EUROPESE COMMISSIE

Brussel, 31.3.2011
COM(2011) 163 definitief

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

betreffende de bescherming van kritieke informatie-infrastructuur

'Bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid'

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

betreffende de bescherming van kritieke informatie-infrastructuur

'Bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid'

1. INLEIDING

Op 30 maart 2009 heeft de Commissie een mededeling aangenomen betreffende de bescherming van kritieke informatie-infrastructuur – 'Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht'[1], waarin een plan (het 'actieplan voor bescherming van kritieke informatie-infrastructuur') is opgesteld om de veiligheid en veerkracht van vitale informatie- en communicatietechnologiestructuren te verbeteren. Het plan had tot doel op nationaal en op Europees vlak de ontwikkeling van een hoog niveau van capaciteiten inzake paraatheid, veiligheid en veerkracht te stimuleren en te ondersteunen. Deze benadering kon rekenen op ruime steun van de Raad in 2009[2].

Het actieplan voor de bescherming van kritieke informatie-infrastructuur is gebouwd op vijf pijlers: paraatheid en preventie, detectie en respons, mitigatie en herstel, internationale samenwerking en criteria voor Europese kritieke infrastructuur in de ICT-sector. Het plan bevat de werkzaamheden die in het kader van de verschillende pijlers moeten worden verricht door de Commissie, de lidstaten en/of het bedrijfsleven, met de steun van het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA).

In de Digitale agenda voor Europa[3] (DAE), die in mei 2010 is aangenomen, en de desbetreffende conclusies van de Raad[4] is gewezen op het gemeenschappelijke besef dat vertrouwen en beveiliging essentiële vereisten zijn voor een ruime verbreiding van ICT en derhalve om de doelstellingen van de dimensie 'slimme groei' van de Europa 2020-strategie[5] te bereiken. De DAE beklemtoont dat alle belanghebbenden hun krachten moeten bundelen in een holistische inspanning om de veiligheid en veerkracht van ICT-infrastructuren te verzekeren, door zich toe te spitsen op preventie, paraatheid en bewustmaking, alsmede om effectieve en gecoördineerde mechanismen te ontwikkelen als respons op nieuwe en steeds complexere vormen van cyberaanvallen en cybercriminaliteit. Deze aanpak zorgt ervoor dat zowel de preventieve als reactieve dimensie van de uitdaging voldoende aandacht krijgen.

In de voorbije maanden zijn de volgende in de digitale agenda aangekondigde maatregelen genomen: in september 2010 heeft de Commissie een voorstel voor een richtlijn over

---

1 COM(2009) 149.

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

3 COM(2010) 245.

4 Conclusies van de Raad van 31 mei 2010 over de digitale agenda voor Europa (10130/10).

5 COM(2010) 2020 en conclusies van de Europese Raad van 25 en 26 maart 2010 (EUCO 7/10).

aanvallen op informatiesystemen[6] aangenomen. Het heeft tot doel de strijd tegen cybercriminaliteit op te voeren door de strafrechtelijke stelsels van de lidstaten op elkaar af te stemmen en de samenwerking tussen gerechtelijke en andere autoriteiten te verbeteren. Voorts worden bepalingen ingevoerd om af te rekenen met nieuwe vormen van cyberaanvallen, in het bijzonder botnets. Ter aanvulling daarop heeft de Commissie tegelijkertijd een voorstel[7] ingediend voor een nieuw mandaat ter versterking en modernisering van het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) om het vertrouwen en de beveiliging van netwerken te verbeteren. Door de versterking en de modernisering van ENISA zullen de EU, de lidstaten en particuliere belanghebbenden hun capaciteiten en paraatheid om problemen op het vlak van cyberveiligheid te voorkomen, op te sporen en te verhelpen, verder kunnen ontwikkelen.

Ten slotte en niet het minst tonen de DAE, het Actieplan ter uitvoering van het programma van Stockholm[8] en de EU-interne-veiligheidsstrategie in actie[9] duidelijk aan dat de Commissie vastbesloten is een digitale omgeving op te bouwen waarin elke Europeaan zijn of haar economisch en sociaal potentieel ten volle tot uiting kan laten komen.

In deze mededeling wordt een balans opgemaakt van de bereikte resultaten sinds de vaststelling van het actieplan voor bescherming van kritieke informatie-infrastructuur in 2009. Zij bevat een beschrijving van de volgende geplande stappen voor elke actie op Europees en internationaal vlak. Voorts wordt aandacht geschonken aan de mondiale dimensie van de uitdagingen en het belang om de samenwerking tussen de lidstaten en de particuliere sector op nationaal, Europees en internationaal vlak te verbeteren, om een antwoord te bieden op de internationale onderlinge afhankelijkheid.

2. EEN SCENARIO IN ONTWIKKELING

Uit de effectbeoordeling bij het actieplan voor bescherming van kritieke informatie-infrastructuur[10] en een ruim gamma van analyses en rapporten van particuliere en openbare belanghebbenden blijkt niet alleen duidelijk dat Europa sociaal, politiek en economisch van ICT afhankelijk is, maar ook dat het aantal, de omvang, de complexiteit en de potentiële impact van – natuurlijke of door de mens veroorzaakte – bedreigingen gestaag toenemen.

Nieuwe en technologisch complexere bedreigingen hebben de kop opgestoken. De mondiale geopolitieke dimensie daarvan wordt steeds duidelijker. Thans zien wij een trend waarin ICT voor politieke, economische en militaire overheersing wordt gebruikt, inclusief door middel van offensieve capaciteiten. 'Cyberoorlogsvoering' of 'cyberterrorisme' worden in dit verband soms genoemd.

Voorts zijn bepaalde regimes, zoals in de recente gebeurtenissen in het zuidelijke Middellandse Zeegebied tot uiting is gekomen, bereid en in staat om de toegang van hun eigen burgers tot IT-communicatiemiddelen – met name internet en mobiele communicatie –

---

6 COM(2010) 517 definitief.
7 COM(2010) 521.
8 COM(2010) 171.
9 COM(2010) 673.
10 SEC(2009) 399.

af te sluiten of te verstoren om politieke redenen. Dergelijke eenzijdige nationale ingrepen kunnen op hun beurt weer zware gevolgen hebben voor andere delen van de wereld[11].

Om een vollediger begrip te krijgen van deze uiteenlopende bedreigingen, kan het nuttig zijn deze in de volgende categorieën onder te brengen:

– **exploitatie**, zoals geavanceerde aanhoudende bedreigingen ("advanced persistent threats")[12] voor economische en politieke spionagedoeleinden (bv. GhostNet[13]), identiteitsdiefstal, de recente aanvallen tegen het emissiehandelssysteem[14] of tegen IT-systemen van regeringen[15];

– **verstoring**, zoals verstikkingsaanvallen (Distributed Denial of Service) of spamming door middel van botnets (bv. het Conficker-netwerk van 7 miljoen machines en het in Spanje gelokaliseerde Mariposa-netwerk van 12,7 miljoen machines[16]), Stuxnet[17] en het afsnijden van communicatiemiddelen;

– **vernietiging**, een scenario dat zich in werkelijkheid nog niet heeft voorgedaan maar dat gelet op de toenemende alomtegenwoordigheid van ICT in kritieke informatie-infrastructuur (bv. intelligente netwerken ("smart grids") en watersystemen) niet kan worden uitgesloten voor de komende jaren[18].

3. DE EUROPESE UNIE EN DE MONDIALE CONTEXT

De voor ons liggende uitdagingen zijn niet specifiek voor de Europese Unie (EU) en kunnen niet door de EU alleen worden overwonnen. De alomtegenwoordigheid van ICT en van het internet maakt efficiëntere, vlottere en rendabelere communicatie, coördinatie en samenwerking tussen belanghebbenden mogelijk en leidt tot een dynamisch ecosysteem van innovatie in alle domeinen van het leven. Bedreigingen kunnen nu echter waar ook ter wereld oprijzen en hebben ten gevolge van de mondiale verwevenheid op elke plaats ter wereld een invloed.

Een zuiver Europese aanpak volstaat niet om de voor ons liggende uitdagingen te beantwoorden. Alhoewel het opbouwen van een coherente en op samenwerking berustende aanpak binnen de EU als doelstelling belangrijker dan ooit is, moet deze aanpak ingebed zijn

---

11 Gezamenlijke mededeling over een partnerschap voor democratie en gedeelde welvaart met het zuidelijke Middellandse Zeegebied; COM(2011) 200 van 8.3.2011.

12 D.w.z. onafgebroken en gecoördineerde aanvallen tegen regeringsinstanties en de overheidssector. Dit is nu ook een probleem aan het worden voor de particuliere sector (zie het "RSA 2011 cybercrime trends report").

13 Zie de verslagen van het project Information Warfare Monitor: "Tracking GhostNet: investigating a Cyber Espionage Network" (2009) en "Shadows in the Cloud: Investigating Cyber Espionage 2.0" (2010).

14 Zie Q&A op: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr.

15 Bv. de recente aanvallen tegen de Franse regering.

16 Zie OESO/IFP-project over "Future Global Shocks", "Reducing systemic cyber-security risks", 14 januari 2011, op http://www.oecd.org/dataoecd/3/42/46894657.pdf.

17 Zie http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis.

18 Zie World Economic Forum, Global Risks 2011.

in een strategie van mondiale coördinatie, waarbij aansluiting wordt gezocht bij sleutelpartners, zowel individuele landen als betrokken internationale organisaties.

Wij moeten werken aan een mondiaal inzicht in de risico's die verbonden zijn aan het wijdverspreide, massale gebruik van ICT door alle segmenten van de samenleving. Meer zelfs, wij moeten strategieën uitdenken om deze risico's passend en effectief te beheren – dat wil zeggen te voorkomen, te bestrijden, te beperken en te beantwoorden. In de oproep van de DAE luidt het dat "*de samenwerking tussen de betrokken actoren op mondiaal niveau [moet] worden georganiseerd, wil men de beveiligingsrisico's efficiënt bestrijden en terugdringen*" en wordt tot doel gesteld "*samen [te] werken met belanghebbenden van over de hele wereld, met name om het **mondiale risicobeheer** in de digitale en fysieke omgeving te versterken en internationaal gecoördineerde gerichte maatregelen te nemen tegen computergebaseerde misdaad en aanvallen tegen de beveiliging*".

4. TENUITVOERLEGGING VAN HET ACTIEPLAN VOOR BESCHERMING VAN KRITIEKE INFORMATIE-INFRASTRUCTUUR: ENKELE AANDACHTSPUNTEN

Het volledige verslag van de verwezenlijkingen en de volgende stappen van het actieplan voor de bescherming van kritieke informatie-infrastructuur is beschikbaar in de bijlage. Hier volgen enkele aandachtspunten in de stand van zaken.

4.1. Paraatheid en preventie:

- Het **Europees forum van lidstaten** (EFMS) heeft aanzienlijke vooruitgang geboekt in het bevorderen van overleg en uitwisseling tussen betrokken autoriteiten over goede beleidspraktijken met betrekking tot de veiligheid en veerkracht van ICT-infrastructuren. EFMS wordt door de lidstaten erkend als een belangrijk platform voor discussie en uitwisseling van goede beleidspraktijken[19]. De toekomstige activiteiten van het forum kunnen op de steun van ENISA blijven rekenen en zullen worden toegespitst op samenwerking tussen nationale/gouvernementele computercalamiteitenteams (Computer Emergency Response Teams - CERT's), waarbij economische en regelgevende stimulansen voor beveiliging en veerkracht worden vastgesteld (met inachtneming van de toepasselijke regels inzake mededinging en staatssteun), de "gezondheidstoestand" van de cyberspace in Europa wordt geëvalueerd, pan-Europese oefeningen op gang worden gebracht, alsook wordt gediscussieerd over prioriteiten met betrekking tot het internationale bereik op het vlak van beveiliging en veerkracht.

- Het **Europees publiek-privaat partnerschap voor veerkracht** (EP3R) is gelanceerd als een Europawijd beheerskader voor de veerkracht van ICT-infrastructuur. Het heeft tot doel de publiek-private samenwerking op het gebied van strategische EU-beleidsaangelegenheden betreffende beveiliging en veerkracht te stimuleren. ENISA heeft een faciliterende rol gespeeld in de activiteiten van EP3R en voorziet, overeenkomstig het voorstel van de Commissie van 2010 tot modernisering van ENISA in een duurzaam langetermijnkader voor EP3R. EP3R zal ook dienen als platform voor kwesties op het vlak van beveiliging en veerkracht die een internationaal bereik hebben wat betreft beleid,

[19] In haar antwoord op het vijfde verslag van de commissie voor de Europese Unie van het Britse Hogerhuis over het actieplan voor de bescherming van kritieke informatie-infrastructuur verklaart de regering van het Verenigd Koninkrijk dat EFMS een succes is geweest en een reële behoefte van beleidsvoerders om ervaring te kunnen uitwisselen aan het licht heeft gebracht.

economie en marktwerking, in het bijzonder om het beheer van mondiale risico's van ICT-infrastructuren te versterken.

- Er is een **minimumset van basiscapaciteiten en -diensten**[20] tot stand gebracht met bijbehorende **beleidsaanbevelingen**[21] om nationale/gouvernementele CERT's efficiënt te laten functioneren en hen een essentiële rol te laten vervullen bij de nationale capaciteit voor paraatheid, informatiedeling, coördinatie en respons. Deze resultaten zullen dienen als bouwsteen om tegen 2012 met de steun van ENISA in alle lidstaten een netwerk van goed functionerende nationale/gouvernementele CERT's op te richten. Dit netwerk zal de ruggengraat vormen van het Europees stelsel voor informatiedeling en alarm (EISAS) voor burgers en mkb's, dat tegen 2013 met nationale middelen en -capaciteiten moet worden opgebouwd.

4.2. Detectie en respons

- ENISA heeft een werkschema op hoog niveau opgesteld om tegen 2013 een Europees informatiedelings- en alarmeringssysteem (**EISAS**) te ontwikkelen[22], waarbij wordt voortgebouwd op de uitvoering van *basisdiensten* op het niveau van nationale/gouvernementele CERT's en van *interoperabiliteitsdiensten* voor nationale informatiedelings- en alarmeringssystemen die in EISAS geïntegreerd moeten worden. Passende bescherming van persoonsgegevens vormt één van de sleutelelementen van deze activiteit.

4.3. Mitigatie en herstel

- Tot op heden hebben slechts 12 lidstaten oefeningen in respons op grootschalige incidenten van netwerkbeveiliging en noodherstel georganiseerd[23]. ENISA heeft een **gids voor goede praktijken voor nationale oefeningen**[24] opgesteld, alsmede **beleidsaanbevelingen** over de ontwikkeling van nationale strategieën[25] ter ondersteuning van de activiteiten van lidstaten, die nog verder moeten worden opgevoerd.

- De eerste **pan-Europese oefening voor grootschalige incidenten van netwerkbeveiliging** (Cyber Europe 2010) heeft plaatsgevonden op 4 november 2010. Alle lidstaten waren hierbij betrokken en 19 lidstaten, plus Zwitserland, Noorwegen en IJsland, hebben actief aan de oefening deelgenomen. Toekomstige pan-Europese cyberoefeningen zullen ongetwijfeld voordeel halen uit een gemeenschappelijk kader, dat voortbouwt op nationale rampenplannen en deze met elkaar verbindt, en zodoende voorziet in basismechanismen en -procedures voor communicatie en samenwerking tussen de lidstaten.

---

20 Zie http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

21 Zie http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

22 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

23 Bron: ENISA.

24 Zie http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

25 Zie http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

4.4. Internationale samenwerking

- In het kader van EFMS zijn **Europese beginselen en richtsnoeren voor veerkracht en stabiliteit van het internet**[26] besproken en verder ontwikkeld. De Commissie zal deze beginselen bespreken en promoten bij de desbetreffende belanghebbenden, in het bijzonder het bedrijfsleven (via EP3R), zowel bilateraal met belangrijke internationale partners, met name de VS, als multilateraal. Zij zal dit doen, binnen haar bevoegdheden, in fora als de G8, de OESO, de NAVO (met name op basis van haar nieuw strategisch concept, dat is aangenomen in november 2010, en de activiteiten van de Cooperative Cyber-defense Center of Excellence), de ITU (in de context of capaciteitsopbouw op het gebied van cyberveiligheid), de OVSE (via haar forum voor samenwerking inzake veiligheid); de ASEAN, Meridian, enz.[27] Het is de bedoeling deze beginselen en richtsnoeren om te vormen tot een gedeeld kader voor een internationaal collectief engagement voor veerkracht en stabiliteit van het internet op lange termijn.

4.5. Criteria voor Europese kritieke infrastructuur in de ICT-sector

- De technische discussie in EFMS heeft geleid tot een **eerste ontwerp van ICT-sectorspecifieke criteria** voor de identificatie van Europese kritische infrastructuren, met speciale aandacht voor **vaste en mobiele communicatie en het internet**. De technische discussie zal worden voortgezet en worden gevoed door de raadplegingen over de ontwerpcriteria, die op nationaal en Europees vlak (via EP3R) met het bedrijfsleven worden gehouden. De Commissie zal met de lidstaten ook de ICT-sectorspecifieke elementen bespreken die in overweging moeten worden genomen bij de herziening, in 2012, van de richtlijn inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak om dergelijke infrastructuren beter te beschermen[28].

5. WAT GEBEURT ER VERDER?

De tenuitvoerlegging van het actieplan voor de bescherming van kritieke informatie-infrastructuur heeft geleid tot positieve resultaten, in het bijzonder door de erkenning dat voor netwerk- en informatiebeveiliging samenwerking is vereist, waarbij alle belanghebbenden moeten worden betrokken. De tenuitvoerlegging stemt bovendien in ruime mate overeen met de mijlpalen en het tijdschema die in 2009 zijn vastgesteld. Toch is zelfgenoegzaamheid ongepast want zowel op nationaal als op Europees vlak moet nog veel werk worden verzet om deze inspanningen met succes te bekronen.

Ook is het zeer belangrijk dat deze inspanningen deel uitmaken van een mondiale coördinatiestrategie en dat zij een internationale dimensie krijgen, waarbij alle belanghebbenden worden betrokken, om andere regio's, landen of organisaties te bereiken die zich met soortgelijke kwesties bezighouden, en partnerschappen te ontwikkelen waarin werkwijzen en daaraan verbonden activiteiten worden gedeeld, zodat dubbel werk wordt voorkomen.

---

[26] Zie http://ec.europa.eu/information_society/policy/nis/enisa/index_en.htm.

[27] Het Meridian-proces beoogt regeringen wereldwijd te voorzien van middelen om te overleggen hoe zij beleidsmatig kunnen samenwerken op het vlak van de bescherming van kritieke informatie-infrastructuur. Zie http://meridianprocess.org/.

[28] Richtlijn 2008/114/EG van de Raad.

Wij moeten een wereldwijde cultuur van risicobeheer promoten. De klemtoon moet liggen op het bevorderen van gecoördineerde acties om elke vorm van verstoring, ongeacht of deze door de mens is veroorzaakt dan wel van natuurlijke aard is, te voorkomen, op te sporen, te beperken en erop te reageren, alsmede om cybermisdrijven van dat soort te vervolgen. Dit betekent dat gerichte actie moet worden ondernomen tegen veiligheidsrisico's en computercriminaliteit.

Daartoe **zal de Commissie**:

- **beginselen voor veerkracht en stabiliteit van het internet promoten** – Internationale beginselen voor veerkracht en stabiliteit van het internet moeten worden ontwikkeld samen met andere landen, met internationale organisaties en, waar passend, met mondiale bedrijfsorganisaties – door gebruik te maken van bestaande *fora* en processen, zoals die met betrekking tot het internetbeheer. Deze beginselen moeten dienen als een instrument waarin alle belanghebbenden hun activiteiten met betrekking tot stabiliteit en veerkracht van het internet kunnen inpassen. De Europese beginselen en richtsnoeren kunnen daartoe als basis dienen.

- **strategische internationale partnerschappen opbouwen** – Strategische partnerschappen moeten worden opgebouwd op basis van aanhoudende inspanningen in kritische domeinen als het beheer van cyberincidenten, met inbegrip van oefeningen en samenwerking tussen CERT's. Hierbij is de betrokkenheid van het bedrijfsleven, dat mondiaal opereert, van uiterst belang. De EU-VS- Werkgroep over cyberbeveiliging en cybercriminaliteit, die is opgericht tijdens de EU-VS- top van november 2010, is een belangrijke stap in deze richting. De werkgroep zal zich toeleggen op cyberincidentbeheer, publiek-private partnerschappen, bewustmaking en cybercriminaliteit. Hij zal ook mogelijkheden onderzoeken om andere regio's of landen te bereiken en met name soortgelijke problemen te behandelen om in voorkomend geval te komen tot een gemeenschappelijke aanpak en bijbehorende gemeenschappelijke activiteit en dubbel werk te voorkomen. In internationale fora, met name in het kader van de G8, dient te worden gestreefd naar een verdere verruiming van het bereik en coördinatie. Belangrijk voor succes aan Europese zijde is een goede coördinatie tussen alle EU-instellingen, de betrokken agentschappen (in het bijzonder ENISA en Europol) en de lidstaten.

- **het vertrouwen in "cloud computing" ontwikkelen** – De discussies over de beste-governancestrategieën voor opkomende technologieën met mondiale impact, zoals cloud computing, moeten verder worden aangezwengeld. Deze discussies moeten ten minste, maar niet uitsluitend, handelen over het passende beheerskader voor de bescherming van persoonsgegevens. Vertrouwen is uiterst belangrijk om er alle vruchten van te kunnen plukken[29].

Aangezien veiligheid een gedeelde verantwoordelijkheid van iedereen is, moeten alle lidstaten ervoor zorgen dat hun nationale maatregelen en inspanningen collectief bijdragen tot een gecoördineerde Europese aanpak om elke vorm van verstoring en aanval in de cyberspace te

[29] Zie bijvoorbeeld de verslagen van ENISA' "Cloud Computing Information Assurance Framework" (2009), op http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport en "Security and resilience in governmental clouds" (2011), op http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/.

voorkomen, op te sporen, te beperken en erop te reageren. In dat verband **moeten de lidstaten er zich toe verbinden**:

- **de paraatheid van de EU te vergroten door tegen 2012 een netwerk van goed functionerende nationale/gouvernementele CERT's op te zetten.** Op vergelijkbare wijze zullen ook de EU-instellingen op hun niveau tegen 2012 een CERT opzetten. Al deze inspanningen moeten hun voordeel halen uit het betrokken minimumset van basiscapaciteiten en -diensten en de bijbehorende beleidsaanbevelingen, die zijn opgesteld door ENISA, dat deze initiatieven verder zal blijven ondersteunen. Deze activiteit zal ook de ontwikkeling van een Europees informatiedelings- en alarmeringssysteem (EISAS) voor het bredere publiek tegen 2013 bevorderen.

- **een Europees rampenplan voor cyberincidenten op te zetten tegen 2012 en regelmatige pan-Europese oefeningen te houden.** Cyberoefeningen zijn een belangrijk onderdeel van een samenhangende strategie voor nationale cyberrampenplanning en herstel op nationaal en Europees vlak. Toekomstige pan-Europese cyberoefeningen moeten gebaseerd zijn op een Europees rampenplan voor cyberincidenten dat voortbouwt op nationale rampenplannen en deze met elkaar verbindt. Een dergelijk plan moet de basismechanismen en -procedures voor communicatie tussen lidstaten bevatten en, wat ook belangrijk is, het moet mee de omvang en de organisatie van toekomstige pan-Europese oefeningen helpen te bepalen. ENISA zal met de lidstaten samenwerken om tegen 2012 een dergelijk Europees rampenplan voor cyberincidenten te ontwikkelen. In dezelfde periode moeten alle lidstaten regelmatig nationale rampenplannen en respons- en hersteloefeningen ontwikkelen.

- **in internationale fora Europese gecoördineerde inspanningen te leveren en overleg te plegen over de verbetering van de veiligheid en de veerkracht van het internet.** De lidstaten moeten samenwerken, onderling en met de Commissie, om te komen tot een op beginselen of normen gebaseerde aanpak van de kwestie van mondiale stabiliteit en veerkracht van het internet. Het is de bedoeling preventie en paraatheid te bevorderen op alle niveaus en door alle belanghebbenden, om zodoende de heersende trend waarbij de discussies zich toespitsen op de aspecten van militaire en/of nationale veiligheid, om te buigen.

6. CONCLUSIE

Uit ervaring blijkt dat een zuiver nationale of regionale aanpak niet volstaat om de uitdagingen op het vlak van veiligheid en veerkracht te kunnen aangaan. De Europese samenwerking is sinds 2009 in aanzienlijke mate verbeterd en heeft bemoedigende resultaten opgeleverd, in het bijzonder de Cyber Europe 2010-oefening. Europa moet zijn inspanningen echter voortzetten om een coherente en op samenwerking gebaseerde aanpak in de EU tot stand te brengen. In dit streven van lange adem moet een gemoderniseerde ENISA haar steun aan de lidstaten, de EU-instellingen en het bedrijfsleven opvoeren.

Willen Europese inspanningen succes hebben, dan moeten zij passen in een gecoördineerde aanpak op mondiaal niveau. Daarom zal de Commissie het overleg over cyberbeveiliging bevorderen in alle relevante internationale fora.

Op 14-15 april 2011 zal het Hongaarse voorzitterschap een ministerconferentie betreffende het actieplan voor de bescherming van kritieke informatie-infrastructuur organiseren. Dit zal

een belangrijke gelegenheid zijn voor de lidstaten om zich sterker te engageren en te komen tot een betere samenwerking en coördinatie, zowel op Europees als op internationaal vlak.

BIJLAGE

Het actieplan voor de bescherming van kritieke informatie-infrastructuur: gedetailleerd overzicht van de resultaten en volgende stappen

De resultaten van de activiteiten in het kader van het actieplan voor de bescherming van kritieke informatie-infrastructuur stemmen in ruime mate overeen met de mijlpalen en het tijdschema die de Commissie in 2009 heeft vastgesteld. Hieronder worden de "resultaten" en "volgende stappen" voor alle pijlers beschreven. In deze momentopname wordt rekening gehouden met het feit dat sommige activiteiten verder zijn uitgewerkt in de Digitale agenda voor Europa (DAE) en de interne-veiligheidsstrategie in actie (ISS).

1. Paraatheid en preventie

Basisniveau van capaciteiten en diensten voor pan-Europese samenwerking

Resultaten

– In 2009 heeft ENISA, samen met de gemeenschap van computercalamiteitenteams (Computer Emergency Response Teams – CERT's) in Europa, in onderlinge overeenstemming een minimumset van basiscapaciteiten en -diensten ontwikkeld waarover de nationale/gouvernementele CERT's moeten beschikken om de pan-Europese samenwerking effectief te kunnen ondersteunen. Er is consensus bereikt over een lijst van 'behoeften' in de domeinen van operationele werking, technische capaciteiten, mandaat en samenwerking[30].

– In 2010 heeft ENISA samengewerkt met de CERT's-gemeenschap in Europa om de bovengenoemde behoeften op het vlak van de operationele werking om te zetten in een reeks beleidsaanbevelingen[31], waarbij aan de nationale/gouvernementele CERT's een sleutelrol wordt toebedeeld in het nationale potentieel voor paraatheid, informatiedeling, coördinatie en respons.

– Tot op heden hebben 20 lidstaten[32] nationale/gouvernementele CERT's ontwikkeld en hebben bijna alle andere plannen om er een op te zetten. Zoals aangekondigd in de DAE en verder verduidelijkt in de ISS, heeft de Commissie maatregelen voorgesteld om tegen 2012 een CERT voor de EU-instellingen op te zetten.

Volgende stappen

– ENISA zal de lidstaten die nog geen nationale/gouvernementele CERT hebben opgezet welke aan de bovengenoemde overeengekomen basisvereisten beantwoordt, blijven ondersteunen. Zodoende wordt gewerkt aan de doelstelling om tegen eind 2011 in alle lidstaten goed functionerende CERT's te hebben. Met deze mijlpaal is de weg geëffend voor het oprichten van een goed functionerend netwerk van CERT's op nationaal niveau **tegen 2012**, zoals voorgesteld in de DAE.

---

30 Zie http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

31 Zie http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

32 Bron ENISA.

– ENISA zal met de medewerking van de nationale/gouvernementele CERT's nagaan of en hoe de "basiscapaciteiten" moeten worden vergroot. Het is de bedoeling de capaciteit van de CERT's tot ondersteuning van de lidstaten bij het waarborgen van de veerkracht en stabiliteit van vitale ICT-infrastructuren aan te passen, zodat zij de ruggengraat worden van het Europees informatiedelings- en alarmeringssysteem (EISAS) voor burgers en mkb's, dat **tegen 2013** met nationale middelen en capaciteiten moet worden uitgebouwd, zoals aangekondigd in de ISS.

Europees publiek-privaat partnerschap voor veerkracht (EP3R).

Resultaten

– In 2009 werd EP3R gelanceerd als een Europawijd beheerskader voor de veerkracht van ICT-infrastructuren, ter bevordering van de samenwerking tussen de overheid en de bedrijfssector inzake doelstellingen van beveiliging en veerkracht, basisvereisten, goede beheerspraktijken en maatregelen. Zoals in de ISS is verklaard, zal EP3R "*samenwerken met internationale partners om het wereldwijde risicobeheer van IT-netwerken te verbeteren*". ENISA heeft de activiteiten van EP3R ondersteund.

– Er zijn raadplegingen gehouden met particuliere en openbare belanghebbenden om de doelstellingen, de beginselen en de structuur van EP3R vast te stellen en stimulansen te identificeren waarmee de betrokken belanghebbenden tot actieve deelname kunnen worden aangezet[33]. In het voorstel tot modernisering van ENISA zijn prioritaire domeinen voor EP3R aangewezen[34].

– Parallel met de vaststelling van de structuur van EP3R zijn eind 2010 drie werkgroepen gelanceerd over (a) hoofdelementen, middelen en functies voor een ononderbroken en veilige levering van elektronische communicatie in de landen; (b) basisvereisten voor veiligheid en veerkracht van elektronische communicatie; (c) behoeften inzake coördinatie en samenwerking en mechanismen om paraat te staan en te reageren ten aanzien van grootschalige verstoringen van elektronische communicatie.

– In 2010 voorzag het voorstel van de Commissie tot modernisering van ENISA in een langlopend en duurzaam kader voor EP3R. Daarin is voorgesteld dat ENISA de taak krijgt "*samenwerking tussen publieke en private belanghebbenden op EU-niveau [te] ondersteunen, onder meer door informatie-uitwisseling en bewustmaking te bevorderen, en hun inspanningen [te] faciliteren om normen voor risicobeheer en voor de beveiliging van elektronische producten, netwerken en diensten te ontwikkelen en toe te passen*".

Volgende stappen

– In 2011 zal EP3R de samenwerking tussen belanghebbenden van de overheids- en bedrijfssector blijven versterken om de veiligheid en veerkracht te verbeteren door middel van innovatieve maatregelen en instrumenten, en de taken van de belanghebbenden vast te stellen. Gebruikmakend van de faciliterende rol en steun van ENISA zullen de EP3R-werkgroepen hun eerste resultaten leveren. In de toekomst zal ook werk worden verricht

[33] Zie http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm.

[34] COM(2010) 521.

om de uitdagingen inzake cyberveiligheid van intelligente netwerken ("smart grids") aan te gaan, voortbouwend op het voorbereidende werk van de Commissie en ENISA.

– EP3R zal dienen als platform ter vergroting van het mondiale bereik van beleids-, economische en marktgebonden kwesties in verband met veiligheid en veerkracht. De Commissie heeft het voornemen EP3R aan te wenden ter ondersteuning van de activiteiten van de EU-VS-werkgroep over cyberbeveiliging en cybercriminaliteit, met het doel coherente voorwaarden voor publiek-private samenwerking te scheppen, met inachtneming van de toepasselijke regels inzake mededinging en staatssteun.

– Op lange termijn en in overeenstemming met het voorstel voor een nieuwe ENISA-verordening wordt overwogen EP3R op te nemen als een hoofdactiviteit van de gemoderniseerde ENISA.

Europees forum van lidstaten (EFMS)

Resultaten

– In 2009 werd EFMS opgericht ter bevordering van overleg en uitwisseling tussen de betrokken overheden met betrekking tot goede beleidspraktijken, teneinde beleidsdoelstellingen en prioriteiten inzake beveiliging en veerkracht van ICT-infrastructuur te delen; dit forum maakt daarbij rechtstreeks gebruik van de werkzaamheden en de steun van ENISA. EFMS komt eenmaal per kwartaal samen en wordt sinds half 2010 ondersteund door een eigen webportaal, dat door ENISA wordt beheerd.

– EFMS heeft aanzienlijke vooruitgang geboekt op het vlak van: (a) het definiëren van criteria om Europese ICT-infrastructuren te identificeren in het kader van de richtlijn inzake de identificatie van Europese kritieke infrastructuren[35]; (b) het vaststellen van Europese prioriteiten, beginselen en richtsnoeren voor veerkracht en stabiliteit van het internet; (c) de uitwisseling van goede beheerspraktijken, in het bijzonder inzake cyberoefeningen.

– EFMS wordt door de lidstaten erkend als een belangrijk platform voor discussie en uitwisseling van goede beleidspraktijken[36].

Volgende stappen

– In 2011 zal EFMS de technische discussie over ICT-criteria voor Europese kritieke infrastructuren afsluiten en de hoofdlijnen en prioriteiten op lange termijn bepalen voor pan-Europese grootschalige oefeningen in netwerk- en informatieveiligheid.

– EFMS zal verder betrokken worden bij discussies over prioriteiten voor de vergroting van het internationale bereik inzake veiligheid en veerkracht, met name wat de activiteiten van de EU-VS- Werkgroep over cyberbeveiliging en cybercriminaliteit betreft.

---

35 Richtlijn 2008/114/EG van de Raad.

36 In haar antwoord op het vijfde verslag van de commissie voor de Europese Unie van het Britse Hogerhuis over het actieplan voor de bescherming van kritieke informatie-infrastructuur verklaart de regering van het Verenigd Koninkrijk dat EFMS een succes is geweest en een reële behoefte van beleidsvoerders om ervaring te kunnen uitwisselen aan het licht heeft gebracht.

– Prioritaire domeinen voor toekomstige EFMS-activiteiten, die zullen voortbouwen op en gebruik maken van de rechtstreekse steun van ENISA, zijn[37]: het vaststellen van methoden voor effectieve samenwerking tussen nationale/gouvernementele CERT's; het afdwingen van minimumvereisten in openbare aanbestedingen ter verhoging van cyberveiligheid; het vaststellen van economische en regelgevende stimulansen voor veiligheid en veerkracht (met inachtneming van de toepasselijke regels inzake mededinging en staatssteun); het evalueren van de "gezondheidstoestand" van de cyberspace in Europa.

2. Detectie en respons

Europees informatiedelings- en alarmeringssysteem (EISAS)

Resultaten

– Twee prototypen van projecten (FISHAS en NEISAS) zijn door de Commissie gefinancierd en leveren thans hun eindresultaten.

– Uitgaande van haar haalbaarheidsstudie van 2007[38] en de analyse van relevante projecten op nationaal en Europees niveau heeft ENISA een werkschema op hoog niveau opgesteld om EISAS tegen 2013 te ontwikkelen[39].

Volgende stappen

– In 2011 zal ENISA de lidstaten ondersteunen bij de uitvoering van het EISAS-werkschema door de 'basisdiensten' te ontwikkelen die de lidstaten nodig hebben voor de invoering van hun nationaal informatiedelings- en alarmeringssysteem (ISAS), dat op basis van hun nationale/gouvernementele CERT-capaciteit wordt opgebouwd.

– In 2012 zal ENISA de 'interoperabiliteitsdiensten' ontwikkelen waarmee elk nationaal informatiedelings- en alarmeringssysteem (ISAS) zich functioneel kan inschakelen in EISAS. ENISA zal de lidstaten ook ondersteunen bij het testen van deze diensten via de gefaseerde integratie van nationale systemen.

– In de loop van 2011-2012 zal ENISA nationale/gouvernementele CERT's betrekken bij de integratie van ISAS-capaciteit in hun diensten.

3. Mitigatie en herstel

Nationale rampenplanning en alarmoefeningen.

Resultaten

– Eind 2010 hadden 12 lidstaten een nationaal rampenplan ontwikkeld en/of oefeningen gehouden voor respons ten aanzien van grootschalige incidenten in netwerkbeveiliging en noodherstel[40].

---

37 COM(2010) 251.

38 Zie http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf.

39 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

40 Zie http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

– Uitgaande van nationale en internationale ervaringen heeft ENISA een gids voor goede praktijken in nationale oefeningen opgesteld[41]; zijn met lidstaten en CERT's over heel de wereld evenementen met nationale oefeningen georganiseerd; en zijn recentelijk beleidsaanbevelingen geformuleerd met betrekking tot de ontwikkeling van nationale strategieën waarbij nationale/gouvernementele CERT's/CSIRT's een sleutelrol is toebedeeld bij het leiden van nationale oefeningen voor rampenplanning en tests, waarbij belanghebbenden uit de publieke en de particuliere sector betrokken waren[42].

Volgende stappen

– ENISA zal de lidstaten steun blijven verlenen om nationale rampenplannen te ontwikkelen en regelmatig oefeningen voor respons ten aanzien van grootschalige incidenten in netwerkbeveiliging en noodherstel te organiseren, als stap naar verdere pan-Europese coördinatie.

Pan-Europese oefening in grootschalige netwerkbeveiligingsincidenten

Resultaten

– De eerste pan-Europese oefening in grootschalige incidenten van netwerkbeveiliging (*Cyber Europe 2010*) heeft plaatsgevonden op 4 november 2010, met de medewerking van alle lidstaten. 19 lidstaten hebben actief aan de oefening deelgenomen. Daarnaast waren ook Zwitserland, Noorwegen en IJsland bij de oefening betrokken. De oefening is georganiseerd en geëvalueerd[43] door ENISA met de actieve betrokkenheid van acht lidstaten in het planningteam en de technologische ondersteuning van het Gemeenschappelijk Centrum voor onderzoek (GCO).

Volgende stappen

– In 2011 zullen de lidstaten betrokken worden bij het overleg over de doelstelling en de omvang van de volgende pan-Europese cyberoefening, die voor 2012 is gepland. De keuze voor een gefaseerde benadering, met meer diepgaande oefeningen voor een kleinere groep van lidstaten, waaraan eventueel internationale actoren zouden deelnemen, wordt overwogen. ENISA zal dit proces blijven ondersteunen.

– De Commissie verleent financiële steun aan het EuroCybex-project, waarbij in de tweede helft van 2011 een desktopoefening zal worden gehouden.

– Cyberoefeningen zijn een belangrijk onderdeel van een samenhangende strategie voor nationale en Europese cyberrampenplanning. Toekomstige pan-Europese cyberoefeningen moeten daarom gebaseerd zijn op een Europees rampenplan voor cyberincidenten dat voortbouwt op nationale rampenplannen en deze met elkaar verbindt. Een dergelijk plan moet de basismechanismen en -procedures voor communicatie tussen lidstaten bevatten en, wat ook belangrijk is, het moet mee de omvang en de organisatie van toekomstige pan-Europese oefeningen helpen te bepalen. ENISA zal samen met de lidstaten werken aan de

41 Zie http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

42 Zie http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

43 Zie http://www.enisa.europa.eu/.

ontwikkeling van een dergelijk Europees rampenplan voor cyberincidenten tegen 2012. In dezelfde periode moeten alle lidstaten op regelmatige basis nationale rampenplannen en respons- en hersteloefeningen ontwikkelen. De coördinatie die vereist is om dit resultaat te bereiken, wordt door EFMS waargenomen.

Verhoogde samenwerking tussen nationale/gouvernementele CERT's.

Resultaten

– De samenwerking tussen nationale/gouvernementele CERT's is toegenomen. Het werk van ENISA op het vlak van basiscapaciteiten voor nationale/gouvernementele CERT's, CERT-oefeningen en nationale oefeningen en beheer van cyberincidenten heeft ertoe bijgedragen de pan-Europese samenwerking tussen nationale/gouvernementele CERT's te stimuleren en te versterken.

Volgende stappen

– ENISA zal de samenwerking tussen nationale/gouvernementele CERT's blijven ondersteunen. Daartoe zal het in 2011 een analyse van de vereisten maken en richtsnoeren over een passend beveiligd communicatiekanaal met CERT's geven, met inbegrip van een werkschema voor uitvoering en toekomstige ontwikkeling. ENISA zal eveneens de operationele kloof op Europees niveau onderzoeken en verslag uitbrengen over de vraag hoe grensoverschrijdende samenwerking tussen CERT's en de betrokken belanghebbenden kan worden verbeterd, in het bijzonder voor de coördinatie van de respons in geval van incidenten.

– In de DAE worden lidstaten opgeroepen **tegen 2012** een netwerk van goed functionerende CERT's op nationaal vlak op te zetten.

4. Internationale samenwerking

Veerkracht en stabiliteit van het internet.

Resultaten

– Europese beginselen en richtsnoeren voor veerkracht en stabiliteit van het internet[44] zijn verder ontwikkeld op basis van de werkzaamheden in het EFMS.

Volgende stappen

– In 2011 zal de Commissie: de beginselen promoten en bespreken, in bilaterale samenwerking met internationale partners, en in het bijzonder de VS, maar ook in multilaterale gesprekken binnen de G8, de OESO, Meridian en de ITU; raadplegingen houden met de betrokken belanghebbenden, in het bijzonder het bedrijfsleven in Europa (via EP3R) en internationaal (via het forum voor internetbeheer en andere passende fora); en discussies bevorderen met belangrijke internetspelers/-organisaties.

[44] Zie http://ec.europa.eu/information_society/policy/nis/enisa/index_en.htm.

– In 2012 zullen de internationale partners verzocht worden om op basis van beginselen en richtsnoeren te komen tot een gedeeld kader voor een internationaal collectief engagement voor veerkracht en stabiliteit van het internet op lange termijn.

Mondiale oefeningen in herstel en mitigatie van grootschalige internetincidenten

Resultaten

– Zeven lidstaten[45] hebben als internationale partner deelgenomen aan de cyberoefening Cyber Storm III in de VS. De Commissie en ENISA hebben deelgenomen als waarnemer.

Volgende stappen

– In 2011 zal de Commissie met de VS, onder toezicht van de EU-VS-werkgroep over cyberveiligheid en cybercriminaliteit, een gemeenschappelijk programma en werkschema opstellen in het vooruitzicht van gemeenschappelijke/gesynchroniseerde transcontinentale cyberoefeningen in 2012/2013. Voorts zullen de mogelijkheden worden overwogen om in een ruimer verband met andere regio's of landen met soortgelijke problemen te komen tot een gemeenschappelijke aanpak en ontwikkeling van activiteiten.

5. Criteria voor Europese kritieke infrastructuur in de ICT-sector

Sectorspecifieke criteria voor het identificeren van Europese kritieke infrastructuur voor de ICT-sector

Resultaten

– De technische discussie over sectorspecifieke criteria voor ICT in het EFMS heeft geleid tot het ontwikkelen van ontwerpcriteria voor vaste en mobiele communicatie en het internet.

Volgende stappen

– EFMS zal de technische discussie over sectorspecifieke criteria voor ICT voortzetten om tegen eind 2011 te komen tot een volledige lijst. Parallel daarmee worden door een aantal lidstaten en op Europees niveau via EP3R raadplegingen met de particuliere sector gehouden over ontwerpcriteria voor ICT.

– De Commissie zal met de lidstaten de ICT-sectorspecifieke elementen bespreken die in aanmerking komen voor de herziening van Richtlijn 2008/114/EG inzake de identificatie van Europese kritieke infrastructuren in 2012.

–

[45] FR, DE, HU, IT, NL, SE en UK.