COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN

Brussel, 22.5.2007
COM(2007) 267 definitief

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

Naar een algemeen beleid voor de bestrijding van cybercriminaliteit

{SEC(2007) 641}
{SEC(2007) 642}

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

Naar een algemeen beleid voor de bestrijding van cybercriminaliteit

1. Inleiding

1.1. Wat is cybercriminaliteit?

De veiligheid van de steeds belangrijker wordende informatiesystemen in onze samenlevingen heeft veel facetten en de bestrijding van cybercriminaliteit staat daarbij centraal. Zonder een algemeen aanvaarde definitie van cybercriminaliteit worden de termen "cybercriminaliteit", "computercriminaliteit", "computer gerelateerde criminaliteit" of "high-tech criminaliteit" vaak door elkaar gebruikt. In deze mededeling wordt onder 'cybercriminaliteit' verstaan "misdrijven gepleegd door gebruikmaking van elektronische communicatienetwerken en informatiesystemen of tegen dergelijke netwerken en systemen".

In de praktijk wordt de term cybercriminaliteit toegepast op drie categorieën strafbare activiteiten. Tot de eerste behoren **traditionele vormen van criminaliteit** zoals fraude of valsheid in geschrifte, maar deze categorie heeft in de context van cybercriminaliteit specifiek betrekking op misdrijven gepleegd via netwerken van elektronische communicatie en informatiesystemen (hierna: "elektronische netwerken" genoemd). De tweede categorie heeft betrekking op de publicatie van **illegaal materiaal** via elektronische media (bijvoorbeeld materiaal betreffende seksueel misbruik van kinderen of aanzetten tot rassenhaat). De derde categorie omvat **misdrijven die alleen op elektronische netwerken** voorkomen, dat wil zeggen aanvallen tegen informatiesystemen, "denial of service" (niet-functioneren) en hacking. Dit soort aanvallen kunnen ook gericht zijn tegen de cruciale kritieke infrastructuur in Europa en op veel gebieden bestaande systemen voor snelle waarschuwing aantasten, met eventueel rampzalige gevolgen voor de gehele samenleving. Alle categorieën misdrijven hebben gemeen dat zij op massale schaal kunnen worden gepleegd en met een grote geografische afstand tussen het misdrijf en de gevolgen ervan. Bijgevolg zijn de technische aspecten van de toegepaste onderzoeksmethoden vaak dezelfde. Deze gemeenschappelijke kenmerken vormen het centrale punt van deze mededeling.

1.2. De recentste ontwikkelingen op het gebied van cybercriminaliteit

1.2.1. In het algemeen

De combinatie van voortdurend evoluerende criminele activiteiten en een gebrek aan betrouwbare informatie maakt het moeilijk om een precies beeld te krijgen van de huidige situatie. Niettemin kunnen een aantal algemene trends worden vastgesteld:

- het aantal cybermisdrijven neemt toe en de criminele activiteiten worden steeds meer gesofisticeerd en geïnternationaliseerd[1];

- er zijn duidelijke aanwijzingen voor een toenemende betrokkenheid van criminele organisaties bij cybercriminaliteit;

- het aantal Europese vervolgingen op grond van grensoverschrijdende samenwerking bij rechtshandhaving stijgt echter niet.

1.2.2. Traditionele misdrijven op elektronische netwerken

De meeste misdrijven kunnen worden gepleegd met gebruikmaking van elektronische netwerken, en verscheidene soorten fraude en pogingen tot fraude zijn bijzonder vaak voorkomende en groeiende vormen van criminaliteit op elektronische netwerken. Instrumenten als identiteitsdiefstal, phishing[2], spam en kwaadaardige software kunnen worden gebruikt om op grote schaal fraude te plegen. Ook doet zich het groeiende probleem van illegale nationale en internationale internethandel voor. Daaronder valt onder meer de handel in drugs, bedreigde diersoorten en wapens.

1.2.3. Illegaal materiaal

Een toenemend aantal websites met illegaal materiaal kan in Europa worden geraadpleegd, waarbij het gaat om materiaal betreffende seksueel misbruik van kinderen, aanzetten tot terroristische activiteiten, onrechtmatige verheerlijking van geweld, terrorisme, racisme en vreemdelingenhaat. De rechtshandhaving tegen dergelijke websites is extreem moeilijk, aangezien eigenaars en beheerders van die websites zich vaak in andere landen bevinden dan het doelland, en vaak buiten de EU. De websites kunnen zeer snel worden verwijderd, ook buiten het grondgebied van de EU, en de definitie van onwettigheid verschilt aanzienlijk van staat tot staat.

1.2.4. Misdrijven die alleen op elektronische netwerken voorkomen

Aanvallen op grote schaal tegen informatiesystemen of organisaties en individuen (vaak via de zogenaamde botnets[3]) lijken zich steeds meer voor te doen. Ook werden recentelijk incidenten waargenomen met systematische, goed gecoördineerde en grootschalige rechtstreekse aanvallen tegen de kritieke informatie-infrastructuur van een staat. Dit werd verergerd door de in elkaar overgaande technologieën en het versneld onderling verbinden van informatiesystemen, hetgeen deze systemen meer kwetsbaar heeft gemaakt. Aanvallen zijn vaak goed georganiseerd en worden gebruikt voor afpersing. Er kan worden aangenomen dat die aanvallen slechts in beperkte mate worden aangegeven, deels omwille van de nadelen voor de bedrijfsactiviteiten die zouden kunnen voortvloeien uit het openbaar maken van de veiligheidsproblemen.

---

1 Het grootste deel van de verklaringen over huidige trends in deze mededeling zijn gehaald uit de studie ter beoordeling van de effecten van een mededeling betreffende cybercriminaliteit, uitgevoerd in 2006 in opdracht van de Commissie (Contract Nr. JLS/2006/A1/003).

2 Phishing is de omschrijving van pogingen om op een frauduleuze manier gevoelige informatie te verwerven, zoals paswoorden en kredietkaartgegevens, door het zich voordoen als een betrouwbare persoon in een elektronische communicatie.

3 Botnet verwijst naar een verzameling aangetaste apparaten waarop onder een gemeenschappelijk commando programma' s worden gedraaid.

1.3. Doelstellingen

Gelet op deze wijzigende leefwereld moeten dringend maatregelen worden getroffen – zowel op nationaal als op Europees niveau – tegen alle vormen van cybercriminaliteit, die steeds grotere bedreigingen vormen voor kritieke infrastructuur, samenleving, ondernemingen en burgers. De bescherming van individuen tegen cybercriminaliteit wordt vaak belemmerd door kwesties die verband houden met het bepalen van de bevoegde rechterlijke instantie, het toepasselijke recht, grensoverschrijdende rechtshandhaving of de erkenning en het gebruik van elektronische bewijsmiddelen. De hoofdzakelijk grensoverschrijdende dimensie van cybercriminaliteit verergert dergelijke moeilijkheden. Bij de aanpak van deze bedreigingen neemt de Commissie een algemeen beleidsinitiatief om de coördinatie op Europees en internationaal niveau in de bestrijding van cybercriminaliteit te verbeteren.

Het doel is de bestrijding van cybercriminaliteit op nationaal, Europees en internationaal niveau te versterken. De verdere ontwikkeling van een specifiek EU-beleid wordt met name reeds lang door de lidstaten en de Commissie als een prioriteit erkend. De klemtoon van het initiatief zal liggen op de rechtshandhavings- en strafrechtelijke aspecten van deze bestrijding en het beleid zal andere EU-maatregelen aanvullen om de veiligheid in cyberspace in het algemeen te verbeteren. Het beleid zal uiteindelijk bestaan uit: betere operationele samenwerking op het gebied van rechtshandhaving; betere politieke samenwerking en coördinatie tussen lidstaten; politieke en gerechtelijke samenwerking met derde landen; bewustmaking; opleiding; onderzoek; versterking van de dialoog met de industrie en eventueel wetgevende acties.

Het beleid over de bestrijding en vervolging van cybercriminaliteit zal worden uitgestippeld en uitgevoerd op een manier die volledig in overeenstemming is met de grondrechten, met name die van de vrijheid van meningsuiting, de eerbiediging het privé-leven, het familie- en gezinsleven en de bescherming van persoonlijke gegevens. Van elke in het kader van dit beleid getroffen wetgevende maatregel wordt de verenigbaarheid met die rechten onderzocht en met name met het Handvest van de grondrechten van de EU. Er zij opgemerkt dat alle dergelijke beleidsinitiatieven zullen worden uitgevoerd met volledige inachtneming van de artikelen 12 tot en met 15 van de zogenaamde richtlijn elektronische handel[4], wanneer dit rechtsinstrument van toepassing is.

Het doel van deze mededeling kan worden ingedeeld in drie onderdelen, die als volgt kunnen worden samengevat:

- verbetering en vergemakkelijking van de samenwerking en coördinatie tussen de in cybercriminaliteit gespecialiseerde eenheden, andere relevante overheden en andere deskundigen in de Europese Unie;

- ontwikkeling van een coherent EU-beleidskader voor de bestrijding van cybercriminaliteit, in coördinatie met de lidstaten, relevante EU- en internationale organisaties en andere belanghebbenden;

- bewustmaking van de kosten en de risico's van cybercriminaliteit.

---

[4] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (PB C 178, 17.7.200, blz. 1).

2. Bestaande rechtsinstrumenten in de bestrijding van cybercriminaliteit

2.1. Bestaande instrumenten en maatregelen op EU-niveau

Deze mededeling over het beleid inzake cybercriminaliteit consolideert de mededeling van 2001 "De informatiemaatschappij veiliger maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden"[5] (hierna "de mededeling van 2001" genoemd) en werkt deze verder uit. In de mededeling van 2001 werden passende materiële en procedurele wettelijke voorschriften voorgesteld, zowel voor binnenlandse als voor grensoverschrijdende criminele activiteiten. Daaruit vloeiden verscheidene belangrijke voorstellen voort, waaronder het voorstel dat heeft geleid tot Kaderbesluit 2005/222/JBZ over aanvallen op informatiesystemen[6]. In deze context moet eveneens worden opgemerkt dat andere, meer algemene wetgeving is vastgesteld die ook betrekking heeft op bepaalde aspecten van de bestrijding van cybercriminaliteit, zoals Kaderbesluit 2001/413/JBZ betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten[7].

Kaderbesluit 2004/68/JBZ ter bestrijding van seksuele uitbuiting van kinderen[8] is een goed voorbeeld van de bijzondere aandacht die de Commissie schenkt aan de **bescherming van kinderen**, vooral met betrekking tot de bestrijding van materiaal betreffende alle vormen van seksueel misbruik van kinderen dat illegaal gepubliceerd is met gebruikmaking van informatiesystemen, hetgeen een horizontale prioriteit is die in de toekomst zal worden gehandhaafd.

Om de uitdagingen op het gebied van veiligheid van de informatiemaatschappij aan te pakken, heeft de Europese Commissie een drieledige aanpak voor netwerk- en informatieveiligheid ontwikkeld: specifieke maatregelen inzake netwerk- en informatieveiligheid, het regelgevend kader voor elektronische communicatie en de bestrijding van cybercriminaliteit. Ofschoon deze drie aspecten tot op zekere hoogte afzonderlijk kunnen worden ontwikkeld, noopt hun onderlinge samenhang tot een strakke coördinatie. Op het verwante gebied van netwerk- en informatieveiligheid nam de Commissie in 2001 een mededeling aan over netwerk- en informatieveiligheid: een voorstel voor een Europese beleidsaanpak[9], parallel met de mededeling van 2001 over cybercriminaliteit. In de e-privacy-richtlijn (2005/58/EG) worden de aanbieders van openbare elektronische communicatiediensten verplicht de veiligheid van hun diensten te waarborgen. Daarin zijn ook voorschriften tegen spam en spyware vastgesteld. Het beleid inzake netwerk- en informatieveiligheid is intussen ontwikkeld via een aantal maatregelen, en zeer recentelijk in de mededelingen over een strategie voor een veilige informatiemaatschappij[10] waarin aan de strategie een nieuwe impuls wordt gegeven en een raamwerk wordt geboden voor de ontwikkeling van een samenhangende benadering voor netwerk- en informatieveiligheid, en betreffende de strijd tegen spam, spyware en kwaadaardige software[11], en door de oprichting

---

5 COM(2000) 890, 26.1.2001.
6 PB L 69, 16.3.2005, blz. 67.
7 PB L 149, 2.6.2001, blz. 1.
8 PB L 13, 20.1.2004, blz. 44.
9 COM(2001) 298.
10 COM(2006) 251.
11 COM(2006) 688.

in 2004 van ENISA[12]. De hoofddoelstelling van ENISA is het ontwikkelen van deskundigheid om de samenwerking tussen de publieke en de private sector te stimuleren, en de Commissie en de lidstaten bij te staan. Ook de **resultaten van onderzoek** op het gebied van technologieën om informatiesystemen te beveiligen zullen een belangrijke rol spelen in de bestrijding van cybercriminaliteit. Dienovereenkomstig worden informatie- en communicatietechnologieën alsook veiligheid vermeld als doelstellingen in het zevende EU-kaderprogramma voor onderzoek (KP 7), dat operationeel zal zijn in de periode 2007-2013[13]. De herziening van het regelgevende kader voor elektronische communicatie zou kunnen leiden tot wijzigingen om de doeltreffendheid van de bepalingen over de veiligheid van de e-privacy-richtlijn en van de universeledienstrichtlijn 2002/22/EG[14] te versterken.

2.2. Bestaande internationale instrumenten

Gelet op de globale aard van informatienetwerken, kan beleid inzake cybercriminaliteit niet doeltreffend zijn wanneer de inspanningen beperkt blijven tot de EU. Delinquenten kunnen niet alleen informatiesystemen aanvallen of misdrijven plegen vanuit een lidstaat naar een andere, maar kunnen dit ook gemakkelijk doen van buiten het rechtsgebied van de EU. Bijgevolg heeft de Commissie actief deelgenomen aan internationale overleg- en samenwerkingsstructuren, onder meer de G 8 Lyon-Rome groep voor high-tech criminaliteit en de door Interpol beheerde projecten. De Commissie volgt met name van nabij de werkzaamheden van het netwerk voor 24-uren contacten voor internationale high-tech criminaliteit (op het 24/7 netwerk)[15], waarvan wereldwijd een groot aantal staten, waaronder de meeste EU-lidstaten, lid zijn. Het G 8 netwerk is een mechanisme om de contacten tussen de deelnemende staten te bespoedigen, met 24-uren contactpunten voor zaken betreffende elektronische bewijsmiddelen en zaken waarbij dringende bijstand is vereist van buitenlandse rechtshandhavingsinstanties.

Het is duidelijk dat het belangrijkste Europese en internationale instrument op dit gebied het Verdrag inzake cybercriminaliteit van de Raad van Europa van 2001 is[16]. Dat verdrag, dat is vastgesteld en in werking is getreden in 2004, bevat gemeenschappelijke definities van verschillende soorten cybercriminaliteit en legt de basis voor een daadwerkelijke justitiële samenwerking tussen de verdragsluitende partijen. Het werd door veel staten ondertekend, waaronder de Verenigde Staten van Amerika en andere niet-Europese staten, alsook door alle lidstaten. Een aantal lidstaten heeft het verdrag of het aanvullend protocol bij het verdrag betreffende via computersystemen gepleegde handelingen van racistische en xenofobische aard echter nog niet geratificeerd. Gelet op het algemeen erkende belang van het verdrag zal de Commissie de lidstaten en relevante derde landen aanmoedigen het verdrag te ratificeren en de mogelijkheid voor de Europese Gemeenschap om partij te worden bij het verdrag, in overweging nemen.

---

12 Verordening nr. 460/2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging, (PB L 77 van 2004, 13.3.2004, blz. 1).

13 De Europese Unie heeft reeds onder het zesde kaderprogramma voor onderzoek en technologische ontwikkeling een aantal relevante en succesvolle onderzoeksprojecten ondersteund.

14 COM(2006) 334, SEC(2006) 816, SEC(2006) 817.

15 Artikel 35 van het Verdrag inzake cybercriminaliteit van de Raad van Europa.

16 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

3. Verdere ontwikkeling van specifieke instrumenten in de bestrijding van cybercriminaliteit

3.1. Versterken van de operationele samenwerking op het gebied van rechtshandhaving en opleidingsinspanningen op EU-niveau

Het ontbreken of het onvoldoende gebruiken van rechtstreekse structuren voor **grensoverschrijdende operationele samenwerking** blijft een zeer zwak punt op het gebied van vrijheid, veiligheid en recht. Traditionele wederzijdse bijstand in dringende gevallen van cybercriminaliteit is traag en ondoeltreffend gebleken en nieuwe samenwerkingsstructuren zijn nog niet voldoende ontwikkeld. Hoewel nationale justitiële en rechtshandhavingsinstanties in Europa nauw samenwerken via Europol, Eurojust en andere structuren, blijft er een duidelijke behoefte bestaan om de verantwoordelijkheden te versterken en te verduidelijken. Uit raadplegingen van de Commissie blijkt dat deze cruciale kanalen niet op optimaal worden benut. Een meer gecoördineerde Europese aanpak moet zowel operationeel als strategisch zijn en tevens de uitwisseling van informatie en beproefde methoden omvatten.

De Commissie zal in de nabije toekomst bijzondere nadruk leggen op **opleidings**behoeften. Het staat vast dat de technologische ontwikkelingen impliceren dat er voor justitiële en rechtshandhavingsinstanties een behoefte bestaat aan voortdurende opleiding inzake kwesties van cybercriminaliteit. Daarom wordt een versterkte en beter gecoördineerde financiële ondersteuning door de EU van multinationale opleidingsprogramma's overwogen. De Commissie zal ook, in nauwe samenwerking met de lidstaten en andere bevoegde instanties zoals Europol, Eurojust, de Europese Politieacademie (CEPOL) en het Europees netwerk voor justitiële opleiding (ENJO), werken aan een coördinatie op EU-niveau en het onderling verbinden van alle relevante opleidingsprogramma's.

De Commissie zal een **bijeenkomst** van rechtshandhavingsdeskundigen uit de lidstaten, Europol, CEPOL en het ENJO organiseren om te bespreken hoe de strategische en operationele samenwerking alsook de opleiding op het gebied van cybercriminaliteit in Europa in 2007 kan worden verbeterd. Onder andere de oprichting van een vast EU-contactpunt voor informatie-uitwisseling en van een EU-opleidingsplatform voor cybercriminaliteit zal worden overwogen. De bijeenkomst van 2007 zal de eerste zijn van een reeks bijeenkomsten die zijn gepland voor de nabije toekomst.

3.2. Versterken van de dialoog met de industrie

Zowel de private als de publieke sectoren hebben er belang bij om gezamenlijk methoden te ontwikkelen om schade die voortvloeit uit criminele activiteiten, vast te stellen en te voorkomen. Gedeelde participatie van de private en de publieke sector, gebaseerd op wederzijds vertrouwen en een gemeenschappelijke doelstelling om de schade te beperken, zou een doeltreffende manier kunnen zijn om de veiligheid te versterken, ook bij de bestrijding van cybercriminaliteit. De publiek-private aspecten van het cybercriminaliteitsbeleid van de Commissie zullen na verloop van tijd deel uitmaken van een gepland alomvattend EU-beleid betreffende de dialoog tussen de publieke en de private sector, waaronder het hele gebied van Europese veiligheid valt. Dit beleid zal met name verder worden uitgevoerd door het Europees forum voor onderzoek en innovatie op het gebied van veiligheid, waarvan de oprichting binnenkort door de Commissie is gepland en waaraan de relevante belanghebbenden van de publieke en de private sector zullen deelnemen.

De ontwikkeling van moderne informatietechnologieën en elektronische communicatiesystemen wordt grotendeels gecontroleerd door private ondernemers. Private ondernemingen voeren risicoanalyses uit, stellen programma's op voor de bestrijding van criminaliteit en ontwikkelen technische oplossingen om misdrijven te voorkomen. De industrie bleek zeer zeker bereid om overheidsinstanties bij te staan in de bestrijding van cybercriminaliteit, in het bijzonder bij de inspanningen om kinderporno en andere soorten illegaal materiaal op het internet te bestrijden[17].

Een andere kwestie betreft het duidelijke gebrek aan uitwisseling van informatie, deskundigheid en beproefde methoden tussen de publieke en de private sector. Om bedrijfsmodellen en -geheimen te beschermen, zijn ondernemers uit de private sector vaak terughoudend, of hebben zij geen duidelijke juridische verplichting om relevante informatie over de frequentie van misdrijven aan de rechtshandhavingsinstanties mee te delen of met hen te delen. Dergelijke informatie kan echter nuttig zijn wanneer overheden een doeltreffend en passend anti-criminaliteitsbeleid moeten uitstippelen. De mogelijkheden om sectoroverschrijdende informatie-uitwisseling te verbeteren zullen ook worden onderzocht in het licht van bestaande regels inzake de bescherming van persoonsgegevens.

De Commissie speelt al een belangrijke rol in verscheidene publiek-private structuren die betrekking hebben op cybercriminaliteit, zoals de deskundigengroep voor fraudepreventie[18]. De Commissie is ervan overtuigd dat een doeltreffend algemeen beleid voor de bestrijding van cybercriminaliteit ook een strategie moet bevatten voor samenwerking tussen betrokkenen uit de publieke en de private sector, met inbegrip van organisaties uit het maatschappelijke middenveld.

Om op dit gebied te komen tot een ruimere publiek-private samenwerking, zal de Commissie in 2007 een conferentie organiseren voor rechtshandhavingsdeskundigen en vertegenwoordigers uit de private sector, vooral internetproviders, om te bespreken hoe publiek-private operationele samenwerking in Europa kan worden verbeterd[19]. De conferentie zal alle onderwerpen behandelen die een toegevoegde waarde kunnen bieden voor beide sectoren, maar vooral:

- verbeteren van de operationele samenwerking in de bestrijding van illegale activiteiten en materiaal op het internet, specifiek op het gebied van terrorisme, materiaal betreffende seksueel misbruik van kinderen en andere illegale activiteiten die vooral gevoelig zijn vanuit het perspectief van de bescherming van kinderen ;

- de aanzet geven tot publiek-private overeenkomsten die tot doel hebben het in de hele EU blokkeren van sites met illegaal materiaal, vooral materiaal betreffende seksueel misbruik van kinderen;

---

17 Een recent voorbeeld van samenwerking op dit gebied, is de samenwerking tussen rechtshandhavingsinstanties en kredietkaartondernemingen, waarbij deze laatste de politie hebben bijgestaan bij het opsporen van kopers van online kinderporno.

18 Zie http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

19 De conferentie kan worden beschouwd als de voortzetting van het EU-Forum dat in punt 6.4 van de mededeling over computercriminaliteit werd voorgesteld.

- ontwerpen van een Europees model voor het uitwisselen van noodzakelijke en relevante informatie tussen de private en de publieke sectoren; onder andere met het oog op het scheppen van een sfeer van wederzijds vertrouwen en teneinde rekening te houden met de belangen van alle partijen;

- creëren van een netwerk van contactpunten voor rechtshandhaving zowel in de private als in de publieke sector

3.3. Regelgeving

Algemene harmonisatie van definities van misdrijven en het nationale strafrecht op het gebied van cybercriminaliteit is nog niet aangewezen, gelet op verschillende soorten misdrijven die onder dat begrip vallen. Aangezien doeltreffende samenwerking tussen rechtshandhavingsinstanties vaak afhankelijk is van het beschikken over op zijn minst gedeeltelijk geharmoniseerde definities van misdrijven, blijft het een langetermijndoelstelling om de wetgeving van de lidstaten verder te harmoniseren[20]. Wat bepaalde definities van belangrijke misdrijven betreft, werd reeds een belangrijke stap gezet in het kaderbesluit over aanvallen op informatiesystemen. Zoals hierboven beschreven zijn daarna nieuwe bedreigingen opgedoken en de Commissie volgt deze evolutie van nabij gelet op het belang van het voortdurend onderzoeken van de behoefte aan aanvullende wetgeving. De evoluerende bedreigingen worden gecontroleerd in nauwe coördinatie met het Europees programma voor de bescherming van kritieke infrastructuur.

Specifieke wetgeving tegen cybercriminaliteit moet nu echter ook worden overwogen. Een bijzondere kwestie die wetgeving kan vereisen, heeft betrekking op een situatie waarin cybercriminaliteit wordt gepleegd samen met **identiteitsdiefstal**. Over het algemeen wordt onder "identiteitsdiefstal" verstaan het gebruik van persoonlijke identificatiegegevens, bijvoorbeeld een kredietkaartnummer, als een instrument om andere misdrijven te plegen. In de meeste lidstaten zal een delinquent wellicht veeleer worden vervolgd voor fraude, of eventueel voor een ander misdrijf, dan voor identiteitsdiefstal; het eerstgenoemde wordt dan als een zwaarder misdrijf beschouwd. Identiteitsdiefstal op zich is niet in alle lidstaten strafbaar gesteld. Het is vaak gemakkelijker om het misdrijf van identiteitsdiefstal te bewijzen dan het misdrijf van fraude, zodat de EU-samenwerking op het gebied van rechtshandhaving beter gediend zou zijn mocht identiteitsdiefstal strafbaar zijn in alle lidstaten. In 2007 zal de Commissie raadplegingen beginnen om te onderzoeken of wetgeving aangewezen is.

3.4. Ontwikkeling van statistische gegevens

Het wordt algemeen aanvaard dat de momenteel beschikbare gegevens betreffende de frequentie van misdrijven ruim onvoldoende is, en in het bijzonder dat veel verbetering nodig is om gegevens tussen lidstaten te kunnen vergelijken. Om dit probleem aan te pakken, stelde de Commissie een ambitieus vijfjarenplan op in de mededeling van 7 augustus 2006 *"Ontwikkeling van een algemene en coherente EU-strategie voor het meten van de omvang van de criminaliteit en het strafrecht: een EU-actieplan 2006 – 2010"*[21]. De onder dat actieplan opgerichte deskundigengroep zou een geschikt forum kunnen zijn om relevante indicatoren te ontwikkelen om de omvang van cybercriminaliteit te meten.

---

[20] Deze langetermijndoelstelling werd reeds vermeld op bladzijde 3 van de mededeling van 2001.

[21] COM(2006) 437, 7.8.2006.

4. Verdere actie

De Commissie zal nu het algemene beleid voor de bestrijding van cybercriminaliteit verder uitwerken. Aangezien de Commissie op het gebied van strafrecht over beperkte bevoegdheden beschikt, kan dat beleid slechts een aanvulling vormen bij de maatregelen van de lidstaten en andere instanties. De belangrijkste maatregelen – die allemaal het gebruik van een, enkele of alle in punt 3 voorgestelde instrumenten impliceren – zullen ook worden ondersteund via het financieel programma "Preventie en bestrijding van criminaliteit":

4.1. De bestrijding van cybercriminaliteit in het algemeen

- Vaststellen van een sterkere operationele samenwerking tussen de justitiële en de rechtshandhavingsinstanties van de lidstaten, een maatregel die zal beginnen met de organisatie van een deskundigenvergadering in 2007 en die de oprichting van een centraal EU-contactpunt voor cybercriminaliteit zou kunnen omvatten

- Verhogen van de financiële ondersteuning van initiatieven voor betere opleiding van justitiële en rechtshandhavingsinstanties wat het behandelen van zaken van cybercriminaliteit betreft en maatregelen treffen om alle multinationale opleidingsinspanningen op dit gebied te coördineren door het oprichten van een EU-opleidingsplatform

- Bevorderen van een sterker engagement van de lidstaten en alle overheidsinstanties om doeltreffende maatregelen te nemen tegen cybercriminaliteit en om voldoende financiële middelen uit te trekken voor de bestrijding ervan

- Ondersteunen van onderzoek dat bijdraagt tot de bestrijding van cybercriminaliteit

- Organiseren van ten minste een grote conferentie (in 2007) met rechtshandhavingsinstanties en private ondernemers, vooral om de samenwerking op gang te brengen op het gebied van de bestrijding van illegale internetactiviteiten op en tegen elektronische netwerken en om een meer doeltreffende niet-persoonlijke uitwisseling van informatie te bevorderen, en gevolg geven aan de conclusies van deze conferentie van 2007 met concrete projecten van publiek-private samenwerking

- Initiatief nemen voor en deelnemen aan publiek-private maatregelen die gericht zijn op de bewustmaking, vooral van consumenten, van de kosten en de risico's van cybercriminaliteit, en tegelijkertijd vermijden dat het vertrouwen van consumenten wordt ondermijnd door alleen de negatieve aspecten van veiligheid te benadrukken

- Actief deelnemen aan en bevorderen van wereldwijde internationale samenwerking op het gebied van bestrijding van cybercriminaliteit

- De aanzet geven tot, bijdragen tot en ondersteunen van internationale projecten die overeenstemmen met het beleid van de Commissie op dit gebied, bijvoorbeeld projecten die worden beheerd door de G 8 en die consistent zijn met de landelijke en regionale strategiedocumenten (wat samenwerking met derde landen betreft)

- Concrete maatregelen treffen om alle lidstaten en relevante derde landen aan te moedigen om het Verdrag inzake cybercriminaliteit van de Raad van Europa en het aanvullend protocol daarbij te ratificeren en de mogelijkheid overwegen voor de Gemeenschap om partij te worden bij het verdrag

- Samen met de lidstaten het fenomeen van gecoördineerde en grootschalige aanvallen tegen de informatie-infrastructuur van lidstaten onderzoeken om deze te voorkomen en te bestrijden, met inbegrip van de coördinatie van reacties en de uitwisseling van informatie en beproefde methoden

4.2. De bestrijding van traditionele misdrijven op elektronische netwerken

- Een diepgaande analyse starten om een voorstel voor te bereiden voor specifieke EU-wetgeving tegen identiteitsdiefstal

- Het bevorderen van de ontwikkeling van technische methoden en procedures om fraude en illegale handel op het internet te bestrijden, ook via projecten van publiek-private samenwerking

- Werkzaamheden op specifieke gebieden voortzetten en ontwikkelen, zoals in de deskundigengroep voor preventie van fraude met girale betaalmiddelen op elektronische netwerken

4.3. Illegaal materiaal

- Maatregelen tegen specifiek illegaal materiaal verder ontwikkelen, vooral wat materiaal betreffende seksueel misbruik van kinderen en aanzetten tot terrorisme betreft en met name via de follow-up van de tenuitvoerlegging van het kaderbesluit ter bestrijding van seksuele uitbuiting van kinderen.

- De lidstaten oproepen om voldoende financiële middelen uit te trekken om de werkzaamheden van de rechtshandhavingsinstanties te versterken met bijzondere aandacht voor de identificatie van de slachtoffers van materiaal betreffende seksueel misbruik dat online is verspreid

- Maatregelen nemen en ondersteunen tegen illegaal materiaal dat minderjarigen zou kunnen aanzetten tot gewelddadig en ander ernstig onwettig gedrag, bijvoorbeeld bepaalde soorten extreem gewelddadige online videospellen

- De aanzet geven tot en het bevorderen van de dialoog tussen de lidstaten en met derde landen over technische methoden om illegaal materiaal te bestrijden alsook over procedures om illegale websites te sluiten, ook met het oog op de eventuele ontwikkeling van formele overeenkomsten over die kwestie met buurlanden en andere landen

- Op EU-niveau vrijwillige overeenkomsten ontwikkelen tussen overheidsinstanties en private ondernemers, vooral internetproviders, betreffende procedures om illegale internetsites te blokkeren en te sluiten

4.4. Follow-up

In deze mededeling werden als verdere actie een aantal maatregelen vermeld om de samenwerkingsstructuren in de EU te verbeteren. De Commissie zal deze maatregelen verder uitwerken, de vooruitgang bij de tenuitvoerlegging van deze activiteiten onderzoeken, en verslag uitbrengen aan de Raad en het Parlement.