COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN

Brussel, 26.1.2001
COM(2000) 890 definitief

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

De informatiemaatschappij veiliger maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden

Samenvatting

De overgang van Europa naar een informatiemaatschappij wordt gekenmerkt door ingrijpende veranderingen in alle aspecten van het leven: op het werk, in het onderwijs en in de vrije tijd, in de regering, de industrie en de handel. De nieuwe informatie- en communicatietechnologie brengt een ommekeer in het hart van onze economie en onze samenleving teweeg. Het welslagen van de informatiemaatschappij is van belang voor de groei, het concurrentievermogen en de werkgelegenheid in Europa, en heeft verstrekkende economische, maatschappelijke en juridische gevolgen.

De Commissie is in december 1999 met het *e*Europe-initiatief gestart om ervoor te zorgen dat Europa de voordelen van de digitale technologie kan benutten en dat in de informatiemaatschappij die nu aan het ontstaan is, niemand wordt uitgesloten. In juni 2000 heeft de Europese Raad van Feira het alomvattende actieplan *e*-Europe 2002 goedgekeurd en aangedrongen op de uitvoering ervan vóór eind 2002. In het actieplan wordt nadrukkelijk gewezen op het belang van netwerkbeveiliging en de bestrijding van computercriminaliteit.

Informatie- en communicatie-infrastructuren zijn een cruciaal onderdeel van onze economie geworden. Helaas hebben deze infrastructuren ook zwakke plekken en bieden zij nieuwe mogelijkheden voor criminele handelingen. Deze criminele activiteiten kunnen vele vormen aannemen en vele grenzen overschrijden. Hoewel er om verschillende redenen geen betrouwbare statistieken bestaan, lijdt het geen twijfel dat deze criminaliteit een bedreiging vormt voor de investeringen en bezittingen van het bedrijfsleven, en voor de veiligheid en het vertrouwen in de informatiemaatschappij. Sommige recente voorbeelden van denial of service attacks en virusaanvallen blijken grote financiële schade te hebben aangericht.

Er moet op twee fronten actie worden ondernomen: de informatie-infrastructuur moet beter worden beveiligd om criminaliteit te voorkomen, en de rechtshandhavingsinstanties moeten de nodige middelen tot hun beschikking krijgen om op te treden, met volledige inachtneming van de fundamentele rechten van het individu.

De Europese Unie heeft al een aantal stappen ondernomen om illegale en schadelijke inhoud op internet tegen te gaan, de intellectuele eigendom en persoonsgegevens te beschermen, de elektronische handel en het gebruik van elektronische handtekeningen te bevorderen en transacties beter te beveiligen. In april 1998 heeft de Commissie de resultaten van een studie over computercriminaliteit ingediend bij de Raad (de zogenoemde 'COMCRIME'-studie). In oktober 1999 concludeerde de Europese Raad van Tampere dat ook voor hightech-criminaliteit moet worden gestreefd naar gemeenschappelijke definities en straffen. Ook het Europees Parlement heeft aangedrongen op gemeenschappelijke definities van computercriminaliteit en op de onderlinge afstemming van de wetgeving, met name in het materiële strafrecht. De Raad van de Europese Unie heeft een gemeenschappelijk standpunt goedgekeurd over de onderhandelingen in de Raad van Europa over het verdrag inzake cybercriminaliteit, en heeft een aantal eerste maatregelen goedgekeurd in het kader van de strategie van de Unie ter bestrijding van hightech-criminaliteit. Sommige EU-lidstaten hebben ook actief deelgenomen aan de activiteiten van de G8 op dit gebied.

In deze mededeling wordt ingegaan op de behoefte aan en de mogelijke vormen van een algemeen beleidsinitiatief dat aansluit bij de bredere doelstellingen op het gebied van de *Informatiemaatschappij* en bij die inzake v*rijheid, veiligheid en rechtvaardigheid*, en dat erop is gericht de informatie-infrastructuur beter te beveiligen en de computercriminaliteit te bestrijden, overeenkomstig het streven van de Europese Unie om de fundamentele mensenrechten te respecteren.

Wat de korte termijn betreft is de Commissie van mening dat er duidelijk behoefte bestaat aan een EU-instrument om ervoor te zorgen dat de lidstaten doeltreffende sancties vaststellen om kinderpornografie op internet te bestrijden. De Commissie zal later dit jaar een voorstel voor een kaderbesluit indienen waarin, in het kader van een pakket maatregelen met betrekking tot de bestrijding van seksuele uitbuiting van kinderen en mensenhandel, bepalingen zijn opgenomen voor de onderlinge afstemming van de wetgeving en de straffen.

Op langere termijn zal de Commissie wetgevingsvoorstellen indienen om zowel het materiële strafrecht als het strafprocesrecht inzake hightech-criminaliteit verder op elkaar af te stemmen, waarbij de resultaten van de onderhandelingen in de Raad van Europa over het verdrag inzake cybercriminaliteit als basis zullen dienen. Overeenkomstig de conclusies van de Europese Raad van Tampere van oktober 1999, zal de Commissie ook de mogelijkheden onderzoeken voor wederzijdse erkenning van aan het proces voorafgaande gerechtelijke bevelen in het kader van onderzoeken in verband met computercriminaliteit.

Daarnaast is de Commissie voornemens de oprichting van in computercriminaliteit gespecialiseerde politie-eenheden, in de lidstaten waar die nog niet bestaan, te bevorderen, steun te verlenen voor technische scholing op het gebied van rechtshandhaving en Europese informatiebeveiligingsmaatregelen te stimuleren.

Op technisch vlak, en overeenkomstig het wettelijk kader, zal de Commissie zich richten op het bevorderen van O&O om inzicht te krijgen in kwetsbare punten, deze te verhelpen en de rechtshandhaving te ondersteunen, en op het stimuleren van kennisverspreiding.

De Commissie is ook voornemens een EU-forum op te richten waarin rechtshandhavingsinstanties, internet service providers, telecommunicatie-exploitanten, organisaties op het gebied van burgerlijke vrijheden, consumentenorganisaties, gegevensbeschermingsinstanties en andere betrokken partijen samenkomen om het wederzijds begrip en de samenwerking op EU-niveau te verbeteren. Het forum zal het publiek wijzen op de gevaren van criminelen op internet, de beste beveiligingsmethoden bevorderen, zoeken naar doeltreffende instrumenten en procedures om computercriminaliteit te bestrijden, en de verdere ontwikkeling van systemen voor vroegtijdige waarschuwing en crisisbeheer bevorderen.

OPROEP OM TE REAGEREN OP DEZE MEDEDELING

De Europese Commissie nodigt alle betrokken partijen uit om op deze mededeling te reageren. Reacties kunnen tot 23 maart 2001 per e-mail worden gestuurd naar:

infso-jai-cybercrime-comments@cec.eu.int

In principe worden alle reacties gepubliceerd op het web, tenzij de afzender uitdrukkelijk verzoekt zijn reactie niet te publiceren. Anonieme reacties worden niet gepubliceerd. De Commissie behoudt zich het recht voor reacties niet te publiceren (b.v. omdat ze beledigend zijn). De reacties zullen toegankelijk zijn via een link op de volgende website:

http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html

Deze website bevat informatie over het technische formaat en over het publicatiebeleid. Het is raadzaam deze site te raadplegen voordat u reacties instuurt.

OPENBARE HOORZITTING

De Europese Commissie organiseert ook een openbare hoorzitting voor de betrokken partijen over de in deze mededeling behandelde problematiek. Deze hoorzitting wordt op 7 maart 2001 gehouden. Tot 20 februari 2001 kunt u een verzoek indienen om tijdens deze hoorzitting een verklaring af te leggen, per e-mail:

infso-jai-cybercrime-hearing@cec.eu.int

of per post:

Europese Commissie
Kantoor BU33-5/9
Wetstraat 200
B-1049 Brussel
België

De Europese Commissie behoudt zich het recht voor om een selectie te maken van de partijen die zullen worden gehoord. Het aantal verzoeken en de wens zoveel mogelijk verschillende partijen te horen zullen daarbij het uitgangspunt vormen.

INHOUDSOPGAVE

1. KANSEN EN BEDREIGINGEN IN DE INFORMATIEMAATSCHAPPIJ

De toenemende betaalbaarheid en het groeiende gebruik van de technologie van de informatiemaatschappij zijn, evenals de globalisering van de economie, kenmerkend voor onze tijd. De verdere technologische ontwikkelingen en het toenemende gebruik van open netwerken zoals internet zullen de komende jaren nieuwe mogelijkheden creëren en nieuwe problemen oproepen.

Tijdens de top van Lissabon van maart 2000 heeft de Europese Raad gewezen op het belang van de overgang naar een concurrerende en dynamische kenniseconomie, en de Raad en de Commissie verzocht een *e*Europe-actieplan op te stellen om deze kans optimaal te benutten.[1] Dit actieplan, dat door de Commissie en de Raad is opgesteld en door de Europese Raad van Feira in juni 2000 is goedgekeurd, omvat maatregelen om voor eind 2002 netwerken beter te beveiligen en een gecoördineerde en samenhangende aanpak van computercriminaliteit te ontwikkelen.[2]

De informatie-infrastructuur is een cruciale schakel geworden in de ruggengraat van onze economie. Gebruikers moeten ervan kunnen uitgaan dat informatiediensten beschikbaar zijn en erop kunnen vertrouwen dat hun berichten en gegevens beschermd zijn tegen toegang of wijziging door onbevoegden. Dat is bepalend voor de ontwikkeling van de elektronische handel en de volledige verwezenlijking van de informatiemaatschappij.

De nieuwe digitale en draadloze technologie is reeds alomtegenwoordig. Deze technologie geeft ons bewegingsvrijheid terwijl we toch aangesloten blijven, aangesloten op talloze diensten die zijn opgebouwd uit netwerken van netwerken. De technologie geeft ons de kans om deelnemer te zijn; om te onderwijzen en te leren, om samen te spelen en te werken, om politiek betrokken te zijn. Nu de samenleving steeds afhankelijker wordt van deze technologie, zijn praktische en juridische instrumenten nodig om de bijbehorende risico's te beheersen.

De technologie van de informatiemaatschappij kan worden gebruikt voor het plegen en vergemakkelijken van verschillende strafbare feiten, en dat gebeurt ook. In handen van personen die te kwader trouw, uit boos opzet of grove nalatigheid handelen, kan deze technologie een instrument worden voor activiteiten die een bedreiging vormen voor of schade toebrengen aan het leven, de eigendommen of de waardigheid van personen, of nadelig zijn voor het algemeen belang.

Bij de traditionele beveiligingsmethode was een strikte organisatorische, geografische en structurele indeling van gegevens nodig naar gevoeligheid en categorie. Dit is niet langer de juiste aanpak in de huidige digitale wereld, waarin gegevensverwerking verspreid plaatsvindt, diensten de mobiele gebruikers volgen en interoperabiliteit van systemen een eerste vereiste is. De traditionele beveiligingsmethoden maken plaats voor nieuwe oplossingen op basis van de opkomende technologieën. Bij deze oplossingen wordt gebruik gemaakt van encryptie en digitale handtekeningen, nieuwe toegangscontrole- en authenticatietechnieken en allerlei

---

[1] Conclusies van het voorzitterschap van de Europese Raad van Lissabon van 23 en 24 maart 2000, te vinden op http://ue.eu.int/en/Info/eurocouncil/index.htm.

[2] http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm.

soorten software filters.[3] Voor een veilige en betrouwbare informatie-infrastructuur zijn niet alleen veel verschillende technieken nodig; deze moeten ook op de juiste manier worden toegepast en doeltreffend worden gebruikt. Sommige van die technieken bestaan al, maar gebruikers zijn daar vaak niet van op de hoogte, of weten niet hoe ze moeten worden gebruikt, of waarom dat nodig zou zijn.

1.1 Nationale en internationale reacties

Computercriminaliteit speelt zich overal in cyberspace af en houdt niet op bij de conventionele landsgrenzen. Dit soort strafbare feiten kan in principe vanaf iedere denkbare plaats worden gepleegd, tegen iedere computergebruiker waar ook ter wereld. Algemeen wordt erkend dat er zowel op nationaal als internationaal niveau moet worden opgetreden tegen computercriminaliteit.[4]

Op nationaal niveau ontbreekt het vaak nog aan breed en internationaal georiënteerde antwoorden op nieuwe problemen zoals netwerkbeveiliging en computercriminaliteit. In de meeste landen zijn de reacties op computercriminaliteit te veel op het nationale recht (met name het strafrecht) gericht, waarbij voorbij wordt gegaan aan alternatieve preventiemaatregelen.

Ondanks de inspanningen van internationale en supranationale organisaties vertonen de nationale wetgevingen wereldwijd opmerkelijke verschillen, onduidelijkheden of mazen, vooral waar het de strafrechtelijke bepalingen inzake privacy-schending, hacking, bescherming van het bedrijfsgeheim en illegale inhoud betreft. Er bestaan ook aanzienlijke verschillen en onduidelijkheden ten aanzien van de bevoegdheid tot het nemen van dwangmaatregelen van opsporingsdiensten (in het bijzonder met betrekking tot geëncrypteerde gegevens en onderzoeken naar internationale netwerken), de jurisdictie in strafzaken, en ten aanzien van de aansprakelijkheid van service providers die als tussenpersoon optreden enerzijds en content providers anderzijds. Richtlijn 2000/31/EG[5] betreffende de elektronische handel ondervangt dit voor zover het de aansprakelijkheid betreft van service providers die als tussenpersoon voor bepaalde diensten optreden, communicatienetwerken, caching- en hostingdiensten. Deze richtlijn verbiedt de lidstaten ook om dergelijke als tussenpersoon optredende service providers een algemene verplichting op te leggen om toe te zien op de informatie die zij doorgeven of opslaan.

Op internationaal en supranationaal niveau bestaat brede overeenstemming over het feit dat doeltreffend moet worden opgetreden tegen computercriminaliteit, en verschillende organisaties werken aan de coördinatie of harmonisatie van de activiteiten op dit gebied. De ministers van Justitie en Binnenlandse Zaken van de G8 hebben in december 1997 een reeks beginselen en een 10-punten actieplan goedgekeurd, dat door de G8-top in Birmingham van

---

3 Informatiestromen worden op alle niveaus gefilterd en gecontroleerd; van de firewall die kijkt naar datapakketjes, via het filter dat verraderlijke sofware opspoort en het e-mailfilter dat discreet spam verwijdert, tot het browserfilter dat de toegang tot schadelijk materiaal verspert.

4 Zie b.v. het *e*-Europe-actieplan op http://europa.eu.int/comm/informaion_society/eeurope/actionplan/index_en/htm, en verklaringen van Commissielid Antõnio Vitorino (op http://europa.eu.int/comm/commissioners/vitorino/speeches/2000/septembre/2000-19-09-en_brussels.pdf) en van de Franse premier Lionel Jospin (op http://www.france.diplomatie.fr/actual/evenements/cybercrim/jospin.gb.html).

5 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 ("Richtlijn inzake elektronische handel").

mei 1998 werd bekrachtigd en momenteel wordt uitgevoerd.[6] De Raad van Europa is in februari 1997 begonnen met de voorbereiding van een internationaal verdrag inzake cybercriminaliteit en zal deze werkzaamheden naar verwachting in 2001 afronden.[7] De bestrijding van cybercriminaliteit staat ook op de agenda van de bilaterale gesprekken die de Europese Commissie voert met een aantal regeringen (buiten de EU). Er is een gemeenschappelijke EG/VS task force voor de bescherming van essentiële infrastructuur opgericht.[8]

Ook de VN en de OESO zijn op dit gebied actief, en er wordt over deze problematiek gesproken in internationale fora zoals de Global Business Dialogue en de Trans-Atlantic Business Dialogue.[9]

Op het niveau van de Europese Unie is tot voor kort voornamelijk wetgeving ontwikkeld in de vorm van maatregelen op het gebied van het auteursrecht, de bescherming van het fundamentele recht op privacy, de bescherming van persoonsgegevens, voorwaardelijke-toegangdiensten, elektronische handel, elektronische handtekeningen en in het bijzonder de liberalisering van de handel in encryptieproducten, die indirect verband houden met computercriminaliteit.

In de afgelopen 3-4 jaar zijn ook een aantal belangrijke niet-wetgevende maatregelen genomen. Daaronder valt ook het Actieplan tegen illegale en schadelijke inhoud op het Internet, in het kader waarvan in de vorm van cofinanciering steun wordt verleend voor bewustmakingsacties, experimenten met het beoordelen en filteren van inhoud en met hotlines, en voor initiatieven op het gebied van de bescherming van minderjarigen en van de menselijke waardigheid in de informatiemaatschappij, kinderpornografie en het aftappen van berichten voor rechtshandhavingsdoeleinden.[10] De EU ondersteunt al heel lang O&O-

---

6 De JBZ-Raad van 19 maart 1998 heeft zich aangesloten bij de 10 door de G8 opgestelde beginselen ter bestrijding van met spitstechnologie verband houdende criminaliteit en heeft de niet-G8-lidstaten van de EU verzocht voorbereidingen te treffen om toe te treden tot het netwerk. Beschikbaar op de website van het Europees justitieel netwerk: http://ue.eu.int/ejn/index.htm.

7 De ontwerptekst is in twee talen beschikbaar op internet; in het Frans: http://conventions.coe.int/treaty/fr/projets/cybercrime.htm.
en in het Engels: http://conventions.coe.int/treaty/en/projets/cybercrime.htm.

8 Onder supervisie van de gemeenschappelijke adviesgroep van de overeenkomst tussen de EG en de VS inzake wetenschappelijke en technologische samenwerking.

9 De Verenigde Naties hebben een handboek over de preventie en bestrijding van computercriminaliteit uitgegeven (Manual on the prevention and control of computer-related crime), dat onlangs is bijgewerkt. In 1983 heeft de OESO een studie verricht naar de mogelijkheid van internationale toepassing en harmonisatie van strafwetgeving om computercriminaliteit of -misbruik aan te pakken. In 1986 werd "Computer-Related Crime: Analysis of Legal Policy" gepubliceerd, een verslag waarin een overzicht werd gegeven van de bestaande wetgeving en van voorstellen voor hervorming in een aantal lidstaten, en waarin werd aanbevolen een minimumlijst op te stellen van misbruiken die strafbaar zouden moeten worden gesteld. Tenslotte ontwikkelde de OESO in 1992 richtsnoeren voor de beveiliging van informatiesystemen, die bedoeld zijn als basis waarop staten en de particuliere sector een kader voor de beveiliging van informatiesystemen kunnen bouwen.

10 Aanbeveling 98/560/EG van de Raad van 24 september 1998 betreffende de ontwikkeling van de concurrentiepositie van de Europese industrie van audiovisuele en informatiediensten door de bevordering van nationale kaders, teneinde een vergelijkbaar en doeltreffend niveau van bescherming van minderjarigen en de menselijke waardigheid te bereiken;
Groenboek over de bescherming van minderjarigen en de menselijke waardigheid in de context van de audiovisuele en informatiediensten; COM(96) 483, oktober 1996, http://europa.eu.int/en/record/green/gp9610/protec.htm;
Mededeling van de Commissie aan de Raad, aan het Europees Parlement, aan het Economisch en Sociaal Comité en aan het Comité van de regio's - Illegale en schadelijke inhoud op het Internet (COM(96) 487 def.);

projecten die gericht zijn op het verbeteren van de veiligheid van en het vertrouwen in de informatie-infrastructuur en elektronische transacties, en heeft onlangs de kredieten daarvoor in het IST-programma verhoogd. Ook voor onderzoek en operationele projecten gericht op gespecialiseerde opleidingen voor het personeel van rechtshandhavingsinstanties en op samenwerking tussen rechtshandhavingsinstanties en het bedrijfsleven, is steun verleend in het kader van de derde-pijler-programma's STOP, FALCONE, OISIN en GROTIUS.[11]

In het actieplan inzake georganiseerde criminaliteit, dat in mei 1997 door de JBZ-Raad werd goedgekeurd en door de Europese Raad van Amsterdam werd bekrachtigd, werd de Commissie verzocht vóór eind 1998 een studie naar computercriminaliteit te verrichten. Deze studie, de zogenoemde 'COMCRIME-studie,' werd door de Commissie in april 1998 ingediend bij de multidisciplinaire werkgroep van de Raad die zich bezighoudt met de bestrijding van georganiseerde criminaliteit.[12] Deze mededeling is ten dele een vervolg op het verzoek van de JBZ-Raad.

Alvorens deze mededeling op te stellen, heeft de Commissie informeel overleg gepleegd met vertegenwoordigers van de nationale rechtshandhavingsinstanties, de instanties die toezicht houden op de gegevensbescherming[13] in de lidstaten en het Europese bedrijfsleven (voornamelijk ISP's en telecommunicatie-exploitanten).[14]

Op basis van de analyse en de aanbevelingen in de studie, de conclusies die uit het overleg kunnen worden getrokken, de nieuwe mogelijkheden die het Verdrag van Amsterdam biedt en het werk dat al is verricht door de EU, de G8 en de Raad van Europa, worden in deze mededeling verschillende mogelijkheden onderzocht voor verdere maatregelen van de EU tegen computercriminaliteit. De gekozen oplossingen mogen op EU-niveau geen belemmeringen voor of versnippering van de interne markt tot gevolg hebben en de bescherming van de grondrechten niet aantasten.[15]

Resolutie over de mededeling van de Commissie over illegale en schadelijke inhoud op het Internet (COM(96) 487 - C4-0592/96);
Resolutie van de Raad van 17 januari 1995 inzake de legale interceptie van telecommunicatieverkeer (PB C 329 van 4.11.1996, blz. 1– 6).

11 http://europa.eu.int/comm/justice_home/jai/prog_nl.htm.

12 "Legal Aspects of Computer-related Crime in the Information Society – COMCRIME." De studie werd uitgevoerd door Prof. U. Sieber van de universiteit van Würzburg, in opdracht van de Europese Commissie. Het eindverslag is beschikbaar op: http://www2.echo.lu/legal/en/crime/sieber.html.

13 Op EU-niveau is de Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens de instantie die toezicht houdt op de gegevensbescherming. Deze Groep is het onafhankelijke adviesorgaan van de EU inzake privacy en gegevensbescherming; zie de artikelen 29 en 30 van Richtlijn 95/46/EG.

14 Er werden twee vergaderingen gehouden met rechtshandhavers, op 10.12.1999 en op 1.3.2000. Op 13.3.2000 vond een vergadering plaats met vertegenwoordigers van de Internet-industrie, op 31.3.2000 met een klein aantal deskundigen op het gebied van de bescherming van persoonsgegevens. De slotvergadering met alle hierboven genoemde betrokkenen vond plaats op 17.4.2000. Notulen van de vergaderingen kunnen schriftelijk worden aangevraagd bij: Europese Commissie, Eenheid INFSO/A5, of bij: Europese Commissie, Eenheid JAI/B2, Wetstraat 200, 1049 Brussel, België.

15 EU-handvest van de grondrechten (http://europa.eu.int/comm/justice_home/unit/charte_en.htm), artikel 6 van het VEU en jurisprudentie van het Europese Hof van Justitie.

2. BEVEILIGING VAN DE INFORMATIE-INFRASTRUCTUUR

In de informatiemaatschappij nemen door de gebruiker gestuurde wereldwijde netwerken geleidelijk de plaats in van de oudere generatie van nationale communicatienetwerken. Een van de verklaringen voor het succes van internet is dat het de gebruikers toegang geeft tot de nieuwste technologie. Volgens de wet van Moore[16] verdubbelt de capaciteit van computers elke 18 maanden. De communicatietechnologie ontwikkelt zich echter in een nog hoger tempo.[17] Een van de gevolgen daarvan is, dat de hoeveelheid gegevens die via internet wordt verspreid, steeds in minder dan een jaar tijd verdubbelt.

De traditionele telefoonnetwerken werden aangelegd en geëxploiteerd door nationale organisaties. De gebruikers ervan hadden weinig keuze aan diensten en geen controle over de omgeving. De eerste gegevensnetwerken werden volgens hetzelfde principe van een centraal gecontroleerde omgeving ontwikkeld. Dat was ook te zien aan de beveiliging van deze omgeving.

Internet en andere nieuwe netwerken zitten heel anders in elkaar, en de beveiliging moet daarop worden afgestemd. Toezicht en controle spelen zich in deze netwerken voornamelijk in de periferie af, bij de gebruikers en de diensten. De kern van het netwerk is eenvoudig en doeltreffend, en voornamelijk bedoeld om informatie over te brengen. Er is slechts in beperkte mate sprake van controle op de inhoud. Pas op de eindbestemming worden de bits het geluid van een stem, het beeld van een röntgenfoto of de bevestiging van een banktransactie. Beveiliging is daarom voor het belangrijk deel een zaak van de gebruikers, omdat alleen zij de waarde kunnen beoordelen van de bits die worden verzonden of ontvangen, en kunnen bepalen welk beschermingsniveau nodig is.

De gebruikersomgeving is daarom een kernonderdeel van de informatie-infrastructuur. Daar moeten, met toestemming en medewerking van de gebruiker, beveiligingstechnieken worden toegepast en toegesneden op zijn/haar behoeften. Dit is bijzonder belangrijk, omdat mensen steeds meer activiteiten van achter de computer ondernemen. Ze werken en spelen, kijken televisie en geven betaalopdrachten, met steeds hetzelfde instrument.

Er zijn verschillende beveiligingstechnieken beschikbaar en er zijn nog nieuwe in ontwikkeling. Het wordt steeds duidelijker dat open source software de nodige voordelen biedt uit het oogpunt van veiligheid. Er is veel werk verricht op het gebied van formele methoden en criteria voor het beoordelen van de veiligheid. Het gebruik van encryptietechnieken en elektronische handtekeningen wordt onvermijdelijk, vooral met de opkomst van de draadloze toegang. Er zijn steeds meer verschillende authenticatietechnieken nodig om te voorzien in onze behoeften, die verschillen naar gelang van de omgeving waarin wij interactief bezig zijn. In sommige omgevingen willen of moeten we misschien anoniem blijven. In andere moeten we misschien bepaalde kenmerken kunnen bewijzen zonder onze identiteit prijs te geven, zoals het feit dat we volwassen zijn, of werknemer of klant van een bepaalde onderneming. In weer ander situaties moeten we misschien onze identiteit kunnen aantonen. Softwarefilters worden ook steeds verfijnder, en maken het ons mogelijk onszelf en degenen voor wie we verantwoordelijk zijn te beschermen tegen informatie die we niet

---

[16] De opmerking uit 1965 van Gordon Moore, mede-oprichter van Intel, over het tempo waarin de dichtheid van transistoren in geïntegreerde circuits toenam. Deze dichtheid verdubbelt nu ongeveer elke 18 maanden, en dit heeft rechtstreeks gevolgen voor de prijs en de capaciteit van computerchips. Veel deskundigen denken dat dit nog zeker tien jaar door zal gaan.

[17] Dankzij de nieuwste technologie kan een enkele glasvezelkabel het equivalent van 100 miljoen telefoongesprekken tegelijk verwerken.

willen, zoals ongewenste inhoud, spam mail, schadelijke software en andere vormen van aanvallen. Het aanbrengen en beheren van dergelijke beveiligingsinstrumenten op internet en andere netwerken brengt aanzienlijke kosten met zich voor de industrie en voor de gebruiker. Daarom moeten innovatie en het commercieel gebruik van beveiligingstechnieken en -diensten worden bevorderd.

Uiteraard zitten er ook veiligheidsaspecten aan de gemeenschappelijke infrastructuur van communicatieverbindingen en name servers. Gegevensoverdracht is afhankelijk van de fysieke verbindingen via welke gegevens van de ene naar de andere computer worden gezonden. Deze verbindingen moeten zo worden aangelegd en beschermd dat verzenden mogelijk blijft ondanks ongelukken, aanvallen en steeds grotere informatiestromen. Communicatie is ook afhankelijk van cruciale diensten zoals die welke worden geleverd door name servers, en in het bijzonder van het geringe aantal root name servers, die de benodigde adressen verstrekken. Deze onderdelen moet ook worden beschermd, waarbij de bescherming varieert naar gelang van het deel van de name space en de user base waar het om gaat.

Omdat wordt geprobeerd flexibiliteit te bieden en in te spelen op de behoeften van het publiek, is de informatie-infrastructuurtechnologie steeds complexer geworden, waarbij in de ontwerpfase vaak te weinig aandacht wordt besteed aan beveiliging. Bovendien zijn voor deze complexe infrastructuur steeds verfijndere en onderling verbonden computerprogramma's nodig, die soms zwakke plekken vertonen, gaten in de beveiliging, die gemakkelijk kunnen worden benut voor aanvallen. Naarmate cyberspace complexer wordt en de bestanddelen ervan verder worden verfijnd, kunnen nieuwe en onvoorziene zwakke plekken aan het licht komen.

Er bestaan al verschillende technologische mechanismen om cyberspace veiliger te maken, en er zijn nieuwe in ontwikkeling. Daarbij gaat het onder meer om:

- de beveiliging van essentiële onderdelen van de infrastructuur door gebruik te maken van openbare sleutelinfrastructuur, veilige protocollen te ontwikkelen, enz.

- de beveiliging van particuliere en openbare omgevingen door middel van de ontwikkeling van goede software, firewalls, anti-virusprogramma's, elektronische systemen voor het beheer van toegangsrechten, encryptie, enz.

- de verificatie van gemachtigde gebruikers, het gebruik van smartcards, biometrische identificatie, elektronische handtekeningen, rolspecifieke technieken, enz.

Deze maatregelen maken het noodzakelijk dat meer wordt gedaan aan de ontwikkeling van beveiligingstechnieken, waarbij aan de hand van internationale standaarden moet worden samengewerkt om te zorgen voor de nodige interoperabiliteit van de verschillende oplossingen.

Tevens is het van belang dat veiligheidsaspecten in de toekomst worden beschouwd als een vast onderdeel van de gehele structuur, waarbij vanaf de eerste ontwerpfase oplossingen worden bedacht voor bedreigingen en zwakke plekken. Dit in tegenstelling tot de traditionele aanpak, waarin systemen achteraf moeten worden uitgebreid om de gaten die door steeds geraffineerdere criminelen worden benut, te dichten.

Het programma van de EU inzake de technologie van de informatiemaatschappij (Information Society Technologies, IST),[18] en met name de werkzaamheden op het gebied van de informatie- en netwerkbeveiliging en andere technologieën ter versterking van het vertrouwen,[19] biedt een kader voor de ontwikkeling van het vermogen en de technologie om nieuwe problemen in verband met computercriminaliteit aan te pakken. Bij deze technologie gaat het onder meer om technische hulpmiddelen die kunnen worden gebruikt om bescherming te bieden tegen de schending van grondrechten zoals het recht op privacy en bescherming van persoonsgegevens en andere persoonlijke rechten, en om computercriminaliteit te bestrijden. Daarnaast is in het kader van het IST-programma een betrouwbaarheidsinitiatief gestart. Dit initiatief moet vertrouwen kweken in de informatie-infrastructuur met zijn vele onderlinge verbindingen en in in netwerken ingebedde systemen, door mensen te wijzen op het belang van betrouwbaarheid en door het gebruik van betrouwbaarheidverhogende technologie te bevorderen. Internationale samenwerking is een belangrijk aspect van dit initiatief. In het kader van het IST-programma zijn contacten gelegd met het DARPA en de NSF en is, in samenwerking met het Amerikaanse ministerie van Buitenlandse Zaken, een gemeenschappelijke EG/VS task force voor de bescherming van essentiële infrastructuur opgericht.[20]

Tenslotte zijn er de beveiligingsvoorschriften van de EU-richtlijnen inzake gegevensbescherming,[21] die bijdragen aan een betere beveiliging van netwerken en gegevensverwerking.

3. COMPUTERCRIMINALITEIT

De moderne informatie- en communicatiesystemen maken het mogelijk om vanaf willekeurig welke plaats ter wereld op willekeurig welk tijdstip illegale activiteiten te ondernemen. Er zijn geen betrouwbare statistieken over de werkelijke omvang van het verschijnsel computercriminaliteit. Het aantal tot nu toe ontdekte en aangegeven inbreuken geeft waarschijnlijk niet de werkelijke omvang van het probleem weer. Vanwege de beperkte kennis en ervaring van systeembeheerders en gebruikers op dit gebied, worden veel inbreuken niet ontdekt. Bovendien zijn veel ondernemingen huiverig om gevallen van computermisbruik te melden, omdat ze bang zijn voor negatieve publiciteit en nieuwe aanvallen. Bij veel politiediensten worden nog geen statistieken bijgehouden over het gebruik van computers en communicatiesystemen bij deze en andere strafbare feiten. Het aantal illegale activiteiten zal echter stijgen naarmate het gebruik van computers en netwerken toeneemt. Het is duidelijk dat er betrouwbare gegevens moet worden verzameld over de omvang van computercriminaliteit.

In deze mededeling wordt de term computercriminaliteit in de ruimste zin van het woord gebruikt, dus voor elk strafbaar feit waarbij op de een of andere manier gebruik wordt gemaakt van informatietechnologie. De opvattingen over wat computercriminaliteit is, lopen echter uiteen. De termen “computercriminaliteit,” “high-techcriminaliteit” en “cybercriminaliteit” worden vaak door elkaar gebruikt. Er kan een onderscheid worden

---

[18] Het IST-programma wordt beheerd door de Europese Commissie. Het maakt deel uit van het 5de Kaderprogramma, dat van 1998 tot 2002 loopt. Verdere informatie is te vinden op: http://www.cordis.lu/ist.

[19] In Kernactiviteit 2 - Nieuwe werkmethoden en elektronische handel.

[20] Onder supervisie van de gemeenschappelijke adviesgroep van de overeenkomst tussen de EG en de VS inzake wetenschappelijke en technologische samenwerking

[21] Zie artikel 4 van Richtlijn 97/66/EG (die ook de verplichting behelst om nog bestaande veiligheidsrisico's te melden) en artikel 17 van Richtlijn 95/46/EG.

gemaakt tussen specifieke computercriminaliteit en traditionele strafbare feiten die worden gepleegd met behulp van de computertechnologie. Dit laatste doet zich bijvoorbeeld voor op douanegebied, waar internet wordt gebruikt voor het plegen van typische schendingen van de douanewetgeving zoals smokkel, vervalsing, enz. Voor specifieke computercriminaliteit moeten de definities van strafbare feiten in de nationale wetboeken van strafrecht worden aangepast, terwijl traditionele criminaliteit die met behulp van computers wordt gepleegd, vraagt om betere samenwerking en procedurele maatregelen.

Al deze vormen van criminaliteit gedijen echter bij de beschikbaarheid van informatie- en communicatienetwerken zonder grenzen en van de ongrijpbaarheid en de vluchtigheid van informatiestromen. Deze kenmerken maken een herziening van de bestaande maatregelen nodig om op te treden tegen illegale activiteiten die via of met behulp van deze netwerken en systemen worden ontplooid.

In veel landen is wetgeving opgesteld om computercriminaliteit aan te pakken. In de lidstaten van de Europese Unie zijn verschillende wettelijke instrumenten ontwikkeld. Afgezien van een besluit van de Raad ter bestrijding van kinderpornografie op internet, zijn er nog geen EU-rechtsinstrumenten die rechtstreeks gericht zijn op de bestrijding van computercriminaliteit, maar wel een aantal indirecte instrumenten die relevant zijn.

De belangrijkste aspecten die in de wetgeving inzake specifieke computercriminaliteit worden behandeld op EU-niveau of op het niveau van de lidstaten, zijn:

Inbreuken op de persoonlijke levenssfeer: verschillende landen hebben strafwetgeving ingevoerd tegen het onwettig verzamelen, opslaan, wijzigen, bekendmaken of verspreiden van persoonsgegevens. In de Europese Unie zijn twee richtlijnen goedgekeurd ter onderlinge afstemming van de wetgeving inzake de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens.[22] Artikel 24 van richtlijn 95/46/EG verplicht de lidstaten passende maatregelen te nemen om de onverkorte toepassing van de bepalingen van de richtlijn te garanderen en met name de sancties vast te stellen die gelden bij inbreuk op de ter uitvoering van deze richtlijn vastgestelde bepalingen. Het recht op een persoonlijke levenssfeer en het recht op gegevensbescherming zijn ook opgenomen in het ontwerphandvest van de grondrechten van de Europese Unie.

Delicten op het gebied van de inhoud: de verspreiding, met name via internet, van pornografie, in het bijzonder kinderpornografie, racistische uitlatingen en informatie die aanzet tot geweld, roept de vraag op in hoeverre tegen deze handelingen kan worden opgetreden via het strafrecht. De Commissie stelt zich op het standpunt dat wat off line onwettig is, on line ook als onwettig moet worden beschouwd. De auteur of de content provider[23] kan strafrechtelijk aansprakelijk zijn. Er is een besluit van de Raad goedgekeurd ter bestrijding van kinderpornografie op internet.[24] De aansprakelijkheid van service providers die als tussenpersoon optreden, waarvan de netwerken of servers worden gebruikt voor het

---

22 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en Richtlijn 97/66/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector. Artikel 24 van Richtlijn 95/46/EG verplicht de lidstaten ertoe sancties vast te stellen voor inbreuken op de ter uitvoering van de richtlijn vastgestelde bepalingen.

23 De contentprovider moet niet worden verward met de service provider.

24 Besluit van de Raad van 29 mei 2000 ter bestrijding van kinderpornografie op internet (PB L 138 van 9.6.2000, blz.1).

doorgeven of opslaan van informatie van derden, is geregeld bij de richtlijn betreffende bepaalde juridische aspecten van de elektronische handel.

Economische delicten, onbevoegde toegang en sabotage: in veel landen zijn wetten goedgekeurd waarin specifieke computercriminaliteit in de vorm van economische delicten wordt aangepakt en nieuwe delicten in verband met de onbevoegde toegang tot computersystemen (b.v. hacking, computersabotage en de verspreiding van virussen, computerspionage, vervalsing per computer en computerfraude[25]) en nieuwe manieren om een delict te plegen, worden beschreven (b.v. door middel van computermanipulatie in plaats van door een persoon te misleiden). Deze delicten zijn vaak gericht op ontastbare zaken zoals geld op bankrekeningen of computerprogramma's. Op dit moment zijn er geen EU-instrumenten die betrekking hebben op dit soort onwettige activiteiten. Wat de preventie betreft heeft de onlangs goedgekeurde verordening betreffende goederen voor tweeërlei gebruik aanzienlijk bijgedragen tot een grotere beschikbaarheid van encryptieproducten.

Delicten op het gebied van de intellectuele eigendom: er zijn twee richtlijnen goedgekeurd, over de rechtsbescherming van computerprogramma's en van databanken,[26] die rechtstreeks betrekking hebben op de Informatiemaatschappij en sancties mogelijk maken. De Raad heeft zijn goedkeuring gehecht aan een gemeenschappelijk standpunt over een voorstel voor een Richtlijn betreffende het auteursrecht en de naburige rechten in de informatiemaatschappij. Deze zal waarschijnlijk begin 2001 worden goedgekeurd.[27] De schending van het auteursrecht en de naburige rechten moet, evenals het ontwijken van de technologische maatregelen die bedoeld zijn om deze rechten te beschermen, worden bestraft. Vóór eind 2000 zal de Commissie een mededeling indienen over namaak en piraterij, waarin de balans wordt opgemaakt van het overleg dat in 1998 met het Groenboek is begonnen en waarin tevens een actieplan wordt aangekondigd. Nu internet commercieel gezien steeds belangrijker wordt, doen zich nieuwe geschillen voor rond domeinnamen, zoals cybersquatting, warehousing en reverse hijacking, en natuurlijk wordt er aangedrongen op regels en procedures om deze problemen op te lossen.[28]

Er moet ook aandacht worden besteed aan het doen naleven van belastingverplichtingen. Bij commerciële transacties met een in de EU gevestigde afnemer van een on line geleverde elektronische dienst, zal in de meeste gevallen belasting moeten worden betaald in het rechtsgebied waarin consumptie van de dienst plaatsvindt.[29] Het niet-nakomen van de

---

25 In de media is veel aandacht besteed aan de recente gevallen van opzettelijke versperring van de toegang tot de server en aan de verspreiding van het zogenoemde LoveBug-virus. Dit moet echter wel in het juiste perspectief worden gezien. Aanvallen waarbij de toegang tot de server opzettelijk of per ongeluk wordt geblokkeerd, en per e-mail verspreide virussen zijn verschijnselen die al jaren bestaan. De Morrisworm en de IBM-Kerstboom e-mail waren daar vroege voorbeelden van. Er bestaan producten en procedures die kunnen helpen bij het oplossen van dit soort problemen. Binnen de internetgemeenschap wordt ook goed samengewerkt om de schade bij dergelijke voorvallen zoveel mogelijk te beperken. Er is ook sprake van samenwerking om de spamming-overlast te beperken.

26 Richtlijn 91/250/EEG van de Raad van 14 mei 1991 betreffende de rechtsbescherming van computerprogramma's (PB L 122 van 17.5.1991, blz. 42–46).
Richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken (PB L 77 van 27.3.1996, blz. 20–28).

27 Gemeenschappelijk standpunt van de Raad met het oog op de goedkeuring van een Richtlijn van het Europees Parlement en de Raad betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij (CS/2000/9512).

28 Mededeling van de Commissie aan de Raad en het Europees Parlement: Organisatie en beheer van het Internet; Internationale en Europese beleidskwesties 1998–2000, april 2000, COM(2000) 202.

29 De Commissie heeft een reeks wijzigingen voorgesteld van het BTW-stelsel in de EU ter verduidelijking van het rechtsgebied van de BTW-plichtigheid (COM(2000)349 - Voorstel voor een richtlijn van de Raad

belastingplicht kan leiden tot civielrechtelijke (en in sommige gevallen strafrechtelijke) sancties, zoals de inbeslagneming van banktegoeden of andere bezittingen. Hoewel vrijwillige nakoming altijd de voorkeur geniet, moet de belastingplicht uiteindelijk afdwingbaar zijn. Samenwerking tussen belastingdiensten is daarbij van wezenlijk belang.

Als voor sommige mensen mogelijkheden worden gecreëerd om hun rechtmatige transacties te beschermen, kunnen criminelen van diezelfde mogelijkheden gebruik kunnen maken om hun onrechtmatige transacties te beschermen. De instrumenten die onze elektronische handel beveiligen, kunnen ook worden gebruikt ter bescherming van de handel in drugs. Er zullen prioriteiten moeten worden gesteld en keuzes worden gemaakt.

Bij de bescherming van slachtoffers van computercriminaliteit moeten ook zaken als aansprakelijkheid, herstel en compensatie worden geregeld. Vertrouwen ontstaat niet alleen door het gebruik van de juiste technologie, maar ook door de bijbehorende wettelijke en economische garanties. Op deze problematiek moet voor alle vormen van computercriminaliteit worden ingegaan.

Er bestaat duidelijk behoefte aan doeltreffende, wereldwijd of in ieder geval op het niveau van de Europese Unie onderling afgestemde instrumenten op het gebied van het materiële recht en het procesrecht, om de slachtoffers van computercriminaliteit te beschermen en de daders te berechten. Tegelijkertijd zijn persoonlijke communicatie, bescherming van de persoonlijke levenssfeer en van persoonsgegevens, toegang tot en verspreiding van informatie grondrechten van de moderne democratie. We moeten kunnen beschikken over doeltreffende preventieve maatregelen, om het gebruik van repressieve maatregelen zoveel mogelijk te beperken. Bij alle wetgeving die eventueel noodzakelijk is ter bestrijding van computercriminaliteit moet het juiste evenwicht worden gezocht tussen deze belangen.

4. VRAAGSTUKKEN OP HET GEBIED VAN HET MATERIËLE RECHT

Door de onderlinge afstemming van het materiële recht op het gebied van hightechcriminaliteit kan een minimumbeschermingsniveau voor slachtoffers van cybercriminaliteit worden gewaarborgd (bijvoorbeeld voor slachtoffers van kinderpornografie), kan gemakkelijker worden voldaan aan de volwaarde dat een handeling strafbaar moet zijn in beide landen voordat er wederzijdse rechtshulp kan worden verleend in een strafrechtelijk onderzoek (dubbele strafbaarheidsvoorwaarde), en krijgt het bedrijfsleven meer duidelijkheid (bijvoorbeeld over wat onder illegale inhoud wordt verstaan).

Een wetgevend EU-instrument ter onderlinge afstemming van het materiële strafrecht inzake computercriminaliteit staat sinds de Europese Raad van Tampere van oktober 1999 op de agenda van de EU[30]. Tijdens deze Top werd hightech-criminaliteit genoemd als een van de sectoren waarin moet worden gestreefd naar gemeenschappelijke definities, strafbaarstellingen en straffen. Dit is overgenomen in Aanbeveling 7 van de strategie van de Europese Unie voor het begin van het nieuwe millennium inzake de voorkoming en bestrijding van de georganiseerde criminaliteit, die door de JBZ-Raad in maart 2000 werd

---

tot wijziging van Richtlijn 77/388/EEG met betrekking tot de regeling inzake de belasting over de toegevoegde waarde die van toepassing is op bepaalde diensten die met elektronische middelen worden verricht), die momenteel worden besproken in de Raad en het Parlement. In sommige gevallen is de leverancier BTW-plichtig, ook als hij niet fysiek aanwezig is in het betrokken rechtsgebied.

30 http://db.consilium.eu.int/nl/Info/eurocouncil/index.htm.

goedgekeurd[31]. Het is ook een onderdeel van het werkprogramma van de Commissie voor 2000 en van het scorebord voor de totstandbrenging van een ruimte van vrijheid, veiligheid en rechtvaardigheid, dat door de Commissie is opgesteld en door de Raad Justitie en Binnenlandse Zaken op 27 maart 2000 is goedgekeurd[32].

De Commissie heeft de werkzaamheden van de Raad van Europa in verband met het verdrag inzake cybercriminaliteit gevolgd. In het huidige ontwerpverdrag inzake cybercriminaliteit zijn vier categorieën strafbare feiten opgenomen: 1) schending van de vertrouwelijkheid, de integriteit en de beschikbaarheid van computergegevens en -systemen; 2) specifieke computercriminaliteit 3) strafbare feiten met betrekking tot de inhoud; 4) schending van het auteursrecht en de naburige rechten.

In de EU zal de onderlinge afstemming van de wetgeving wellicht verder gaan dan in het verdrag van de Raad van Europa, waarin internationale afstemming tot een minimum beperkt blijft. Deze afstemming zou eerder een feit kunnen zijn dan de inwerkingtreding van het verdrag van de Raad van Europa.[33] Daarmee zou computercriminaliteit binnen de werkingssfeer van het gemeenschapsrecht worden gebracht en zouden EU-nalevingsmechanismen in het leven worden geroepen.

De Commissie vindt het van groot belang dat de Europese Unie in staat wordt gesteld doeltreffend op te treden tegen met name kinderpornografie op internet. De Commissie juicht het besluit van de Raad ter bestrijding van kinderpornografie op internet toe, maar is het met het Europees Parlement eens dat verdere maatregelen moeten worden genomen met het oog op de onderlinge afstemming van de wetgeving van de lidstaten. De Commissie is voornemens later dit jaar een voorstel in te dienen voor een kaderbesluit van de Raad waarin bepalingen zijn opgenomen met betrekking tot de onderlinge afstemming van de wetgeving over en de straffen op kinderpornografie op internet.[34]

In aansluiting op de conclusies van Tampere zal de Commissie met een wetgevingsvoorstel komen in het kader van Titel VI van het VEU om de nationale wetgeving inzake hightechcriminaliteit onderling af te stemmen. De resultaten van de werkzaamheden in de Raad van Europa zullen als uitgangspunt dienen voor dit voorstel, waarin met name zal worden ingegaan op de noodzaak om de wetgeving inzake hacking en denial of service attacks onderling af te stemmen. Daartoe zullen in het voorstel standaarddefinities voor de Europese Unie worden opgenomen. Het voorstel zou in dit opzicht ook verder kunnen gaan dan het ontwerpverdrag van de Raad van Europa, door voor alle lidstaten een minimumstraf in te stellen voor ernstige gevallen van hacking en denial of service.

---

31 Voorkoming en bestrijding van de georganiseerde criminaliteit: een strategie van de Europese Unie voor het begin van het nieuwe millennium (PB C 124 van 3.5.2000).

32 http://europa.eu.int/comm/dgs/justice_home/index_nl.htm.

33 Het verdrag van de Raad van Europa treedt pas in werking nadat het is geratificeerd.

34 Dit initiatief maakt deel uit van een pakket voorstellen waarin ook andere vraagstukken met betrekking tot de seksuele uitbuiting van kinderen en mensenhandel worden behandeld, zoals werd aangekondigd in de mededeling van de Commissie van december 1998 over mensenhandel. De tekst van het voorstel voor een kaderbesluit van de Raad is gehecht aan de mededeling van de Commissie aan de Raad en het Europees Parlement over de bestrijding van mensenhandel en de seksuele uitbuiting van kinderen: twee voorstellen voor kaderbesluiten van de Raad, die tegelijk met dit voorstel worden ingediend.

Voorts zal de Commissie onderzoeken welke maatregelen mogelijk zijn tegen racisme en vreemdelingenhaat op internet, teneinde een voorstel te formuleren voor een kaderbesluit van de Raad in het kader van Titel VI van het VEU over zowel off line- als on line-activiteiten op het gebied van racisme en vreemdelingenhaat. Daarbij zal rekening worden gehouden met de verwachte evaluatie van de tenuitvoerlegging door de lidstaten van het gemeenschappelijk optreden van 15 juli 1996 ter bestrijding van racisme en vreemdelingenhaat[35]. Dit gemeenschappelijk optreden was een eerste stap in de richting van de onderlinge afstemming van de strafwetgeving inzake racisme en vreemdelingenhaat, maar verdere afstemming in de Europese Unie blijft nodig. Dat dit uiterst belangrijke en gevoelige onderwerpen zijn, is ook gebleken uit de beslissing van een Franse rechter van 20 november 2000 om Yahoo te verplichten Franse gebruikers de toegang tot sites waar Nazi-memorabilia worden verkocht, te versperren.[36]

Tenslotte zal de Commissie nagaan hoe de illegale drugshandel op internet doeltreffender kan worden bestreden. Het belang daarvan wordt ook onderkend in de drugsstrategie van de Europese Unie (2000-2004), die door de Europese Raad van Helsinki werd onderschreven.[37]

5. VRAAGSTUKKEN OP HET GEBIED VAN HET PROCESRECHT

De aard van computercriminaliteit heeft tot gevolg dat nationaal en internationaal wordt gekeken naar procedurele kwesties. Bij dit soort strafbare feiten zijn immers verschillende soevereine staten, jurisdicties en wetten betrokken. Meer dan bij elke andere vorm van grensoverschrijdende criminaliteit vormen de snelheid, de mobiliteit en de flexibiliteit van computercriminaliteit een probleem voor de bestaande regels van het strafprocesrecht.

Onderlinge afstemming van de bevoegdheden in het procesrecht kan slachtoffers een betere bescherming bieden als rechtshandhavingsinstanties beschikken over de bevoegdheden die nodig zijn om strafbare feiten op hun eigen grondgebied te onderzoeken en snel en doeltreffend kunnen reageren op verzoeken om samenwerking van andere landen.

Het is ook van belang dat strafrechtelijke maatregelen, die in het algemeen onder de bevoegdheid van de lidstaten en onder Titel VI van het VEU vallen, in overeenstemming zijn met het Gemeenschapsrecht. Het Hof van Justitie heeft herhaaldelijk verklaard dat dergelijke wettelijke maatregelen niet discriminerend mogen zijn ten aanzien van personen die krachtens het Gemeenschapsrecht gelijk moeten worden behandeld, of de in het Gemeenschapsrecht gewaarborgde fundamentele vrijheden mogen beperken.[38] Nieuwe bevoegdheden voor rechtshandhavingsinstanties moeten altijd worden getoetst aan het Gemeenschapsrecht en worden beoordeeld op hun gevolgen voor de privacy.

---

35 PB L 85 van 24.7.1996, blz. 5-7. Ook te vinden op de website van het Europees justitieel netwerk: http://ue.eu.int/ejn/index.htm

36 Tribunal de grande instance de Paris, Ordonnance de Référé van 20 november 2000, nr. RG 00/05308.

37 Actieplan van de Europese Unie inzake drugsbestrijding (2000-2004). COM(1999)239 def. http://europa.eu.int/comm/justice_home/unit/drogue_en.htm.

38 zaak C-274/96 Bichel & Franz (1998) Jurispr. I-7637, overweging 17; zaak C-186/87 Cowan (1989) Jurispr. 195, overweging 19. Met name mogen administratieve maatregelen of sancties niet verder gaan dan strikt noodzakelijk is, de controle mag niet op zodanige wijze zijn geregeld, dat de door het Verdrag beoogde vrijheid wordt beperkt , en er mag geen straf worden opgelegd die zozeer onevenredig is aan de ernst van de overtreding , dat zij de vrijheid gaat belemmeren (zaak C-203/80 Casati (1981), Jurispr. 2595, overweging 27).

5.1. Het aftappen van telecommunicatieverkeer

In de Europese Unie geldt in het algemeen het beginsel dat berichten (en de daarmee verband houdende verkeersgegevens) vertrouwelijk zijn. Het aftappen daarvan is onwettig, tenzij het voor bepaalde gevallen om een beperkt aantal redenen bij de wet is toegestaan. Dit vloeit voort uit artikel 8 van Europees verdrag ter bescherming van de rechten van de mens, waarnaar wordt verwezen in artikel 6 van het VEU, en in het bijzonder uit de Richtlijnen 95/46/EG en 97/66/EG.

Alle lidstaten beschikken over regelgeving op grond waarvan rechtshandhavingsinstanties een bevelschrift (of, in het geval van twee lidstaten, een door een minister persoonlijk ondertekende volmacht) kunnen verkrijgen voor het aftappen van berichten op het openbare telecommunicatienetwerk.[39] In deze wetgeving, die in overeenstemming moet zijn met het Gemeenschapsrecht voor zover dat van toepassing is, zijn strenge waarborgen opgenomen om het fundamentele recht op privacy te beschermen, b.v. door aftappen alleen toe te staan bij onderzoeken naar zware criminaliteit, of door middel van de voorwaarde dat aftappen noodzakelijk en evenredig moet zijn, of in de vorm van de vereiste dat de betrokkene wordt ingelicht over het aftappen zodra dat niet langer schadelijk is voor het onderzoek. In veel lidstaten zijn telecommunicatie-exploitanten (als verstrekker van een openbare dienst) wettelijk verplicht aftappen mogelijk te maken. In 1995 keurde de Raad een resolutie goed ter coördinatie van de eisen op dit gebied.[40]

Traditionele netwerkexploitanten, in het bijzonder degenen die spraakdiensten aanbieden, hebben in het verleden een bepaalde samenwerking ontwikkeld met rechtshandhavingsinstanties om het legaal aftappen van berichten mogelijk te maken. De liberalisatie van de telecommunicatiemarkt en de explosieve toename van het gebruik van internet hebben vele nieuwkomers naar de markt gelokt, voor wie de aftapvoorwaarden nieuw zijn. Vragen betreffende voorschriften, technische uitvoerbaarheid, verdeling van kosten en commerciële gevolgen moeten worden besproken in een dialoog tussen de overheid en het bedrijfsleven, waarbij ook alle andere partijen zijn betrokken, inclusief de instanties die toezicht houden op de gegevensbescherming.

De nieuwe technologie maakt het voor de lidstaten noodzakelijk om samen te werken om hun mogelijkheden voor het legaal aftappen van telecommunicatieverkeer te behouden. De Commissie is van mening dat nieuwe technische aftapeisen die door de lidstaten aan telecommunicatie-exploitanten en internet service providers worden gesteld, internationaal

---

39 In twee lidstaten zijn onderschepte berichten niet toegelaten als bewijs in strafprocedures.

40 Resolutie van de Raad van 17 januari 1995 inzake de legale interceptie van telecommunicatieverkeer (PB C 329 van 4.11.1996, blz. 1– 6). In de bijlage is een lijst opgenomen van de interceptie-eisen vanuit het oogpunt van rechtshandhaving waarmee de lidstaten rekening dienden te houden bij het opstellen en uitvoeren van nationaal beleid en nationale maatregelen op dit gebied. In 1998 diende het Oostenrijkse voorzitterschap een voorstel in voor een resolutie van de Raad ter uitbreiding van de werkingssfeer van de resolutie van 1995, zodat deze ook betrekking zou hebben op nieuwe technologische ontwikkelingen, met inbegrip van internet en communicatie per satelliet. Dit voorstel is besproken in twee commissies van het Europees Parlement, de Commissie openbare vrijheden en binnenlandse zaken en de Commissie juridische zaken en rechten van de burger, die tot verschillende conclusies kwamen. De Commissie openbare vrijheden en binnenlandse beschouwde dit voorstel als een verduidelijking en een bijwerking van de oude resolutie en vond de nieuwe resolutie aanvaardbaar. De Commissie juridische zaken en rechten van de burger had veel kritiek op de resolutie, zowel uit het oogpunt van potentiële inbreuken op de mensenrechten als wat de kosten voor de exploitanten betreft, verwierp daarom het voorstel en riep de Commissie op een nieuw voorstel in te dienen na de inwerkingtreding van het Verdrag van Amsterdam. De Raad of de werkgroepen daarvan hebben zich de afgelopen maanden niet actief beziggehouden met de ontwerpwetsolutie.

moeten worden gecoördineerd, om verstoring van de interne markt te voorkomen, om de kosten voor het bedrijfsleven zo laag mogelijk te houden en om ervoor te zorgen dat de voorschriften inzake privacy- en gegevensbescherming worden nageleefd. De standaarden moeten voor zover mogelijk open en doorzichtig zijn en mogen de communicatie-infrastructuur niet aantasten.

In het kader van de Overeenkomst betreffende wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie[41] zijn afspraken gemaakt om samenwerking op het gebied van het legaal aftappen te vergemakkelijken[42]. De overeenkomst bevat bepalingen over het aftappen van telefoonverkeer via de satelliet,[43] en over het aftappen van telecommunicatieverkeer van een persoon die zich op het grondgebied van een andere lidstaat bevindt.[44] De Commissie denkt dat de aftapregels die in de Overeenkomst betreffende de wederzijdse rechtshulp zijn vervat, het maximum is dat op dit moment haalbaar is. De tekst van de overeenkomst is technologisch neutraal; de praktijk moet uitwijzen hoe de overeenkomst werkt, voordat eventuele verbeteringen kunnen worden overwogen. De Commissie zal de tenuitvoerlegging van de overeenkomst evalueren met de lidstaten, het bedrijfsleven, de gebruikers en instanties die toezicht houden op de gegevensbescherming, om ervoor te zorgen dat initiatieven op dat gebied doeltreffend, transparant and evenwichtig zijn.

Oneigenlijk, onzorgvuldig gebruik van aftapfaciliteiten, zeker op internationaal niveau, zal leiden tot protesten vanuit het oogpunt van de mensenrechten en het vertrouwen van de burgers in de informatiemaatschappij ondermijnen. De Commissie is ernstig bezorgd over berichten betreffende het vermoeden van misbruik van aftapfaciliteiten.[45]

5.2. Het bewaren van verkeersgegevens

Bij het onderzoeken en vervolgen van strafbare feiten waarbij communicatienetwerken een rol spelen, met inbegrip van internet, maken rechtshandhavingsinstanties vaak gebruik van verkeersgegevens wanneer die, voornamelijk voor factureringsdoeleinden, zijn opgeslagen

---

41 PB C 197 van 12.7.2000 Deze overeenkomst werd goedgekeurd op 29 mei 2000. De bepalingen inzake het aftappen van telecommunicatie van deze overeenkomst gelden alleen voor de lidstaten van de Europese Unie, niet voor derde landen.

42 In de Overeenkomst zijn minimumwaarborgen opgenomen voor de bescherming van de persoonlijke levenssfeer en van persoonsgegevens.

43 Oorspronkelijk waren de onderhandelingen bedoeld om de mogelijkheid te scheppen telefoonverkeer af te tappen van personen die via de satelliet vanuit de aftappende lidstaat communiceren. Technisch gezien is het grondstation van de satelliet echter het punt waar dit verkeer moet worden afgetapt. Daarom zou technische bijstand moeten worden gevraagd van de lidstaat waar het grondstation is gevestigd. De overeenkomst biedt daartoe twee mogelijkheden: een versnelde procedure voor wederzijdse rechtshulp waarin de lidstaat van het grondstation voor elk geval afzonderlijk om bijstand moet worden verzocht, en een technische oplossing op basis van toegang op afstand van de aftappende lidstaat tot het grondstation, waarvoor geen afzonderlijke verzoeken nodig zijn.

44 De overeenkomst vormt tevens een wettelijk kader voor verzoeken om telecommunicatieverkeer van iemand op het grondgebied van een andere lidstaat (de aangezochte lidstaat) af te tappen. In dat geval moet zowel de aftappende als de aangezochte lidstaat een aftapbevel volgens de nationale wetgeving aanvragen. Tenslotte bevat de overeenkomst regels voor situaties waarin de aftappende lidstaat de mogelijkheid heeft het telecommunicatieverkeer van een persoon op het grondgebied van een andere lidstaat af te tappen zonder technische bijstand te hoeven vragen van die lidstaat.

45 In het Europees Parlement is een openbare hoorzitting gehouden over een lang en uitvoerig gedocumenteerd verslag van de heer Campbell over een aftaptienetwerk met de naam ECHELON (http://www.gn.apc.org/duncan/stoa_cover.htm). In het verslag wordt beweerd dat ECHELON werd ontwikkeld voor nationale veiligheidsdoeleinden, maar ook werd gebruikt voor industriële spionage. Het Europees Parlement heeft een tijdelijke commissie opgericht die zich over dit onderwerp zal buigen en binnen een jaar een verslag zal voorleggen aan de voltallige vergadering .

door service providers. Omdat de prijs van communicatie steeds minder afhankelijk wordt van afstand en bestemming en service providers opschuiven in de richting van uniforme tarieven, is het niet langer nodig verkeersgegevens te bewaren voor factureringsdoeleinden. Rechtshandhavingsinstanties vrezen dat daardoor gegevens die nuttig kunnen zijn voor strafrechtelijke onderzoeken verloren gaan, en pleiten ervoor service providers te verplichten gedurende een bepaalde minimumperiode verkeersgegevens te bewaren, zodat deze kunnen worden gebruikt voor rechtshandhavingsdoeleinden.[46]

Krachtens de EU richtlijnen betreffende de bescherming van persoonsgegevens, dat wil zeggen zowel krachtens de algemene beperkingen van Richtlijn 95/46/EG als volgens de meer specifieke bepalingen van Richtlijn 97/66/EG, moeten verkeersgegevens onmiddellijk na het verlenen van de telecommunicatiedienst worden gewist of anoniem gemaakt, tenzij ze noodzakelijk zijn voor de facturering. Voor telecommunicatiediensten die kosteloos of tegen uniform tarief toegankelijk zijn, mogen in beginsel geen verkeersgegevens worden bewaard.

Krachtens de EU-richtlijnen betreffende gegevensbescherming kunnen de lidstaten wettelijke maatregelen treffen ter beperking van de verplichting om verkeersgegevens te wissen indien dit noodzakelijk is voor, onder meer, het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het telecommunicatiestysteem.[47]

Nationale wettelijke maatregelen waarin het bewaren van verkeersgegevens voor rechtshandhavingsdoeleinden is geregeld, moeten echter wel aan bepaalde voorwaarden voldoen: deze maatregelen moeten passend, noodzakelijk en evenredig zijn, zoals krachtens het Gemeenschapsrecht en het internationale recht is vereist, onder meer krachtens Richtlijn 97/66/EG, Richtlijn 95/46/EG, het Europees Verdrag tot bescherming van de rechten van de mens van 4 november 1950 en Het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van 28 januari 1981. Dat is in het bijzonder van belang voor maatregelen die betrekking hebben op het routinematig bewaren van gegevens over een groot deel van de bevolking.

Sommige lidstaten nemen initiatieven op wetgevingsgebied om service providers te verplichten of toe te staan nadat de dienst is verleend, bepaalde categorieën verkeersgegevens te bewaren die niet nodig zijn voor de facturering, maar die nuttig kunnen zijn in strafrechtelijke onderzoeken.

Hoewel deze initiatieven qua werkingssfeer en vorm sterk uiteenlopen, zijn ze allemaal gebaseerd op de idee dat rechtshandhavingsinstanties over meer gegevens moeten kunnen beschikken dan het geval zou zijn indien service providers alleen gegevens zouden verwerken die strikt noodzakelijk zijn voor het verlenen van de dienst. De Commissie onderzoekt deze maatregelen in het licht van het bestaande gemeenschapsrecht.

---

[46] Daarbij gaat het ook om strafrechtelijke onderzoeken in gevallen die weliswaar geen verband houden met computers of communicatienetwerken, maar waarbij deze gegevens kunnen bijdragen aan de oplossing van het misdrijf.

[47] Artikel 14 van Richtlijn 97/66/EG en artikel 13 van Richtlijn 95/46/EG.

Het Europees Parlement is gevoelig voor privacy-kwesties en heeft zich in het algemeen voorstander getoond van een strenge bescherming van persoonsgegevens. In discussies over de bestrijding van kinderpornografie op internet heeft het Europees Parlement echter positief geadviseerd over een algemene verplichting om verkeersgegevens gedurende drie maanden te bewaren.[48]

Dit geeft aan hoe belangrijk de context is waarin wordt gesproken over een onderwerp dat zo gevoelig ligt als het bewaren van verkeersgegevens en laat zien dat het voor beleidsmakers niet eenvoudig is het juiste evenwichtig te vinden.

De Commissie is van mening dat de ingewikkelde kwestie van het bewaren van verkeersgegevens om goed gefundeerde oplossingen vraagt, waarbij evenredigheid voorop moet staan en een billijk evenwicht moet worden gevonden tussen de verschillende behoeften en belangen van de betrokkenen. Alleen als overheid, bedrijfsleven, instanties die toezicht houden op gegevensbescherming en gebruikers hun deskundigheid en hun capaciteiten bundelen, kan een aanpak worden ontwikkeld waarin deze strijdige belangen met elkaar kunnen worden verzoend. Het is zeer wenselijk dat alle lidstaten dezelfde aanpak hanteren, zodat deze doeltreffend en evenredig werkt en zodat wordt voorkomen dat zowel de rechtshandhavingsinstanties als de internetgemeenschap te maken krijgen met een lappendeken van technische en wettelijke voorschriften.

Er moet met nogal uiteenlopende belangen rekening worden gehouden. Enerzijds stellen instanties voor het toezicht op gegevensbescherming zich op het standpunt dat de doeltreffendste manier om onaanvaardbare risico's voor de bescherming van de persoonlijke levenssfeer te beperken, terwijl wordt erkend dat een doeltreffende wetshandhaving noodzakelijk is, erin bestaat dat verkeersgegevens in beginsel niet uitsluitend voor wetshandhavingsdoeleinden mogen worden bewaard.[49] Anderzijds zijn rechtshandhavingsinstanties van oordeel dat het in het belang van strafrechtelijke onderzoeken noodzakelijk is een minimum aan verkeersgegevens gedurende een bepaalde minimumperiode te bewaren.

Het bedrijfsleven heeft er belang bij mee te werken aan de bestrijding van criminaliteit zoals hacken en computerfraude, maar moet geen maatregelen opgelegd krijgen die onredelijk veel geld kosten. Elke maatregel moet zorgvuldig worden beoordeeld op zijn economische gevolgen, die moeten worden afgewogen tegen het effect van de maatregel op de bestrijding van cybercriminaliteit, om te voorkomen dat het gebruik van internet duurder en daardoor minder toegankelijk wordt voor de gebruikers. Verkeersgegevens die worden bewaard, moeten goed worden beveiligd.

---

48 Wetgevingsresolutie houdende advies van het Europees Parlement inzake het ontwerp van gemeenschappelijk optreden, door de Raad aangenomen op grond van artikel K.3 van het Verdrag betreffende de Europese Unie, ter bestrijding van kinderpornografie op Internet, amendement 17 (PB C 219 van 30.7.1999, blz. 68).

49 "Grootschalig verkennend of algemeen toezicht moet verboden zijn …de doeltreffendste manier om onaanvaardbare risico's voor de bescherming van de persoonlijke levenssfeer te beperken, terwijl wordt erkend dat een doeltreffende wetshandhaving noodzakelijk is, bestaat erin dat verkeersgegevens in beginsel niet uitsluitend voor wetshandhavingsdoeleinden mogen worden bewaard en dat nationale wetten telecommunicatie-exploitanten, telecommunicatiediensten- en Internet service providers er niet toe mogen verplichten om verkeersgegevens langer bij te houden dan voor het opstellen van rekeningen noodzakelijk is". Aanbeveling 3/99 van de werkgroep gegevensbescherming van 7 september 1999; http:/europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

Het bedrijfsleven kan in ieder geval een belangrijke bijdrage leveren aan het veiliger maken van de informatiemaatschappij. Gebruikers moeten erop kunnen vertrouwen dat de informatiemaatschappij veilig is en zich beschermd voelen tegen criminaliteit en inbreuken op hun privacy.

De Commissie steunt en stimuleert een constructieve dialoog tussen rechtshandhavingsinstanties, bedrijfsleven, gegevensbeschermingsautoriteiten, consumentenorganisaties en andere betrokken partijen. In het kader van het voorgestelde EU-forum (zie punt 6.4 van deze mededeling) zal de Commissie er bij alle betrokken partijen op aandringen zich in de eerste plaats te buigen over de ingewikkelde problematiek van het bewaren van verkeersgegevens, om gezamenlijk passende, evenwichtige en evenredige oplossingen te vinden, waarbij de fundamentele rechten op bescherming van de persoonlijke levenssfeer en van persoonsgegevens in acht worden genomen.[50] Op basis van de resultaten van deze werkzaamheden kan de Commissie beoordelen in hoeverre er wettelijke of andere maatregelen op EU-niveau moeten worden getroffen.

5.3. Anonieme toegang en anoniem gebruik

Rechtshandhavingsdeskundigen hebben de vrees geuit dat anonimiteit kan leiden tot niet-aansprakelijkheid en daarom het pakken van bepaalde criminelen ernstig kan bemoeilijken. In sommige landen (niet in alle) is anoniem gebruik van mobiele telefonie mogelijk door middel van vooruit betaalde kaarten. Sommige service en acces providers, waaronder remailers en internetcafés, bieden de mogelijkheid anoniem toegang te krijgen tot en gebruik te maken van internet. Een bepaalde mate van anonimiteit wordt ook geboden door het systeem van dynamische Internetadressering, waarbij adressen niet permanent aan gebruikers worden toegewezen, maar slechts voor de duur van een bepaalde sessie.

In hun gesprekken met de Commissie hebben sommige vertegenwoordigers van het bedrijfsleven verklaard geen voorstander te zijn van volledige anonimiteit, deels met het oog op de eigen veiligheid, fraudebestrijding en netwerkintegriteit. De London Internet Exchange heeft richtsnoeren inzake de beste praktijken uitgebracht die hun nut in het Verenigd Koninkrijk reeds hebben bewezen.[51] Andere vertegenwoordigers van het bedrijfsleven en privacydeskundigen hebben echter verklaard dat zonder anonimiteit de grondrechten niet kunnen worden gewaarborgd.

De gegevensbeschermingsgroep van artikel 29 heeft een aanbeveling uitgegeven over het anoniem gebruiken van internet.[52] Volgens de Groep vormt anonimiteit op internet een dilemma voor overheden en internationale organisaties. Enerzijds is de mogelijkheid om anoniem te blijven essentieel voor het handhaven van het recht op privacy en de vrijheid van meningsuiting in cyberspace. Anderzijds staat de mogelijkheid om on line te zijn en te communiceren zonder je identiteit prijs te geven, haaks op de initiatieven die worden ontwikkeld ter ondersteuning van andere belangrijke beleidsterreinen, zoals de bestrijding van illegale en schadelijke inhoud, financiële fraude of inbreuken op het auteursrecht. Dergelijke tegenstrijdige doelstellingen in het overheidsbeleid zijn natuurlijk geen nieuw verschijnsel. Bij de traditionele

---

50 Zoals verankerd in het Europees Verdrag tot bescherming van de rechten van de mens (artikel 8, recht op eerbiediging van het privé-leven), het EU-handvest van de grondrechten, het EG-Verdrag en de richtlijnen inzake gegevensbescherming.

51 http://www.linx.net/noncore/bcp.

52 Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens. Aanbeveling 3/97 Anonimiteit op internet. Goedgekeurd door de Groep op 3 december 1997. http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

communicatiemogelijkheden, zoals brieven en pakketten, telefoon, krant, of radio- en televisie-uitzendingen, is een evenwicht gevonden tussen deze doelstellingen. De beleidsmakers van nu staan voor de taak om dit evenwicht, waarin de basisrechten zijn gewaarborgd terwijl evenredige beperkingen van deze rechten zijn toegestaan in een beperkt aantal specifieke gevallen, te handhaven in de huidige cyberspace-context. Daarbij spelen de mate waarin mensen anoniem on line kunnen communiceren en de beperkingen die daarvoor gelden, een cruciale rol.

In de slotverklaring van de ministersconferentie over wereldwijde informatienetwerken die van 6 tot 8 juli 1997 in Bonn werd gehouden, werd tot uitgangspunt genomen dat wanneer de gebruiker er off line voor kan kiezen anoniem te blijven, hij die keuzemogelijkheid on line ook moet hebben. Men is het er dus duidelijk over eens dat bij activiteiten met betrekking tot netwerken van dezelfde juridische basisbeginselen moet worden uitgegaan als op andere terreinen. Internet is geen anarchistisch getto waar de regels van de samenleving niet gelden. Evenzeer geldt echter dat de mogelijkheid waarover regeringen en overheidsorganen beschikken om de rechten van individuen te beperken en toezicht op potentieel onwettig gedrag uit te oefenen, op openbare netwerken niet groter mag zijn dan daarbuiten, in de off line-wereld. De vereiste dat beperkingen van fundamentele rechten en vrijheden naar behoren moeten worden gerechtvaardigd, noodzakelijk moeten zijn en evenredig moeten zijn ten opzichte van andere doelstellingen van het overheidsbeleid, moet ook in cyberspace gelden.

In de aanbeveling van de artikel 29-Groep wordt uitvoerig beschreven hoe dat in bepaalde gevallen kan worden bereikt (bijvoorbeeld voor e-mail, nieuwsgroepen, enz).[53] De Commissie is het met de standpunten van de Groep eens.

5.4. Praktische samenwerking op internationaal niveau

In het recente verleden is bij wereldwijde gezamenlijke rechtshandhavingsoperaties, zoals Starburst en Cathedral tegen pedofiele netwerken, gebleken hoe waardevol gecoördineerd internationaal optreden door rechtshandhavingsinstanties en de rechterlijke macht is, zowel voor de uitwisseling van informatie in de voorbereidende fase als om te voorkomen dat andere leden van het netwerk worden gewaarschuwd bij arrestaties en inbeslagnemingen. Internet is ook een nuttig instrument gebleken voor politie- en douaneonderzoeken naar met behulp van de computer gepleegde traditionele strafbare feiten zoals vervalsing en smokkel. Anderzijds hebben deze operaties ook duidelijk gemaakt wat de belangrijkste juridische en operationele problemen waren voor rechtshandhavingsinstanties en de rechterlijke macht, zoals het voorbereiden van grensoverschrijdend bewijsmateriaal of *rogatoire commissie*, de identificatie van slachtoffers, en de rol van intergouvernementele politie-organisaties (met name Interpol en Europol).

Internationale netwerken voor de uitwisseling van informatie worden voor politie en douane steeds belangrijker voor de praktische internationale samenwerking.

In de G8 is al een praktische vorm van internationale samenwerking tot stand gebracht: er is een 24-uurs/7-dagen-per-week informatienetwerk van rechtshandhavingscontactpunten opgericht, dat ook al operationeel is. Het netwerk is voornamelijk bedoeld om snel te kunnen reageren op dringende verzoeken om samenwerking bij zaken waarin het gaat om elektronisch bewijs. Er is in een aantal gevallen al met succes gebruik van gemaakt. De JBZ-Raad heeft op 19 maart 1998 zijn goedkeuring uitgesproken over de 10 beginselen van de G8 ter bestrijding van hightech-criminaliteit en heeft de niet-G8 lidstaten van de EU verzocht

---

53 http://europa.eu/int/comm/dg15/en/media/dataprot/wpdocs/index.htm.

zich aan te sluiten bij het netwerk.[54] Deze contactpunten moeten rechtstreeks samenwerken en vormen een aanvulling op bestaande communicatiekanalen en instrumenten voor wederzijdse bijstand.[55]

In het ontwerpverdrag van de Raad van Europa is ook in de oprichting van zo'n netwerk voorzien. En ook in het besluit van de Raad ter bestrijding van kinderpornografie op internet en in het Gemeenschappelijk standpunt over het verdrag inzake cybercriminaliteit is sprake van een 24-uurs netwerk van contactpunten,[56] evenals in het besluit van de Raad tot goedkeuring van het G8- actieplan,[57] maar er zijn nog geen concrete initiatieven op EU-niveau ontwikkeld.

De Commissie is van mening dat gezien de behoefte aan deskundigheid en snelle actie op dit gebied, de bedoelingen van de Raad onmiddellijk in de praktijk moeten worden gebracht**.** Voor het welslagen van zo'n netwerk is echter juridisch en technisch geschoold personeel nodig. Er moeten dus voldoende opleidingsmogelijkheden worden geboden.

Ook bij de douaneautoriteiten bestaat behoefte aan intensievere samenwerking en meer gegevensuitwisseling. Bestaande samenwerkingsvormen moeten worden uitgebreid en er moeten nieuwe wegen worden gevonden om gezamenlijk op te treden en informatie uit te wisselen. Met inachtneming van de voorschriften inzake gegevensbescherming, zijn steeds meer douaneautoriteiten ervan overtuigd dat er internationale netwerken moeten worden gevormd om de uitwisseling van gegevens te vergemakkelijken. Er is ook behoefte aan meer middelen op dit gebied, zowel om computersystemen aan te passen als om personeel op te leiden, zodat de douaneautoriteiten hun taken doeltreffender kunnen vervullen.

5.5. Bevoegdheden op het gebied van het procesrecht

Op nationaal niveau moeten rechtshandhavingsinstanties, als aan de in de wet verankerde voorwaarden is voldaan, snel genoeg in computers opgeslagen gegevens kunnen opsporen en in beslag nemen om te voorkomen dat bewijsmateriaal wordt vernietigd. Rechtshandhavingsinstanties vinden dat zij over voldoende dwangmiddelen moeten beschikken om binnen het kader van hun bevoegdheden computersystemen te raadplegen en gegevens in beslag te nemen, personen te bevelen bepaalde computergegevens over te leggen, de snelle bewaring van specifieke gegevens overeenkomstig de normale wettelijke waarborgen en procedures te gelasten of te verkrijgen. Momenteel zijn de waarborgen en procedures echter niet op elkaar afgestemd.

Er kunnen zich problemen voordoen wanneer rechtshandhavingsinstanties, wanneer zij zich toegang verschaffen tot een computer, constateren dat meerdere computers en netwerken in

---

54 Naast de G8-leden hebben zich tot nu toe vijf EU-lidstaten aangesloten bij het 24/7-netwerk.

55 Op de wereldconferentie tegen de commerciële seksuele uitbuiting van kinderen van 28 augustus 1996 in Stockholm werd voorgesteld INTERPOL bij deze netwerken te betrekken. Het besluit van de Raad van de EU ter bestrijding van kinderpornografie op internet gaat ook uit van samenwerking met Europol op dit gebied.

56 Artikel 1, lid 4 van het Gemeenschappelijk standpunt: "De lidstaten moeten hun steun verlenen aan de vaststelling van bepalingen die de internationale samenwerking vergemakkelijken, waaronder bepalingen betreffende wederzijdse rechtsbijstand op zo groot mogelijke schaal. Het verdrag inzake cybercriminaliteit moet de snelle samenwerking vergemakkelijken waar het gaat om misdrijven op het vlak van of met behulp van computers. Deze vorm van samenwerking kan inhouden dat permanent toegankelijke contactpunten voor wetshandhaving worden opgezet, die de bestaande structuren voor wederzijdse bijstand aanvullen."

57 Zie http://www.usdoj.gov/criminal/cybercrime/action.htm, en ook http://www.usdoj.gov/criminal/cybercrime/principles.htm.

het hele land bij de zaak betrokken zijn. Maar de zaak wordt veel ingewikkelder wanneer rechtshandhavingsinstanties bij het raadplegen van een computer, of gewoon in de loop van een onderzoek, zich toegang verschaffen of moeten verschaffen tot gegevens die zich in een of meer andere landen bevinden. Dan staan er uiteenlopende belangen op het gebied van soevereiniteit, mensenrechten en rechtshandhaving op het spel, die met elkaar in evenwicht moeten worden gebracht.

De bestaande instrumenten voor internationale samenwerking in strafzaken, d.w.z. wederzijdse rechtshulp, bieden niet de juiste of onvoldoende mogelijkheden, omdat het meestal verschillende dagen, weken of maanden kost om ze toe te passen. Er moet een mechanisme komen waarmee landen snel en doeltreffend strafbare feiten kunnen onderzoeken en bewijsmateriaal kunnen verkrijgen, of waarmee tenminste wordt voorkomen dat belangrijk bewijsmateriaal in grensoverschrijdende rechtshandhavingsprocedures verloren gaat. Daarbij moeten nationale soevereiniteitsbeginselen, grondwettelijke rechten en mensenrechten, met inbegrip van de privacybescherming, in acht worden genomen.

In nieuwe voorstellen die momenteel in de Raad van Europa worden behandeld in het kader van het verdrag inzake cybercriminaliteit, is sprake van bevelen tot bewaring van gegevens in het belang van bepaalde onderzoeken. Andere punten, zoals grensoverschrijdende opsporing en inbeslagneming, vormen echter moeilijke en tot op heden onopgeloste beleidskwesties. Het is duidelijk dat er meer discussie nodig is tussen alle betrokken partijen voordat er concrete initiatieven kunnen worden genomen.

De subgroep voor hightech-criminaliteit van de G8 heeft zich over de problematiek van de grensoverschrijdende opsporing en inbeslagneming gebogen en, vooruitlopend op een permanentere overeenkomst, overeenstemming bereikt over voorlopige uitgangspunten[58]. Men overweegt vergelijkbare bepalingen op te nemen in het verdrag inzake cybercriminaliteit van de Raad van Europa. Daarvoor moeten echter belangrijke kwesties worden opgelost, die vooral te maken hebben met de vraag in welke situaties kan worden overgegaan tot snelle opsporing en inbeslagneming voordat de staat waarin dit plaatsvindt, wordt ingelicht, en moeten de nodige waarborgen dat de grondrechten in acht worden genomen, worden ingebouwd. In het Gemeenschappelijk standpunt over het verdrag van de Raad van Europa inzake cybercriminaliteit hebben de ministers dit open gelaten.[59]

Bij grensoverschrijdende zaken op het gebied van computercriminaliteit zijn ook duidelijke regels nodig over welk land bevoegd is voor vervolging. Met name moet worden voorkomen dat geen enkel land bevoegd is. De hoofdregel in het ontwerpverdrag van de Raad van Europa luidt dat een staat bevoegd is wanneer het strafbare feit op zijn grondgebied of door een van zijn onderdanen is gepleegd. Indien meerdere staten de bevoegdheid opeisen, moeten de betrokken staten overleg plegen om te bepalen waar de bevoegdheid moet liggen. Veel zal

---

58 Communiqué van de ministersconferentie van de G8-landen over de bestrijding van grensoverschrijdende georganiseerde criminaliteit. Moskou, 19-20 oktober 1999 (zie http://www.usdoj.gov/criminal/cybercrime/action.htm en ook http://www.usdoj.gov/criminal/cybercrime/principles.htm).

59 PB L 142/2: "Onder voorbehoud van constitutionele beginselen en specifieke garanties om op passende wijze de soevereiniteit, de veiligheid, de openbare orde en andere wezenlijke belangen van andere staten te eerbiedigen, kan in uitzonderlijke gevallen een grensoverschrijdende computeropsporing voor een onderzoek naar een nader in het verdrag inzake cybercriminaliteit te omschrijven ernstig misdrijf worden overwogen, en in het bijzonder wanneer er spoed vereiste is, bijvoorbeeld wanneer dit nodig is (...) om misdrijven te voorkomen die de dood of ernstig lichamelijk letsel van een persoon tot gevolg kunnen hebben."

echter afhangen van bilateraal of multilateraal overleg. De Commissie zal zich hier nader over buigen om te zien of er op EU-niveau verdere maatregelen nodig zijn.

De Commissie heeft deelgenomen aan de discussies in de Raad van Europa en in de G8, en kent de complexiteit van de problematiek op het gebied van het procesrecht. Maar samenwerking binnen de EU om cybercriminaliteit te bestrijden is van wezenlijk belang voor een veiliger informatiemaatschappij en voor de totstandbrenging van een ruimte van vrijheid, veiligheid en rechtvaardigheid.

De Commissie is voornemens om het overleg met alle betrokken partijen de komende maanden voort te zetten en op de reeds verrichte werkzaamheden voort te bouwen. Over deze problematiek zal ook worden gesproken in verband met de werkzaamheden van de Commissie op het gebied van de tenuitvoerlegging van de conclusies van de Europese Raad van Tampere van oktober 1999. Deze heeft de Commissie met name verzocht vóór december 2000 een programma goed te keuren ter uitvoering van het beginsel van wederzijdse erkenning van rechterlijke beslissingen. De Commissie heeft al een mededeling over de wederzijdse erkenning van definitieve beslissingen in strafzaken gepubliceerd.[60] Als onderdeel van haar bijdrage aan de tenuitvoerlegging van het deel van het programma dat betrekking heeft op aan het proces voorafgaande gerechtelijke bevelen, zal de Commissie, met het oog op de indiening van een wetgevingsvoorstel in het kader van Titel VI van het VEU, de mogelijkheden onderzoeken voor wederzijdse erkenning van aan het proces voorafgaande gerechtelijke bevelen in onderzoeken naar cybercriminaliteit.

5.6. Bewijskracht van computergegevens

Ook als rechtshandhavingsinstanties toegang hebben gekregen tot computergegevens die strafbare feiten lijken te bewijzen, moeten zij deze in handen kunnen krijgen en authentiek verklaren, voordat ze bij strafrechtelijke onderzoeken en vervolgingen kunnen worden gebruikt. Dat is niet eenvoudig, gezien de vluchtige aard van elektronische gegevens en het gemak waarmee deze gemanipuleerd, vervalst, technologisch beschermd of verwijderd kunnen worden. De forensische informatica houdt zich bezig met deze problematiek, en richt zich op de ontwikkeling en het gebruik van wetenschappelijke protocollen en procedures voor het opsporen van computergegevens en het analyseren en het handhaven van de authenticiteit van de verkregen gegevens.

Op verzoek van deskundigen van de G8 zal de Internationale organisatie inzake computerbewijs (IOCE) aanbevelingen voor standaarden opstellen, waarbij gemeenschappelijke definities en identificatiemethoden en -technieken worden ontwikkeld en een gemeenschappelijk formaat voor gerechtelijke verzoeken wordt opgesteld. De EU moet deelnemen aan deze werkzaamheden, zowel op het niveau van de in onderzoek naar computercriminaliteit gespecialiseerde instanties van de lidstaten als via O&O dat wordt gesteund door het 5e kaderprogramma (IST-programma).

6. NIET-WETGEVENDE MAATREGELEN

Toepasselijke wetgeving is nodig, zowel op nationaal als op internationaal niveau, maar op zichzelf niet voldoende om computercriminaliteit en misbruik van netwerken doeltreffend te bestrijden. Ter aanvulling van de wettelijke maatregelen moeten ook een aantal bijkomende, niet-wetgevende voorwaarden worden geschapen. De meeste daarvan worden vermeld in de

---

60 COM(2000)495, Brussel, 26.7.2000.

aanbevelingen van de COMCRIME-studie, de G8 hebben ze voorgesteld in het 10-punten actieplan van de G8, en ze kregen brede steun van alle betrokkenen in het informele overleg dat aan deze mededeling is voorafgegaan. Het gaat om:

- de oprichting van speciale in computercriminaliteit gespecialiseerde politie-eenheden op nationaal niveau, waar die nog niet bestaan;

- verbetering van de samenwerking tussen de rechtshandhavingsinstanties, het bedrijfsleven, consumentenorganisaties en gegevensbeschermingsautoriteiten;

- bevordering van initiatieven vanuit het bedrijfsleven en vanuit de gemeenschap, bijvoorbeeld op het gebied van veiligheidsproducten.

In dit verband blijft encryptie waarschijnlijk een belangrijk punt. Encryptie is een essentieel instrument om het verstrekken en aannemen van nieuwe diensten, zoals elektronische handel, te vergemakkelijken en kan een wezenlijke bijdrage leveren aan criminaliteitspreventie op internet. De Commissie heeft haar beleid op het gebied van encryptie uiteengezet in haar mededeling over veiligheid van en vertrouwen in elektronische communicatie van 1997[61], waarin zij verklaarde dat zij zou proberen alle beperkingen van het vrije verkeer van encryptieproducten binnen de Europese Gemeenschap op te heffen. In de mededeling verklaarde de Commissie tevens dat binnenlandse beperkingen van het vrije verkeer van encryptieproducten in overeenstemming moeten zijn met het Gemeenschapsrecht en dat zij zal nagaan of deze nationale restricties gerechtvaardigd en evenredig zijn in het licht van de verdragsbepalingen inzake vrij verkeer, de jurisprudentie van het Hof van Justitie en de voorwaarden van de richtlijnen inzake gegevensbescherming. Dat neemt niet weg dat de Commissie inziet dat encryptie rechtshandhavingsinstanties ook voor nieuwe en moeilijke problemen stelt.

De Commissie is daarom blij met de onlangs goedgekeurde herziene verordening inzake goederen voor tweeërlei gebruik, die in belangrijke mate bijdraagt tot een grotere beschikbaarheid van encryptieproducten, waarbij zij tegelijkertijd erkent dat dit moet samengaan met een betere dialoog tussen gebruikers, bedrijfsleven en rechtshandhavingsinstanties. De Commissie probeert aan de verbetering van deze dialoog op EU-niveau bij te dragen door middel van het EU-Forum voor hightech-criminaliteit. Wanneer in de gehele EU beveiligingsproducten beschikbaar zijn, zoals goede encryptieproducten, waar nodig erkend op basis van daartoe overeengekomen criteria, bevordert dat zowel de mogelijkheden op het gebied van criminaliteitspreventie als het vertrouwen van de gebruikers in de processen die zich afspelen in de informatiemaatschappij.

6.1. Gespecialiseerde eenheden op nationaal niveau

Vanwege de technische en juridische complexiteit van bepaalde met de computer verband houdende strafbare feiten, is het van essentieel belang dat op nationaal niveau gespecialiseerde eenheden worden opgezet. Deze gespecialiseerde eenheden, met deskundig, multidisciplinair (rechtshandhaving en rechterlijke macht) personeel, moeten over voldoende technische faciliteiten beschikken en optreden als snelle contactpunten die:

---

[61] COM (97)503.

- snel reageren op verzoeken om informatie over veronderstelde strafbare feiten. Er moet een gemeenschappelijk formaat worden ontwikkeld voor de uitwisseling van dergelijke informatie, hoewel uit discussies van deskundigen van de G8 is gebleken dat dat geen eenvoudige opgave is, gezien de verschillen in nationale juridische culturen;

- nationaal en internationaal functioneren als rechtshandhavings-contactpunt voor hotlines[62] die klachten van internetgebruikers ontvangen over illegale inhoud;

- gespecialiseerde computeronderzoekstechnieken ontwikkelen en/of verbeteren gericht op het opsporen, onderzoeken en vervolgen van computercriminaliteit;

- dienst doen als kenniscentrum op het gebied van cybercriminaliteit, waar goede praktijken en ervaringen kunnen worden uitgewisseld.

Sommige EU-lidstaten hebben al dergelijke gespecialiseerde eenheden opgezet die zich specifiek bezighouden met computercriminaliteit. De Commissie vindt dat dit een taak van de lidstaten is en dringt er krachtig bij hen op aan stappen in die richting te zetten. De aanschaf van de nieuwste hard- en software voor deze eenheden en de opleiding van het personeel brengt aanzienlijke kosten met zich, waarover op het daartoe aangewezen regeringsniveau prioriteiten moeten worden gesteld en politieke besluiten moeten worden genomen.[63] De ervaring van reeds bestaande eenheden in de lidstaten kan bijzonder waardevol zijn. De Commissie zal de uitwisseling van dergelijke ervaringen sterk aanmoedigen.

De Commissie is ook van mening dat Europol een bijdrage kan leveren op EU-niveau, in de vorm van coördinatie, analyse en andere bijstand aan de nationale gespecialiseerde eenheden. De Commissie zal daarom pleiten voor de uitbreiding van de opdracht van Europol, zodat cybercriminaliteit daar ook onder valt.

6.2. Gespecialiseerde opleiding

Er moeten grote inspanningen worden geleverd op het gebied van de continue, gespecialiseerde opleiding van de politiemensen en het gerechtelijk personeel. De technieken en mogelijkheden op het gebied van computercriminaliteit veranderen veel sneller dan die bij meer traditionele criminele activiteiten.

Sommige lidstaten hebben maatregelen getroffen om personeel van rechtshandhavingsinstanties te scholen op hightech gebied. Zij zouden de lidstaten die dat nog niet hebben gedaan, van advies kunnen dienen en kunnen begeleiden.

---

62 Tot nu toe beschikt slechts een beperkt aantal landen over hotlines. Voorbeelden daarvan zijn Cybertipline in de VS en Internet Watch Foundation (IWF) in het VK, dat sinds dec. 1996 een telefonische- en een e-mailhotline voert, waarop het publiek kan melden dat zij materiaal op internet zijn tegengekomen dat zij illegaal achten. De IWF beoordeelt of dat inderdaad het geval is en licht vervolgens de internet service providers en de politie in. Ook in andere landen bestaan controleorganen, bijvoorbeeld in Noorwegen (Redd Barna), Nederland (Meldpunt), Duitsland (Newswatch, FSM en Jugendschutz), Oostenrijk (ISPAA) en Ierland (ISPAI). In het kader van het EU-Daphneprgrogramma, loopt bij Childnet International momenteel een project dat rechtstreeks verband houdt met deze problematiek ("International Hotline Providers in Europe Forum"). De deskundigen van de UNESCO die in januari 1999 in Parijs bijeenkwamen, toonden zich ook voorstander van nationale hotlines en van de oprichting van netwerken van hotlines of van een internationale "elektronische wachttoren".

63 Voor de ervaring in de VS op dit gebied, zie Michael A. Sussmann “The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium”, Duke Journal of Comparative and International Law, Deel 9, voorjaar 1999, blz. 464.

Met steun van door de Commissie beheerde programma's (met name STOP, FALCONE en GROTIUS) zijn al projecten opgezet om dat te bewerkstelligen, in de vorm van de uitwisseling van ervaringen en studiebijeenkomsten over gemeenschappelijke problemen waarmee de betrokken beroepsgroepen te maken krijgen. De Commissie zal voorstellen doen voor meer activiteiten op dit gebied, onder andere voor computer- en on line-opleidingen.

Europol heeft het initiatief genomen tot een opleidingsweek voor personeel van rechtshandhavingsinstanties in november 2000, waarin kinderpornografie centraal staat. Het thema van zo'n week zou kunnen worden uitgebreid tot computercriminaliteit in het algemeen. Ook Interpol is al een aantal jaren actief op dit gebied. De Interpol-activiteiten zouden kunnen worden uitgebreid zodat er meer cursisten kunnen deelnemen.

De G8 heeft initiatieven ontwikkeld voor het uitwisselen van ervaringen tussen rechtshandhavingsinstanties en het opzetten van gemeenschappelijke onderzoekstechnieken op basis van concrete gevallen. In de tweede helft van 2000 en het begin van 2001 wordt een nieuw opleidingsinitiatief verwacht. De EU-lidstaten die deel uitmaken van de G8 zouden de andere lidstaten deelgenoot kunnen maken van deze ervaringen.

Bij de bestrijding van kinderpornografie op internet zou het opsporen van slachtoffers en daders, het vaststellen van de aard van de strafbare feiten en het opleiden van gespecialiseerde politiemensen worden vergemakkelijkt als er een digitale centrale bibliotheek van kinderpornografische beelden op internationaal niveau zou worden opgezet en bijgehouden (die via internet toegankelijk moet zijn voor nationale ter zake gespecialiseerde rechtshandhavingseenheden, met inachtneming van de nodige regels en beperkingen op het gebied van toegang en privacybescherming).[64]

6.3. Betere informatie en gemeenschappelijk regels voor het bijhouden van gegevens

Geharmoniseerde regels voor het bijhouden van gegevens door politie en justitie en goede instrumenten voor de statistische analyse van computercriminaliteit zouden het voor rechtshandhavingsinstanties en gerechtelijke autoriteiten gemakkelijker maken om de formele informatie over dit nog steeds veranderende gebied beter te bewaren, analyseren en beoordelen.

Uit het oogpunt van de particuliere sector gezien, zijn dergelijke statistieken nodig om de risico's goed te beoordelen en een kosten-batenanalyse te maken van het beheersen ervan. Dat is niet alleen belangrijk uit operationeel oogpunt (bijvoorbeeld om te besluiten welke beveiligingsmaatregelen nodig zijn), maar ook in verband met verzekeringen.

De database over de voorschriften op het gebied van computercriminaliteit, die deel uitmaakte van de COMCRIME-studie, wordt momenteel bijgewerkt en toegankelijk gemaakt voor de Commissie. De Commissie zal nagaan hoe de inhoud en de bruikbaarheid van deze database kunnen worden verbeterd (wetten, rechtszaken en literatuur opnemen).

---

64 Het "Excalibur"-project van de Zweedse nationale criminele inlichtingendienst, dat in het kader van het STOP-programma mede door de Europese Commissie werd gefinancierd, is een succesvol voorbeeld in dit verband. Dit project is opgezet in samenwerking met politiediensten in Duitsland, het VK, Nederland en België, en samen met Europol en Interpol uitgevoerd. Ook andere projecten, zoals die van het Duitse BKA ("Perkeo") en het Franse ministerie van Binnenlandse Zaken ("Surfimage", ook medegefinancierd in het kader van het STOP-programma) zijn goede voorbeelden.

6.4. Samenwerking tussen de verschillende betrokken partijen: het EU-Forum

Doeltreffende samenwerking tussen overheid en bedrijfsleven, binnen het wettelijk kader, wordt beschouwd als een essentieel aspect van elke vorm van overheidsbeleid ter bestrijding van computercriminaliteit.[65] Vertegenwoordigers van rechtshandhavingsinstanties geven toe dat zij niet altijd duidelijk genoeg hebben aangegeven wat zij verlangen van internet service providers. Vertegenwoordigers van het bedrijfsleven staan in het algemeen positief tegenover een betere coördinatie met rechtshandhavingsinstanties, waarbij zij benadrukken dat de bescherming van de fundamentele rechten en vrijheden van de burgers, met name het recht op privacy,[66] de noodzaak om criminaliteit te bestrijden en de economische lasten die de providers krijgen opgelegd, goed op elkaar moeten worden afgestemd.

Samen kunnen het bedrijfsleven en de rechtshandhavingsinstanties het publiek wijzen op de gevaren van criminelen op internet, de beste beveiligingspraktijken bevorderen en doeltreffende instrumenten en procedures voor de bestrijding van criminaliteit ontwikkelen. In een aantal lidstaten zijn al initiatieven op dit gebied ontwikkeld, waarvan het Internet Crime Forum in het VK waarschijnlijk het oudste en meestomvattende is.[67]

De Commissie juicht deze initiatieven toe en vindt dat ze in alle lidstaten moeten worden gestimuleerd. De Commissie is voornemens een EU-Forum op te richten waarin rechtshandhavingsinstanties, internet service providers, telecommunicatie-exploitanten, organisaties op het gebied van burgerlijke vrijheden, consumentenorganisaties, gegevensbeschermingsautoriteiten en andere belanghebbende partijen worden samengebracht om de samenwerking op EU-niveau zoveel mogelijk kracht bij te zetten. In eerste instantie gaat het daarbij om door de lidstaten aangewezen ambtenaren, technologiedeskundigen, privacy-deskundigen die door de Groep voor gegevensbescherming van artikel 29 worden aangewezen, en vertegenwoordigers van het bedrijfsleven en van de consumenten die in nauw overleg met bedrijfs- en consumentenorganisaties worden benoemd. In een later stadium zullen ook vertegenwoordigers van nationale initiatieven op dit gebied deel uitmaken van het Forum.

Het EU-Forum zal open en doorzichtig tewerk gaan, relevante documenten op een website toegankelijk maken en alle betrokken partijen om reacties vragen.

---

65 In het communiqué van 9/10 december 1997 over de beginselen en het 10-punten actieplan ter bestrijding van hightech-criminaliteit, verklaarden de ministers van Justitie en van Binnenlandse Zaken van de G8 dat het bedrijfsleven de wereldwijde netwerken ontwerpt, aanlegt en onderhoudt, en dus ook als eerste verantwoordelijk is voor het ontwikkelen van technische standaarden. En dus moet het bedrijfsleven volgens de G8 bijdragen aan de ontwikkeling en verspreiding van veiligheidssystemen waarmee het opsporen van computermisbruik, het bewaren van elektronisch bewijsmateriaal en het vaststellen van de verblijfplaats en identiteit van criminelen kunnen worden vergemakkelijkt. In het besluit van de EU ter bestrijding van kinderpornografie op internet wordt onderstreept dat de lidstaten een constructieve dialoog met het bedrijfsleden moeten voeren en moeten samenwerken door hun ervaringen uit te wisselen.

66 Zoals beschreven in de EU-richtlijnen over gegevensbescherming, het mensenrechtenverdrag van de Raad van Europa en verdrag nr. 108 van de Raad van Europa voor de bescherming van personen in verband met de geautomatiseerde verwerking van persoonsgegevens, en nationale wetgeving op dit gebied.

67 Het Internet Crime Forum werd opgericht in 1997 en bestaat uit politieambtenaren, ambtenaren van Binnenlandse Zaken, gegevensbeschermingsambtenaren en vertegenwoordigers van de Internetsector; het Forum houdt 3-4 maal per jaar een plenaire vergadering en telt daarnaast een aantal permanente werkgroepen.

Het is de bedoeling dat het EU-Forum zich in het bijzonder gaat bezighouden met:

- het instellen, waar nodig, van 24-uurs contactpunten tussen overheid en bedrijfsleven;

- het ontwikkelen van een standaardformaat voor verzoeken om informatie van rechtshandhavingsinstanties aan het bedrijfsleven, waarbij rechtshandhavingsinstanties meer via internet moeten communiceren met internet service providers;

- het stimuleren van de ontwikkeling en/of de toepassing van gedragscodes en beste praktijken en het uitwisselen van dergelijke codes tussen het bedrijfsleven en de overheid[68]

- het bevorderen van de uitwisseling van informatie over trends in hightech-criminaliteit tussen de verschillende partijen, met name tussen het bedrijfsleven en de rechtshandhavingsinstanties;

- de rechtshandhavingsaspecten bij de ontwikkeling van nieuwe technologie;

- het bevorderen van de verdere ontwikkeling van systemen voor vroegtijdige waarschuwing en crisisbeheersing, teneinde bedreigingen of ontwrichtende gebeurtenissen op informatie-infrastructuren te voorkomen, te achterhalen en op te lossen;

- het leveren, indien nodig, van extra deskundigheid bij lopende werkzaamheden in de Raad en andere internationale fora, zoals de Raad van Europa en de G8;

- het bevorderen van de samenwerking tussen de betrokken partijen, onder andere door gemeenschappelijk uitgangspunten van rechtshandhavingsinstanties, bedrijfsleven en gebruikers te formuleren (b.v. memoranda van overeenstemming, gedragscodes).

6.5. Maatregelen vanuit het bedrijfsleven

Bestrijding van computercriminaliteit is in het belang van de gemeenschap als geheel. Om consumenten vertrouwen te geven in de elektronische handel, moeten maatregelen om computercriminaliteit een vanzelfsprekend goed zakelijk gebruik zijn. Veel sectoren, zoals het bankwezen, de elektronische communicatiesector en de sector van creditcards en auteursrecht, alsmede hun klanten, zijn potentiële slachtoffers van computercriminaliteit. Ondernemingen beschermen vanzelfsprekend hun naam en handelsmerk, en hebben dan ook een taak op het gebied van fraudebestrijding. Bepaalde organisaties die de software- en audiosector vertegenwoordigen (zoals British Phonographic Industry - BPI) hebben teams die onderzoek doen naar piraterij (met inbegrip van internet-piraterij). In verschillende lidstaten hebben internet service providers telefoonlijnen opengesteld waar illegale en schadelijke inhoud op internet kan worden gemeld.

De Commissie steunt sommige van deze initiatieven door ze op te nemen in het O&O-kaderprogramma van de EU**,** het Internet-actieplan[69] en Programma's in het kader van titel VI, zoals STOP en DAPHNE.

---

[68] Voor zover het gaat om gedragscodes in de zin van artikel 27 van Richtlijn 95/46/EG (die bijvoorbeeld betrekking zouden kunnen hebben op onderwerpen die onder Richtlijn 97/66/EG vallen, zoals aftappen), zijn de Groep voor gegevensbescherming van artikel 29 en de nationale instanties die toezichthouden op gegevensbescherming, daarbij betrokken.

[69] Meer informatie over het Internet-actieplan: Actieplan ter bevordering van een veiliger gebruik van Internet, beschikbaar op http://158.169.50.95:10080/iap/.

In het kader van het EU-Forum zullen goede praktijken op deze gebieden worden uitgewisseld.

6.6. Door de EU gesteunde OTO-projecten

In het OTO-Programma Technologieën van de informatiemaatschappij (IST), dat deel uitmaakt van het vijfde Kaderprogramma 1998 - 2002, ligt de nadruk op de ontwikkeling en het gebruik van vertrouwenwekkende technologie. Daaronder worden zowel informatie- als netwerkbeveiligingstechnieken verstaan, alsmede technische instrumenten en methoden om inbreuk op het fundamentele recht op bescherming van de persoonlijke levenssfeer en van persoonsgegevens en andere persoonlijke rechten tegen te gaan en computercriminaliteit te bestrijden.

Het IST-programma, en met name de werkzaamheden op het gebied van de *informatie- en netwerkbeveiliging en andere technologieën ter versterking van het vertrouwen*, in Kernactiviteit 2 - *Nieuwe werkmethoden en elektronische handel*, vormt het kader waarbinnen de vaardigheden en de technologie kunnen worden ontwikkeld om inzicht te krijgen in en oplossingen te vinden voor de problemen op het gebied van de preventie en de bestrijding van computercriminaliteit waarmee de nieuwe technologie gepaard gaat, en ervoor te zorgen dat op het niveau van de EU, op het niveau van virtuele gemeenschappen en op het niveau van het individu aan de beveiligings- en privacyeisen kan worden voldaan.

Eveneens in het kader van het IST-programma is een betrouwbaarheidsinitiatief ontwikkeld om problemen die verband houden met het vertrouwen in de informatiemaatschappij, zoals de preventie en bestrijding van computercriminaliteit, op te lossen. Dit initiatief moet vertrouwen kweken in de informatie-infrastructuur met zijn vele onderlinge verbindingen en in volkomen in netwerken ingebedde systemen, door mensen te wijzen op het belang van betrouwbaarheid en door het gebruik van betrouwbaarheidverhogende technologie te bevorderen. Internationale samenwerking is een belangrijk aspect van dit initiatief. In het kader van het IST-programma zijn contacten gelegd met het DARPA en de NSF en is, in samenwerking met het Amerikaanse ministerie van Buitenlandse Zaken, een gemeenschappelijke EG/VS task force voor de bescherming van essentiële infrastructuur opgericht, onder supervisie van de gemeenschappelijke adviesgroep van de overeenkomst tussen de EG en de VS inzake wetenschappelijke en technologische samenwerking.[70]

Het Gemeenschappelijk Centrum voor Onderzoek (GCO), dat het betrouwbaarheidsinitiatief van het IST-programma ondersteunt, zal zich, in overleg met andere betrokken partijen, inclusief Europol, vooral richten op de ontwikkeling van passende en geharmoniseerde maatregelen, indicatoren en statistieken. Dit om de illegale activiteiten, de geografische spreiding en de toename ervan en de doeltreffendheid van maatregelen ter bestrijding van deze activiteiten, in kaart te brengen en er meer inzicht in te verkrijgen. Waar nodig zal het GCO andere onderzoeksgroepen bij de werkzaamheden betrekken en voortbouwen op hun resultaten. Het Centrum zal een website opzetten en verslag uitbrengen aan het EU-Forum over de voortgang van de werkzaamheden.

---

[70] Meer informatie over het IST-programma is te vinden op: http://www.cordis.lu/ist.

7. CONCLUSIES EN VOORSTELLEN

Om computercriminaliteit te kunnen voorkomen en bestrijden moet aan een aantal voorwaarden worden voldaan:

- beschikbaarheid van preventieve technieken. Dit vereist een regelgevend klimaat waarin innovatie en onderzoek worden gestimuleerd. Soms is overheidsfinanciering nodig om de ontwikkeling en het gebruik van beveiligingstechnieken te steunen.

- bewustzijn van de potentiële veiligheidsrisico's en de manieren om die te beperken;

- passende materiële en procedurele wettelijke voorschriften, zowel voor binnenlandse als voor grensoverschrijdende criminele activiteiten. Nationaal materieel strafrecht moet breed en doeltreffend zijn, zodat ernstige met de computer verband houdende inbreuken strafbaar kunnen worden gesteld en sancties kunnen worden opgelegd, dubbele strafbaarheid kan worden voorkomen[71] en internationale samenwerking wordt vergemakkelijkt. Wanneer rechtshandhavingsinstanties om gegronde redenen binnen hun nationale bevoegdheden snel computergegevens moeten kunnen opsporen, in beslag nemen en kopiëren, om een bepaald geval van computercriminaliteit te kunnen onderzoeken, moet het procesrecht in deze mogelijkheid voorzien, met inachtneming van de beginselen en uitzonderingen van het Gemeenschapsrecht en het Europese Verdrag tot bescherming van de rechten van de mens. De Commissie denkt dat de afspraken over aftappen in het kader van de Overeenkomst betreffende de wederzijdse rechtshulp het maximum is dat op dit moment haalbaar is. De Commissie zal de tenuitvoerlegging van de overeenkomst voortdurend evalueren met de lidstaten, het bedrijfsleven en de gebruikers, om ervoor te zorgen dat initiatieven op dat gebied doeltreffend, transparant and evenwichtig zijn;

- beschikbaarheid van voldoende goed opgeleid en goed uitgerust rechtshandhavingspersoneel. Nauwe samenwerking met internet service providers en telecommunicatie-exploitanten op opleidingsgebied zal verder worden aangemoedigd;

- betere samenwerking tussen alle betrokken partijen; gebruikers en consumenten, bedrijfsleven, rechtshandhavingsinstanties en instanties die toezicht houden op gegevensbescherming. Dit is van wezenlijk belang voor het onderzoeken van computercriminaliteit en het beschermen van de openbare veiligheid. Het bedrijfsleven moet met duidelijke regels en verplichtingen werken. De overheid moet erkennen dat de behoeften van de rechtshandhavingsinstanties lasten voor het bedrijfsleven met zich kunnen brengen en moet daarom in redelijkheid maatregelen treffen om deze lasten zoveel mogelijke te beperken. Tegelijkertijd moet het bedrijfsleven in de bedrijfsvoering rekening houden met de openbare veiligheid. Daarvoor zal in toenemende mate de actieve medewerking en steun van de individuele gebruiker en consument nodig zijn;

- voortdurende initiatieven vanuit het bedrijfsleven en vanuit de gemeenschap. Hotlines die al worden gebruikt voor het melden van illegale en schadelijke inhoud op internet, kunnen ook worden gebruikt voor andere soorten inbreuken. Zelfregulering van het bedrijfsleven en een multidisciplinair memorandum van overeenstemming moeten worden toegepast door zoveel mogelijk betrokken partijen en worden gebruikt om computercriminaliteit te helpen voorkomen en bestrijden en de alertheid en het vertrouwen te verhogen;

---

[71] Wanneer bij strafrechtelijke onderzoeken de bijstand van autoriteiten in een ander land is, zijn bepaalde vormen van wederzijdse rechtshulp en uitlevering vaak wettelijk gekoppeld aan de voorwaarde dat het gepleegde feit in beide landen strafbaar is.

- de resultaten en de mogelijkheden van O&O moeten zoveel mogelijk worden benut. Het beleid zal erop gericht zijn de ontwikkelingen op het gebied van betaalbare en doeltreffende beveiligings- en andere vertrouwenwekkende technologie en de EU-beleidsinitiatieven op elkaar af te stemmen.

Wanneer maatregelen worden genomen op EU-niveau, moet daarbij echter rekening worden gehouden met het feit dat de kandidaat-landen geleidelijk moeten worden opgenomen in de samenwerkingsverbanden binnen en buiten de EU op dit gebied en dat moet worden voorkomen dat zij worden gebruikt als vrijhavens voor computercriminaliteit. Overwogen moet worden vertegenwoordigers van deze landen bij sommige of alle EU-vergaderingen hierover te betrekken.

De voorstellen van de Commissie kunnen als volgt worden onderverdeeld:

7.1. Wetgevingsvoorstellen

De Commissie zal op grond van Titel VI van het Verdrag betreffende de Europese Unie wetgevingsvoorstellen indienen:

- om de wetgevingen van de lidstaten op het gebied van kinderpornografie meer op elkaar af te stemmen. Dit initiatief zal deel uitmaken van een pakket voorstellen over seksuele uitbuiting van kinderen en mensenhandel, zoals de Commissie heeft aangekondigd in haar mededeling over mensenhandel van december 1998. Zo'n voorstel sluit goed aan bij de wens van het Europees Parlement om het Oostenrijkse initiatief voor een besluit van de Raad over kinderpornografie om te zetten in een kaderbesluit dat de onderlinge afstemming van wetgeving vereist. Dit is eveneens in overeenstemming met de conclusies van Tampere en met de EU-strategie voor het nieuwe millennium ter bestrijding van de georganiseerde criminaliteit. Dit maakt al deel uit van het scorebord voor de totstandbrenging van een ruimte van vrijheid, veiligheid en rechtvaardigheid.

- om het materiële strafrecht op het gebied van hightech-criminaliteit meer op één lijn te brengen. Daarbij gaat het onder meer om strafbare feiten die verband houden met hacking, denial of service attacks. Voorts zal de Commissie onderzoeken welke maatregelen mogelijk zijn tegen racisme en vreemdelingenhaat op internet, teneinde een voorstel te formuleren voor een kaderbesluit van de Raad in het kader van Titel VI van het VEU over zowel off line- als on line-activiteiten op het gebied van racisme en vreemdelingenhaat. Ook het probleem van de illegale drugshandel via internet zal worden onderzocht.

- om het wederzijdse erkenningsbeginsel toe te passen op aan het proces voorafgaande gerechtelijke bevelen in verband met onderzoeken naar cybercriminaliteit en om met de computer verband houdende strafrechtelijke onderzoeken waarbij meer dan één lidstaat is betrokken, gemakkelijker te maken, waarbij de nodige waarborgen ten aanzien van de grondrechten worden ingebouwd. Dit voorstel sluit aan bij het ontwerpprogramma voor wederzijdse erkenningsmaatregelen, waarin wordt gezegd dat moet worden nagedacht over voorstellen inzake het overleggen en bevriezen van bewijsmateriaal.

Of er maatregelen, met name van wetgevende aard, moeten worden genomen met betrekking tot het bewaren van verkeersgegevens, zal door de Commissie onder meer worden beoordeeld aan de hand van de resultaten van de werkzaamheden van het EU-Forum op dit gebied.

7.2. Niet-wetgevende voorstellen

De volgende maatregelen worden voorgesteld:

- de Commissie zal een EU-Forum opzetten en voorzitten waarin rechtshandhavingsinstanties, internet service providers, netwerk-exploitanten, consumentenorganisaties en gegevensbeschermingsautoriteiten worden samengebracht om de samenwerking op EU-niveau te verbeteren, door het publiek te wijzen op de gevaren van criminelen op internet, goede praktijken voor IT-beveiliging te bevorderen, doeltreffende instrumenten en procedures te ontwikkelen ter bestrijding van computercriminaliteit en de verdere ontwikkeling van mechanismen voor vroegtijdige waarschuwing en crisisbeheersing te stimuleren. Dit zou een EU-variant zijn van soortgelijke succesvolle fora in bepaalde lidstaten. De Commissie zal de lidstaten die nog niet zulke fora hebben, aanmoedigen die op te zetten. Het EU-Forum zou de samenwerking tussen deze verschillende fora bevorderen en vergemakkelijken.

- de Commissie zal veiligheid en vertrouwen blijven bevorderen in het kader van het the *e*Europe-initiatief, het Internet Actieplan, het IST-programma en het volgende OTO-kaderprogramma. Zij zal daarbij streven naar een grotere beschikbaarheid van producten en diensten die voldoende veiligheid bieden, en door middel van een dialoog met alle betrokken partijen het gebruik van encryptie op grotere schaal bevorderen.

- de Commissie zal in het kader van de bestaande programma's steun blijven verlenen voor projecten die zijn gericht op de scholing van rechtshandhavingspersoneel op het gebied van hightech-criminaliteit, en op onderzoek op het gebied van forensische informatica.

- de Commissie zal overwegen geld beschikbaar te stellen voor de verbetering van de inhoud en de bruikbaarheid van de database over de nationale wetgeving van de lidstaten die de COMCRIME-studie heeft opgeleverd, en zal een studie laten verrichten om een beter beeld te krijgen van de aard en de omvang van computercriminaliteit in de lidstaten.

7.3. Werkzaamheden in andere internationale fora

De Commissie zal blijven toezien op de coördinatie tussen de lidstaten in andere internationale fora waarin wordt gesproken over cybercriminaliteit, zoals de Raad van Europa en de G8. De Commissie zal er in het bijzonder naar streven de onderhandelingen in de Raad van Europa over het verdrag inzake cybercriminaliteit spoedig af te ronden. Bij haar initiatieven op EU-niveau zal de Commissie volop rekening houden met de werkzaamheden die in andere internationale fora zijn verricht, en daarbij streven naar onderlinge afstemming binnen de EU.

* * * * *

FINANCIEEL MEMORANDUM

1. BENAMING VAN DE MAATREGEL

De informatiemaatschappij veiliger maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden.

2. BEGROTINGSPLAATS(EN)

B5-302

B5-820

B6-1110, B6-2111, B6-1210

3. RECHTSGRONDSLAG

Artikelen 95, 154 en 155 van het EG-Verdrag en artikelen 29 en 34 van het Verdrag betreffende de Europese Unie

4. OMSCHRIJVING VAN DE MAATREGEL

4.1 Algemene doelstelling

De Commissie zal een EU-forum oprichten en voorzitten waarin rechtshandhavingsinstanties, internet service providers, telecommunicatie-exploitanten, organisaties op het gebied van burgerlijke vrijheden, consumentenorganisaties, gegevensbeschermingsinstanties en andere betrokken partijen samenkomen om het wederzijds begrip en de samenwerking op EU-niveau te verbeteren. Het forum zal het publiek wijzen op de gevaren van criminelen op internet, de beste beveiligingsmethoden bevorderen, zoeken naar doeltreffende instrumenten en procedures om computercriminaliteit te bestrijden, en de verdere ontwikkeling van systemen voor vroegtijdige waarschuwing en crisisbeheer bevorderen. Het EU-Forum zal relevante documenten op een website toegankelijk maken.

4.2 Looptijd en verlenging

2001-2002. In 2002 zal worden bekeken of het forum moet worden voortgezet.

5. INDELING VAN DE UITGAVEN/ONTVANGSTEN

5.1 Niet-verplichte uitgaven

5.2 Gesplitste kredieten

6. AARD VAN DE UITGAVEN/ONTVANGSTEN

Vergaderingen: reiskostenvergoeding voor deskundigen			
B5 302A	2001		27.000 €
B5 302A	2002		40.500 €
Werking van het forum, onderhoud van een website			
B6 1110	2001	JRC Dienstreizen	10.000 €
B6 2111	2001	JRC Specifieke kosten (diversen)	15.000 €
B6 1210	2001	JRC Algemene kosten	50.000 €
B6 1110	2002	JRC Diensreizen	10.300 €
B6 2111	2002	JRC Specifieke kosten (diversen)	15.450 €
B6 1210	2002	JRC Algemene kosten	51.500 €
Studies over bepaalde onderwerpen			
B6 2111	2001	JRC Specifieke kosten (studies)	25.000 €
B6 2111	2002	JRC Specifieke kosten (studies)	25.750 €
Totaal	2001 + 2002		270.500 €

7. FINANCIËLE GEVOLGEN

Wijze van berekening van de totale kosten van de maatregel (verhouding individuele/totale kosten)

DG INFSO: vergoeding van reiskosten voor de deelnemers aan de vergaderingen. Er zullen naar schatting 2 vergaderingen in 2001 worden gehouden en 3 in 2002. Per vergadering worden de reiskosten van 15 deskundigen vergoed. De gemiddelde kosten per persoon worden geraamd op 900 euro.

De kosten (zowel de specifieke als de personeelskosten) voor infrastructuur en administratieve en technische ondersteuning worden toegewezen in verhouding tot het aantal personeelsleden dat bij de desbetreffende activiteiten is betrokken. Bij de berekening van het budget voor studies is uitgegaan van 2 studies per jaar van elk ongeveer één man/maand.

8. MAATREGELEN TER BESTRIJDING VAN FRAUDE

Routinecontroles. Er zijn geen extra fraudebestrijdingsmaatregelen voorzien.

9. GEGEVENS KOSTEN-BATENANALYSE

9.1 Specifieke en kwantificeerbare doelstellingen; doelgroep

Bevordering van wederzijds begrip en samenwerking op EU-niveau tussen verschillende belangengroepen. Doelgroepen: rechtshandhavingsinstanties, internet service providers, telecommunicatie-exploitanten, organisaties op het gebied van burgerlijke vrijheden, consumentenorganisaties, gegevensbeschermingsinstanties en andere betrokken partijen.

9.2 Motivering van de maatregel

Het forum wordt opgericht om het wederzijds begrip en de samenwerking op EU-niveau tussen verschillende belangengroepen te verbeteren. Het forum zal het publiek wijzen op de gevaren van criminelen op internet, de beste beveiligingsmethoden bevorderen, zoeken naar doeltreffende instrumenten en procedures om computercriminaliteit te bestrijden, en de verdere ontwikkeling van systemen voor vroegtijdige waarschuwing en crisisbeheer bevorderen.

9.3 Follow-up en evaluatie van de maatregel

De Commissie zal de bijeenkomsten van het forum organiseren en voorzitten, en tevens deelnemen aan de discussies. De Commissie zal de bijbehorende website beheren. In 2002 zal worden bekeken of het forum in 2003 en daarna moet worden voortgezet.

10. ADMINISTRATIEVE UITGAVEN

De personeelsbehoeften zullen worden gedekt door de inzet van huidig personeel.

10.1 Gevolgen voor het aantal posten

Aard van de posten		Personeel voor het beheer van de maatregel		uit		periode
		Permanent	Tijdelijk	Bestaande middelen van betrokken DG of dienst	extra middelen	
Ambtenaren of tijdelijke functionarissen	A B C	0,05	1,75 0,15	1,75 0,15 0,05		per jaar, gedurende 2 jaar
Overige middelen						
Totaal		0,05	1,9	1,95		

10.2 Totale financiële weerslag van de inschakeling van personeel

	Bedragen	Berekeningsmethode (2001 - 2002)
Ambtenaren	421.200 €	2 jaar x 108.000 € x 1,95 pers.