

Bestrijding van Cybercrime en de noodzaak van internationale regelingen

Prof. Mr. H.W.K. Kaspersen¹

1. De ondragelijke lichtheid van het elektronisch bestaan.

Terwijl ik deze regels op mijn PC in Word verwerk, meldt mijn *firewall* zich met de boodschap dat een onbevoegd programma heeft getest of er poorten van mijn PC openstaan. Nadere analyse leert dat de *port scan* is uitgevoerd vanaf een computersysteem in Oslo. Blijkens de verder beschikbare informatie correspondeert het IP-nummer van het systeem vanwaar de *port scan* is uitgevoerd met een computersysteem dat bestemd is voor intern gebruik door de betreffende organisatie. Hieruit kan men gevoeglijk afleiden dat het scannen van mijn poorten niet geschiedt door of namens een rechtmatige gebruiker van dit laatste systeem maar dat het systeem wordt misbruikt door een *hacker* die zich een aantal bevoegdheden van dat systeem heeft toegeëigend en die na wil gaan of hij in mijn PC kan binnendringen. *Hacken* en het veroorzaken van ander ongerief lijkt de laatste tijd alleen maar in populariteit toe te nemen, waarbij de betrokkenen zich weinig aan de wettelijke normen gelegen laten liggen. Twee recente voorbeelden:

OvJ Tonino zet zijn privé PC aan de straat zonder deze van de inhoud te ontdoen. De PC komt in handen van tv-programmamaker P.R. de Vries die een deel van de inhoud bekend maakt. Hierbij wordt het privé e-mailadres van OvJ Tonino bekend, hetgeen krakers op het spoor brengt van Tonino's provider. De hackers slagen er vervolgens in om Tonino's mailbox bij deze provider op te sporen, te kraken en persoonlijke documenten uit die mailbox te publiceren.²

Een 18-jarige Bredenaar geeft leiding aan een hackergroep 0x1feCrew met een gelijknamige site in het domein.org. Deze groep richtte rond het weekend van 5 oktober 2004 een zgn. DDoS-aanval³ op de websites regering.nl en kabinet.nl waardoor deze sites en tot het domein behoren emailadressen een paar dagen buiten bedrijf waren. Het weblog Greenstijl beschikte over gegevens van de dader en bracht deze naar buiten om vervolgens zelf slachtoffer van een DDoS-aanval te worden.⁴ Betrokkene kwam desgevraagd op 19 oktober 2004 voor de TV uitleggen dat de 'actie' moest worden gezien als een protest tegen het regeringsbeleid.

Gezien de gelatenheid waarmee de gemiddelde internetgebruiker de risico's van het gebruik van die voorziening aanvaardt, lijkt hier geen groot maatschappelijk probleem aan de orde. Ik zie dat anders en gelukkig is dat ook de visie van het OM.⁵ De Nederlandse wetgever heeft het merendeel van bovenstaande gedragingen weliswaar strafbaar gesteld⁶, maar gezien het

¹ Hoogleraar Informatica en Recht, Vrije Universiteit, Amsterdam.

² Persoonlijk heb ik mij bijzonder geërgerd aan het bekend worden van het privé e-mailadres van OvJ Tonino, gevolgd door het kraken van diens mailbox en het publiceren van persoonlijke documenten uit die mailbox. Deze handelingen kunnen onder geen enkele omstandigheid worden gerechtvaardigd met een beroep op de vrijheid van meningsuiting. Kennelijk beschouwen de betrokkenen het kraken van computersystemen en mailboxen als vanzelfsprekend, 'normaal gedrag'.

³ Distributed Denial-of-Service Attack, d.w.z. tegelijkertijd ingezet vanaf verschillende computersystemen.

⁴ Webwereld 7 oktober 2004, <http://www.webwereld.nl/nieuws/19697.phtml>

⁵ In beide genoemde zaken loopt inmiddels strafrechtelijk onderzoek.

⁶ Zie Wet Computercriminaliteit, Stbl. 1993, 33.

geringe aantal vervolgingen dat in verband hiermee heeft plaatsgevonden, ontbreekt het kennelijk aan een systematische en effectieve opsporing van deze delicten.⁷ Teneinde daarin verbetering te kunnen brengen is behoefte aan een toereikend wettelijk kader, voldoende opsporingscapaciteit en technische expertise en, waar nodig, de mogelijkheid tot internationale samenwerking.⁸

In het onderstaande wil ik gaarne aandacht besteden aan wetgeving en internationale samenwerking. Paragraaf 2 bespreekt in kort bestek de aard en de omvang van crimineel gedrag op het internet met nadruk op het internationale, grensoverschrijdende karakter ervan. Voor het geheel van criminele activiteit op het internet wordt de term *Cybercrime* gebruikt. Paragraaf 3 behandelt wat daaronder moet worden verstaan. De opsporing van *Cybercrime* is in de regel geen eenvoudige zaak. Paragraaf 4 staat daarom kort stil bij de vergaring van zgn. elektronisch bewijs en de behoefte aan internationale bijstand. Paragraaf 5 richt zich op de noodzaak tot internationale strafrechtelijke samenwerking en bespreekt de inhoud en betekenis van het Cybercrimeverdrag van de Raad van Europa. Paragraaf 6 vat de bevindingen van dit opstel samen.

2. Internet als vrijplaats?

Hacken, sabotage, spionage en ander misbruik van de zegeningen van het internet vormen een ernstige bedreiging van de integriteit van dit inmiddels bepalend en onmisbare communicatiemiddel. Daarnaast bestaan er aanwijzingen dat criminele activiteit op het internet in een aantal gevallen verbindingen heeft met georganiseerde criminaliteit⁹ of terrorisme.¹⁰ Statistieken tonen een sterke groei van het aantal strafbare feiten in de loop der tijd. Ik moge hier bijvoorbeeld verwijzen naar periodieke rapporten van CSI in samenwerking met de FBI¹¹ en on-line slachtofferonderzoek over internetmisbruik¹² en de meerjarige systematische registratie van het aantal zaken dat in Duitsland ter kennis van politie en justitie is gekomen.¹³

Voor deze toename zijn allerlei redenen aan te voeren waarover de criminologisch deskundigen hun licht maar eens moeten laten schijnen. Er kan niet worden voorbijgegaan aan het feit dat de inrichting en de gebruiksmogelijkheden van het internet belangrijke criminogene factoren zijn. Zonder pretentie volledig te zijn, noem ik er een aantal in

⁷ Zie vragen Kamerleden Gerkens (Aanhangsel Handelingen TK 2004-2005, 227) en van Gerkens, Algra en van Haersma Buma (Aanhangsel Handelingen TK 2004-2005, vragen 2040501980 en 2040501990).

⁸ Die opvatting blijken ook de verantwoordelijke bewindslieden van Justitie, BZK en EZ toegegaan, gezien de in de landelijke pers op 5 november 2004 bekend geworden oprichting van een Nationaal High Tech Crime Center (NHTCC) als onderdeel van het KLPD.

⁹ Peter Grabosky, Russel G. Smith, *Crime in the Digital Age*, New Brunswick (NJ), 1998, p. 186 e.v. Council of Europe, *Organised Crime Situation Report 2004, Focus on the Threat of Cybercrime*, Restrcted, Strasbourg 10 september 2004, p.100-105. Zie ook de Kamervragen in het Nederlandse Parlement in noot 8.

¹⁰ Council of Europe, *a.w.*, p. 106-111. Wat in dit verband te denken van het ANP-bericht van 6 oktober 2004, dat Noord-Korea 600 computerexperts heeft opgeleid voor een internet-oorlog tegen de Verenigde Staten en Korea.

¹¹ Zie *Computer Crime and Security Survey 2004*, <http://www.gocsi.com>

¹² Werner R  ther, *Zusammenfassung der Ergebnisse der 1. Onlinebefragung zum Thema "Sicherheit und Delinquenz im Internet"*, Kriminologisch Seminar der Universit  t Bonn, 2003, [www.jura.uni-bonn.de/institute/krimsem/ Online-Publikationen/Sudi03/8Zusammenfassung.PDF](http://www.jura.uni-bonn.de/institute/krimsem/Online-Publikationen/Sudi03/8Zusammenfassung.PDF)

¹³ Bundes Kriminal Amt Wiesbaden, <http://www.bka.de>.

willekeurige volgorde. Internet biedt de burger grote mogelijkheden om geavanceerde computerprogramma's in te zetten voor crimineel gedrag, welke programma's of hulpmiddelen vaak via datzelfde internet door derden ter beschikking worden gesteld. Voorbeelden hiervan zijn software voor het ontwerpen en verspreiden van virussen, spamprogramma's, kraakprogramma's enz. Verder bestaat een belangrijk deel van de internetgemeenschap uit jonge mensen die ten aanzien van crimineel gedrag en de gevolgen daarvan vaak een andere instelling hebben dan leden van oudere generaties. Ook is een niet onbelangrijk gegeven dat internet globaal op dit moment meer dan 800 miljoen gebruikers heeft op een wereldbevolking van meer dan 6 miljard personen kent, met nog steeds groeipercentages in Afrika en het Midden-Oosten.¹⁴ Met het aantal gebruikers stijgt de criminaliteit mee, niet in de laatste plaats doordat de kans op het vinden van een slachtoffer ergens in de wereldwijde internetgemeenschap voor de elektronisch opererende cybercrimineel nauwelijks een probleem is, terwijl deze niet of nauwelijks wordt geconfronteerd met de gevolgen die zijn handelen voor het slachtoffer heeft. Evenmin is onbelangrijk dat het voor de gemiddelde internetcrimineel niet al te moeilijk is om zijn identiteit te verhullen, hetgeen zijn of haar opsporing aanstonds gecompliceerd maakt. Het leveren van bewijs dat een verdachte een cybercrime heeft begaan vergt dan ook dikwijls kostbare inspanningen.¹⁵ Het gegeven dat een succesvolle uitvoering van een cyberdelict in veel gevallen mogelijk was door nalatigheid van het slachtoffer zelf, dat geen adequate beveiliging op zijn computersysteem in werking had, prikkelt verantwoordelijke overheden wellicht wel tot het geven van voorlichting aan het publiek¹⁶ maar niet tot het stellen van opsporingsprioriteiten. Bovendien gaat van internationale regelingen zoals de (niet-) aansprakelijkheid van providers, zoals inmiddels vorm gegeven in art. 6: 196cBW¹⁷ een in dit opzicht een verkeerde boodschap uit, aangezien het voorschrift eerder gericht lijkt op de beëindiging van het strafbare feit en daarmee de verwijdering van bewijs dan op actieve opsporing.¹⁸

Internet is van een elektronische proeftuin geëvolueerd tot volwaardige segment van het maatschappelijk verkeer. Handhaving van de rechtsorde op het internet behoort dan ook niet anders te worden aangepakt dan bij andere, meer traditionele vormen van maatschappelijk verkeer. Een stevige complicatie daarbij is het internationale karakter van het internet en het grensoverschrijdende karakter van het internetverkeer. Deelnemers aan het internet maken deel uit van de rechtsorde die verbonden is met het grondgebied waarop zij wonen of verblijven, of in het andere geval, waar de computerapparatuur is opgesteld waarmee zij met internet in verbinding zijn. Dit leidt tot twee soorten problemen. De eerste bestaat uit de gevolgen van mogelijke verschillen tussen de betrokken nationale wetgevingen. Wat binnen de ene nationale rechtsorde als strafbaar, resp. onrechtmatig geldt, hoeft dat nog niet binnen een andere nationale rechtsorde te zijn. Souvereine staten zijn in het internationale

¹⁴ Internet World Stats, Usage and Population Statistics, <http://www.internetworldstats.com/stats.htm>, d.d. 27 oktober 2004.

¹⁵ Zie bijvoorbeeld Rechtbank Amsterdam d.d. 12 augustus 2004, LJN AQ6858, met een omstandige toelichting van het technisch bewijs door de forensisch deskundige. Naast het vergaarde materiaal dat aantoonde dat een bepaalde handeling door middel van een bepaald computersysteem is verricht, moet ook steeds worden bewezen dat het de verdachte was die de computer op het relevante moment bediende.

¹⁶ Zie <http://www.surfopsafe.nl> en <http://www.waarschuwingsdienst.nl> beide van het Ministerie van Economische Zaken.

¹⁷ Stbl. 2004, 210 i.w.tr.open.

¹⁸ Daaraan doet niet af dat niet alle providers in de praktijk in de aangewezen gevallen tot verwijdering overgaan. Zie Bits of Freedom d.d. 1 oktober 2004, <http://www.bof.nl>.

publiekrecht bevoegd om de nationale rechtsorde in te richten naar eigen behoefte en ideeën. Tussen nationale wetstelsels – het strafrecht is daar geen uitzondering op – kunnen derhalve grote verschillen bestaan. Dat klemmt des te meer indien de ene nationale wet bepaalde gedragingen verbiedt terwijl een andere - buitenlandse - wet die gedraging juist vrijlaat. Dat laatste bevordert het ontstaan van zogenaamde *data havens*, elektronische plaatsen van waaruit men onder bescherming van de eigen rechtsorde strafbare feiten kan plegen die effect hebben op het territorium van andere staten. Het is daarom aanbevelenswaardig dat de staten van deze wereld die door middel van het internet met elkaar zijn verbonden, zich inspannen om te komen tot meer gemeenschappelijke gedragsregels voor het internationaal elektronisch maatschappelijk verkeer. Daarvoor is (nog steeds) internationaal overleg nodig.

Het stellen van een gemeenschappelijke norm is een ding, het handhaven ervan is minstens zo belangrijk. Omdat internetverkeer internationaal is, is het voor rechtshandhavende instanties onontbeerlijk dat zij een beroep te kunnen doen op assistentie door collega's in andere landen. De bevoegdheid van Nederlandse opsporingsambtenaren houdt, behoudens toestemming van een bevoegde buitenlandse autoriteit, immers op bij de eigen landsgrens en dat ligt voor buitenlandse opsporingsautoriteiten niet anders.¹⁹ Het vergaren en de overdracht van elektronisch bewijs in andere landen moet derhalve aan de opsporingsautoriteiten van die landen worden overgelaten. Of, en op welke wijze rechtshulp wordt verleend wordt gemeenlijk geregeld in bilaterale of multilaterale verdragen die op hun beurt het resultaat zijn van internationaal overleg.

3. Cybercrime

Uit het pre-internet-tijdperk stamt het verzamelbegrip 'computercriminaliteit'. Daarbinnen kan men onderscheiden tussen 'computercriminaliteit in enge zin' en 'computercriminaliteit in brede zin'. Als computercriminaliteit in enge zin worden beschouwd de strafbare handelingen die zich richten op het verstoren of beïnvloeden van de werking van computersystemen of met die systemen onderhouden geautomatiseerde processen. Onder computercriminaliteit in ruimere zin begrijpt men gedragingen waarbij IT een belangrijke rol bij de uitvoering speelt, of die in een geautomatiseerde omgeving – bijvoorbeeld het internet - worden begaan.²⁰ Als overkoepelend begrip komt men tegenwoordig de populaire term *cybercrime* tegen. Hoewel niet alle computercriminaliteit zich on-line en in de internetomgeving af hoeft te doen en bovenstaande begrippen elkaar niet geheel dekken, is een aansprekende terminologie hier te prefereren. Onder *cybercrime* zijn derhalve te begrijpen alle strafbare gedragingen die gericht zijn tegen de vertrouwelijkheid, de integriteit en de beschikbaarheid van geautomatiseerde processen en middelen (computercriminaliteit in enge zin) en de strafbare handelingen waarbij ICT instrument of bepalende omgevingsfactor is (computercriminaliteit in brede zin). Voorbeelden van de eerste groep zijn het inbreken in computersystemen, (D)DoS-aanvallen en het lanceren van computervirussen en –wormen. In de tweede groep kan men strafbare handelingen plaatsen als elektronische vermogensdelicten (betalingsverkeer, telefoonfraude, afpersing), inhoud-gerelateerde delicten (kinderporno, racisme en discriminatie, het aanbod van illegale diensten

¹⁹ Art. 539a derde lid Sv. Het door middel van grensoverschrijdend onderzoek verkregen bewijs geldt als onrechtmatig, zie HR 12 december 2000, LJN AA8965.

²⁰ Internationaal – bijvoorbeeld in het kader van de G8 en politiesamenwerking - komt men wel de term 'high tech crime' tegen. Aangezien hedendaagse *high tech* vrijwel in alle gevallen gebruik maakt van enige vorm van informatietechnologie komen de genoemde begrippen praktisch op hetzelfde neer.

als internetcasino's en producten als medische preparaten), delicten op het gebied van de intellectuele eigendom en aantasting van de persoonlijke levenssfeer (spionage, *spam*, internet *stalking*). Wat betreft computercriminaliteit in enge zin vindt men in het Wetboek van Strafrecht vaak een specifieke strafbaarstelling. In geval van computercriminaliteit in brede zin valt de gedraging vaak in een technologie-onafhankelijke strafbaarstelling die correspondeert met de klassieke delictscategorieën van de nationale strafwet.²¹

In oude definities wordt als belangrijkste kenmerk van de dader van computercriminaliteit genoemd, dat deze over een grote mate van gespecialiseerde informaticakennis beschikt. Met de opkomst van gebruikersvriendelijke systemen en de openlijke beschikbaarheid op het internet van allerlei programmatuur, heeft de gemiddelde computercrimineel wellicht een kennisvoorsprong op de gemiddelde internetgebruiker, maar de computercrimineel is niet langer in alle gevallen van huis uit een ICT-expert. De voor de euveldaad benodigde kennis en middelen kunnen vaak op een betrekkelijk eenvoudige wijze worden verkregen.²² Vergoelijkend wordt in geval van computerinbraak en –sabotage wel gesproken van *cybervandalisme* om aan te geven dat men van doen heeft met jeugdige en daarom dikwijls onverantwoordelijke daders. Daarnaast worden via internet ook 'gewone' misdrijven gepleegd, waarbij een al dan niet handig gebruik wordt gemaakt van de vele mogelijkheden die het internet biedt.

4. De vergaring van elektronisch bewijs

Voor een succesvolle vervolging is toereikend bewijs nodig dat de verdachte in verbinding brengt met het strafbare feit. Meestal kan men bij de bewijsvoering twee stappen onderscheiden. De eerste stap betreft het bewijs dat bepaalde commando's, berichten of programma's vanaf een bepaald computersysteem zijn verstuurd. Indien dit systeem niet bekend is dient het spoor vanaf het slachtoffersysteem terug te worden gevolgd. *Hackers* dringen binnen in slecht beveiligde systemen en zijn in staat om de controle hiervan over te nemen. Die methode is populair om vanuit zo'n derde systeem bijvoorbeeld *spam* of computervirussen te verspreiden, waarbij het lijkt of die handeling door de niets vermoedende eigenaar van dat systeem is geïnitieerd. Voor identificatie van de werkelijke bron zijn gegevens nodig die door de *servers* in de communicatieketen zijn vastgelegd. Indien het computersysteem is geïdentificeerd en de locatie ervan bepaald is, dient tevens te worden vastgesteld dat het de verdachte was die de gewraakte datacommunicatie(s) initieerde.

In veel gevallen is er sprake van grensoverschrijdende communicaties. Voor het vergaren van bewijs zal veelal assistentie van buitenlandse opsporingsautoriteiten nodig zijn. In de internationale rechtspraktijk behoeft deze bijstand gemeenlijk een verdragsrechtelijke basis. Een verdrag bepaalt in die gevallen de omvang en de gevallen waarin dergelijke bijstand wordt verleend en onder welke voorwaarden het vergaarde bewijsmateriaal aan de

²¹ Zie bijvoorbeeld de terminologie van Russell G. Smith, Peter Graboski, Grogor Urbas, *Cyber Criminals on Trial*, Cambridge 2004, p. 7 die de volgende categorieën onderscheiden : a) IT speelt een rol bij het begaan van de misdaad ; b) het misdrijf is gericht tegen elektronische gegevensverwerking of communicatietechnologie; c) ICT is een factor bij het begaan van andere misdrijven.

²² Zie de beschrijving in het vonnis tegen de vervaardiger van het Anna Kournikova virus, Rechtbank Leeuwarden d.d. 27 september 2001. Zie het arrest van de Hoge Raad d.d. 28 september 2004, LJN AO7009. In Duitsland loopt een opsporingsonderzoek tegen een destijds 17-jarige scholier maker en verspreider van de zeer schadelijke Netsky en Sasser-virussen. (<http://www.egocrew.de>).

verzoekende staat ter beschikking wordt gesteld. Nederland heeft ten behoeve van het verkrijgen van internationale rechtshulp verschillende multi²³- en bilaterale verdragen in werking. Speciaal voor rechtshulpverlening met betrekking tot de vergaring van zgn. elektronisch bewijsmateriaal is door de Raad van Europa het Cybercrimeverdrag ontwikkeld.

5. Internationale rechtshulp: het Cybercrimeverdrag

5.1 De betekenis van het verdrag

Nederland heeft dit verdrag op 23 november 2001 ondertekend²⁴ en beoogt tot ratificatie van dit verdrag over te gaan. Tevens heeft Nederland op 21 januari 2003 het eerste Aanvullende Protocol²⁵ bij het verdrag ondertekend, dat eveneens door Nederland zal worden geratificeerd. Daartoe is nodig dat de nationale wetgeving uitvoering van de met het verdrag en het Protocol aangegane verplichtingen mogelijk maakt. Dat is nog niet (helemaal) het geval. In verband met het verdrag werd reeds wetswijziging voorzien. Het wetsvoorstel Computercriminaliteit II²⁶ is echter door een aantal ontwikkelingen ingehaald en is in de Tweede Kamer niet verder behandeld. Wel is inmiddels van kracht geworden het Wetsvoorstel Vorderen gegevens Telecommunicatie²⁷ dat een tevens deel van de verdragstekst implementeert. Bij de Tweede Kamer is inmiddels aanhangig het Wetsvoorstel Vorderen gegevens in Strafvordering²⁸ dat een ander deel van de verdragstekst implementeert en wetsvoorstel dat een gedeeltelijke herziening inhoudt van het genoemde wetsvoorstel Computercriminaliteit II en dat strekt tot implementatie van de nog openstaande onderdelen van het Cyber Crime Verdrag, ligt thans voor advies bij de Raad van State.

De Europese Unie heeft zich achter het Cybercrimeverdrag geschaard en beoogt met deze kaderbesluiten een verdere harmonisatie tussen de wetgevingen van haar lidstaten te komen dan het Cyber Crime Verdrag vereist. Hiertoe is een aantal Kaderbesluiten in procedure gebracht.²⁹ Van andere Europese instrumenten zoals de Overeenkomst tot wederzijdse Rechtshulp (zie hierboven) en het Europese Arrestatiebevel³⁰ gaat een krachtige impuls tot internationale samenwerking uit die zich mede tot het terrein van de Cybermisdad uitstrekt. De recente ondertekening van de Europese Grondwet manifesteert mede de politieke wil van de Europese leiders om het domein van het strafrecht niet langer aan de nationale wetgever en beleidsmakers over te laten.

²³ Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken van 20 april 1959, Trb. 1965, 10. (Zie eerste aanvullende protocol bij dit verdrag – Trb. 1979, 121). EU-overeenkomst betreffende wederzijdse rechtshulp in strafzaken van 29 mei 2000, Trb. 2000, 96 alsmede Protocol bij deze Overeenkomst, Trb. 2001, 187.

²⁴ Trb. 2002, 18.

²⁵ Trb. 2003, 60.

²⁶ TK 1999-2000, 26 671, nrs 1-6.

²⁷ Stb. 2004, 105 jo 395, i.w.tr. 1 september 2004.

²⁸ TK 2004-2005, 29441, nrs. 1-6.

²⁹ Voor stel voor een kaderbesluit over aanvallen op informatiesystemen, COM (2002) 173, PbEG C203 van 27 augustus 2002. Kaderbesluit van de Raad ter bestrijding van seksuele uitbuiting van kinderen en kinderpornografie, PbEG, L 13/44 van 20 januari 2004. Voorstel voor een kaderbesluit van de Raad betreffende de bestrijding van racisme en vreemdelingenhaat COM2001-664 def - PbEG C 75 E 26 maart 2002. Voorstel voor een Kaderbesluit van de Raad betreffende het Europees bewijsverkrijgingsbevel ter verkrijging van voorwerpen. Documenten en gegevens voor gebruik in strafprocedures, van 14 november 2003, COM (2003) 688 def.

³⁰ Zie voor implementatie Overleveringswet van 29 april 2004, Stb. 2004, 195 in het bijzonder Bijlage I.

Het Cybercrime verdrag is thans ondertekend door 38 staten. Dat aantal lijkt gezien het totale aantal staten in deze wereld beperkt, maar dat is schijn. Partij bij het verdrag zijn behalve Europese Staten ook belangrijke Staten als de USA, Canada, Japan en Zuid-Afrika. Gezien naar economische entiteiten houdt dit in dat partij bij het verdrag zijn de gehele G-7 partij, de gehele Europese Unie van voor 1 mei 2004 en meer dan twee derde van het aantal lidstaten van de Raad van Europa. De Russische Federatie is nog geen partij maar heeft te kennen gegeven dat te willen worden. Het proces van ratificatie – dat naar zijn aard niet als snel en flitsend kan worden omschreven – ligt overigens op schema. Op dit moment zijn in Straatsburg 8 ratificaties ontvangen. Komend jaar worden het merendeel der ratificaties verwacht. Nederland mag hopen nog juist voor het eind van het kalenderjaar 2005 te kunnen melden dat aan de verplichtingen van het verdrag wordt voldaan.

Naast formele gebondenheid aan de verdragstekst hebben een aantal staten vrijwillig (gedeelten) van de verdragstekst in hun nationale wetgeving overgenomen. Op supranationaal niveau wordt gesproken over de ontwikkeling van regionale instrumenten, zoals ten behoeve van de OAS (Organization of American States) en ten behoeve van leden van de ASEAN (Association of South-East Asian Nations). Ook binnen de UN gaan stemmen op om met een eigen verdrag te komen.³¹ Vanuit een oogpunt van harmonisatie en verbetering van internationale samenwerking zou het te prefereren zijn indien de betrokken landen en hun organisaties zouden streven naar aansluiting bij het Cyber Verdrag in stede van zelf het *cyber*-wiel nog eens uit te vinden. Of het daarvan komt kan intussen betwijfelen. Niet alle lidstaten van genoemde organisaties passen goed bij de visie van de Raad van Europa op mensenrechten en het is maar de vraag of over de handhaving daarvan werkbare afspraken mogelijk zijn. Met het in het leven roepen van een UN-verdrag zal veel tijd verloren gaan. Gezien de bestaande ratificatiepraktijk bij UN-verdragen lijkt een spoedige inwerkingtreding van zo'n verdrag illusoir, indien het al mogelijk zal zijn om vrijwel alle landen tot toetreding te inspireren. De meerwaarde ten opzichte van het Cybercrimeverdrag, waarbij de landen met de hoogste IT-penetratiegraad³² al partij zijn, is gering.

5.2 Inhoud en werking van het Cybercrimeverdrag

Het Cybercrimeverdrag regelt een aantal belangrijke zaken.³³ De doelstellingen van het verdrag zijn achtereenvolgens: harmonisatie van het cyber crime strafrecht; harmonisatie van strafvorderlijke bevoegdheden tot het vergaren van elektronisch bewijsmateriaal; en het faciliteren van internationale rechtshulp.

³¹ Voor bereiding voor 11^e UN Congress on Crime Prevention and Criminal Justice (april 2005), zie <http://www.unis.unvienna.org/unis/pressrels/2004/uniscp498.html>

³² Zie voetnoot 14 hierboven.

³³ Voor een uitgebreide bespreking zie H. Kaspersen in: B-J.Koops, *Strafrecht & ICT*, Den Haag 2004, p. 133-174. Buitenlandse literatuur: Marco Gerke, *Die Cybercrime Konvention des Europarats*, *Computerrecht* 2004, p. 762 e.v. Christian, Schwarzenegger, *Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cyber Crime vom 23. November 2001*, in: Donatsch (et. al, ed.), *Strafrecht, Strafprozessrecht und Menschenrechte*, *Festschrift für Stefan Trechsel zum 65. Geburtstag*, Zürich 2002, p. 305-324. Marco Gercke, *Die Cybercrime Konvention des Europarats*, *Computerrecht*, 2004, p. 762-770. Cedric J. Magnin, *The 2001 Council of Europe Convention on Cyber Crime: an efficient tool to fight crime in cyberspace?*, www.magnin.org/Publications/home.htm

Het verdrag geeft in de eerste plaats een belangrijke aanzet tot de harmonisatie van het materiële cybercrime strafrecht. Ik spreek hier van aanzet omdat meer en beter altijd mogelijk is. Het verdrag legt vast over welke strafbaarstellingen de verdragspartijen het eens zijn geworden. Dat sluit niet uit dat bepaalde gedragingen in meerdere verdragstaten strafbaar zijn, maar als regel kan men aannemen geen eenstemmigheid heeft bestaan over de vraag of, en zo ja, op welke wijze het betreffende gedrag met straf zou moeten worden bedreigd. De redenen voor deze verschillen zijn legio, gelegen in principiële opvattingen over de betekenis en rol van het strafrecht, voortkomende uit bestaande wetgevingstradities of anders vanwege verschil van opvatting over de ernst van de betreffende gedraging. Het Cybercrimeverdrag vertoont daarvan de tekenen. Zo werden de gedragingen van Cybercrimine en discriminatie onder gebracht in een afzonderlijk Additioneel Protocol omdat de toepassing van het strafrecht op dat gebied slechts voor bepaalde aspecten kon worden verzoend met de eisen van het Amerikaanse First Amendment (freedom of expression). De strafbaarstelling van kinderporno in het verdrag bevat een relatief groot aantal reserveringsmogelijkheden, speciaal ten behoeve van diezelfde USA, maar ook ten behoeve van een verdragspartij als Japan, waar kinderporno niet even verwerpelijk is als in onze westerse opvattingen. Tot strafbaarstelling van *spam* (ongevraagde elektronische commerciële communicatie) werd bijvoorbeeld niet besloten, omdat dit gedrag ten tijde van de onderhandelingen naar gemeenschappelijke opvattingen niet als voldoende schadelijk werd gezien. De harmonisatiedoelstelling heeft als zelfstandig doel het nader tot elkaar brengen van nationale criminele politieke doelstellingen op het gebied van cybercrime. Daarnaast dient er overeenstemming te bestaan met betrekking tot welke gedragingen de verdragstaten elkaar bereid zijn rechtshulp te verlenen. De eis van *dual criminality* wordt weliswaar in moderne verdragen niet zo scherp gesteld, maar is ook in een afgezwakte vorm een *sine qua non* voor het verlenen van rechtshulp. Een verdragsstaat zal niet genegen zijn burgers uit te leveren of aan meer de toepassing van dwangmiddelen te onderwerpen indien de onderliggende gedraging naar het recht van de eigen staat niet strafbaar is. Het Europese rechtshulpverdrag van 1957 noemt geen voorwaarde van dubbele strafbaarheid, maar uit de neergelegde reserveringen blijkt dat de verdragstaten die conditie wel degelijk willen toepassen. In het EU-rechtshulp-verdrag is de eis van dubbele strafbaarheid gereduceerd tot de eis dat de onderliggende gedraging moet behoren tot een van de in het verdrag genoemde categorieën strafbare feiten.

Cybercrime is een van de benoemde categorieën, waarbij men ervan uit mag gaan dat de daartoe behorende individuele strafbepalingen voorwerp van harmonisatie zijn geweest of nog steeds zijn, zoals blijkt uit de 'eigen', hierboven genoemde raamwerkbesluiten van de Europese Unie.

Het Cybercrimeverdrag regelt een aantal belangrijke andere zaken niet. Uit de *terms of reference* is af te leiden dat de het de oorspronkelijke bedoeling was dat de verdragspartijen elkaar onder voorwaarden zouden toestaan grensoverschrijdende onderzoekshandelingen in elektronische netwerken te verrichten. Een aanzet daartoe is gegeven in een Aanbeveling van de Raad van Ministers van de Raad van Europa van 1995³⁴ en was bekend onder de term 'trans border network search'. In de literatuur vindt men wel analyses over rechtsmacht en de bepaling van de *locus delicti* in verband met de berechting van strafbare feiten.³⁵ Over de (on) mogelijkheid tot het verrichten van grensoverschrijdende opsporingsonderzoek bestaat weinig verschil van mening. Een zodanige bevoegdheid kan dan ook alleen ontstaan in geval van

³⁴ R(1995) 13, in het bijzonder paragraaf 80.

³⁵ In Nederland uitgebreid C.B. van der Net, Grenzen stellen op het internet, Arnhem 2000.

toestemming van de betrokken staat of op grond van een verdragsrechtelijke regeling. In het kader van het Cybercrime verdrag is langdurig overlegd of hoe zo'n regeling er uit zou kunnen zien, maar dit heeft niet geleid tot overeenstemming. Het verdrag beperkt zich in art. 32 tot het beschrijven van twee situaties waarin grensoverschrijdend opsporingsonderzoek is toegestaan. De eerste betreft het benaderen van aan het publiek ter beschikking gestelde informatie ('*open source*'). Dat lijkt triviaal, maar toch. Allereerst of men dat onder onderzoekshandelingen kan begrijpen. Het *down loaden* van *open source* informatie door een opsporingsambtenaar ten behoeve van bewijsgaring kan men naar Nederlands recht in ieder geval wel als zodanig beschouwen. Het verdrag neemt op dit punt alle (internationale) twijfel weg. Minder frequent zal de tweede situatie aan de orde zijn, waar een persoon die rechtmatig toegang heeft tot informatie in zich in een computersysteem op het grondgebied van een andere verdragspartij bevindt en die bevoegd is om die informatie te verstrekken, aan de autoriteiten van de onderzoekende staat toestemming geeft om die informatie te benaderen. Dat kan bijvoorbeeld door het verstrekken van toegangscodes maar ook door het feitelijk openen van de verbinding ten behoeve van de opsporingsautoriteiten. Voor alle andere situaties, zo is de opzet van het verdrag, dient een verzoek tot internationale rechtshulp te worden gedaan.

Ter uitwerking van de rechtshulp – ik beperk mij hier tot de kernbepalingen – specificiert het verdrag een aantal bevoegdheden die gericht zijn op het veilig stellen van elektronisch bewijs. De achterliggende gedachte is dat de verdragspartijen zich van deze bevoegdheden dienen te voorzien zodat in ieder geval de wettelijke middelen aanwezig zijn om rechtshulp te verlenen. Dat geldt in het bijzonder voor de zgn. voorlopige maatregelen van het verdrag. Het verdrag gaat uit van de gedachte dat het voor een succesvolle opsporing van cybercrime nodig kan zijn de bron van een bepaalde communicatie te kunnen achterhalen. Met het verloop van de tijd kunnen de daarvoor benodigde gegevens verloren gaan. Het meest kansrijk verloopt die opsporing als de betreffende verbinding nog "hot" is en de opsporingsorganen tegelijkertijd de benodigde gegevens over die verbinding kunnen veiligstellen. Het verdrag werkt daartoe een systeem uit dat als "*quick freeze, slow thaw*" kan worden beschreven. Het verplicht de nationale wetgever tot het in het leven roepen van een bevoegdheid ter bevroering van zgn. verkeersgegevens. Het bevel strekt ertoe dat een telecomoperator of een internetprovider de verkeersgegevens betreffende een bepaalde communicatie onmiddellijk veilig stelt en deze beschikbaar houdt voor een later volgend bevel tot uitlevering. Indien de provider bij het vastleggen constateert dat bij de communicatie nog een andere provider is betrokken, dient hij de bevelgevende autoriteit onverwijld te informeren zodat deze alsnog een zgn. bevroeringsbevel tot die provider kan richten. Het bevel wordt geacht te worden omgeven met zo weinig mogelijk formaliteiten en dient tevens ter uitvoering van rechtshulpverzoeken. Daarnaast kent het verdrag een verplichting tot invoering van een bevoegdheid tot het in *real-time* vergaren van verkeersgegevens.

Het verdrag gaat ervan uit dat verkeersgegevens – mits de vergaring daarvan binnen redelijke tijd na het ontdekken van het strafbare feit is gestart - wel gedurende enige tijd beschikbaar zijn. In voorkomende gevallen kan bewaring worden veiliggesteld door toepassing van de voorlopige maatregelen. In Europa verplicht Richtlijn 2002/58/EG – inmiddels geïmplementeerd in de Telecommunicatiewet, zoals gewijzigd in 2004³⁶ de aanbieders van elektronische communicatienetwerken en diensten om verkeersgegevens na het beëindigen

³⁶ Stb. 2004, 189, tekstplaatsing Stb 2004, 308.

van een communicatie te vernietigen tenzij deze nodig zijn voor berekening van de nota of gebruikt kunnen worden voor marketingdoeleinden. Internet-providers hebben geen belang van facturering en zullen deze gegevens zelfs eerder verwijderen. Een en ander kan meebrengen dat verkeersgegevens – zeker op langere termijn – niet meer beschikbaar zijn en derhalve niet ter beschikking van de strafvordering kunnen worden gebracht.

De Europese Unie kiest daarom voor een systeem van verplichte opslag bij de aanbieder van een elektronische communicatienetwerk of dienst van alle verkeersgegevens teneinde de beschikbaarheid daarvan gedurende een periode van ten minste anderhalf jaar te verzekeren.³⁷ Een dergelijk systeem kan een systematische en ingrijpende bedreiging van de persoonlijke levenssfeer van de betrokkenen vormen. Gegeven de onbekendheid met de behoefte waarin het systeem moet voorzien, kan men er op voorhand aan twijfelen of invoering van een dergelijk systeem voldoet aan eisen van proportionaliteit en subsidiariteit. Daarnaast heerst onzekerheid over de kosten van de inrichting en de exploitatie van zo'n systeem, inclusief beveiliging, die op de betrokkenen zullen drukken met daarnaast de vraag welke regels de wetgever zal stellen en op welke wijze deze regels worden gehandhaafd. Dan is vervolgens de vraag wat het nuttig effect van het beschreven systeem is – met name ten opzichte van de door het verdrag voorgestelde maatregelen – als de regeling niet ook het genereren van bepaalde gegevens voorschrijft.

Het Cybercrimeverdrag roept Partijen in art. 25 lid 1 op om elkaar rechtshulp te verlenen “*to the widest extent possible*”. Het vijfde lid van hetzelfde artikel staat weigering van een rechtshulpverzoek toe indien dubbele strafbaarheid ontbreekt. Zoals boven aangegeven speelt het vereiste van dubbele strafbaarheid in de Europese verhoudingen een minder pregnante rol dan vooreen, in de bilaterale relaties tussen individuele Europese Verdragspartijen en niet-lidstaten ligt dat veelal anders.³⁸ Een rechtshulpverzoek om toepassing van de zgn. voorlopige maatregelen (art. 29 en 30) kan wegens het ontbreken van dubbele strafbaarheid niet worden geweigerd tenzij *a prima facie* duidelijk is dat aan de uitlevering en de overdracht van het veiliggestelde materiaal onder de nationale wetgeving niet mogelijk is. Verder terugdringen van de beperkende invloed van dubbele strafbaarheid bleek in het kader van het verdrag niet mogelijk. Toch is er bij een internationaal medium als internet aanleiding voor nadere bezinning. Het medium maakt het immers mogelijk om vanaf willekeurig welk aansluitpunt handelingen te verrichten die elders effecten hebben. Met de komst van draagbare apparatuur en de integratie van mobiele communicatienetten en internet (zie bijvoorbeeld UTMS) wordt het begrip ‘locatie’ buitengewoon betrekkelijk. Ik moge dit illustreren aan de hand van de volgende casus. Stel dat bij een Amerikaanse *webhost* een site wordt onderhouden met racistisch materiaal in de Nederlandse taal en dat dit feit naar Nederlands recht een strafbaar feit oplevert (bijvoorbeeld art. 137c Sr). Stel verder dat de Amerikaanse wet zich niet tegen deze gedraging verzet.³⁹ Het identificeren van de verdachte dader is zonder gegevens van de betrokken Amerikaanse *webhost* normaal gesproken niet mogelijk. Een rechtshulpverzoek om abonnee-, resp. verkeersgegevens met betrekking tot deze *web-site* zal door de USA wegens het ontbreken van dubbele strafbaarheid niet worden gehonoreerd, terwijl de gedraging zelf geen enkele relatie met de Amerikaanse rechtsorde heeft. In het omgekeerde geval – een

³⁷ Ontwerp Kaderbesluit van de Raad van de Europese Unie van 14 oktober 2004, COPEN 122 TELECOM 150.

³⁸ Zie o.m. J. Koers, Nederland als verzoekende staat bij de wederzijdse rechtshulp in strafzaken, Zutphen 2001, p. 480 e.v.

³⁹ Inperking van vrijheid van meningsuiting onder het First Amendment is in het algemeen slechts mogelijk ingeval van dreiging met geweld of erger.

verzoek om rechtshulp aan Nederland – lijkt de tekst van art. 552k tweede lid Sv meer ruimte te bieden. In geval van een verdrag dient aan een rechtshulpverzoek zoveel mogelijk gevolg te worden gegeven.⁴⁰ Deze bepaling spreekt immers van een ‘redelijk verzoek’ doch hierbij moet worden bedacht dat het ontbreken van dubbele strafbaarheid aan de toepassing van dwangmiddelen en het uitleveren van stukken van overtuiging in de weg staat.⁴¹ In het genoemde voorbeeld leidt het hanteren van een formele eis van dubbele strafbaarheid zonder acht te slaan op de overige omstandigheden van het geval tot een onbevredigende uitkomst voor de verzoekende partij, hetgeen *a fortiori* geldt bij toevallige en tijdelijke verschillen tussen nationale strafwetten.

In het kader van het verdrag is uiteindelijk geen regeling tot stand gekomen om rechtshulpverlening bij ontbreken van (gekwalificeerde) dubbele strafbaarheid mogelijk te maken, bijvoorbeeld in gevallen waarin dat de verdachte geen enkele andere band heeft met de rechtsorde van de aangezochte staat maar die kennelijk alleen gebruikt om strafrechtelijke aansprakelijkheid onder de eigen nationale wetgeving te ontgaan (*abuse of jurisdiction*). Verdere harmonisatie van het materiële strafrecht teneinde in enige vorm van dubbele strafbaarheid te kunnen voorzien blijft daarom geboden, maar dat is naar zijn aard nu eenmaal geen korte termijn oplossing.

Uit de verdragstekst wordt duidelijk dat Partijen oog hebben voor het feit dat *cyber space* geen statisch gebeuren is. Anders dan bij veel andere bedragen dienen Partijen periodiek voor overleg bijeen te komen binnen – de eerste maal drie jaar na in werkingtreden van het verdrag - en is iedere Partij bevoegd tot het voorstellen van wijzigingen aanvullingen, als de ontwikkeling van ICT daarvoor aanleiding geeft.⁴²

6. Slotbeschouwing

Internet is een wereldomvattend communicatienetwerk dat voor zowel zakelijk als privé-gebruik dat van grote betekenis is voor het maatschappelijk verkeer. In geïndustrialiseerde landen is de meerderheid van de bevolking voor meerdere uren per week gebruiker. Het grote publiek is zich onvoldoende bewust van de risico's waaraan zij zich door deelname aan het internet blootstellen. Dit betreft enerzijds elektronische aanvallen op en andere schadelijke elektronische ingrepen in hun computerapparatuur. Het vergt alertheid en voldoende technisch inzicht en daarnaast ook bereidheid om zich van adequate beveiliging te voorzien. Daarnaast is kan een internetgebruiker gemakkelijk slachtoffer worden van frauduleus of anderszins schadelijke informatieaanbod. Toezicht of andere beschermende maatregelen worden niet altijd toegepast.

Het geheel van strafbare feiten dat gericht is tegen de beoogde en ongestoorde werking van computersystemen (computercriminaliteit in enge zin) en andere delicten waarbij ICT als instrument wordt gebruikt of waarvan de uitvoering gebruik maakt van de eigenschappen van

⁴⁰ Tenzij zich voor de uitvoering belemmeringen van wezenlijke aard voordoen, voortvloeiend uit het toepasselijke verdrag of uit de wet dan wel indien door inwilliging van het rechtshulpverzoek zou worden gehandeld in strijd met fundamentele beginselen van Nederlands strafprocesrecht (zie HR 19 maart 2002, LJN ZD2927, NJ 2002, 580).

⁴¹ Zie RNL aantekening 5 op art. 552k Sv., p.15 en aantekening 8 op art. 552n Sv, p. 24-36.

⁴² Art. 46 derde lid, art. 46 eerste lid, art. 44 lid eerste lid Cybercrimeverdrag. Het verdrag is op grond van art. 36 derde lid sinds 1 juli 2004 van kracht.

het internet (computercriminaliteit in ruime zin) worden in dit artikel onder de noemer *cybercrime* samengebracht. Kwaadwillende vinden op het internet gemakkelijk mogelijkheden voor de uitvoering van *cybercrimes*. Statistieken tonen een sterke groei van het aantal strafbare feiten dat door middel van internetcommunicatie wordt gepleegd.

Bij gebruik van internet en mobiele communicatie wordt de betekenis van de fysieke locatie waar de cybercrimineel handelt steeds geringer. Ten behoeve van de opsporing van cybercriminelen is het vinden van het elektronisch spoor tussen daad en dader onmisbaar. Dit spoor kan lopen over vele (internationale) schakels. Internationale samenwerking ter vergaring van elektronisch bewijs is daarom onontbeerlijk. Het Cybercrimeverdrag geeft vorm aan deze internationale samenwerking. Het verdrag is echter geen finale oplossing. Met name ten aanzien van verdere harmonisatie van cyberstrafbepalingen. Het internationale karakter van het internet dwingt tot verdergaande internationale samenwerking bij de opsporing van strafbare feiten. Naast de juridische inbedding van internationale samenwerking moet worden voorzien in en veelheid van zgn. flankerende maatregelen zoals bijvoorbeeld de beschikbaarheid van voldoende opsporingscapaciteit, voldoende technische middelen, adequate beveiliging en bewustwording van de internetgebruiker.⁴³ Hiervoor zijn en blijven internationale verdragen nodig, bij voorkeur in de vorm een Aanvullend Protocol bij het Cybercrimeverdrag.

Summary

Today, an increasing number of incidents is reported of in principle criminal behaviour, such as computer hacking, distributed denial-of-service-attacks and other computer sabotage, spamming, spyware and related acts. Although national Dutch law has already criminalised most of these acts, law enforcement seems to fail in taking appropriate actions to reduce and prevent criminal conduct in and around the internet. The article points at the global nature of the internet to tune national laws and to provide for effective international co-operation. As a first step the notion of *cybercrime* is discussed including some factors that have a strong impact on its occurrence and present growth. The need to collect electronic evidence requires adequate legal and technical powers. International co-operation is only achievable if there is a common understanding about the behaviour to be criminalized and if the law provides for adequate powers to investigate those crimes. Both elements require a more or less permanent form of international deliberations. The article thereto discusses the content, major features and merits of the Council of Europe Cyber Crime Convention (2001) and related measures taken by the European Union, including the implementation of these measures in the Dutch Criminal Code.

⁴³ Zie bijvoorbeeld Seymour E. Goodman, Towards a Treaty-based international Regime on Cyber Crime and Terrorism, in: James A. Lewis (ed), Cyber Security, Washington 2003, p. 71-76.