, aangezien CERT een gedeponeerd EU-handelsmerk is, nodig kan zijn in de richtlijn een andere terminologie te hanteren, zoals "reactieteam bij incidenten met computers" (Computer Security Incident Response Team - CSIRT).

Hoofdstuk II: nationale kaders voor NIB (artikelen 4 t/m 7)

8. De delegaties zijn in het algemeen voorstander van schrapping van artikel 4 (beginsel).

9. Met betrekking tot artikel 5 (nationale NIB-strategie), heeft het voorzitterschap geconstateerd dat er brede steun bestaat voor de volgende oriëntatie:

- *Hoewel de ontwikkeling van een NIB-strategie, met inbegrip van een samenwerkingsplan, in beginsel wordt gesteund, moeten de bewoordingen van dit artikel meer de nadruk leggen op "toekomstbestendige", algemene beginselen in plaats van op concrete eisen voor de NIB-strategie en het NIB-samenwerkingsplan, aangezien een dergelijke aanpak het best bijdraagt tot het opbouwen van vertrouwen.*

10. Met betrekking tot artikel 6 (bevoegde autoriteit) en rekening houdend met het subsidiariteitsbeginsel, lijken de delegaties geporteerd te zijn voor een aanpak die terdege rekening zou houden met de bestaande praktijken in de lidstaten:

- *De richtlijn moet de lidstaten de nodige flexibiliteit bieden, in die zin dat zij een of meer sectorspecifieke en beleidsgerichte bevoegde autoriteiten kunnen aanwijzen of behouden.*
- *Elke lidstaat dient wel één centraal contactpunt aan te wijzen, waarvan de taken nader dienen te worden gedefinieerd.*

11. Met betrekking tot artikel 7 (CERT's) steunen de lidstaten over het algemeen de bepaling in de richtlijn dat zij een of meer CERT's moeten aanwijzen of behouden, die dezelfde entiteit kan zijn als de "bevoegde autoriteit" of het "centraal contactpunt" en zijn zij het eens met de voorgestelde oriëntaties met betrekking tot de CERT's in doc. 7404/14, vooral wat betreft het volgende:

- *De lidstaten moeten kunnen beschikken over voldoende flexibiliteit ten aanzien van de technische aspecten en de financiële en personele middelen van de CERT's, wat tot uiting dient te komen in de bewoordingen van dit artikel en van BIJLAGE I, maar de richtlijn moet wel strikt zijn ten aanzien van de mate van ambitie die wordt nagestreefd en de eisen die voor de CERT's en voor hun onderlinge samenwerking worden geformuleerd.*

Hoofdstuk III: samenwerking (artikelen 8 t/m 13)

12. Hoofdstuk III van het voorstel ziet op de invulling van de NIB-samenwerking. Volgens het voorzitterschap erkennen alle lidstaten dat er een manier van samenwerken moet worden gevonden die de mogelijkheid biedt in de gehele EU gelijkaardige, hogere niveaus van NIB-paraatheid te bewerkstelligen, en daardoor tevens eventueel de condities te creëren voor een gemeenschappelijke en gecoördineerde respons op NIB-uitdagingen, overal waar een dergelijke respons nodig mocht blijken. Er moet echter nog nader worden bestudeerd hoe een dergelijk netwerk voor strategische samenwerking/beleidssamenwerking moet worden ingevuld en welke implicaties dat netwerk in voorkomend geval zou hebben voor het bieden van een gecoördineerde operationele respons op cyberincidenten met een nationale en wellicht grens-overschrijdende impact.

13. Met betrekking tot artikel 8 (samenwerkingsnetwerk), is het voorzitterschap van mening dat de delegaties in het algemeen voorstander zijn van de volgende aanpak:

- *Met de richtlijn moet vorm worden gegeven aan een beleidsaanpak/strategische aanpak met betrekking tot het samenwerkingsnetwerk (of de "groep"), die enerzijds voortbouwt op de in het kader van hoofdstuk II te ontwikkelen vermogens en anderzijds, indien gepast, sturing biedt voor het in detail uitwerken van de wijze waarop de operationele samenwerking in de relevante instanties gestalte moet krijgen.*
- *In het geval van een noodsituatie is het bieden van een gerichte respons de verantwoordelijkheid van nationale organen, zoals de CERT's en/of de bevoegde autoriteiten, terwijl daarnaast, indien nodig in nog nader te specificeren (grensoverschrijdende) gevallen, verdere vrijwillige samenwerking kan plaatsvinden in een operationele samenwerkingsgemeenschap, die alle 28 nationale CERT's omvat, en eventueel een gecoördineerde EU-respons kan mogelijk maken.*
- *Het samenwerkingsnetwerk zou voorts op basis van vrijwilligheid collegiale toetsingen van vermogens en paraatheid kunnen verrichten.*

14. Ten aanzien van artikel 9 (beveiligd informatie-uitwisselingssysteem) heeft het voorzitterschap geconstateerd dat de lidstaten niet echt te vinden zijn voor het opnemen in de richtlijn van dwingende eisen voor de uitwisseling van (commercieel gevoelige of vertrouwelijke) informatie in het samenwerkingsnetwerk, voor het voorzien in beveiligde infrastructuur voor dat doel, en evenmin voor de rol die in dat verband aan de Commissie was toegedacht. In het licht van het bovenstaande is het voorzitterschap van oordeel dat dit artikel anders moet worden geformuleerd, met het volgende oogmerk:

- *De richtlijn mag geen dwingende eisen voor het uitwisselen van informatie bevatten en artikel 9 moet in die zin worden aangepast of eventueel zelfs worden geschrapt, met dien verstande dat niet-gevoelige en niet-gerubriceerde informatie in het samenwerkingsnetwerk of relevante informatie tussen de CERT's en/of de bevoegde instanties kan worden uitgewisseld.*

15. Met betrekking tot artikel 10 (vroegtijdige waarschuwingen) lijken de delegaties over het algemeen steun te kunnen verlenen aan de algemene oriëntaties in doc. 7404/14, met de volgende kanttekeningen:

- *Het doen uitgaan van vroegtijdige waarschuwingen moet op basis van vrijwilligheid blijven geschieden en de uitwisseling van relevante informatie in het samenwerkingsnetwerk moet eerst en vooral ten dienste staan van het opbouwen van vertrouwen tussen de particuliere sector en de nationale bevoegde autoriteiten alsook tussen de nationale bevoegde autoriteiten onderling.*
- *De uitwisseling van informatie over strafbare feiten op het gebied van aanvallen op informatiesystemen valt onder Richtlijn 2013/40/EU en behoeft derhalve niet in onderhavige richtlijn aan bod te komen (lid 4 kan dus worden geschrapt).*
- *Het is aan de lidstaten te beslissen of en welke informatie aan het coördinatienetwerk wordt verstrekt (lid 5 kan dus worden geschrapt).*
- *Vroegtijdige waarschuwing mag geen belemmerend of vertragend effect hebben op nationaal optreden bij bedreigingen en incidenten.*

16. Voorts heeft het voorzitterschap met betrekking tot artikel 11 (gecoördineerde reactie) geconstateerd dat er brede steun is voor de oriëntaties in document 7404/14, met de volgende kanttekeningen:

- *Het gaat niet aan een feitelijke Europese bevoegdheid inzake coördinatie met het oog op een EU-respons op (nationale) incidenten in het leven te roepen; in plaats daarvan is nader beraad nodig om te verduidelijken of, en wanneer er behoefte is aan een gecoördineerde EU-respons: in het geval van een majeure grensoverschrijdende cybercrisis of ook in geval van beperktere, meer alledaagse incidenten, en welke zijn die gevallen?*
- *Aangezien veiligheidsaangelegenheden een nationale bevoegdheid zijn, dient de richtlijn voort te bouwen op bestaande regelingen om te zorgen voor politieke coördinatie op EU-niveau in het geval van grootschalige cybercrises, in plaats van te voorzien in nieuwe en potentieel trage mechanismen.*
- *Naast politieke coördinatie op EU-niveau moet de richtlijn de technische/praktische samenwerking faciliteren (bijv. tussen de CERT's); voor dat aspect zouden nadere voorschriften voor een operationele respons op cybercrises kunnen worden ontwikkeld.*

17. Het voorzitterschap heeft geconstateerd dat, hoewel de lidstaten hun definitieve standpunt inzake artikel 12 (NIB-samenwerkingsplan van de Unie) afhankelijk stellen van de uitkomst omtrent de artikelen 8 t/m 11, de meeste delegaties ermee zouden kunnen instemmen dat de volgende aanpak zijn beslag krijgt in de tekst van het voorstel:

- *De richtlijn moet niet zozeer voorzien in een "EU-plan" als wel in een "EU-kader" voor NIB-samenwerking, dat is toegespitst op beleidscoördinatie en beleidsontwikkeling, ten volle gebruik maakt van de relevante expertise van het Enisa en regelmatig wordt doorgelicht door het bij artikel 8 ingestelde samenwerkingsnetwerk.*

- *Het "kader" voor samenwerking zou aspecten moeten omvatten zoals de modaliteiten voor de communicatie tussen de CERT's, de uitwisseling van beste praktijken, bewustmaking en oefeningen en opleiding, en zou profijt moeten trekken uit de expertise van het Enisa op dit gebied.*

18. Met betrekking tot artikel 13 (internationale samenwerking) constateerde het voorzitterschap dat de lidstaten voorstander zijn van een bepaling volgens welke alle deelnemers aan het samenwerkingskader moeten instemmen met deelname van derde staten of internationale organisaties aan dat kader.

Hoofdstuk IV: beveiliging van netwerken (artikelen 14 t/m 16), hoofdstuk V: slotbepalingen (artikelen 17 t/m 23) en bijlagen I en II: CERT's en marktdeelnemers

19. Met betrekking tot artikel 14 (beveiligingseisen en melding van incidenten) constateerde het voorzitterschap dat de lidstaten waar een nationale praktijk van vrijwillige melding voor bevredigende samenwerking tussen belanghebbende partijen en de overheid heeft gezorgd, de richtlijn liever in die richting zouden willen bijsturen. Andere lidstaten vroegen zich af of er daarnaast voorschriften inzake verplichte rapportage moeten worden opgenomen. Alle lidstaten zijn het erover eens dat er behoefte is aan nadere verduidelijking betreffende de diverse vereisten inzake melding waarin bij verschillende EU-wetgevingsinstrumenten wordt voorzien. In het licht van het voorgaande zou het voorzitterschap aanbevelen dat de volgende aanpak nader wordt overwogen:

- *De richtlijn zou kunnen voorzien in dwingende voorschriften inzake rapportage over incidenten met een significante grensoverschrijdende impact waarbij meerdere lidstaten betrokken zijn.*
- *In geval van interne incidenten met beperkte gevolgen, zouden de lidstaten de mogelijkheid moeten hebben om overeenkomstig artikel 2 te bepalen of en hoe op nationaal niveau rapportage plaatsvindt.*
- *De richtlijn moet parameters bevatten voor het bepalen van de impact van (sectorspecifieke) incidenten, maar het is aan de lidstaten om op basis van die parameters te bepalen of over een specifiek incident moet worden gerapporteerd.*
- *De lidstaten zouden naar eigen inzicht de modaliteiten moeten kunnen bepalen voor rapportage aan sectorspecifieke bevoegde autoriteiten en/of aan het nationale "centrale contactpunt".*

20. Met betrekking tot artikel 15 (uitvoering en handhaving), en op basis van de standpunten van de delegaties, stelt het voorzitterschap het volgende voor:

    - *De richtlijn moet voldoende ruimte laten voor nationale oplossingen om de particuliere sector in sterkere mate te betrekken dan thans wordt voorgesteld, bijvoorbeeld met betrekking tot beveiligingsaudits, ontwikkeling van technische vermogens, opleidingen enz.*
    - *De richtlijn moet ruimte laten om, in voorkomend geval, te beschikken over meerdere, sectorspecifieke bevoegde autoriteiten, die ook verantwoordelijkheden ten aanzien van uitvoering en handhaving hebben.*

21. Wat betreft artikel 16 (normalisatie) concludeert het voorzitterschap dat verder moet worden nagedacht over een nieuwe formulering.

22. Met betrekking tot artikel 17 (sancties), en in het bijzonder lid 2, is nadere bestudering nodig om verder te verduidelijken hoe de NIB-richtlijn zich verhoudt tot de aangekondigde verordening inzake gegevensbescherming.

23. Ten slotte heeft het voorzitterschap er nota van genomen dat de delegaties in een later stadium wensen terug te komen op de aspecten overgangsperiode en inwerkingtreding (artikelen 21 en 22), en dat de uiteindelijke versie van BIJLAGE I inzake voorschriften en taken voor de CERT's en van BIJLAGE II met betrekking tot de sectoren en entiteiten die moeten worden opgenomen in een "limitatieve" of "illustratieve" lijst in een later stadium moet worden herbekeken, afhankelijk van de onderhandelingen over de inhoud van de artikelen van het voorstel.

CONCLUSIE

24. Het Griekse voorzitterschap heeft geconstateerd dat alle lidstaten, zonder uitzondering, zich terdege bewust zijn van de dringende noodzaak om de netwerk- en informatiebeveiliging te verbeteren en om in dit verband op EU-niveau actie te ondernemen. In dit verband hebben de lidstaten het voorstel van de Commissie met de grootst mogelijke aandacht bestudeerd en is het de afgelopen maanden veel duidelijker geworden in welke richting het voorstel dient te worden bijgestuurd, zoals hierboven is uiteengezet.

25. Met betrekking tot de bepalingen van de hoofdstukken I, II en IV, en op basis van de besprekingen in de voorbereidende instanties van de Raad, is het voorzitterschap van mening dat de voorgestelde oriëntaties en aanpakken in dit voortgangsverslag een toereikende grondslag bieden voor de verdere ontwikkeling van het voorstel onder het aantredende Italiaanse voorzitterschap. Bij de opstelling van deze oriëntaties en aanpakken is getracht het juiste evenwicht te vinden tussen het verbeteren van de cyberbeveiliging, het opbouwen van het noodzakelijke vertrouwen en het ten volle benutten van bestaande ervaring en het voorkomen van duplicatie van de expertise van bestaande organen en mechanismen.

26. Met betrekking tot hoofdstuk III zijn de lidstaten het, zoals hierboven vermeld (punt 12) erover eens dat de strategische samenwerking/beleidssamenwerking op het gebied van NIB op EU-niveau moet worden geïntensiveerd. Een aantal lidstaten is van mening dat de richtlijn zou moeten voorzien in meer specifieke criteria en voorschriften voor operationele samenwerking in geval van NIB-incidenten. De meeste lidstaten zien strategische samenwerking/beleids-samenwerking echter als een eerste prioriteit voor het opbouwen van het noodzakelijke vertrouwen, terwijl de modaliteiten voor operationele samenwerking tegelijkertijd verder kunnen worden uitgewerkt in het kader van bestaande structuren en organen. Zoals hierboven voorgesteld (punten 12-18), beschouwt het voorzitterschap strategische samenwerking/beleids-samenwerking en operationele samenwerking niet als elkaar uitsluitende mogelijkheden, maar is het van mening dat de richtlijn eerst en vooral betrekking moet hebben op strategische samenwerking/beleidssamenwerking en dat tegelijkertijd sturing moet worden gegeven aan bestaande organen en mechanismen wat de operationele samenwerking betreft.

*

* *

Dit voortgangsverslag zal door het Coreper worden behandeld op 28 mei, waarna het voorzitterschap het aan de Raad zal doen toekomen met het verzoek er kennis van te nemen.