Dinsdag 12 juni 2012

65. vestigt de aandacht erop dat vrijwilligerswerk moet worden bevorderd, met name tijdens het Europees jaar van de burgers in 2013, en roept de Commissie tevens op om steun voor vrijwilligerswerk op te nemen in het beleid inzake internationale ontwikkelingssteun, in het bijzonder om alle streefdoelen die werden vastgelegd in de millenniumontwikkelingsdoelstellingen te halen;

66. is voorstander van een formeel onderzoek naar het voorstel van Solidarité voor een institutioneel programma voor menselijke hulpbronnen in de EU-instellingen om het voor het personeel en de stagiaires van de instellingen gemakkelijker te maken vrijwilligerswerk te verrichten, zowel als onderdeel van de personeelsopleiding als in hun eigen tijd;

67. beklemtoont dat het voorgestelde programma kostenbesparend is, een hoge toegevoegde waarde biedt en helpt het beleid en de programma's van de EU uit te voeren;

68. beveelt de Commissie aan om de nuttige contactpunten te behouden die werden vastgesteld zowel met de "EYV 2011 Alliance" en zijn opvolger, het vrijwilligerswerkplatform, die vele maatschappelijke organisaties voor vrijwilligerswerk en netwerking bevatten, als met nationale coördinerende instanties, strategische partners en woordvoerders van nationale regeringen in deze sector, omwille van de zeer grote verscheidenheid van diensten die verantwoordelijk zijn voor het vrijwilligerswerk in de EU, en moedigt die contactpunten aan om zich in te zetten voor het voorstel voor een centraal EU- portaal, in de vorm van een pan-Europees platform, voor het vergemakkelijken van verdere coördinatie en verhoogde grensoverschrijdende activiteit;

69. benadrukt het belang van contactnetwerken en de uitwisseling van goede praktijken om informatie te verspreiden over bestaande EU-procedures die het grensoverschrijdend vrijwilligerswerk kunnen helpen en ondersteunen;

70. vraagt aan de Commissie om, wanneer zij dit geschikt acht, maatregelen te nemen betreffende de politieke agenda voor vrijwilligerswerk in Europa, die is opgesteld door de vrijwilligersorganisaties die verenigd zijn binnen de "EYV 2011 Alliance";

71. verzoekt zijn Voorzitter deze resolutie te doen toekomen aan de Raad, de Commissie, en de regeringen en parlementen van de lidstaten.

Bescherming van kritieke informatie-infrastructuur: naar mondiale cyberveiligheid

P7_TA(2012)0237

Resolutie van het Europees Parlement van 12 juni 2012 over de bescherming van kritieke informatie-infrastructuur - bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid (2011/2284(INI))

(2013/C 332 E/03)

Het Europees Parlement,

— gezien zijn resolutie van 5 mei 2010 getiteld "Een nieuwe digitale agenda voor Europa: 2015.eu" ([1]),

— gezien zijn resolutie van 15 juni 2010 getiteld "Internetgovernance: de volgende stappen" ([2]),

— gezien zijn resolutie van 6 juli 2011 met als titel: "Breedband in Europa: investeren in digitale groei" ([3]),

— gezien artikel 48 van zijn Reglement,

— gezien het verslag van de Commissie industrie, onderzoek en energie en het advies van de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken (A7-0167/2012),

([1]) PB C 81 E van 15.3.2011, blz. 45.
([2]) PB C 236 E van 12.8.2011, blz. 33.
([3]) Aangenomen teksten P7_TA(2011)0322.

A. overwegende dat de informatie en communicatietechnologieën (ICT) slechts hun volle potentieel voor de vooruitgang van de economie en de maatschappij kunnen ontwikkelen als de gebruikers kunnen vertrouwen op de veiligheid en veerkracht ervan en als de bestaande wetgeving inzake kwesties zoals de bescherming van de persoonlijke levenssfeer en intellectuele-eigendomsrechten doeltreffend in de internetomgeving worden opgelegd;

B. overwegende dat de weerslag van internet en ICT op de verschillende aspecten van het leven van de burgers snel toeneemt en overwegende dat ze een cruciale drijvende kracht zijn achter onze sociale interactie, culturele verrijking en economische groei;

C. overwegende dat ICT- en internetbeveiliging een veelomvattend concept is met een algehele weerslag op economische, sociale, technologische en militaire aspecten waarvoor een duidelijke definitie en differentiatie van de verantwoordelijkheden en een degelijk internationaal samenwerkingsmechanisme vereist zijn;

D. overwegende dat het kerninitiatief "Een digitale agenda voor Europa" gericht is op het bevorderen van het mededingingsvermogen van Europa door ICT te versterken, en op het creëren van de nodige voorwaarden voor een sterke, degelijke groei en op technologie gebaseerde banen;

E. overwegende dat de privésector de belangrijkste belegger, eigenaar en beheerder blijft op het gebied van informatiebeveiligingsproducten, -diensten, -toepassingen en -infrastructuur, waarin in het afgelopen decennium miljarden euro zijn geïnvesteerd; overwegende dat deze betrokkenheid moet worden versterkt via passende beleidsstrategieën ter bevordering van de veerkracht van infrastructuur die in handen is van of beheerd wordt door overheids-, particuliere of publiek-private organisaties;

F. overwegende dat de ontwikkeling van een hoge mate van beveiliging en veerkracht van de ICT-netwerken, -diensten en -technologieën het concurrentievermogen van de EU-economie zou moeten vergroten, zowel door de evaluatie en het beheer van cyberrisico's te verbeteren als door de gehele EU-economie degelijkere informatie-infrastructuren te bieden ter ondersteuning van innovatie en groei waardoor voor bedrijven nieuwe kansen ontstaan om productiever te worden;

G. overwegende dat de bij de wetshandhaving beschikbare gegevens over cybercriminaliteit (waaronder cyberaanvallen, maar ook andere soorten onlinecriminaliteit) op een sterke stijging in verschillende Europese landen wijzen; overwegende echter dat statistisch representatieve gegevens over cyberaanvallen afkomstig van zowel rechtshandhavingsinstanties als de CERT-gemeenschap (computercrisisteam) schaars blijven en in de toekomst beter moeten worden geaggregeerd, waardoor rechtshandhavingsinstanties in de gehele EU beter zullen kunnen optreden en de wetgeving over betere informatie zal beschikken om in te spelen op de voortdurende cyberdreigingen;

H. overwegende dat een toereikend niveau van informatiebeveiliging van doorslaggevend belang is voor een degelijke uitbreiding van op het internet gebaseerde diensten;

I. overwegende dat recente cyberincidenten, -verstoringen en -aanvallen tegen de informatie-infrastructuur van de EU-instellingen, de industrie en de lidstaten aantonen dat een degelijk, vernieuwend en doeltreffend systeem moet worden vastgelegd voor de bescherming van kritieke informatie-infrastructuur, gebaseerd op volledige internationale samenwerking en minimumnormen voor veerkracht in de verschillende lidstaten;

J. overwegende dat de snelle ontwikkeling van nieuwe ICT-middelen, zoals cloud computing, een sterke focus op de beveiliging vereist om de voordelen van de technologische verwezenlijkingen volledig te kunnen benutten;

K. overwegende dat het Europees Parlement herhaaldelijk heeft aangedrongen op de toepassing van hoge normen voor de bescherming van de persoonlijke levenssfeer en gegevensbescherming, netwerkneutraliteit en de bescherming van intellectuele-eigendomsrechten;

Maatregelen ter bevordering van de bescherming van kritieke informatie-infrastructuur op nationaal en Unieniveau

1. is ingenomen met de uitvoering door de lidstaten van het Europees programma voor de bescherming van kritieke informatie-infrastructuur, waaronder het opzetten van het waarschuwings- en informatienetwerk op het gebied van kritieke infrastructuur (CIWIN);

2. is van mening dat de inspanningen ter bescherming van kritieke informatie-infrastructuur niet enkel de algehele veiligheid van de burgers zullen vergroten, maar ook ten goede zullen komen aan de veiligheidsperceptie van de burgers en hun vertrouwen in de beschermingsmaatregelen van de overheid;

Dinsdag 12 juni 2012

3. is erkentelijk dat de Commissie de herziening overweegt van Richtlijn 2008/114/EG van de Raad ([1]) en vraagt dat bewijsmateriaal wordt verstrekt over de doeltreffendheid en impact van de richtlijn alvorens verdere stappen worden ondernomen; dringt erop aan dat wordt overwogen de reikwijdte ervan uit te breiden, met name door de ICT-sector en de financiële diensten erin op te nemen; dringt bovendien erop aandacht te besteden aan gebieden zoals gezondheid, voedsel- en watertoevoersystemen, nucleair onderzoek en industrie (wanneer die niet vallen onder specifieke bepalingen); is van mening dat deze sectoren ook moeten profiteren van de intersectorale aanpak die wordt gekozen in het kader van CIWIN (dat bestaat uit samenwerking, een waarschuwingssysteem en de uitwisseling van de optimale praktijken);

4. onderstreept het belang van duurzame integratie van het Europese onderzoek om de Europese uitmuntendheid op het vlak van de bescherming van kritieke informatie-infrastructuur te handhaven en te verbeteren;

5. dringt, in het licht van de onderling verbonden en sterk van elkaar afhankelijke, gevoelige, strategische en kwetsbare aard van nationale en Europese kritieke informatie-infrastructuren, erop aan dat de minimumnormen voor veerkracht regelmatig worden bijgewerkt met het oog op paraatheid voor en reactie op verstoringen, incidenten, vernietigingspogingen of aanvallen, zoals diegene die voortvloeien uit onvoldoende degelijke infrastructuur of onvoldoende beveiligde eindterminals;

6. onderstreept het belang van normen en protocollen voor de informatiebeveiliging, en is verheugd over het feit dat CEN, Cenelec en ETSI in 2011 de opdracht hebben gekregen beveiligingsnormen op te stellen;

7. verwacht dat eigenaren en exploitanten van kritieke informatie-infrastructuren gebruikers in staat zullen stellen en zo nodig zullen helpen om passende middelen te gebruiken ten einde zichzelf te beschermen tegen kwaadaardige aanvallen en/of verstoringen, middels zowel menselijk als geautomatiseerd toezicht, waar nodig;

8. is voorstander van samenwerking tussen publieke en particuliere belanghebbenden op het niveau van de Unie en moedigt hun inspanningen aan om normen te ontwikkelen en toe te passen voor de beveiliging en veerkracht van civiele (publieke, private of publiek-private) nationale en Europese kritieke informatie-infrastructuren;

9. benadrukt het belang van pan-Europese oefeningen om op grootschalige netwerkbeveiligingsincidenten voorbereid te zijn, en van de definitie van één enkele reeks normen voor dreigingsanalyse;

10. verzoekt de Commissie om, in samenwerking met de lidstaten, de invoering van het actieplan voor de bescherming van kritieke informatie-infrastructuren te beoordelen; dringt er bij de lidstaten op aan om goed werkende nationale/gouvernementele CERT's samen te stellen, nationale cyberbeveiligingsstrategieën te ontwikkelen, regelmatige nationale en pan-Europese cyberincidentoefeningen te organiseren, nationale noodplannen voor cyberincidenten te ontwikkelen en bij te dragen aan de ontwikkeling van een Europees noodplan voor cyberincidenten tegen eind 2012;

11. beveelt aan dat de beveiligingsplannen van de exploitant of gelijkwaardige maatregelen worden ingevoerd voor alle Europese kritieke informatie-infrastructuren en dat er veiligheidscoördinatoren worden aangesteld;

12. is ingenomen met de huidige herziening van Kaderbesluit 2005/222/JBZ van de Raad ([2]) over aanvallen op informatiesystemen; wijst op de noodzaak om de inspanningen van de EU bij de bestrijding van grootschalige cyberaanvallen te coördineren door de bevoegdheden van ENISA, de CERT's van de lidstaten en de toekomstige Europese CERT's op te nemen;

13. is van mening dat ENISA op Europees niveau een sleutelrol kan spelen bij de bescherming van kritieke informatie-infrastructuren door de lidstaten en de instellingen en organen van de Europese Unie technische deskundigheid te verschaffen, evenals door middel van rapporten en analyses over de beveiliging van informatiesystemen op Europees en mondiaal niveau;

Overige EU-activiteiten voor degelijke internetbeveiliging

14. spoort ENISA aan om elk jaar maanden voor de bewustwording van de internetbeveiliging in de EU te coördineren en uit te voeren, zodat de lidstaten en de burgers van de EU speciaal worden gewezen op kwesties inzake cyberveiligheid;

([1]) PB L 345 van 23.12.2008, blz. 75.
([2]) PB L 69 van 16.3.2005, blz. 67.

15. steunt ENISA, overeenkomstig de doelstellingen van de Digitale agenda, bij de uitvoering van zijn taken op het vlak van netwerkinformatiebeveiliging, met name via sturing en advies aan de lidstaten over de wijze waarop zij aan de basiscapaciteiten voor hun CERT's kunnen voldoen, alsmede middels het ondersteunen van de uitwisseling van optimale praktijken door een klimaat van vertrouwen te ontwikkelen; roept het agentschap op om de betrokken belanghebbenden te raadplegen om soortgelijke cyberbeveiligingsmaatregelen uit te werken voor de eigenaren en exploitanten van particuliere netwerken en infrastructuur, en om de Commissie en lidstaten bij te staan bij het bijdragen aan de ontwikkeling en toepassing van certificeringsregelingen voor informatiebeveiliging, gedragsnormen en samenwerkingspraktijken tussen nationale en Europese CERT's en eigenaren en exploitanten van infrastructuur, waar en wanneer nodig, door technologisch neutrale, gemeenschappelijke minimumeisen vast te leggen;

16. is ingenomen met het huidige voorstel inzake de herziening van het mandaat van ENISA en met name de uitbreiding ervan, en inzake de uitbreiding van de taken van het agentschap; is van mening dat ENISA, naast zijn bijstand aan de lidstaten door het verstrekken van deskundigheid en analyses, bevoegd zou moeten zijn om een aantal uitvoerende taken op EU-niveau te beheren en, in samenwerking met de tegenhangers in de VS, taken met betrekking tot de preventie en opsporing van netwerk- en informatiebeveiligingsincidenten en de bevordering van de samenwerking tussen de lidstaten. wijst erop dat het agentschap, uit hoofde van de ENISA-verordening, ook aanvullende verantwoordelijkheden zou kunnen krijgen met betrekking tot de reactie op internetaanvallen voor zover dit een duidelijke meerwaarde biedt voor de bestaande nationale responsmechanismen;

17. is ingenomen met de resultaten van de pan-Europese cyberbeveiligingsoefeningen van 2010 and 2011, die in de hele Unie onder toezicht van ENISA zijn uitgevoerd en die tot doel hadden de lidstaten te helpen bij het opzetten, onderhouden en testen van een pan-Europees noodplan; verzoekt ENISA om dergelijke oefeningen op zijn agenda te handhaven en indien nodig geleidelijk relevante particuliere exploitanten hierbij te betrekken om de totale internetbeveiligingscapaciteiten van Europa te vergroten; kijkt uit naar een verdere internationale uitbreiding met gelijkgestemde partners;

18. verzoekt de lidstaten om nationale noodplannen inzake cyberveiligheid op te stellen en belangrijke elementen op te nemen zoals relevante contactpunten en bijstandsvoorzieningen, beheersing en herstel bij cyberverstoringen of -aanvallen van regionaal, nationaal of grensoverschrijdend belang; merkt op dat de lidstaten ook op nationaal vlak gepaste coördinatiemechanismen en -structuren moeten vastleggen die moeten zorgen voor een betere coördinatie tussen bevoegde nationale autoriteiten en voor een grotere samenhang van hun acties;

19. stelt voor dat de Commissie via het EU-noodplan inzake cyberincidenten bindende maatregelen voorstelt voor een betere coördinatie op EU-niveau van de technische en sturingsfuncties van de nationale en gouvernementele CERT's;

20. verzoekt de Commissie en de lidstaten om de noodzakelijke maatregelen te nemen om kritieke infrastructuur tegen cyberaanvallen te beschermen en voorzieningen te treffen ten einde de toegang tot kritieke infrastructuur hermetisch af te sluiten als een rechtstreekse cyberaanval een ernstige bedreiging vormt voor de goede werking van de infrastructuur;

21. kijkt uit naar de volledige invoering van EU-CERT dat een sleutelrol zal vervullen bij de preventie en opsporing van, de reactie op en het herstel van opzettelijke en kwaadaardige cyberaanvallen die tegen de EU-instellingen zijn gericht;

22. beveelt aan dat de Commissie bindende maatregelen voorstelt die erop gericht zijn minimumnormen inzake beveiliging en veerkracht op te leggen en de coördinatie tussen de nationale CERT's te verbeteren;

23. verzoekt de lidstaten en de EU-instellingen om te zorgen voor goed werkende CERT's met minimumcapaciteiten voor beveiliging en veerkracht op grond van overeengekomen optimale praktijken; wijst erop dat nationale CERT's deel moeten uitmaken van een effectief netwerk waarin relevante informatie wordt uitgewisseld overeenkomstig de vereiste normen inzake vertrouwelijkheid; verzoekt om de invoering van een ononderbroken continuïteit van de dienst voor de bescherming van kritieke informatie-infrastructuur voor elke lidstaat en om de opstelling van een gemeenschappelijk Europees noodprotocol dat tussen de nationale contactpunten dient te worden toegepast;

24. onderstreept dat het scheppen van vertrouwen en het bevorderen van de samenwerking tussen de lidstaten cruciaal is voor de bescherming van gegevens en nationale netwerken en infrastructuren; verzoekt de Commissie om een gemeenschappelijke procedure voor te stellen voor de afbakening en vaststelling van een gemeenschappelijke aanpak om grensoverschrijdende dreigingen op het gebied van ICT weg te nemen, waarbij wordt verwacht dat de lidstaten de Commissie van algemene informatie voorzien over risico's, dreigingen en kwetsbaarheden van hun kritieke informatie-infrastructuur;

25. is ingenomen met het initiatief van de Commissie voor de ontwikkeling van een Europees stelsel voor informatiedeling en alarm tegen 2013;

26. is ingenomen met het feit dat de Commissie de verscheidene belanghebbenden inzake internetbeveiliging en bescherming van kritieke informatie-infrastructuur heeft geraadpleegd, zoals het Europees publiek-privaat partnerschap voor veerkracht; erkent de reeds significante betrokkenheid en het engagement van ICT-leveranciers bij dergelijke inspanningen en moedigt de Commissie aan om haar inspanningen voort te zetten om de academische wereld en ICT-gebruikersorganisaties aan te moedigen om een actievere rol te spelen en om een constructieve dialoog met de verschillende belanghebbenden over cyberveiligheidskwesties te bevorderen; is voorstander van een verdere ontwikkeling van de digitale vergadering als een kader voor governance op het vlak van de bescherming van kritieke informatie-infrastructuur;

27. is ingenomen met het werk dat tot dusverre door het Europees forum van lidstaten is verricht ten aanzien van de vaststelling van sectorspecifieke criteria voor het opsporen van Europese kritieke infrastructuren, met een nadruk op vaste en mobiele communicatiemiddelen, alsook ten aanzien van de bespreking van de beginselen en richtsnoeren van de EU betreffende de veerkracht en stabiliteit op het internet; kijkt ernaar uit om te blijven werken aan de consensus tussen de lidstaten en moedigt in dit verband het forum aan om de huidige op fysieke voorzieningen gerichte aanpak te koppelen aan inspanningen om ook logische-infrastructuurvoorzieningen erin op te nemen die, naarmate virtualisatie- en cloudtechnologieën verder ontwikkeld worden, steeds belangrijker worden voor de doeltreffendheid van de bescherming van kritieke informatie-infrastructuur;

28. stelt voor dat de Commissie een openbaar pan-Europees onderwijsinitiatief lanceert dat gericht is op het onderricht en de bewustmaking van zowel particuliere als zakelijke eindgebruikers inzake potentiële dreigingen in het internet en op vaste en mobiele ICT-toestellen op elk niveau van de gebruiksketen, alsmede op het bevorderen van een veiliger individueel gedrag online; herinnert in dit verband aan de risico's in verband met verouderde IT-apparatuur en software;

29. verzoekt de lidstaten om, met de steun van de Commissie, de opleidings- en onderwijsprogramma's over informatiebeveiliging, die gericht zijn op nationale rechtshandhavings- en gerechtelijke instanties en op de relevante EU-agentschappen, te versterken;

30. ondersteunt de invoering van een EU-curriculum voor academische deskundigen op het gebied van informatiebeveiliging, aangezien dit een positieve weerslag zou hebben op de deskundigheid en paraatheid van de EU ten aanzien van de zich voortdurend ontwikkelende cyberspace en de dreigingen hiervoor;

31. bepleit de bevordering van opleidingen in cyberveiligheid (promotieplaatsen, universitaire cursussen, workshops, scholing voor studenten, enz.) en gespecialiseerde opleidingen op het gebied van de bescherming van kritieke informatie-infrastructuur;

32. verzoekt de Commissie om tegen eind 2012 een uitgebreide strategie inzake internetbeveiliging voor de Unie voor te stellen, gebaseerd op duidelijke terminologie; is van mening dat de strategie inzake internetbeveiliging erop gericht moet zijn om op basis van een veilige en veerkrachtige infrastructuur en open normen een cyberspace tot stand te brengen die leidt tot innovatie en welvaart middels vrij verkeer van informatie, terwijl gezorgd wordt voor degelijke bescherming van de persoonlijke levenssfeer en andere burgerlijke vrijheden; blijft bij zijn standpunt dat de strategie in detail de beginselen, doelstellingen, methoden, instrumenten en beleidsterreinen (zowel intern als extern) moet bepalen die nodig zijn om de nationale en EU-inspanningen te stroomlijnen en om minimumnormen voor veerkracht tussen de lidstaten vast te leggen, die moeten zorgen voor een veilige, duurzame, gedegen en veerkrachtige dienstverlening, zowel in verband met de kritieke infrastructuur als voor het algemeen gebruik van internet;

33. onderstreept dat de komende strategie inzake internetbeveiliging van de Commissie de bescherming van kritieke informatie-infrastructuur als uitgangspunt moet nemen en gericht moet zijn op een holistische en systematische aanpak van cyberveiligheid met enerzijds proactieve maatregelen, zoals de invoering van minimumnormen voor beveiligingsmaatregelen en de scholing van individuele gebruikers, bedrijven en openbare instellingen, en anderzijds reactieve maatregelen, zoals strafrechtelijke, civielrechtelijke en bestuursrechtelijke sancties;

34. dringt er bij de Commissie op aan om een degelijk mechanisme voor te stellen voor het coördineren van de tenuitvoerlegging en periodieke bijwerking van de strategie inzake internetbeveiliging; is van oordeel dat dit mechanisme dient te worden ondersteund met toereikende administratieve, deskundige en financiële middelen en dat het onder andere tot taak heeft de afbakening van EU-posities in de betrekkingen met zowel interne als internationale belanghebbenden over aan internetbeveiliging verwante kwesties te faciliteren;

35. doet een beroep op de Commissie om een EU-kader voor te stellen voor de melding van veiligheidsinbreuken in kritieke sectoren, zoals energie, vervoer, water en voedselvoorziening, alsmede ICT en financiële diensten, om ervoor te zorgen dat de betrokken autoriteiten van de lidstaten en gebruikers worden geïnformeerd over cyberincidenten, -aanvallen en -verstoringen;

36. dringt er bij de Commissie op aan om de beschikbaarheid van statistisch representatieve gegevens over de kosten van cyberaanvallen in de EU, de lidstaten en de industrie (met name de sector van de financiële diensten en de ICT-sector) te verbeteren door de capaciteit voor gegevensverzameling van het geplande Europees cybercriminaliteitscentrum (dat tegen 2013 moet worden opgezet), de CERT's en andere initiatieven van de Commissie, zoals het Europees stelsel voor informatiedeling en alarm, te vergroten om aldus te zorgen voor een systematische verslaglegging en gegevensuitwisseling over cyberaanvallen en andere vormen van cybercriminaliteit waar de Europese industrie en de lidstaten mee te maken hebben, alsmede om de wetshandhaving te versterken;

37. pleit voor een nauwe band en interactie tussen de private sector in de lidstaten en ENISA om de nationale/gouvernementele CERT's te koppelen met de ontwikkeling van het Europees informatie-uitwisselings- en waarschuwingssysteem (EISAS);

38. wijst erop dat de voornaamste drijvende kracht achter de ontwikkeling en het gebruik van technologieën die de internetbeveiliging moeten verhogen, de ICT-industrie is; herinnert eraan dat het beleid van de EU de groei van de Europese interneteconomie niet mag belemmeren en de nodige stimulansen moet bevatten om het potentieel van bedrijven en publiek-private partnerschappen ten volle aan te wenden; beveelt aan om extra stimulansen voor de industrie te onderzoeken opdat zij degelijkere beveiligingsplannen van de exploitanten ontwikkelt overeenkomstig Richtlijn 2008/114/EG;

39. verzoekt de Commissie om een wetgevingsvoorstel in te dienen voor het verder strafbaar stellen van cyberaanvallen ((d.w.z. spear-phishing, onlinefraude, enz.);

Internationale samenwerking

40. herinnert eraan dat internationale samenwerking het kerninstrument is voor de invoering van doeltreffende maatregelen inzake cyberveiligheid; erkent dat de EU thans niet permanent actief betrokken is bij internationale samenwerkingsprocessen en -gesprekken in verband met cyberveiligheid; verzoekt de Commissie en de EDEO om een constructieve dialoog op te starten met gelijkgestemde landen om een gemeenschappelijk standpunt en beleid te ontwikkelen ter vergroting van de veerkracht van het internet en de kritieke infrastructuur; blijft tegelijk bij het standpunt dat de EU internetbeveiligingskwesties permanent moet opnemen in de reikwijdte van haar externe betrekkingen, onder andere bij het ontwerpen van verschillende financiële instrumenten of bij het aangaan van internationale overeenkomsten die de uitwisseling en opslag van gevoelige gegevens met zich meebrengen;

41. neemt nota van de positieve resultaten van het Verdrag inzake cybercriminaliteit van de Raad van Europa van Boedapest in 2001; wijst er echter op dat de EDEO niet alleen meer landen moet aanmoedigen om het verdrag te tekenen en te ratificeren, maar ook bilaterale en multilaterale overeenkomsten over internetbeveiliging en -veerkracht met gelijkgestemde internationale partners moet uitwerken;

42. wijst erop dat het grote aantal lopende activiteiten van uiteenlopende internationale en EU- instellingen, -instanties en -agentschappen alsook van de lidstaten coördinatie vergt om dubbel werk te voorkomen en dat het derhalve de moeite loont om een officiële verantwoordelijke voor de coördinatie aan te stellen, bijvoorbeeld een EU-cyberveiligheidscoördinator;

43. onderstreept het bijzondere belang van een gestructureerde dialoog tussen de belangrijkste Europese en Amerikaanse spelers en wetgevers op het gebied van de bescherming van kritieke informatie-infrastructuur met het oog op de totstandbrenging van een consensus en gemeenschappelijke interpretaties en standpunten ten aanzien van het kader voor wetgeving en beheer;

44. is ingenomen met de oprichting van de EU-VS-Werkgroep over cyberveiligheid en cybercriminaliteit tijdens de EU-VS-top van november 2010 en steunt de inspanningen om internetbeveiligingskwesties op te nemen in de trans-Atlantische beleidsdialoog; is verheugd over de gezamenlijke uitwerking door de Commissie en de regering van de VS, onder de paraplu van de EU-VS-Werkgroep, van een gemeenschappelijk programma en een stappenplan voor gezamenlijke/gesynchroniseerde transcontinentale cyberoefeningen in 2012/2013;

45. stelt voor om een gestructureerde dialoog tussen wetgevers van de EU en de VS in te stellen om internetgerelateerde kwesties te bespreken als onderdeel van een streven naar consensus, gemeenschappelijke interpretatie en standpunten;

46. dringt er bij de EDEO en de Commissie op aan om op basis van het werk van het Europees forum van lidstaten een actief standpunt in te nemen binnen de relevante internationale fora, onder meer door de standpunten van de lidstaten te coördineren met het oog op de bevordering van de kernwaarden, doelstellingen en het beleid van de EU inzake internetbeveiliging en veerkracht van het internet; merkt op dat tot deze fora instellingen behoren zoals de NAVO, de VN (in het bijzonder via de Internationale Telecommunicatie-unie en het forum voor internetbeheer), de Internet Corporation for Assigned Names and Numbers, de Internet Assigned Numbers Authority, de OVSE, de OESO en de Wereldbank;

47. moedigt de Commissie en ENISA aan om deel te nemen aan de dialogen met de voornaamste belanghebbenden ten einde technische en wettelijke normen op het vlak van cyberspace te bepalen op internationaal niveau;

*

* *

48. verzoekt zijn Voorzitter deze resolutie te doen toekomen aan de Raad en de Commissie.

Samenwerking op het gebied van energiebeleid met partners van buiten onze grenzen

P7_TA(2012)0238

Resolutie van het Europees Parlement van 12 juni 2012 over samenwerking op het gebied van energiebeleid met partners buiten onze grenzen: een strategische benadering van gegarandeerde, duurzame en concurrerende energievoorziening (2012/2029(INI))

(2013/C 332 E/04)

Het Europees Parlement,

— gezien de mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's inzake energievoorzieningszekerheid en internationale samenwerking: "Het energiebeleid van de EU: verbintenissen met partners buiten onze grenzen" (COM(2011)0539),

— gezien het voorstel van de Commissie voor een besluit van het Europees Parlement en de Raad tot instelling van een mechanisme voor informatie-uitwisseling met betrekking tot intergouvernementele overeenkomsten tussen lidstaten en derde landen op energiegebied (COM(2011)0540),

— gezien de conclusies van de Raad van 24 november 2011 inzake energievoorzieningszekerheid en internationale samenwerking – "Het energiebeleid van de EU: verbintenissen met partners buiten onze grenzen",

— gezien zijn resolutie van 25 november 2010 over een nieuwe energiestrategie voor Europa 2011-2020 ([1]),

— gezien artikel 48 van zijn Reglement,

— gezien het verslag van de Commissie industrie, onderzoek en energie en de adviezen van de Commissie buitenlandse zaken, de Commissie ontwikkelingssamenwerking en de Commissie internationale handel (A7-0168/2012),

([1]) PB C 99 E van 3.4.2012, blz. 64.