EUROPESE COMMISSIE

Brussel, 28.3.2012
COM(2012) 140 final

MEDEDELING VAN DE COMMISSIE AAN DE RAAD EN HET EUROPEES PARLEMENT

De aanpak van criminaliteit in het digitale tijdperk – Oprichting van een Europees Centrum voor de bestrijding van cybercriminaliteit

MEDEDELING VAN DE COMMISSIE AAN DE RAAD EN HET EUROPEES PARLEMENT

De aanpak van criminaliteit in het digitale tijdperk – Oprichting van een Europees Centrum voor de bestrijding van cybercriminaliteit

1. INLEIDING: HET EUROPESE ANTWOORD OP GRENSOVERSCHRIJDENDE CRIMINALITEIT

Het internet is een vast en onmisbaar onderdeel van onze samenleving en economie geworden. Tachtig procent van de jonge Europeanen houdt via online sociale netwerken contact met elkaar en met de wereld[1], en wereldwijd bedraagt de jaarlijkse omzet van de elektronische handel ongeveer 8 biljoen Amerikaanse dollar[2]. Maar nu persoonlijke en handelscontacten steeds vaker via het internet verlopen, blijven ook de cybercriminelen niet achter: mondiaal wordt elke dag meer dan een miljoen mensen het slachtoffer van cybercriminaliteit[3]. Het scala aan criminele activiteiten op het internet is breed en omvat onder meer de verkoop van gestolen kredietkaarten (voor minder dan één euro), diefstal van identiteitsgegevens, kindermisbruik en ernstige cyberaanvallen op instellingen en infrastructuur.

Cybercriminelen brengen de samenleving grote schade toe. Volgens een recent verslag zou cybercriminaliteit wereldwijd jaarlijks ongeveer 388 miljard Amerikaanse dollar opbrengen, en daarmee winstgevender zijn dan de mondiale handel in marihuana, cocaïne en heroïne[4]. Die informatie moet voorzichtig worden geïnterpreteerd, omdat de ramingen van de opbrengsten kunnen verschillen naargelang de manier waarop cybercriminaliteit wordt gedefinieerd. De consensus is echter dat cybercriminaliteit bijzonder winstgevend is, weinig risico's meebrengt, zich snel uitbreidt en veel schade veroorzaakt. Nu het bevorderen van economische groei absolute prioriteit heeft, is het zeer belangrijk dat de strijd tegen cybercriminaliteit wordt opgevoerd, opdat de burgers en de ondernemingen vertrouwen blijven houden in de veiligheid van communicatie en handel via het internet. Dit zal ook de groeidoelstellingen van de Europa 2020-strategie[5] en de digitale agenda voor Europa[6] ten goede komen.

De digitale revolutie van de voorbije jaren valt in de eerste plaats toe te schrijven aan het feit dat het internet vrij is. Een open internet kent noch nationale grenzen noch een wereldwijde controlestructuur. Overeenkomstig het Handvest van de grondrechten van de EU moet deze onlinevrijheid worden bevorderd en beschermd, maar tegelijkertijd moeten de burgers worden beschermd tegen georganiseerde criminele bendes die van die openheid misbruik willen maken. Omdat geen enkele vorm van criminele activiteit zo grensoverschrijdend is als

---

1 Eurostat, "Toegang tot en gebruik van het internet", 14 december 2010.

2 McKinsey Global Institute, "*Internet Matters: the Net's sweeping impact on growth, jobs and prosperity*", verslag van mei 2011, geraadpleegd op 8 februari 2012.

3 Symantec, "*Norton Cybercrime Report 2011*", 7 september 2011, geraadpleegd op 6 januari 2012.

4 Ibid.

5 Europa 2020 – Een strategie voor slimme, duurzame en inclusieve groei (COM(2010) 2020 van 3 maart 2010).

6 Een digitale agenda voor Europa (COM(2010) 245 definitief van 26 augustus 2010).

cybercriminaliteit, zullen de rechtshandhavingsinstanties zowel met publieke als particuliere belanghebbenden over de nationale grenzen heen op een gecoördineerde manier moeten samenwerken. Juist op dit punt blijkt de EU een grote meerwaarde te kunnen bieden.

De Europese Unie heeft reeds verschillende initiatieven ontwikkeld om cybercriminaliteit te bestrijden, zoals de richtlijn van 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en een voorstel voor een richtlijn over aanvallen op informatiesystemen, dat het gebruik van instrumenten voor het plegen van cyberdelicten, en dan vooral botnets[7], strafbaar stelt en dat in 2012 zou moeten worden aangenomen. Europol is actiever geworden in de strijd tegen cybercriminaliteit en heeft een belangrijke rol gespeeld in de recente "Operation Rescue", waarbij de politie 184 vermoedelijke daders van kindermisbruik heeft aangehouden en meer dan 200 slachtoffers van kindermisbruik heeft geïdentificeerd, na een van de grootste onderzoeken die rechtshandhavingsinstanties wereldwijd ooit op touw hebben gezet. Dankzij de hulp van de analisten van Europol bij het kraken van de beveiligingskenmerken van een belangrijke centrale computerserver van het netwerk konden de identiteit en de activiteiten van de vermoedelijke daders worden ontdekt.

De bestrijding van cybercriminaliteit, waarvoor het Verdrag van de Raad van Europa inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken[8] het belangrijkste rechtsinstrument is, blijft een topprioriteit. De bestrijding van cybercriminaliteit is opgenomen in de EU-beleidscyclus tegen georganiseerde en ernstige internationale misdaad[9] en is een vast onderdeel van de inspanningen om op EU-niveau een gezamenlijke strategie inzake internetveiligheid te ontwikkelen. De EU onderhoudt ook nauwe contacten met internationale partners, bijvoorbeeld in de gemeenschappelijke werkgroep van de EU en de VS op het gebied van internetveiligheid en cybercriminaliteit.

Hoewel er dus vooruitgang is geboekt, zijn er op Europees niveau nog altijd diverse factoren die het onderzoek van cybercriminaliteit en de vervolging van daders belemmeren, zoals de grenzen van de jurisdicties, onvoldoende capaciteit om informatie te delen, technische moeilijkheden bij het traceren van daders van cyberdelicten, verschillen in onderzoeks- en forensische capaciteit, gebrek aan opgeleid personeel en onvoldoende samenwerking met andere belanghebbenden die verantwoordelijk zijn voor internetveiligheid. Via het stabiliteitsinstrument pakt de EU de zich snel ontwikkelende grensoverschrijdende cyberdreigingen ook aan in ontwikkelings- en overgangslanden, waar het vaak ontbreekt aan de nodige capaciteit om deze vorm van georganiseerde criminaliteit te bestrijden.

Met het oog op deze problemen heeft de Commissie van haar voornemen een Europees Centrum voor de bestrijding van cybercriminaliteit op te richten, een van de prioriteiten van

---

7 Voorstel voor een richtlijn van het Europees Parlement en de Raad over aanvallen op informatiesystemen, COM (2010)517 definitief, 30 september 2010. Botnets zijn netwerken van computers die zijn besmet met kwaadaardige software, die kunnen worden ingezet voor specifieke acties, zoals cyberaanvallen.

8 Verdrag van de Raad van Europa inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23 november 2001, ook bekend als het Verdrag van Boedapest. Bij het verdrag hoort ook een *Aanvullend Protocol bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken* betreffende de strafbaarstelling van handelingen van racistische of xenofobische aard verricht via computersystemen.

9 De EU-beleidscyclus tegen georganiseerde en ernstige internationale misdaad, die de jaren 2011/2013 bestrijkt, heeft acht prioriteiten. Een daarvan is het opvoeren van de strijd tegen cybercriminaliteit en het criminele misbruik van het internet door georganiseerde criminele bendes.

de interneveiligheidsstrategie gemaakt[10]. Zij heeft op verzoek van de Raad[11] onderzocht of het haalbaar is een dergelijk centrum op te richten[12] en stelt nu voor om binnen Europol een Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) op te richten, dat het zenuwcentrum moet worden van de strijd tegen cybercriminaliteit in de EU. In deze mededeling, die op basis van de haalbaarheidsstudie is opgesteld, worden de voorgestelde kerntaken van het EC3 toegelicht en wordt uitgelegd waarom het bij Europol moet worden ondergebracht en hoe het kan worden opgericht. Voordat het EC3 volledig operationeel kan worden, moet echter nog worden bekeken over welke budget het moet kunnen beschikken. Bij de geplande herziening van de rechtsgrondslag van Europol zal rekening worden gehouden met de oprichting van het centrum.

2. VOORSTEL VOOR DE OPRICHTING VAN EEN EUROPEES CENTRUM VOOR DE BESTRIJDING VAN CYBERCRIMINALITEIT

Het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) moet met eerbiediging van het subsidiariteitsbeginsel meerwaarde bieden en daarom wordt voorgesteld dat het EC3 zich bezighoudt met de volgende belangrijke vormen van cybercriminaliteit:

i) cyberdelicten die worden gepleegd door georganiseerde criminele bendes, en dan vooral de delicten die zeer winstgevend zijn, zoals internetoplichterij;

ii) cyberdelicten waarbij de slachtoffers ernstige schade wordt berokkend, zoals seksuele uitbuiting van kinderen via het internet; en

iii) cyberdelicten (waaronder cyberaanvallen) waarbij de kritieke infrastructuur en informatiesystemen in de Unie worden geschaad[13].

Omdat cybercriminaliteit voortdurend evolueert, moet het EC3 ook maatregelen kunnen nemen op verzoek van de lidstaten en kunnen reageren op nieuwe cyberdreigingen waarmee de Unie wordt geconfronteerd.

2.1. Kerntaken van het Europees Centrum voor de bestrijding van cybercriminaliteit en verwachte resultaten

Het EC3 zou vier kerntaken moeten hebben:

a) Fungeren als Europese knooppunt voor informatie over cybercriminaliteit

Het is de bedoeling om de politiegegevens te verrijken met informatie over cybercriminaliteit uit een breed scala van openbare, particuliere en open bronnen. Op die manier zouden de huidige leemten in de informatie waarover de voor internetveiligheid en de bestrijding van cybercriminaliteit verantwoordelijke instanties beschikken, geleidelijk worden opgevuld. Er

---

10 "Tegen 2013 zal de EU […] een cybercriminaliteitscentrum oprichten, dat de lidstaten en de EU-instellingen in staat zal stellen om hun operationele en analytische capaciteit voor onderzoek en samenwerking met internationale partners op te voeren", De EU-interneveiligheidsstrategie in actie: vijf stappen voor een veiliger Europa (COM(2010) 673 definitief, 22 november 2010).

11 Conclusies van de Raad over een actieplan ter uitvoering van de gecoördineerde strategie tegen cybercriminaliteit, 3010e Raad Algemene Zaken, Luxemburg, 26 april 2010.

12 *Feasibility study for a European Cybercrime Centre, Final Report, February 2012.*

13 Zoals gedefinieerd in Richtlijn 2008/114/EG van de Raad van 8 december 2008. Deze richtlijn wordt momenteel herzien. Het EC3 zal rekening houden met verdere ontwikkelingen.

zou informatie worden geïntegreerd over cyberdelicten, de methoden die door de daders worden toegepast en de verdachten. Hierdoor zou de kennis over cybercriminaliteit toenemen en zouden cyberdelicten beter kunnen worden voorkomen, opgespoord en vervolgd. Ook zou het creëren van banden tussen rechtshandhavingsinstanties, computercrisisteams (CERT's) en specialisten uit de particuliere sector op het gebied van beveiliging van informatie- en communicatietechnologieën worden bevorderd. De informatie moet worden gedeeld met inachtneming van de vertrouwelijkheidsovereenkomsten en –regels die de verschillende belanghebbenden hebben vastgesteld.

De integratie van informatie zou ook nuttig zijn voor de rapportage en het delen van informatie over cybercriminaliteit. De Commissie wil de lidstaten aanmoedigen om de melding van ernstige cyberdelicten bij de nationale rechtshandhavingsinstanties verplicht te stellen[14]. De nationale politiediensten zouden dan meer samenhangende informatie over ernstige cyberdelicten kunnen verstrekken aan het EC3, dat die informatie op zijn beurt zou kunnen doorgeven aan collega's in andere lidstaten die wellicht met hetzelfde probleem bezig zijn en gebaat zouden zijn bij die informatie.

Het doel is gaandeweg een breder beeld van de cybercriminaliteit in Europa te krijgen, hoogwaardige strategische verslagen over tendensen en dreigingen op te stellen, op basis van uitgebreide misdaadstatistieken kennis te vergaren en de operationele inlichtingen uit diverse bronnen te verbeteren.

b) Bijeenbrengen van de Europese deskundigheid op het gebied van cybercriminaliteit om de lidstaten bij de opbouw van capaciteit te ondersteunen

Het EC3 zou de lidstaten bij het tegengaan van cybercriminaliteit moeten bijstaan met deskundigheid en opleiding. In de eerste plaats moeten de rechtshandhavingsinstanties worden ondersteund, maar er zouden ook opleidingsinitiatieven voor aanklagers en rechters moeten worden genomen. Na een grondige analyse van de behoeften zouden de bestaande opleidingsinitiatieven van Europol, de Europese Politieacademie en de lidstaten beter moeten worden gestroomlijnd om ervoor te zorgen dat deze op elkaar aansluiten. Er zouden zowel diepgaande technische opleidingen als algemene opleidingen moeten worden aangeboden om bij politieambtenaren, aanklagers en rechters capaciteit voor de bestrijding van cybercriminaliteit op te bouwen.

Er zou een helpdesk cybercriminaliteit moeten worden opgericht om beste praktijken en kennis uit te wisselen en om onder andere bij cyberaanvallen of nieuwe vormen van internetoplichterij vragen van lidstaten, internationale rechtshandhavingsinstanties, aanklagers, rechters, de particuliere sector en maatschappelijke organisaties te beantwoorden.

Deze helpdesk zou steun en advies moeten bieden voor de activiteiten van deskundigen op het gebied van cybercriminaliteit, zoals de EU-taskforce cybercriminaliteit en de deskundigen op het gebied van de bestrijding van kindermisbruik via het internet, en zou daarnaast een samenwerkingsverband moeten aangaan met het netwerk van kenniscentra op het gebied van cybercriminaliteit (het project "2Centre", dat in volle ontwikkeling is) en met de onderzoeksgemeenschap.

[14] Bijvoorbeeld de delicten die zijn opgenomen in de artikelen 3 tot en met 7 van de ontwerprichtlijn over aanvallen tegen informatiesystemen (COM(2010) 517 definitief van 30 september 2010).

Het EC3 zou ook de lidstaten moeten helpen bij hun inspanningen om op basis van afgesproken normen een internetapplicatie voor de melding van cyberdelicten te ontwikkelen en in te voeren die de communicatie tussen diverse actoren (ondernemingen, nationale/gouvernementele CERT's, burgers enz.) en de nationale rechtshandhavingsinstanties en tussen de nationale rechtshandhavingsinstanties en het EC3 verzekert.

Het EC3 zou ook de uitwisseling van beste praktijken tussen rechtshandhavingsinstanties en gerecht moeten faciliteren. Om de daders van ernstige cyberdelicten beter te kunnen vervolgen, is het van het grootste belang dat het gerecht in de lidstaten zo doeltreffend mogelijk bij de strijd tegen cybercriminaliteit wordt betrokken.

c) Ondersteunen van de onderzoeken in verband met cybercriminaliteit van de lidstaten

Het EC3 zou operationele steun moeten bieden voor de onderzoeken in verband met cybercriminaliteit, bijvoorbeeld door gezamenlijke onderzoeksteams op te richten en aan te moedigen dat in lopende onderzoeken operationele informatie wordt uitgewisseld.

Het centrum zou in onderzoeken in verband met cybercriminaliteit ook hoogwaardige forensische bijstand (faciliteiten, opslag, instrumenten) en deskundigheid op het gebied van encryptie moeten bieden.

d) De spreekbuis worden van de onderzoekers van cybercriminaliteit van de rechtshandhavingsinstanties en de gerechten in de EU

Het EC3 zou mettertijd kunnen fungeren als een trefpunt voor de Europese onderzoekers van cybercriminaliteit en hun spreekbuis kunnen worden in discussies met de ICT-industrie en andere ondernemingen uit de particuliere sector, de onderzoeksgemeenschap, gebruikersverenigingen en maatschappelijke organisaties over de vraag hoe cybercriminaliteit kan worden voorkomen en hoe gerichte onderzoeksactiviteiten kunnen worden gecoördineerd.

Het EC3 zou het natuurlijke contactpunt zijn voor de activiteiten van Interpol op het gebied van cybercriminaliteit en van andere internationale politiediensten die zich met de bestrijding van cybercriminaliteit bezighouden. Het zou ook de input kunnen coördineren voor lopende initiatieven in verband met controle van het internet en voor de intergouvernementele groep van deskundigen op het gebied van cybercriminaliteit van de Verenigde Naties, die een mandaat van onbepaalde duur heeft gekregen.

Het EC3 zou ook kunnen samenwerken met organisaties als Insafe[15] om ervoor te zorgen dat voorlichtingscampagnes inspelen op de meest recent vastgestelde ontwikkelingen op het gebied van cybercriminaliteit, ter bevordering van voorzichtig en veilig internetgedrag.

2.2. Vestiging

Volgens de haalbaarheidsstudie zou het Europees Centrum voor de bestrijding van cybercriminaliteit bij Europol moeten worden ondergebracht.

Die oplossing heeft verschillende voordelen. De rol van Europol, dat reeds een mandaat heeft om cybercriminaliteit te bestrijden[16], wordt erkend door de lidstaten en andere

[15] Europees netwerk van centra die jongeren erop wijzen hoe zij veilig en verantwoordelijk gebruik kunnen maken van het internet en mobiele apparaten.

belanghebbenden, waaronder Interpol en internationale rechtshandhavingsinstanties. Europol heeft in de eerste plaats als taak een veiliger Europa te creëren voor alle burgers door de rechtshandhavingsinstanties in de Europese Unie te ondersteunen met de uitwisseling en de analyse van inlichtingen over criminaliteit.

2.3. Budget van het EC3

In de haalbaarheidsstudie zijn verschillende middelenscenario's onderzocht. Die zullen nader moeten worden beoordeeld[17], waarbij onder meer rekening zal worden gehouden met andere taken die Europol in de toekomst misschien zal moeten uitvoeren en met de algemene context van het personeelsbeleid van de EU-agentschappen. Daarbij zullen in het bijzonder de geplande herziening van de rechtsgrondslag van Europol en de lopende besprekingen in verband met het Commissievoorstel inzake de oprichting van een fonds voor interne veiligheid in aanmerking worden genomen. Het is echter duidelijk dat detachering vanuit de lidstaten nodig zal zijn.

Bij het inschatten van de benodigde middelen laat de Commissie zich leiden door drie overwegingen: ten eerste, dat in verhouding tot de massale toename van cybercriminaliteit het totale aantal onderzochte zaken slechts licht zal stijgen, ten tweede, dat de lidstaten hun eigen capaciteit voor de bestrijding van cybercriminaliteit zullen vergroten en ten derde, dat het EC3 zich enkel op bepaalde cyberdelicten zal richten.

2.4. Bestuur

Als het EC3 bij Europol wordt ondergebracht, is het belangrijk om ook andere belanghebbenden bij de strategische leiding van het centrum te betrekken. De Commissie stelt derhalve voor om binnen de beheersstructuur van Europol een eigen programmaraad voor het EC3 op te richten, die door het hoofd van het EC3 wordt voorgezeten. In die programmaraad zouden de andere belanghebbenden, zoals Eurojust, EPA, de lidstaten (vertegenwoordigd door de EU-taskforce cybercriminaliteit), Enisa en de Commissie, hun respectieve knowhow kunnen inbrengen, zonder onnodige administratieve lasten. De programmaraad moet ervoor zorgen dat het EC3 in staat is verantwoording af te leggen over zijn activiteiten op het gebied van cybercriminaliteit en dat die activiteiten worden verricht in partnerschappen waarin de knowhow van alle belanghebbenden wordt erkend en hun mandaten worden geëerbiedigd.

2.5. Samenwerking met de belangrijkste actoren

Het EC3 zou ervoor moeten zorgen dat de strijd tegen cybercriminaliteit gecoördineerd verloopt door samenwerking tussen EU-agentschappen te faciliteren en als enkel Europees contactpunt te fungeren.

a) Lidstaten

Het EC3 heeft als hoofddoel de lidstaten bij te staan in hun strijd tegen cybercriminaliteit. Met zijn helpdesk, precieze dreigingsanalyses en op basis van degelijke informatie onderbouwde operationele steun moet het EC3 zich nuttig maken voor onderzoekers van cybercriminaliteit in heel Europa. Via de EU-taskforce cybercriminaliteit zullen de lidstaten specifieke

---

[16] Besluit 2009/371/JBZ van de Raad van 6 april 2009 tot oprichting van de Europese Politiedienst (artikel 4, lid 1, en de bijlage).

[17] De beoordeling moet stroken met de totale toewijzingen op het gebied van personeel en budget voor de agentschappen in de begroting van 2013 en het volgende meerjarig financieel kader.

problemen aan de programmaraad van het EC3 kunnen voorleggen. Voorts zullen de lidstaten moeten blijven investeren in hun nationale structuren voor de bestrijding van cybercriminaliteit, zodat zij een aanspreekpunt hebben waarmee het EC3 contact kan onderhouden.

b) Europese agentschappen en andere actoren

De bevoegde agentschappen, zoals met name Eurojust, EPA en Enisa, alsook de EU-CERT, moeten rechtstreeks bij de activiteiten van het EC3 worden betrokken, niet alleen via de programmaraad van het EC3, maar in voorkomend geval ook door operationele samenwerking, voor zover die binnen hun mandaat valt.

c) Internationale partners

Als Europese spil voor informatie over cybercriminaliteit moet het EC3 een belangrijk aanspreekpunt worden voor de internationale partners op het gebied van cybercriminaliteit. Samen met Interpol en strategische partners overal ter wereld zou het EC3 ernaar moeten streven dat de strijd tegen cybercriminaliteit beter wordt gecoördineerd en dat bij de verdere ontwikkeling van cyberspace rekening wordt gehouden met het aspect rechtshandhaving.

d) Particuliere sector, onderzoeksgemeenschappen en maatschappelijke organisaties

Voor de bestrijding van cybercriminaliteit is het van het grootste belang dat er tussen de particuliere sector en de rechtshandhavingsinstanties vertrouwen wordt opgebouwd. Het EC3 zou de samenwerking tussen Europol en bestaande en nieuwe partners moeten consolideren en betrouwbare netwerken en platformen moeten opzetten voor de uitwisseling van informatie met de industrie en andere actoren, zoals de onderzoeksgemeenschap en maatschappelijke organisaties. Hierdoor zouden gemeenschappen gemakkelijker informatie kunnen uitwisselen over diverse aangelegenheden, bijvoorbeeld vroegtijdige waarschuwingen voor cyberdreigingen, zodat met taskforces kan worden gereageerd op cyberaanvallen en andere vormen van cybercriminaliteit.

Het EC3 zou ook moeten bijdragen aan de algemene inspanningen van particuliere ondernemingen met een aanzienlijk digitaal vermogen, zoals banken en internetwinkels, om cybercriminaliteit te bestrijden en er zich beter tegen te beschermen, en om bij de ontwikkeling van technologieën de zwakke punten zoveel mogelijk te beperken.

De rechtshandhavingsinstanties en de particuliere sector hebben er beide belang bij dat de ontwikkelingen op het gebied van cybercriminaliteit op de voet worden gevolgd en nieuwe werkmethoden van cybercriminelen doeltreffender worden geïdentificeerd, zodat de daders snel kunnen worden aangehouden en hun netwerken kunnen worden opgerold.

3. ROUTEKAART VOOR DE OPRICHTING VAN HET EUROPEES CENTRUM VOOR DE BESTRIJDING VAN CYBERCRIMINALITEIT

3.1. Activiteiten tot eind 2013

Om te zorgen voor de eerste operationele capaciteit zal de Commissie in nauwe samenwerking met Europol nagaan welke personele en financiële middelen er tot het einde van het huidige financieel kader nodig zijn om een team samen te stellen voor de oprichting van het EC3. Dat team zou bijvoorbeeld de voorwaarden en de organisatiestructuur van het EC3 moeten vaststellen en moeten bepalen aan welke indicatoren de resultaten van het EC3

kunnen worden afgemeten. De rol en de werking van de programmaraad zullen worden vastgesteld in samenspraak met alle daarbij betrokken belanghebbenden.

Om ervoor te zorgen dat het EC3 het contactpunt wordt waar alle informatie wordt geïntegreerd, zou het team in voorkomend geval contacten moeten leggen met het preconfiguratieteam van EU-CERT en met Enisa (in aanmerking nemend dat hun middelen beperkt zijn). Om de rapportage over cybercriminaliteit te verbeteren, zullen de bestaande systemen voor rapportage over cybercriminaliteit in de lidstaten in kaart worden gebracht om na te gaan hoe zij interoperabel kunnen worden gemaakt.

Er zou een helpdesk cybercriminaliteit moeten worden opgericht. Die helpdesk zou kunnen worden ondersteund met een speciaal beveiligd online platform. Het EC3 en zijn programmaraad zouden de huidige opleidingsinitiatieven van Europol, EPA en de Europese groep voor opleiding in verband met cybercriminaliteit kunnen beoordelen met het oog op betere coördinatie. De opleidingsbehoeften, waaronder die van rechters en aanklagers, zouden moeten worden geanalyseerd. Op basis daarvan zou een basisopleiding in verband met cybercriminaliteit kunnen worden samengesteld ten behoeve van iedereen die bij de strafrechtelijke vervolging betrokken is.

Daarnaast zal een precieze raming van de nodige personele en financiële middelen moeten worden gemaakt, zodat daarover in het volgende meerjarig financieel kader kan worden besloten. Die raming zal van invloed zijn op de verdere ontwikkeling van het EC3.

4. CONCLUSIE

Nu de georganiseerde misdaad ook gebruikmaakt van het internet, mag de rechtshandhaving niet achterblijven. De EU kan de lidstaten en de industrie de nodige instrumenten aanreiken voor de bestrijding van de moderne en zich voortdurend ontwikkelende dreiging van cybercriminaliteit, die per definitie geen grenzen kent. Als de nodige personele en financiële middelen kunnen worden vrijgemaakt, zal het Europees Centrum voor de bestrijding van cybercriminaliteit kunnen fungeren als contactpunt in de Europese strijd tegen cybercriminaliteit: het zal deskundigheid bijeenbrengen, strafonderzoeken ondersteunen, helpen bij het vinden van oplossingen voor de hele EU en de problematiek in de hele Unie onder de aandacht brengen. Op die manier zou het EC3 ertoe bijdragen dat een open internet en de legale interneteconomie worden gevrijwaard en de internetactiviteiten van de burgers en de ondernemingen van Europa worden beschermd.

De Commissie verzoekt de Raad dit voorstel te steunen en moedigt het Europees Parlement en andere belanghebbenden aan tot de ontwikkeling van het centrum bij te dragen.