RAAD VAN DE EUROPESE UNIE

Brussel, 22 juli 2013
(OR. en)

12109/13

POLGEN 138
JAI 612
TELECOM 194
PROCIV 88
CSC 69
CIS 14
RELEX 633
JAIEX 55
RECH 338
COMPET 554
IND 204
COTER 85
ENFOPOL 232
DROIPEN 87
CYBER 15
COPS 276
POLMIL 39
COSI 93
DATAPROTECT 94

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
aan:	de delegaties
nr. vorig doc.:	11357/13
Betreft:	Conclusies van de Raad over de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid over de Strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberspace

Voor de delegaties gaan hierbij de conclusies van de Raad over de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid over de Strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberruimte, waarover de Raad Algemene Zaken op 25 juni 2013 overeenstemming heeft bereikt.

BIJLAGE

Conclusies van de Raad over de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid over de Strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberspace

De Raad van de Europese Unie,

1. ERKENNENDE dat de cyberspace, die intrinsiek transnationaal is, bestaat uit onderling afhankelijke netwerken en informatie-infrastructuren, waaronder het internet en telecommunicatienetwerken, dat het vandaag en in de toekomst een van de belangrijkste middelen is en zal zijn om te voorzien in de behoeften van de burgers en de lidstaten van de EU en hun belangen en rechten te vrijwaren, en dat de cyberspace een onontbeerlijke factor is voor economische groei in de EU;

2. DE AANDACHT VESTIGEND OP de respectieve rollen en rechten op cybergebied van de individuele burgers, de particuliere sector en het maatschappelijk middenveld, alsmede op de belangrijke rol van de EU bij het ondersteunen en handhaven van een open, beveiligde en veerkrachtige cyberspace die is gebaseerd op de kernwaarden van de EU zoals democratie, mensenrechten en rechtsstatelijkheid ten behoeve van onze economieën, overheidsdiensten en samenleving en van de goede werking van de interne markt;

3. ERKENNENDE dat verbeteringen nodig zijn wat betreft de vertrouwelijkheid, beschikbaarheid en integriteit van netwerken en infrastructuur en van de informatie die deze bevatten;

4. ZICH ERVAN BEWUST dat waarborgen en maatregelen nodig zijn met het oog op het voorkómen van dreigingen die betrekking hebben op of schade kunnen aanrichten aan onderling afhankelijke netwerken en informatie-infrastructuren, alsmede op het beschermen van de cyberspace op civiel en militair gebied;

5. BEVESTIGEND dat de EU op het standpunt staat dat in de cyberspace dezelfde normen, beginselen en waarden moeten gelden als die welke de EU in de concrete wereld handhaaft, met name het Handvest van de grondrechten van de Europese Unie;

6. ZICH ERVAN BEWUST dat het internationaal recht, onder meer internationale verdragen zoals het Verdrag van de Raad van Europa inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (het Verdrag van Boedapest) en relevante verdragen inzake internationaal humanitair recht en mensenrechten, zoals het Internationaal Verdrag inzake burgerrechten en politieke rechten, het Internationaal Verdrag inzake economische, sociale en culturele rechten, een wetgevingskader vormen dat toepasselijk is in de cyberspace; dat derhalve inspanningen dienen te worden geleverd om ervoor te zorgen dat deze instrumenten in cyberspace worden gehandhaafd; dat de EU bijgevolg niet om nieuwe internationale rechtsinstrumenten inzake cyberkwesties vraagt;

7. BEVESTIGEND dat een geïntegreerde, multidisciplinaire en horizontale aanpak van cyberbeveiliging nodig is en dat de maatregelen een reeks kwesties met velerlei aspecten in verband met cyberspace moeten bestrijken;

8. HERINNEREND AAN de talrijke uniale en internationale initiatieven op het gebied van cyberbeveiliging, onder meer die welke in de bijlage bij dit document worden opgesomd;

9. HERINNEREND AAN de bepalingen van artikel 222 van het Verdrag betreffende de werking van de Europese Unie en rekening houdend met de lopende besprekingen over de toepassing ervan;

10. ZICH ERVAN BEWUST dat de inspanningen met betrekking tot het vergroten van de cyberbeveiliging en de bestrijding van de cybercriminaliteit niet uitsluitend binnen de Europese Unie, maar ook in derde landen moeten worden geleverd, onder meer in de landen van waaruit cybercriminele organisaties opereren;

VERKLAART HET VOLGENDE:

11. IS INGENOMEN met de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie over een strategie inzake cyberbeveiliging van de Europese Unie;

12. IS VAN OORDEEL dat de verdere ontwikkeling en toepassing van een alomvattende aanpak van het EU-cyberspacebeleid essentieel en dringend noodzakelijk is; dat beleid moet:

    - de uitoefening van de mensenrechten beschermen en bevorderen en gebaseerd zijn op de fundamentele waarden van de EU wat betreft democratie, mensenrechten en de rechtsstaat;

    - de welvaart in Europa en de sociale en economische baten van de cyberspace, met inbegrip van het internet, bevorderen;

- een effectieve en verbeterde cyberbeveiliging in de gehele EU en daarbuiten bevorderen;

- de inspanningen met het oog op het dichten van de mondiale digitale kloof stimuleren en de internationale samenwerking op het gebied van cyberbeveiliging ondersteunen;

- een goede afspiegeling zijn van de rol en de rechten van individuele burgers, de particuliere sector en het maatschappelijk middenveld wat betreft cyberkwesties; dit omvat tevens een versterking van de publiek-private samenwerking en informatie-uitwisseling,

EN

13. VERZOEKT de lidstaten, de Commissie en de hoge vertegenwoordiger om, onder eerbiediging van hun respectieve bevoegdheden en het subsidiariteitsbeginsel, samen te werken om de strategische doelstellingen te verwezenlijken die in deze conclusies worden uiteengezet;

Waarden

14. ONDERSTREEPT dat individuele mensenrechten, waaronder de vrijheid van meningsuiting en het recht op een persoonlijke levenssfeer, te allen tijde moeten worden geëerbiedigd bij de ontwikkeling van beleid en praktijken inzake cyberspaceaangelegenheden en in de wetgeving, en neemt nota van de lopende onderhandelingen met het oog op een akkoord over een EU-wetgevingskader voor de bescherming van persoonsgegevens dat doeltreffend kan functioneren in cyberspace;

15. ERKENT dat de waarden en belangen die binnen de Unie worden gepropageerd en beschermd, ook moeten worden uitgedragen in het extern beleid van de Unie in verband met cyberaangelegenheden;

16. ROEPT de EU en de lidstaten ERTOE OP:

- hun uniform en krachtig standpunt wat betreft de universele toepasselijkheid van de mensenrechten en de fundamentele vrijheden, inclusief de vrijheid van mening, meningsuiting, informatie, vergadering en vereniging in cyberspace, te verdedígen;

- vast te stellen hoe de bestaande verplichtingen in de cyberspace kunnen worden gehandhaafd ;

17. VERZOEKT de EU en haar lidstaten de digitale geletterdheid te bevorderen en gebruikers te helpen om zich meer bewust te worden van hun individuele verantwoordelijkheid wanneer zij persoonsgegevens op het internet plaatsen;

18. ONDERSTREEPT de belangrijke rol van de EU bij het handhaven van het multistakeholder-model voor het beheer van het internet;

19. VERZOEKT de lidstaten al het redelijkerwijs mogelijke te doen om ervoor te zorgen dat alle EU-burgers toegang tot internet hebben en de voordelen ervan kunnen genieten;

Welvaart

20. VERZOEKT de Commissie specifieke inspanningen te doen ter bevordering van de digitale eengemaakte markt en werk te maken van gerelateerde aangelegenheden in het kader van de Unie en van internationale gremia (bijvoorbeeld de Wereldhandelsorganisatie (WTO), en de onderhandelingen over de Informatietechnologieovereenkomst (ITA)), alsmede te zorgen voor markttoegang in deze sectoren bij de onderhandelingen over vrijhandelsovereenkomsten met derde landen,

21. ONDERSTREEPT dat het belangrijk is dat wetgeving in deze sector technologieneutraal is, en spoort ertoe aan een zo groot mogelijke netneutraliteit na te streven, zodat de mededinging niet wordt belemmerd doordat grensoverschrijdende onlinehandel en nieuwe bedrijfsmodellen worden gediscrimineerd;

22. SPREEKT ZIJN TEVREDENHEID UIT over de erkenning van de noodzaak van investeringen in onderzoek en ontwikkeling op het gebied van cyberspace, dat een belangrijk gebied is en kan zorgen voor banen van hoge kwaliteit en economische groei;

23. BEKLEMTOONT de volgende elementen:

- met betrekking tot de versterking van de cyberbeveiliging is het van cruciaal belang dat de EU beschikt over een vitale sector voor informatie- en communicatietechnologie (ICT) en ICT-beveiliging, en de Raad VERZOEKT de lidstaten en de Commissie om na te gaan welke stappen kunnen worden gedaan met het oog op de ontwikkeling van die sector en om daarover verslag uit te brengen;

- de wetgeving ter ondersteuning van de cyberbeveiliging moet innovatie en groei bevorderen, en toegespitst zijn op de bescherming van de infrastructuur en de vitale functies die volgens de lidstaten kritiek zijn;

- de digitale economie is een belangrijke motor van groei, innovatie en werkgelegenheid, en cyberbeveiliging is cruciaal voor de bescherming van de digitale economie;

- de bescherming van de kritieke informatie-infrastructuur is op nationaal niveau belangrijk;

Cyberspace veerkrachtig maken

24. IS INGENOMEN met de doelstellingen van het Commissievoorstel voor een richtlijn, waarin maatregelen worden voorgesteld ter versterking van:

    - de netwerk- en informatiebeveiliging in de gehele EU;

    - de paraatheid en capaciteit inzake cyberbeveiliging op nationaal niveau;

    - de samenwerking tussen de lidstaten en in de gehele EU, en ter stimulering van een cultuur van risicobeheer in de publieke en particuliere sector;

25. ROEPT alle EU-instellingen, -agentschappen en organen ERTOE OP om in samenwerking met de lidstaten de nodige stappen te doen teneinde hun eigen cyberbeveiliging te garanderen, door in samenwerking met het Enisa overeenkomstig de passende beveiligingsnormen hun beveiliging te versterken, teneinde aan de beste praktijken te voldoen, in overeenstemming met Verordening (EU) nr. 526/2013[1];

26. MEMOREERT dat een computercrisisteam (CERT - Computer Emergency Response Team) voor de EU-instellingen, -agentschappen en -organen is ingesteld na een proefperiode van een jaar en dat de rol en doeltreffendheid ervan gunstig zijn beoordeeld;

27. ONDERSTREEPT dat het Enisa van het allergrootste belang is voor het ondersteunen van de inspanningen van de lidstaten en de Unie met het oog op het bereiken van een hoog niveau van netwerk- en informatiebeveiliging, in het bijzonder door het ondersteunen van de capaciteitsopbouw van de lidstaten en het ontwikkelen van een solide nationale capaciteit om de cyberspace veerkrachtig te maken, het ondersteunen van Europese oefeningen met betrekking tot cyberincidenten en van de inspanningen van de Unie inzake O&O en normalisering, en VERZOEKT het Enisa om met andere instellingen, agentschappen en organen van de Unie samen te werken in aangelegenheden inzake netwerk- en informatiebeveiliging, overeenkomstig Verordening (EU) nr. 526/2013;

---

[1] PB L 165 van 18.6.2013

28. BEKLEMTOONT dat moet worden gezorgd voor veerkrachtiger kritieke infrastructuren in de gehele EU en voor intensivering van de nauwe samenwerking en coördinatie tussen de betrokken actoren, met name civiele en militaire EU-actoren en de publieke en de particuliere sector, wat betreft de reactie op incidenten en problemen inzake cyberbeveiliging, door middel van initiatieven zoals de ontwikkeling van gemeenschappelijke normen, bewustmaking, opleiding en onderwijs en de lopende evaluatie en tests (of ontwikkeling) van mechanismen voor vroegtijdige waarschuwing en reactie. Tevens moet er nauwere samenwerking en coördinatie bij de respons op cyberincidenten door defensieactoren, de rechtshandhaving, de particuliere sector en de cyberbeveiligingsautoriteiten tot stand worden gebracht om een doeltreffend antwoord te vinden op cyberuitdagingen, inclusief incidentbeheer;

29. VERZOEKT de lidstaten om:

- maatregelen te nemen teneinde een doeltreffend nationaal niveau van cyberbeveiliging te bereiken, door deugdelijke beleidsvormen, organisationele en operationele capaciteiten te ontwikkelen en toe te passen met het oog op de bescherming van informatiesystemen in de cyberspace, in het bijzonder de systemen die als kritiek worden beschouwd;

- contacten te leggen met het bedrijfsleven en de academische wereld met het oog op het bevorderen van vertrouwen als cruciaal onderdeel van de nationale cyberbeveiliging, bijvoorbeeld door het opzetten van publiek-private partnerschappen;

- ondersteuning te bieden voor bewustmakingscampagnes wat betreft de aard van de dreigingen en de grondbeginselen van goede digitale praktijken, op alle niveaus;

- de eigenaars en aanbieders van ICT-systemen steun te verlenen bij de bescherming van hun eigen systemen en de vitale diensten die zij verlenen;

- pan-Europese samenwerking inzake cyberbeveiliging te bevorderen, in het bijzonder door de pan-Europese oefeningen inzake cyberbeveiliging uit te breiden;

- te zorgen voor doeltreffende samenwerking en coördinatie tussen lidstaten op EU-niveau, met als doel een gemeenschappelijke dreigingsevaluatie;

- de samenwerking tussen gebruikers uit de lidstaten en de EU te versterken en uit te breiden, voortbouwend op de bestaande structuren;

- rekening te houden met cyberbeveiligingsvraagstukken in het licht van de lopende besprekingen met betrekking tot de solidariteitsclausule;

Cybercriminaliteit

30. GEEFT UITDRUKKING AAN ZIJN WAARDERING VOOR de door de Raad JBZ op 6-7 juni 2013 aangenomen conclusies inzake de vaststelling van de prioriteiten van de Unie ter bestrijding van zware en georganiseerde criminaliteit voor de periode 2014-2017, waarin de bestrijding van cybercriminaliteit als een prioriteit wordt aangemerkt;

31. ONDERSTREEPT dat cybercriminaliteit in de dreigingsevaluatie van zware en georganiseerde criminaliteit (SOCTA) van Europol voor 2013 wordt aangemerkt als een misdaadterrein dat uitgroeit tot een steeds grotere bedreiging voor de EU, in de vorm van grootschalige inbreuken in verband met informatiegegevens, onlinefraude en seksuele uitbuiting van kinderen, terwijl de op geldgewin gerichte cybercriminaliteit voorts een faciliterende factor is voor andere criminele activiteiten,

32. HEEFT WOORDEN VAN LOF voor de oprichting bij Europol van het Europese centrum inzake cybercriminaliteit (EC3) en VERZOEKT de lidstaten om EC3 in het kader van het mandaat ervan te gebruiken als middel om de samenwerking tussen nationale agentschappen te versterken,

33. VERZOEKT Europol en Eurojust om hun samenwerking met alle relevante belanghebbenden, waaronder de EU-agentschappen, Interpol, de CERT-gemeenschap en de particuliere sector, bij de bestrijding van cybercriminaliteit verder te versterken, onder meer door meer aandacht te besteden aan synergieën en complementaire aspecten in overeenstemming met hun respectieve mandaten en bevoegdheden;

34. ZIET UIT naar de spoedige bekrachtiging door alle lidstaten van het Verdrag van Boedapest inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken;

35. ROEPT de Commissie, Europol, Cepol en het Enisa ERTOE OP om steun te verlenen aan de opleiding en het verbeteren van vaardigheden ten behoeve van lidstaten waarvan de overheden en wetshandhavingsinstanties cybervermogens ter bestrijding van cyber-criminaliteit moeten opbouwen;

36. VERZOEKT de Commissie om:

- de lidstaten op hun verzoek te helpen bij het in kaart brengen van lacunes en het versterken van hun vermogen om cybercriminaliteit te onderzoeken en te bestrijden;

- het fonds voor interne veiligheid (ISF) binnen de grenzen van zijn begroting (en met inachtneming van de andere prioriteiten ervan) te gebruiken ter ondersteuning van autoriteiten die betrokken zijn bij de bestrijding van cybercriminaliteit;

- het stabiliteitsinstrument (IfS) te gebruiken voor de ontwikkeling van de bestrijding van cybercriminaliteit en van initiatieven inzake capaciteitsopbouw, onder meer ten behoeve van politiële en justitiële samenwerking in derde landen van waaruit cybercriminele organisaties opereren;

- de coördinatie van capaciteitsopbouwprogramma's te faciliteren teneinde doublures te voorkomen en voor synergieën te zorgen;

- informatie te verstrekken wat betreft de vorderingen van de wereldwijde alliantie tegen seksuele uitbuiting van kinderen via het internet;

- onverminderd de monitoring te faciliteren van het EU-beleidskader in verband met de bestrijding van cybercriminaliteit, in het bijzonder in het licht van de door Europol (EC3) verstrekte resultaten en strategische informatie;

- de samenwerking tussen gemeenschappen te faciliteren, in het bijzonder door steun te verlenen aan Europol (EC3);

<u>Gemeenschappelijk veiligheids- en defensiebeleid (GVDB)</u>

37. ATTENDEERT in verband met het GVDB op:

- de dringende noodzaak om de GVDB-gerelateerde cyberdefensieaspecten van de strategie voor de ontwikkeling van een cyberdefensiekader, waar passend, tot uitvoering te brengen en er verder aan te werken, en in dat verband concrete stappen te bepalen, mede met het oog op het voor december 2013 geplande debat van de Europese Raad over veiligheid en defensie. In de EDEO moet er één contactpunt komen voor het aansturen van deze werkzaamheden;

- de noodzaak van versterking van de cyberdefensievermogens van de lidstaten, mede door het uitwerken van gemeenschappelijke normen, van bewustmaking door middel van opleiding en onderwijs in cyberbeveiliging, met behulp van de Europese Veiligheids- en defensieacademie en door verdere verbetering van de opleidings- en oefengelegenheden voor de lidstaten;

- de benutting van de beschikbare mechanismen voor "bundelen en delen" en de benutting van synergieën met bredere beleidsontwikkelingen van de EU teneinde op een zo doelmatig mogelijke wijze de vereiste cyberdefensievermogens in de lidstaten op te bouwen;

- de noodzaak van onderzoek en ontwikkeling. Er wordt prioriteit geschonken aan het aanmoedigen van de lidstaten om beveiligde, veerkrachtige technologieën voor cyberdefensie te ontwikkelen, waarbij een grote inbreng is weggelegd voor de particuliere sector en de universiteiten, en aan de zorg dat er in de EDA-onderzoeks-projecten meer nadruk op cyberbeveiligingsaspecten komt te liggen op basis van samenwerking en als een goed voorbeeld van een tussen de EDA en de Commissie binnen het Europees samenwerkingskader te coördineren vermogen voor tweeërlei gebruik;

- het feit dat de mechanismen voor vroegtijdige waarschuwing en respons geëvalueerd en getest moeten worden in het licht van nieuwe cyberdreigingen, en wel door middel van een dialoog tussen de EDEO, het Enisa, het EC3, de EDA, de Commissie en de lidstaten met het oog op synergieën en dwarsverbanden met de defensiegemeenschap;

- de noodzaak om de samenwerking tussen de EU en de NAVO inzake cyberdefensie voort te zetten en te versterken, en daarbij prioriteiten te bepalen voor een verdere EU-NAVO- cyberdefensiesamenwerking binnen het bestaande kader, inclusief wederzijdse deelname aan cyberdefensieoefeningen en -opleidingen;

- het feit dat cyberdefensieaspecten moeten worden opgenomen in een ruimer cyberspacebeleid;

Industrie/technologie

38. VANUIT HET INZICHT dat Europa, om een toereikende mate van diversiteit en vertrouwen binnen zijn netwerken en ICT-systemen te bewerkstelligen, zijn industrieel en technologisch potentieel verder zal moeten ontwikkelen, BEGROET de Raad MET INSTEMMING de in de EU-cyberbeveiligingsstrategie voor Europa geformuleerde vraag om steun te verlenen aan een krachtig industriebeleid, met het oogmerk om door middel van O&O betrouwbare Europese ICT- en cyberbeveiligingsindustrieën te bevorderen en de interne markt te stimuleren;

39. VERZOEKT de lidstaten, de Commissie en het Enisa zich nog meer in te zetten voor onderzoek en ontwikkeling op het gebied van ICT en cyberbeveiliging, alsmede voor de beschikbaarheid van goed voorbereide beroepskrachten op het gebied van cyberbeveiliging, wat essentieel is om het concurrentievermogen van de Europese industrieën op het gebied van informatie- en communicatietechnologie (ICT), dienstverlening en beveiliging te stimuleren, evenals hun vermogen om betrouwbare en veilige oplossingen te ontwikkelen; om die reden MOEDIGT de Raad de Commissie AAN om het Horizon 2020-kaderprogramma voor onderzoek en innovatie als hefboom in te zetten,

40. BEKLEMTOONT dat de ontwikkeling van publiek-private partnerschappen een nuttig instrument zal zijn om de vermogens inzake cyberbeveiliging op te voeren; en VERZOEKT de Commissie derhalve om binnen H2020 synergieën tussen exploitanten van kritieke infrastructuren, ICT en beveiligingsonderzoek voor cyberbeveiliging en vraagstukken in verband met cybercriminaliteit, alsook met het Uniebeleid voor interne en externe beveiliging, te bevorderen;

41. VERZOEKT de lidstaten en de Commissie specifieke maatregelen te treffen ter ondersteuning van de cyberbeveiliging in het midden- en kleinbedrijf, dat bij uitstek kwetsbaar is voor cyberaanvallen, en moedigt de lidstaten aan om veilige en veerkrachtige cyberbeveiligingstechnologieën te ontwikkelen, in samenwerking met en met inbreng van de particuliere sector en de universiteiten;

42. VERZOEKT de Commissie om bestaande cyberbeveiligingsnormen in overweging te nemen en BENADRUKT dat samen met de lidstaten, de sector en andere relevante belanghebbenden verder moet worden gewerkt aan samenwerking en informatie-uitwisseling inzake normen, bijvoorbeeld voor risicobeheer;

Internationale samenwerking op het gebied van de cyberspace

43. HERHAALT dat de EU steun zal blijven verlenen aan de ontwikkeling van maatregelen tot vertrouwensopbouw op het gebied van cyberbeveiliging, zulks om de transparantie te vergroten en het risico op verkeerde percepties van overheidsgedrag te verminderen door het bevorderen van de invoering van internationale normen op dit gebied;

44. VERZOEKT de Commissie en de hoge vertegenwoordiger om volgens de bij de Verdragen voorgeschreven procedures ter zake:

- a) zich in te zetten voor het Verdrag van Boedapest als model voor het opstellen van nationale wetgeving inzake cybercriminaliteit en als grondslag voor internationale samenwerking op dit gebied, b) eerbiediging van de grondrechten in de cyberspace te bevorderen, en c) alle beschikbare instrumenten voor internationale samenwerking optimaal te benutten teneinde gestalte te geven aan de strijd tegen cybercriminaliteit en op dit gebied te komen tot politiële en justitiële samenwerking met derde landen van waaruit cybercriminele organisaties opereren;

- gebruik te maken van in de lidstaten aanwezige deskundigheid op het gebied van cyberbeleid en van hun uit bilaterale afspraken/samenwerking opgedane ervaring voor het ontwikkelen van gemeenschappelijke EU-boodschappen over cyberspace-aangelegenheden, en nauw met de lidstaten samen te werken aan de praktische aspecten;

- in samenwerking met de lidstaten alsmede met relevante particuliere en maatschappelijke organisaties optimaal gebruik te maken van de desbetreffende EU-steuninstrumenten voor de opbouw van ICT-capaciteit, ook op het gebied van cyberbeveiliging;

45. VERZOEKT de lidstaten, de Commissie en de hoge vertegenwoordiger om volgens de bij de Verdragen voorgeschreven procedures, naar een samenhangend internationaal cyberspacebeleid van de EU toe te werken door:

- meer in te zetten op samenwerking met belangrijke internationale partners en organisaties, en wel zo dat alle lidstaten ten volle kunnen profiteren van deze samenwerking;

- cyberaangelegenheden in het GBVB te integreren;

- te werken aan betere coördinatie inzake mondiale cybervraagstukken en door cyberbeveiliging, inclusief maatregelen ter bevordering van vertrouwen en transparantie, te mainstreamen in het algemene kader voor het onderhouden van betrekkingen met derde landen en internationale organisaties, mede via nauwere coördinatie tussen de lidstaten, de Commissie en de EDEO wat betreft het voeren van dialogen en het ondernemen van andere activiteiten op het gebied van cyberbeveiliging;

- de coördinatie te verbeteren via de bevoegde voorbereidende Raadsinstanties (waaronder de Groep vrienden van het voorzitterschap inzake cybervraagstukken);

- ondersteuning voor capaciteitsopbouw in derde landen te verlenen door middel van opleiding en bijstand voor het ontwerpen van nationale beleidsmaatregelen, strategieën en instellingen ter zake, opdat volledig gebruik wordt gemaakt van het economisch en sociaal potentieel van ICT's, de ontwikkeling van veerkrachtige systemen in die landen wordt gesteund en de cyberrisico's voor de EU-instellingen en de lidstaten worden teruggedrongen, met behulp van bestaande netwerken en fora voor beleidscoördinatie en informatie-uitwisseling;

<u>Rol en verantwoordelijkheden</u>

46. ROEPT de overige belanghebbenden - uit de particuliere sector, de technische en academische gemeenschappen, het maatschappelijk middenveld en individuele burgers - OP hun respectieve rol te vervullen en verantwoordelijkheden op zich te nemen teneinde een open, vrije en veilige cyberspace te verwezenlijken;

47. ROEPT de Commissie en de hoge vertegenwoordiger OP erop toe te zien dat de Europese activiteiten verenigbaar zijn met de structuren, het constitutioneel recht en de cyberbeveiligingsinitiatieven van de lidstaten, teneinde tot een geïntegreerde aanpak te komen en dubbel werk te voorkomen;

EN

48. VRAAGT de Commissie en de hoge vertegenwoordiger een voortgangsverslag over de cyberbeveiligingsstrategie op te stellen en dat te presenteren tijdens de Conferentie op hoog niveau in februari 2014, en STELT VOOR dat in de bevoegde voorbereidende Raadsinstanties (met name in de Groep vrienden van het voorzitterschap inzake cybervraagstukken) regelmatig vergaderingen worden gehouden om te helpen binnen een alomvattend beleidskader cyberprioriteiten en strategische doelstellingen van de EU te bepalen, en om de thans aan de gang zijnde uitvoering van de strategie te evalueren en te ondersteunen;

49. Voor de uitvoering van deze conclusies van de Raad zal alleen gebruik worden gemaakt van bestaande fondsen en financiële programma's, waarbij niet wordt vooruitgelopen op de onderhandelingen over het toekomstig financieel kader, en om die reden VERZOEKT de Raad de Commissie bij de presentatie van de financiering van de strategie de aanstaande onderhandelingen met het Europees Parlement in aanmerking te nemen.

Referenties

1. Europees Parlement, Raad en Commissie

   – Handvest van de grondrechten van de Europese Unie[2],

2. Europees Parlement en Raad

   – 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[3],

   – Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten (Kaderrichtlijn), als gewijzigd bij Richtlijn 2009/140/EG[4],

3. Europees Parlement

   – Resolutie van het Europees Parlement van 11 december 2012 over een strategie voor digitale vrijheid in het buitenlandbeleid van de EU,

   – Verslag van het Europees Parlement van 2012 over cyberveiligheid en defensie,

4. Raad

   – Het programma van Stockholm - een open en veilig Europa ten dienste en ter bescherming van de burger[5],

   – Een veiliger Europa in een betere wereld – Europese veiligheidsstrategie, 12 december 2003[6],

2 PB C 364 van 18.12.2010, blz. 1.
3 PB L 77 van 13.3.2004.
4 PB L 108 van 24.4.2002, blz. 33, en PB L 337 van 18.12.2009, blz. 37.
5 Doc. 17024/09 CO EUR-PREP 3 JAI 896, blz. 229:
6 Doc. 15849/03 PESC 783.

– Interneveiligheidsstrategie voor de Europese Unie: "Naar een Europees veiligheidsmodel" [7],

– Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren[8],

– Conclusies van de Raad over de mededeling van de Commissie "De EU-interneveiligheidsstrategie in actie"[9],

– Conclusies van de Raad over de mededeling van de Commissie betreffende de bescherming van kritieke informatie-infrastructuur (CIIP), "Bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid"[10],

– Conclusies van de Raad inzake de vaststelling van de prioriteiten van de Unie ter bestrijding van zware en georganiseerde criminaliteit voor de periode 2014-2017[11],

– Conclusies van de Raad over de oprichting van een Europees Centrum voor de bestrijding van cybercriminaliteit[12],

---

7 Doc. 5842/2/10 JAI 90

8 PB L 345 van 23.12.2008.

9 Doc. 6699/11, JAI 124

10 Doc. 10299/11 TELECOM 71 DATAPROTECT 55 JAI 332 PROCIV 66 Deze mededeling volgt op de Commissiemededeling betreffende de bescherming van kritieke informatie-infrastructuur, "Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht" (doc. 8375/09).

11 9849/13 JAI 407 COSI 62 ENFOPOL 151 CRIMORG 77 ENFOCUSTOM 89 PESC 569 RELEX 434.

12 Doc. 10603/12 ENFOPOL 154 TELECOM 116

– Voorstel voor een richtlijn van het Europees Parlement en de Raad over aanvallen op informatiesystemen ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad. Goedkeuring van de definitieve compromistekst met het oog op een akkoord met het Europees Parlement in eerste lezing[13],

– Conclusies van de Raad over de Europese strategie voor een beter internet voor kinderen[14],

– Conclusies van de Raad over de bestrijding van de seksuele uitbuiting van kinderen en kinderpornografie op het internet - het politieoptreden in de lidstaten en derde landen doeltreffender maken[15],

– Conclusies van de Raad over een wereldwijde alliantie tegen seksuele uitbuiting van kinderen via het internet[16],

– Conclusies van de Raad over een gemeenschappelijke werkstrategie en concrete maatregelen tegen cybercriminaliteit[17] en conclusies van de Raad over een actieplan ter uitvoering van de gecoördineerde strategie tegen cybercriminaliteit[18],

– Partiële algemene oriëntatie van de Raad over het voorstel van de Commissie voor een verordening tot vaststelling van "Horizon 2020" - het kaderprogramma voor onderzoek en innovatie (2014-2020)[19],

– Gemeenschappelijk optreden van de Raad betreffende de oprichting van het Europees Defensiebureau[20],

---

13 Doc. 11399/12 DROIPEN 79 TELECOM 126 CODEC 1673

14 Doc. 15850/12 AUDIO 111 JEUN 95 EDUC 330 TELECOM 203 CONSOM 136 JAI 766 GENVAL 81

15 Doc. 15783/2/11 REV 2 GENVAL 108 ENFOPOL 368 DROPIEN 119 AUDIO 53

16 Doc. 10607/12 +COR 1 GENVAL 39 ENFOPOL 155 DROIPEN 69 AUDIO 62 JEUN 46

17 Doc. 15569/08 ENFOPOL 224 CRIMORG 190.

18 Doc. 5957/2/10 REV 2 CRIMORG 22 ENFOPOL 32

19 Doc. 10663/12 RECH 207 COMPET 364 IND 102 MI 398 EDUC 152 TELECOM 118 ENER 233 ENV 446 REGIO 75 AGRI 362 TRANS 187 SAN 134 CODEC 1511.

20 Doc 10556/04 COSDP 374 POLARM 17 IND 80 RECH 130 ECO 121

– Gezamenlijk voorstel voor een besluit van de Raad inzake de regelingen voor de toepassing van de solidariteitsclausule van de Unie[21],

– Conclusies van de Raad over mediageletterdheid in de digitale omgeving[22],

– Mensenrechten en democratie: strategisch EU-kader en EU-actieplan[23],

– Verslag over de toepassing van de Europese veiligheidsstrategie[24],

5. Commissie

– De digitale agenda voor Europa[25], een van de zeven vlaggenschipinitiatieven van de Europa 2020-strategie voor slimme, duurzame en inclusieve groei[26], en de mededeling "De digitale agenda voor Europa - Europese groei bevorderen op basis van digitale technologieën"[27], waarin de digitale agenda wordt geheroriënteerd,

– Mededeling over privacywaarborging in het online tijdperk "Een Europees gegevensbeschermingskader voor de 21e eeuw"[28],

– Mededeling "De aanpak van criminaliteit in het digitale tijdperk: oprichting van een Europees Centrum voor de bestrijding van cybercriminaliteit"[29],

21 Doc. 18124/12 CAB 39 POLGEN 220 CCA 13 JAI 946 COSI 134 PROCIV 225 ENFOPOL 430 COPS 485 COSDP 1123 PESC 1584 COTER 125 COCON 45 COHAFA 165

22 Doc. 15441/09 AUDIO 47 EDUC 173 TELECOM 233 RECH 380

23 Doc. 11855/12 COHOM 163 PESC 822 COSDP 546 FREMP 100 INF 110 JAI 476 RELEX 603

24 Doc. 17104/08 CAB 66 PESC 1687 POLGEN 139

25 Doc. 9981/1/10 TELECOM 52 AUDIO 17 COMPET 165 RECH 193 MI 168 DATA PROTECT 141.

26 Doc. 7110/10 CO EUR-PREP 7 POLGEN 28 AG 3 ECOFIN 136 UEM 55 SOC 174 COMPET 82 RECH 83 ENER 63 TRANS 55 MI 73 IND 33 EDUC 40 ENV 135 AGRI 74.

27 Doc. 17963/12 TELECOM 262 MI 839 COMPET 786 CONSOM 161 DATAPROTECT 149 RECH 472 AUDIO 137 POLGEN 216

28 Doc. 5852/12 DATAPROTECT 8 JAI 43 MI 57 DRS 10 DAPIX 11 FREMP 6

29 Doc. 8543/12 ENFOPOL 94 TELECOM 72

– Mededeling van de Commissie "Het aanboren van het potentieel van cloud computing in Europa"[30],

– Mededeling van de Commissie betreffende de bescherming van kritieke informatie-infrastructuur (CIIP) "Bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid"[31],

– Mededeling van de Commissie betreffende de bescherming van kritieke informatie-infrastructuur "Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht"[32],

6. VN

– Resolutie A/RES 57/239 van de Algemene Vergadering van de VN over een wereldwijde cultuur van cyberveiligheid,

– Resolutie A/HRC/20/L.13 van de VN-Mensenrechtenraad van 29 juni 2012 over de bevordering, bescherming en uitoefening van de mensenrechten op het internet,

– Resolutie A/RES 67/27 van de Algemene Vergadering van de VN over de ontwikkelingen op het gebied van informatie en telecommunicatie in de context van de internationale veiligheid,

– Oprichting van een open intergouvernementele deskundigengroep cybercriminaliteit met UNODC op grond van Resolutie 65/230 van de Algemene Vergadering van de VN,

7. Raad van Europa

– Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van de Raad van Europa van 28 januari 1981,

– Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken van de Raad van Europa van 23 november 2001,

---

30 Doc. 14411/12 TELECOM 170 MI 586 DATAPROTECT 112 COMPET 585

31 Doc. 8548/11 TELECOM 40 DATAPROTECT 27 JAI 213 PROCIV 38

32 Doc. 8375/09 TELECOM 69 DATAPROTECT 24 JAI 192 PROCIV 46

8. Organisatie voor Veiligheid en Samenwerking in Europa (OVSE)

– Besluit nr. 1039 van de Permanente Raad van 26 april 2012, betreffende het ontwikkelen van maatregelen tot vertrouwensopbouw ter verminderingen van de risico's op conflicten ten gevolge van het gebruik van informatie- en communicatie-technologieën,

– Ministerieel Besluit nr. 4/12 van 7 december 2012: de OVSE-inspanningen ter bestrijding van transnationale dreigingen,

– Instelling van een open OVSE-werkgroep die ontwerpmaatregelen tot vertrouwens-opbouw moet uitwerken ter bevordering van de samenwerking tussen staten, transparantie, voorspelbaarheid en stabiliteit, en ter vermindering van de risico's op mogelijke verkeerde perceptie, escalatie en conflicten ten gevolge van het gebruik van ICT's (Besluit nr. 1039 van de Permanente Raad van de OVSE van 26 april 2012),

9. Conferenties, initiatieven en evenementen

– Internationale conferentie over cyberspace, Londen, 1-2 november 2011, gevolgd door de Internationale conferentie over cyberspace, Boedapest, 4-5 oktober 2012,

– Gezamenlijke EU-VS-simulatie-cyberincidentoefening "Cyber Atlantic 2011" en pan-Europese cyberincidentoefeningen met deelname van alle lidstaten (Cyber Europe 2010 en Cyber Europe 2012),

– Ad-hocgroep nucleaire beveiliging, met in haar eindverslag bevindingen en beraadslagingen over computerbeveiliging / cyberveiligheid[33],

[33] Doc. 10616/12 AHGS 20 ATO 84

10. Overige

– EU-dreigingsevaluatie van zware en georganiseerde criminaliteit (SOCTA), Europol, 2013[34],

– Het beleid[35] en de richtsnoeren[36] inzake Information Assurance Security op het gebied van netwerkverdediging.

[34] Doc. 7368/13 JAI 200 COSI 26 ENFOPOL 75 CRIMORG 41 CORDROGUE 27 ENFOCUSTOM 43 PESC 286 JAIEX 20 RELEX 211

[35] Doc. 8408/12 CSCI 11 CSC 20

[36] Doc. 10578/12 CSCI 20 CSC 34