Advies van het Comité van de Regio's — Strategie voor cyberbeveiliging

(2013/C 280/05)

HET COMITÉ VAN DE REGIO'S

— is ingenomen met de strategie van de Europese Commissie inzake cyberbeveiliging en haar richtlijn over netwerk- en informatiebeveiliging (NIB), en is het eens met de doelstelling van de strategie: zorgen voor een open en veilige cyberspace en de online omgeving van de EU tot de veiligste ter wereld maken;

— is van mening dat een beleidspakket dat bestaande en voorgestelde maatregelen op dit gebied bundelt, hoognodig is en zal bijdragen aan een gecoördineerde strategische visie voor Europa. Zo'n pakket is van belang om voor coördinatie te zorgen, samenwerking te stimuleren, duidelijke daadkrachtige maatregelen te kunnen nemen, een gemeenschappelijk niveau van cyberbeveiliging te bereiken, de weerbaarheid van IT-systemen en -netwerken tegen nieuwe gevaren te vergroten, en versnippering in de EU tegen te gaan;

— vindt dat de Commissie een actieplan zou moeten publiceren waarin zij uitlegt hoe de ambitieuze doelstellingen van het beleidspakket verwezenlijkt moeten worden. Dat actieplan moet ook als richtsnoer dienen voor het beoordelen en meten van het effect van de strategie, zodat kan worden nagegaan of er sprake is van samenwerking en vooruitgang;

— benadrukt dat het nieuwe beleidspakket zou moeten bijdragen aan de verbetering van de preventie, opsporing en aanpak van cyberincidenten en zou moeten leiden tot betere informatie-uitwisseling en coördinatie tussen lidstaten en de Commissie ter voorkoming van grote cyberincidenten. Onmisbaar in dit verband zijn echte partnerschappen tussen lidstaten, EU-instellingen, lokale en regionale overheden, bedrijfsleven en maatschappelijk middenveld.

Rapporteur	Robert BRIGHT (UK/PSE), lid van de gemeenteraad van Newport
Referentiedocumenten	Gezamenlijke mededeling — Strategie inzake cyberbeveiliging van de Europese Unie (JOIN(2013) 1 final) Voorstel voor een richtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen (COM(2013) 48 final)

I. **BELEIDSAANBEVELINGEN**

HET COMITÉ VAN DE REGIO'S

1. is ingenomen met de strategie van de Europese Commissie inzake cyberbeveiliging en haar richtlijn over netwerk- en informatiebeveiliging (NIB), en is het eens met de doelstelling van de strategie: zorgen voor een open en veilige cyberspace en de online omgeving van de EU tot de veiligste ter wereld maken.

2. Het nieuwe cyberbeveiligingspakket (met onder meer de strategie en de richtlijn) zal, zo verwacht het Comité van de Regio's (CvdR), de lat hoger leggen en een grote bijdrage leveren aan de ontwikkeling van EU-normen voor cyberbeveiliging. Dat leidt tot minder rechtsonzekerheid, meer vertrouwen in online diensten en minder onnodige kosten en rompslomp, en ondersteunt aldus de digitale interne markt en de Europa 2020-strategie.

3. Een beleidspakket dat bestaande en voorgestelde maatregelen op dit gebied bundelt is hoognodig en zal bijdragen aan een gecoördineerde strategische visie voor Europa. Zo'n pakket is van belang om voor coördinatie te zorgen, samenwerking te stimuleren, duidelijke daadkrachtige maatregelen te kunnen nemen, een gemeenschappelijk niveau van cyberbeveiliging te bereiken, de weerbaarheid van IT-systemen en -netwerken tegen nieuwe gevaren te vergroten, en versnippering in de EU tegen te gaan.

4. Organisaties, waaronder overheidsinstanties, moeten inzien dat de bestrijding van cybercriminaliteit een zaak van lange adem is. Zij dienen kwetsbare punten in kaart te brengen en organisatorische capaciteit voor de aanpak van beveiligingslekken te ontwikkelen en aldus prioritaire aandacht te besteden aan het gevaar van verstoringen van het internetverkeer of cyberaanvallen. Aangezien internet niet meer is weg te denken uit ons dagelijks leven, kan cybercriminaliteit des te meer schade aanrichten. In al haar verschijningsvormen vormt cybercriminaliteit in de 21e eeuw een zich razendsnel ontwikkelend en geraffineerd nieuw gevaar voor lidstaten, organisaties en EU-burgers, dat steeds vaker de kop opsteekt, steeds complexer wordt en zich niets van grenzen aantrekt.

5. Wat de bescherming van burgers tegen online criminaliteit betreft, heeft de EU al grote vooruitgang geboekt. Zo heeft zij wetsvoorstellen gedaan voor de aanpak van aanvallen op informatiesystemen en de aanzet gegeven tot een wereldwijde alliantie tegen seksuele uitbuiting van kinderen via het internet. Het beleidspakket zou moeten voortbouwen op eerdere maatregelen, waaronder die uit de Digitale Agenda voor Europa van 2010 ([1]), en de weg moeten banen naar een krachtig beleid voor cyberdefensie. De medewetgevers die zich momenteel buigen over het voorstel van de Commissie voor een richtlijn over aanvallen op informatiesystemen ([2]) zouden hierover wat dit betreft snel tot overeenstemming moeten komen.

6. De strategie verdient bijval omdat het doel ervan niet alleen is om de cyberbeveiligingscapaciteiten van de lidstaten te harmoniseren en de diverse bestaande en voorgestelde maatregelen te bundelen, zodat voor gemeenschappelijke normen en gelijke voorwaarden kan worden gezorgd, maar ook om van drie beleidsterreinen — wetshandhaving, de Digitale Agenda en defensie-, veiligheids- en extern beleid, die tot nu toe elk hun eigen bevoegdheden kennen — een gecoördineerd en samenhangend geheel te maken.

7. Het beleidspakket zou baat kunnen hebben bij door nationale overheden ingezamelde gegevens en zou voorstellen voor geharmoniseerde normen voor NIB moeten bevatten.

8. Het is een goede zaak dat er bij de beleidsvorming in het kader van het pakket een groot aantal partijen wordt betrokken. In het pakket wordt erkend hoe belangrijk publiek-private samenwerking en echte, van adequate middelen voorziene partnerschappen zijn. Het pakket heeft ook de voltooiing van de digitale interne EU-markt ten doel, teneinde voor bedrijven, overheden en burgers een veilige en gezonde digitale omgeving creëren.

([1]) COM(2010) 245, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:NL:HTML

([2]) COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:NL:HTML

9. De in de richtlijn voorgestelde maatregelen verdienen bijval. Zo wordt aanbevolen dat de lidstaten een nationale NIB-strategie vaststellen, computercalamiteitenteams (CERT's) opzetten die moeten samenwerken met het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA), en dat er een duidelijk mechanisme voor samenwerking tussen de lidstaten en de Commissie in het leven wordt geroepen voor vroegtijdige waarschuwing over risico's en incidenten via een beveiligde infrastructuur. Deze maatregelen en de voorgestelde regelgevingsaanpak zijn een grote stap in de richting van meer samenhang, een gemeenschappelijk minimumniveau van paraatheid van de lidstaten en een betere cyberdefensie in de hele EU.

10. Het Europees Parlement en de Raad doen er goed aan het voorstel voor een richtlijn inzake een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de EU zonder dralen goed te keuren.

11. Het beleidspakket zou nog kunnen worden uitgebreid met nadere informatie over de manier waarop lidstaten gegevens over cybercriminaliteit verzamelen en doorgeven en over methoden voor het uitvoeren van maatregelen. Om onzekerheid en een gebrek aan samenhang te vermijden als het aankomt op de manier waarop nationale met NIB belaste instanties cyberincidenten met een "aanzienlijke impact" omschrijven en meten, zijn gemeenschappelijke verslagleggingssystemen en meer duidelijkheid over kennisgevingseisen van cruciaal belang. Bij het opzetten van nationale, voor NIB verantwoordelijke instanties moet bovendien rekening worden gehouden met de verdeling van bevoegdheden in de lidstaten, vooral als deze een sterk federale of decentrale bestuursstructuur hebben.

12. Bepaalde regelgevings- en juridische aspecten van het pakket baren het CvdR dan ook zorgen. Het gaat hierbij met name om de onduidelijke definitie van de criteria waaraan de lidstaten moeten voldoen om te mogen deelnemen aan het systeem voor veilige informatie-uitwisseling, de nadere specificatie van incidenten die het systeem van vroegtijdige waarschuwing in werking stellen, en de omschrijving van de omstandigheden waarin marktdeelnemers en overheden incidenten dienen te melden. Het ontbreken van duidelijke regels voor deze zaken ondermijnt de rechtszekerheid.

13. Door de richtlijn zou de regeldruk op bedrijven en overheden wel eens nodeloos kunnen toenemen. Uit alle macht moeten overlappingen in regelgeving worden voorkomen en dient ervoor te worden gezorgd dat aanvullende regels stroken met het evenredigheidsbeginsel. Dit is met name belangrijk voor organisaties voor wie al een kennisgevingsplicht geldt die grotendeels overeenkomt met wat nu wordt voorgesteld.

14. De Commissie zou een actieplan moeten publiceren waarin zij uitlegt hoe de ambitieuze doelstellingen van het beleidspakket verwezenlijkt moeten worden. Dat actieplan moet ook als richtsnoer dienen voor het beoordelen en meten van het effect van de strategie, zodat kan worden nagegaan of er sprake is van samenwerking en vooruitgang.

15. In aanvulling op de nieuwe EU-strategie moeten alle lidstaten ook eigen cyberbeveiligingsstrategieën opzetten (slechts tien lidstaten hadden zich in 2012 al van deze taak gekweten). Omwille van de samenhang is complementariteit tussen nationale strategieën en de EU-strategie van groot belang. Verder dienen EU-maatregelen bestaande structuren en goede praktijken in de lidstaten aan te vullen.

16. De maatregelen die de Commissie van plan is te nemen om de cyberbeveiligingscapaciteit van de EU te vergroten zijn een goede zaak. Zo staat er een proefproject ter bestrijding van botnets en malware op stapel, wordt de samenwerking tussen nationale CERT's, ENISA en het Europees centrum voor de bestrijding van cybercriminaliteit opgevoerd, wordt een netwerk van nationale topcentra voor de bestrijding van cybercriminaliteit opgezet, en komt er een publiek privaat platform voor NIB-oplossingen dat een stimulans moet vormen voor veilige ICT-praktijken. Ook het doel van de strategie om alle betrokken partijen ter evaluatie van de geboekte vooruitgang na twaalf maanden bijeen te brengen, verdient bijval.

17. Voor een succesvolle strategie voor cyberbeveiliging is nauwe samenwerking tussen NIB-instanties en wetshandhavingsautoriteiten een voorwaarde. Wat dit betreft is het van cruciaal belang dat incidenten waarvan wordt vermoed dat ze van ernstig criminele aard zijn, systematisch aan wetshandhavingsautoriteiten worden gemeld.

Betrokkenheid van de lokale en regionale overheden

18. De in het beleidspakket geschetste prioriteiten zijn evenwichtig en passend. Die prioriteiten — zoals bescherming van de grondrechten, persoonsgegevens en privacy, efficiënte multistakeholder governance en een gedeelde verantwoordelijkheid om beveiliging te garanderen — zijn allemaal gebieden waarop steden en regio's, als bezitters van overheidsinformatie, een sleutelrol zouden moeten spelen.

19. Naast de lidstaten zouden ook de regio's moeten worden erkend als belangrijke voortrekkers van nauwere samenwerking tussen gebruikers en producenten van ICT-innovaties op uiteenlopende gebieden van overheid en openbaar bestuur, waaronder cyberbeveiliging en gegevensbescherming.

20. Het nieuwe beleidspakket zou moeten bijdragen aan de verbetering van de preventie, opsporing en aanpak van cyberincidenten en moeten leiden tot betere informatie-uitwisseling en coördinatie tussen lidstaten en de Commissie ter voorkoming van grote cyberincidenten. Onmisbaar in dit verband zijn echte partnerschappen tussen lidstaten, EU-instellingen, lokale en regionale overheden, bedrijfsleven en maatschappelijk middenveld.

21. Om cyberbedreigingen het hoofd te bieden, moeten meer middelen worden ingezet, moet er een groter besef komen van de risico's van cybercriminaliteit en is er een efficiënte en adequate cyberbeveiliging nodig. Vanuit het oogpunt van multilevel governance vereist een krachtige cyberbeveiliging deelname van de lokale en regionale overheden, die volledig en adequaat bij het beheer van ICT-initiatieven moeten worden betrokken.

22. Aangezien inbreuken op de beveiliging een bedreiging vormen voor nutsvoorzieningen (zoals de lokale water- en energievoorziening) en de lokale en regionale overheden veel digitale informatieproducten en -diensten gebruiken en bezitten, dienen deze overheden een sleutelrol te spelen bij de aanpak van cybercriminaliteit, de verzameling van cybergerelateerde data en gegevensbeveiliging. Lokale en regionale overheden worden in steeds grotere mate verantwoordelijk voor de levering van digitale diensten aan burgers en gemeenschappen en voor het geven van trainingen in netwerk- en informatiebeveiliging op scholen. Het openbaar bestuur, waaronder dat op lokaal en regionaal niveau, is verantwoordelijk voor de waarborging van toegang en openheid, de naleving en bescherming van de grondrechten en de instandhouding van de betrouwbaarheid en interoperabiliteit van het internet.

23. Om de regelgeving te verbeteren en gelet op de bevoegdheden van de lokale en regionale overheden en de sleutelrol die zij spelen bij de planning en implementatie van maatregelen op ICT-gebied (met name m.b.t. privacy, gegevensbescherming en cyberbeveiliging), zouden deze overheden stelselmatig door de EU-instellingen en lidstaten moeten worden geraadpleegd over zowel de uitwerking als uitvoering van de maatregelen waarmee aan de Digitale Agenda concreet vorm wordt gegeven. Daarom valt te betreuren dat tijdens de voorbereiding van het richtlijnvoorstel niet specifiek actie is ondernomen om de standpunten van de lokale en regionale overheden te inventariseren. Het CvdR heeft duidelijk aangegeven bereid te zijn om de Commissie te helpen met prelegislatieve raadplegingen, zoals vermeld in zijn samenwerkingsprotocol met de Commissie. ([3])

24. In artikel 14, lid 1, van de Richtlijn, zouden maatregelen moeten worden opgenomen die bestemd zijn voor de lokale en regionale overheden. Hierbij moet bijvoorbeeld worden gedacht aan de instelling van een procedure voor risicobeoordeling en -beheer, maatregelen voor de handhaving van informatiebeveiligingsbeleid, vergroting van het besef van cyberbeveiligingskwesties en verbetering van digitale geletterdheid en vaardigheden.

25. Op subnationaal niveau zouden alle betrokkenen moeten worden aangemoedigd partnerschappen te vormen, teneinde gecoördineerd actie op het vlak van cyberbeveiliging te ondernemen en zo bij te dragen aan nationale en Europese cyberbeveiligingsmaatregelen. Doel hiervan is misdaad — financiële diefstal of diefstal van intellectuele eigendom, verstoring van de communicatie of schade aan gegevens die cruciaal zijn voor bedrijven — te bestrijden.

([3]) Protocol betreffende de samenwerking tussen de Europese Commissie en het Comité van de Regio's, ondertekend op 16 februari 2012, R/CdR 39/2012 pt 7.

Subsidiariteit en evenredigheid

26. In het algemeen lijkt te worden voldaan aan de twee voorwaarden voor naleving van het subsidiariteitsbeginsel, hetgeen vereist is voor EU-maatregelen en bijkomende maatregelen op EU-niveau. De voorgestelde maatregelen zijn noodzakelijk omdat ze transnationale aspecten betreffen die niet naar behoren door de lidstaten en/of de lokale en regionale overheden alleen kunnen worden geregeld. De voorgestelde maatregelen zullen waarschijnlijk ook duidelijke voordelen opleveren t.o.v. afzonderlijke maatregelen op nationaal, regionaal of lokaal niveau, bijvoorbeeld omdat persoonsgegevens steeds sneller over grenzen heen worden uitgewisseld (zowel binnen als tussen landen). Bovendien zullen verplichte EU-regels hier aanzienlijk bijdragen aan de totstandbrenging van gelijke randvoorwaarden voor iedereen en hiaten in de wetgeving afdichten.

27. Het CvdR is ermee ingenomen dat de Richtlijn in het algemeen voldoet aan het subsidiariteits- en het evenredigheidsbeginsel. Gelet op de grensoverschrijdende dimensie van incidenten en risico's op het gebied van netwerk- en informatiebeveiliging, kunnen de doelstellingen van de Richtlijn beter op EU-niveau worden gerealiseerd, overeenkomstig het subsidiariteitsbeginsel. Onderzoek toont aan dat de Europese burgers vertrouwen hebben in instellingen als de Commissie als het gaat over de bescherming van persoonsgegevens. ([4]) De Richtlijn voldoet in het algemeen ook aan het evenredigheidsbeginsel, omdat de Commissie ervoor zorgt dat de maatregelen niet verder gaan dan nodig om de geformuleerde doelstellingen te halen. De voorstellen echter voor één verantwoordelijke instantie en één CERT per lidstaat druisen in tegen het evenredigheidsbeginsel en sluiten niet aan op de interne bestuursstructuren van de lidstaten.

28. De rechtsgrondslag voor het beleidspakket wordt gevormd door de artikelen 26 en 114 VWEU, maar de voorgestelde maatregelen gaan verder, omdat het voorstel betrekking heeft op alle overheidsinformatiesystemen, waaronder interne informatiesystemen zoals een intranet.

Handvest van de grondrechten

29. Het CvdR juicht toe dat de Richtlijn het Handvest van de grondrechten van de EU in acht neemt. De normen, beginselen en waarden die de EU er offline op na houdt, zouden ook online moeten gelden. In informatie- en communicatietechnologieën zouden de behoeften van alle groepen in de samenleving in aanmerking moeten worden genomen, ook die van mensen die buitengesloten dreigen te worden. Alle internetgebruikers zouden minimumnormen mogen verwachten voor zeer uiteenlopende aspecten als betrouwbaarheid, beveiliging, transparantie, eenvoud, interoperabiliteit en vermindering van risico's en aansprakelijkheid. Met het oog op een adequate bescherming van de grondrechten en de rechtszekerheid en met inachtneming van het voorbehoud voor parlementaire behandeling dringt het CvdR erop aan in de Richtlijn zelf een concrete, materieelrechtelijke regeling inzake normen voor NIB op

([4]) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

te nemen. Daarin zouden in het bijzonder eisen moeten worden gesteld aan NIB op het vlak van grondrechten en gegevensbescherming en -beveiliging.

30. De inspanningen om de belangen van burgers online te beschermen en te verdedigen moeten naar behoren in evenwicht zijn met de rechten, vrijheden en beginselen die de burgers in het Handvest van de grondrechten zijn toegekend. Positief is het belang dat wordt gehecht aan de verankering van het cyberbeleid binnen de kernwaarden van de EU. Zoals het CvdR in een eerder advies ([5]) heeft opgemerkt, is het essentieel dat op elk niveau aan alle beveiligingseisen wordt voldaan om een optimaal privacyniveau en een optimale bescherming van persoonsgegevens te garanderen en ongeoorloofde informatievergaring over persoonlijke aangelegenheden en het aanmaken van profielen te voorkomen.

31. Ondanks dat particuliere exploitanten steeds verantwoordelijker worden voor kritieke infrastructuur en voor online dienstverlening en moet worden erkend dat het bedrijfsleven een cruciale rol speelt, dient uiteindelijk bij de overheid de verantwoordelijkheid te liggen voor de bescherming van de vrijheid en de waarborging van de veiligheid van haar burgers online.

Vereenvoudiging

32. Als overal in Europa het beginsel wordt toegepast dat persoons- en objectgegevens maar één keer hoeven te worden opgegeven, en het dus niet meer nodig is ze telkens opnieuw in te vullen, zou de onnodige bureaucratische rompslomp voor de burgers aanzienlijk worden verminderd en worden bespaard op de kosten van de overheid. Daarbij dient er wel op te worden gelet dat de wetgeving inzake gegevensbescherming wordt nageleefd.

Opleiding

33. Voor een doeltreffende cyberdefensie moet personeel worden bijgeschoold en opgeleid, ook binnen lokale en regionale overheden. Uitgebreide opleiding zou moeten worden verstrekt aan alle personeelsleden, in het bijzonder aan gespecialiseerde technici, personeelsleden die rechtstreeks worden geconfronteerd met beveiligingsprocedures waarin verschillende methodes worden gebruikt en personeelsleden die in het algemeen of indirect betrokken zijn bij innovatie en modernisering m.b.t. kwesties op het vlak van vertrouwen en beveiliging. Permanente opleiding is belangrijk voor het welslagen van e-overheidsdiensten op lokaal niveau, terwijl de lokale en regionale overheden ook een steeds belangrijkere rol spelen in het verstrekken van informatie en richtsnoeren die burgers in staat stellen systemen op een behoorlijke manier te gebruiken en cyberbedreigingen te herkennen ([6]).

34. Een uiterst belangrijke succesfactor is het "engagement van de leiding". Daarom moeten mensen met staffuncties en leidende functies een gerichte opleiding krijgen, zodat zij inzicht verwerven en goed in staat zijn om in hun organisatie een beveiligingscultuur op te bouwen.

35. Het CvdR neemt nota van de verbetering van onderwijs en opleiding via de inrichting van NIB-scholingsprogramma's en de organisatie van een kampioenschap cyberbeveiliging in 2014. Daarbij moet rekening worden gehouden met bestaande evenementen in de lidstaten en moet de uitwisseling van goede praktijken worden aangemoedigd. Positief is de in de strategie doorklinkende ambitie om NIB-lessen op scholen in te voeren. Omdat onderwijs echter een bevoegdheid van de lidstaten is, zullen er aanzienlijke middelen en een belangrijke mate van planning nodig zijn om deze ambitie in 2014 te verwezenlijken.

Steun voor ondernemingen, innovatie en technische oplossingen

36. Voor de bescherming van de persoonlijke levenssfeer zijn een aantal factoren van belang, onder meer de manier waarop overheidsinstanties zijn gestructureerd (de meeste hebben een lokaal karakter), de mate van convergentie van EU-wetgeving, de bevordering van een innovatiecultuur onder ambtenaren (bijvoorbeeld door een gemeenschappelijke gedragscode te gebruiken) en onder burgers (door hun digitale consumentenrechten vast te leggen en daaraan bekendheid te geven), evenals het beheer van op ICT gebaseerde toepassingen.

37. Er zouden nog meer initiatieven moeten worden ontplooid, enerzijds ter stimulering van de ontwikkeling en toepassing van technische oplossingen waarmee illegale inhoud en schadelijk online gedrag kunnen worden bestreden, en anderzijds ter bevordering van de samenwerking en uitwisseling van beste praktijken tussen tal van actoren op lokaal, regionaal, Europees en internationaal niveau. Uiterst belangrijk zijn in dit opzicht de helplijnen voor kinderen, ouders en verzorgers, de noodnummers voor het melden van misbruik en de software om misbruik van inhoud beter op te sporen en problemen eenvoudig en snel te melden.

38. Het CvdR raadt aan alles op alles te zetten om te komen tot een verhoging van het momenteel beperkte percentage (26 % in januari 2012) van EU-bedrijven die over een formeel ICT-beveiligingsbeleid beschikken ([7]). Ongeacht hun omvang moeten ondernemingen worden aangemoedigd om te investeren in cyberbeveiliging, hetgeen naar potentiële klanten toe ook een marketinginstrument kan zijn en waarmee de catastrofale gevolgen van cybercriminaliteit kunnen worden afgezwakt. Ondernemingen moeten een bedrijfsgebaseerde en technologisch ondersteunde aanpak van cyberbeveiliging overwegen, waarin de bescherming van hun belangrijkste bedrijfsactiva en processen prioriteit krijgt.

([5]) CdR 104/2010 fin.

([6]) http://www.enisa.europa.eu/publications/archive/scandinavian-approaches-survey

([7]) http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises

Economisch potentieel van ICT

39. Gelet op het enorme economische potentieel van ICT voor de Europese economie (momenteel bijna 6 % van het bbp van de EU ([8])) zijn er nu concrete stappen vereist om het hoofd te bieden aan het toenemende fenomeen van cybercriminaliteit en zowel bij burgers als bedrijven het vertrouwen in de veiligheid van het internet te herstellen. Zo dient er een vermindering te worden bewerkstelligd van het aantal internetgebruikers die in de EU bezorgd zijn over, bijvoorbeeld, de veiligheid van online betalingen. ([9])

40. Op het vlak van de strijd tegen cybercriminaliteit zijn er dringend inspanningen nodig op lokaal/regionaal, nationaal en EU-niveau, zodat er een dalende tendens ontstaat in de reusachtige bedragen die door cybercriminaliteit verloren gaan en het vertrouwen van de consument groeit.

41. Het zou goed zijn als in de strategie meer details worden opgenomen over manieren om cloud computing, dat een enorm economisch potentieel biedt, te beschermen en te ontwikkelen. De snelle groei van het gebruik van elektronische mobiele apparaten lijkt niet te vertragen. Volgens Gartner zal tegen 2016 op zijn minst 50 % van de zakelijke e-mailgebruikers afhankelijk zijn van een mailprogramma op een mobiel apparaat ([10]). Er dient te worden onderzocht welke nieuwe kansen en problemen elektronische mobiele apparaten en cloud computing met zich meebrengen. Bovendien vereist cloud computing een aangepaste structuur om optimale beveiligingsniveaus te bereiken ([11]). Het CvdR heeft zelfs zijn bezorgdheid uitgesproken over het feit dat de Commissie in haar recente mededeling over cloud computing te weinig aandacht besteedt aan de dwarsverbanden tussen de voorgestelde strategie en andere zaken, zoals beveiligde gegevensverwerking, auteursrechten en toegankelijkheid en portabiliteit van gegevens. ([12])

Internationale samenwerking

42. Aangezien cybercriminaliteit een wereldwijde, overal vertakte en grensoverschrijdende bedreiging is, worden ook internationale samenwerking en EU-overschrijdende dialoog aangemoedigd, teneinde te komen tot een aanpak waarin cyberbeveiliging echt mondiaal wordt gecoördineerd. Op dit vlak zouden alle lidstaten moeten worden aangemoedigd om het internationale verdrag inzake cybercriminaliteit (verdrag van Boedapest) ([13]) te eerbiedigen. Het is ook belangrijk dat samenwerking blijft bestaan op bilateraal vlak, met name met de Verenigde Staten, alsook in de multilaterale fora van verschillende internationale organisaties.

Verband met de financieringsprogramma's en het begrotingskader van de EU

43. Van belang is de samenhang te verbeteren met bestaande en toekomstige financieringsinstrumenten, zoals Horizon 2020, het Europese samenwerkingskader en het fonds voor interne veiligheid, teneinde een meer gecoördineerde aanpak inzake cybergerelateerde investeringen mogelijk te maken.

44. Het CvdR vraagt zich af of 1,25 miljoen euro zal volstaan om een stevige en degelijke NIB-infrastructuur tot stand te brengen. Te betreuren valt dat er in het akkoord van de Raad (8 februari) over het meerjarig financieel kader voor 2014-2020 slechts een beperkt bedrag wordt uitgetrokken voor de financieringsfaciliteit voor Europese verbindingen. Er is een adequaat, uitgebreid budget nodig om te kunnen voorzien in voldoende ondersteuning voor sleutelinfrastructuur op ICT-gebied waarmee meer samenhang wordt gebracht in de NIB-capaciteiten van de lidstaten, zodat het eenvoudiger wordt om binnen de EU samen te werken.

II. AANBEVELINGEN VOOR WIJZIGINGEN

Wijzigingsvoorstel 1

Preambule (4)

Door de Commissie voorgestelde tekst	Wijzigingsvoorstel van het CvdR
Op het niveau van de Unie moet een samenwerkingsmechanisme worden opgezet dat informatie-uitwisseling en gecoördineerde opsporing en reactie met betrekking tot netwerk- en informatiebeveiliging ("NIB") mogelijk maakt. Opdat dat mechanisme doeltreffend en inclusief zou zijn, is het essentieel dat alle lidstaten over minimumcapaciteit en een strategie beschikken om op hun grondgebied een hoog niveau van NIB te waarborgen. Om een cultuur van risicobeheer te bevorderen en ervoor te zorgen dat de ernstigste incidenten worden gemeld, moeten ook voor overheden en exploitanten van kritieke informatie-infrastructuur minimumeisen inzake beveiliging gelden.	Op het niveau van de Unie moet een samenwerkingsmechanisme worden opgezet dat informatie-uitwisseling en gecoördineerde opsporing en reactie met betrekking tot netwerk- en informatiebeveiliging ("NIB") mogelijk maakt. Opdat dat mechanisme doeltreffend en inclusief zou zijn, is het essentieel dat alle lidstaten over minimumcapaciteit en een strategie beschikken om op hun grondgebied een hoog niveau van NIB te waarborgen. Om een cultuur van risicobeheer te bevorderen en ervoor te zorgen dat de ernstigste incidenten worden gemeld, moeten ook voor overheden, **inclusief lokale en regionale overheden**, en exploitanten van kritieke informatie-infrastructuur minimumeisen inzake beveiliging gelden.

([8]) http://europa.eu/rapid/press-release_MEMO-13-71_en.htm
([9]) http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf
([10]) http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf
([11]) http://www.mcafee.com/hk/resources/reports/rp-sda-cyber-security.pdf
([12]) CdR 1673/2012.
([13]) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG%20

Wijzigingsvoorstel 2

Preambule (9)

Door de Commissie voorgestelde tekst	Wijzigingsvoorstel van het CvdR
Om een hoog gemeenschappelijk beveiligingsniveau van netwerk- en informatiesystemen te bereiken en te handhaven, moet elke lidstaat een nationale NIB-strategie hebben waarin de te verwezenlijken strategische doelstellingen en concrete beleidsmaatregelen zijn vastgesteld. Op nationaal niveau moeten aan essentiële eisen beantwoordende NIB-samenwerkingsplannen worden ontwikkeld om een niveau van reactiecapaciteit te bereiken dat in geval van incidenten doeltreffende en efficiënte samenwerking op nationaal niveau en op het niveau van de Unie mogelijk maakt.	Om een hoog gemeenschappelijk beveiligingsniveau van netwerk- en informatiesystemen te bereiken en te handhaven, moet elke lidstaat een nationale NIB-strategie hebben waarin de te verwezenlijken strategische doelstellingen en concrete beleidsmaatregelen zijn vastgesteld. Op nationaal niveau moeten, **met een volwaardige inbreng van lokale en regionale overheden**, aan essentiële eisen beantwoordende NIB-samenwerkingsplannen worden ontwikkeld om een niveau van reactiecapaciteit te bereiken dat in geval van incidenten doeltreffende en efficiënte samenwerking op nationaal niveau en op het niveau van de Unie mogelijk maakt.

Wijzigingsvoorstel 3

Preambule (35)

Door de Commissie voorgestelde tekst	Wijzigingsvoorstel van het CvdR
Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadpleging overgaat, onder meer op deskundigenniveau. De Commissie moet er bij de voorbereiding en opstelling van de gedelegeerde handelingen voor zorgen dat de desbetreffende documenten tijdig en op gepaste wijze gelijktijdig worden toegezonden aan het Europees Parlement en aan de Raad.	Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadpleging overgaat, onder meer op deskundigenniveau. **Ter aanvulling of wijziging van bepaalde niet-essentiële onderdelen van het basisbesluit moet** ~~D~~de Commissie ~~moet~~ er bij de voorbereiding en opstelling van de gedelegeerde handelingen voor zorgen dat de desbetreffende documenten tijdig en op gepaste wijze gelijktijdig worden toegezonden aan het Europees Parlement en aan de Raad.

Wijzigingsvoorstel 4

Hoofdstuk 4

Artikel 14, lid 1

Door de Commissie voorgestelde tekst	Wijzigingsvoorstel van het CvdR
Beveiligingseisen en melding van incidenten 1. De lidstaten zorgen ervoor dat overheden en marktdeelnemers passende technische en organisatorische maatregelen nemen ter beheersing van de risico's voor de beveiliging van de netwerken en informatiesystemen die zij controleren en bij hun activiteiten gebruiken. Deze maatregelen zorgen, rekening houdend met de meest recente technische mogelijkheden, voor een beveiligingsniveau dat is afgestemd op de risico's die zich voordoen. Overheden en marktdeelnemers nemen met name maatregelen om de impact te voorkomen en te minimaliseren van incidenten met betrekking tot hun netwerk- en informatiesysteem op de door hen verleende kerndiensten en aldus te zorgen voor de continuïteit van de op die netwerken en informatiesystemen gebaseerde diensten.	Beveiligingseisen en melding van incidenten 1. De lidstaten zorgen ervoor dat overheden en marktdeelnemers passende technische en organisatorische maatregelen nemen ter beheersing van de risico's voor de beveiliging van de netwerken en informatiesystemen die zij controleren en bij hun activiteiten gebruiken. **Hierbij valt op lokaal en regionaal niveau te denken aan de instelling van een procedure voor risicobeoordeling en -beheer, maatregelen voor de handhaving van informatiebeveiligingsbeleid, vergroting van het besef van cyberbeveiligingskwesties en verbetering van digitale geletterdheid en vaardigheden.** Deze maatregelen zorgen, rekening houdend met de meest recente technische mogelijkheden, voor een beveiligingsniveau dat is afgestemd op de risico's die zich voordoen. Overheden en marktdeelnemers nemen met name maatregelen om de impact te voorkomen en te minimaliseren van incidenten met betrekking tot hun netwerk- en informatiesysteem op de door hen verleende kerndiensten en aldus te zorgen voor de continuïteit van de op die netwerken en informatiesystemen gebaseerde diensten.

Motivering

De rol van lokale en regionale overheden in de bestrijding van cybercriminaliteit is cruciaal en moet ten volle worden onderkend.

Wijzigingsvoorstel 5

Hoofdstuk 4

Artikel 16

Door de Commissie voorgestelde tekst	Wijzigingsvoorstel van het CvdR
Normalisatie	Normalisatie
1. Met het oog op de geharmoniseerde uitvoering van artikel 14, lid 1, moedigen de lidstaten het gebruik van normen en/of specificaties voor netwerk- en informatiebeveiliging aan.	1. Met het oog op de geharmoniseerde uitvoering van artikel 14, lid 1, moedigen de lidstaten het gebruik van **geharmoniseerde** normen en/of specificaties voor netwerk- en informatiebeveiliging aan.
2. De Commissie stelt, door middel van uitvoeringshandelingen, een lijst op van de in lid 1 bedoelde normen. De lijst wordt bekendgemaakt in het Publicatieblad van de Europese Unie.	2. De Commissie stelt, door middel van uitvoeringshandelingen, een lijst op van de in lid 1 bedoelde normen. De lijst wordt bekendgemaakt in het Publicatieblad van de Europese Unie.

Motivering

De Commissie geeft toe dat de toepassing van uiteenlopende normen door verschillende lidstaten een groot probleem is. Om te kunnen zorgen voor een gemeenschappelijk niveau van NIB is harmonisatie van normen dan ook van cruciaal belang.

Brussel, 3 juli 2013

De voorzitter
van het Comité van de Regio's
Ramón Luis VALCÁRCEL SISO