Universele handhavingsjurisdictie in cyberspace?

M. Hildebrandt en M.E. Koning

Van computer- naar cybercriminaliteit

Cyberspace, functioneel daderschap en extraterritoriale rechtsmacht

In deze bijdrage verstaan we onder cyberspace de verzameling van online en offline contexten waarin burgers hun sporen achterlaten als websurfers, consumenten, weggebruikers, sporters, gebruikers van zoekmachines, gezondsheidsplatforms, sociale netwerken en allerlei andere software. Cyberspace kan inmiddels worden beschreven als een slimme digitale omgeving, waarin een veelheid van geautomatiseerde beslissystemen functioneert – ook zonder dat de gebruiker dat merkt of zelfs maar kan weten.[1] Cyberspace wordt in toenemende mate gebruikt voor allerlei vormen van 'cybercrime' of cybercriminaliteit, die zich onder meer onderscheidt van niet-cyber criminaliteit doordat locatie en afstand – en daarmee territorialiteit – een andere rol spelen dan voorheen.[2] De locatie van de dader en die van het strafbaar gestelde effect, en/of de strafbaar gestelde handeling vallen niet meer automatisch samen. Hoewel dat automatisme al veel langer is gerelativeerd, lijkt cyberspace de 'defaults' om te draaien. De traditionele omgang met deze problematiek binnen de strafrechtsdogmatiek vinden we bijvoorbeeld in de leer van het functioneel daderschap en de gronden voor uitbreiding van territoriale rechtsmacht. Sinds het IJzerdraad-arrest[3] en de strafbaarstelling van rechtspersonen[4] kennen we het zogenaamde functioneel daderschap, dat daderschap niet meer koppelt aan een 'gewilde spierbeweging' maar aan de vraag of (het gevolg van) een handeling aan een rechtssubject kan worden toegerekend. De rol van de locatie van de dader en de afstand tot de gevolgen van haar handeling waren daarmee reeds gerelativeerd. Tegelijkertijd bleek een variant van eenzelfde soort 'functioneel' daderschap zich te lenen voor het oplossen van rechtsmachtsproblemen van een vervolgende staat, bijvoorbeeld wanneer de dader zich weliswaar buiten het territorium van die staat bevond, maar de gevolgen van haar handelen zich manifesteerden binnen dat territorium of ten aanzien van slachtoffers met de nationaliteit van de vervolgende staat.[5] De materiële rechtsmacht kon langs die weg worden uitgebreid op basis van

---

1 M Hildebrandt, De Rechtsstaat in Cyberspace? (Inaugurele rede Radboud Universiteit) Nijmegen 2011.

2 In het verlengde van de Engelse term 'cybercrime' en de omschrijving van cyberspace in Hildebrandt 2011, spreken wij hier van cybercriminaliteit in plaats van computercriminaliteit, nu het niet meer gaat om de computer, maar om onderling verbonden computersystemen met hun platforms en applicaties die zowel online als offline beslissende invloed uitoefenen op wat wij kennen en kunnen.

3 HR 23 februari 1954, *NJ* 1954, 378 m. nt. B.V.A. Röling (IJzerdraad).

4 Zie bijvoorbeeld HR 21 oktober 2003, *NJ* 2006, 328 m. nt. P.A.M. Mevis (Drijfmest).

5 Zie bijvoorbeeld HR 6 april 1954, *NJ* 1954, 368 m. nt. B.V.A. Röling (Singapore).

het beschermingsbeginsel, of het passief personaliteitsbeginsel.[6]

Wilde Westen of *Mare Liberum*

Op het moment dat de fysieke locatie van de dader en de afstand tot de fysieke locatie van haar slachtoffers er eigenlijk helemaal niet meer toe doen ontstaat een nieuwe situatie. In cyberspace is dit in toenemende mate aan de orde. De 'defaults' veranderen. Wat voorheen uitzondering was, lijkt regel te worden. De veronderstelling dat strafbare feiten die de rechtsorde van een bepaalde staat raken gepleegd zijn door een rechtssubject dat zich binnen het territorium van die staat bevindt of de nationaliteit van die staat heeft, gaat in cyberspace niet op.

Daarmee stelt zich een fundamenteel probleem van jurisdictie, waar al sinds het begin van cyberspace over is gesteggeld. Na het ongebreidelde optimisme van de jaren 90, waarbij cyberseparatisten betoogden dat cyberspace per definitie onreguleerbaar is en gezien moet worden als een nieuwe, separate ruimte waar directe democratie (zo niet anarchie) aan de orde is,[7] en waar staten 'niets te makken hebben', kwam al snel aandacht voor de manier waarop staten hun verloren terrein terug zouden kunnen winnen,[8] gevolgd door waarschuwingen voor de teloorgang van cyberspace als onbegrensde, vrije, openbare ruimte.[9] Het mag intussen duidelijk zijn dat cyberspace wel degelijk reguleerbaar is, maar dat daartoe zowel internationale samenwerking (verdragen, justitiële en politiële samenwerking) als politieke en juridische aandacht voor de architectuur van cyberspace noodzakelijk zijn (standaardisering, open source software, 'privacy by design').[10] Het samenspel tussen beide zal bepalend zijn voor de mate waarin inherent transnationale cybercriminaliteit bestreden kan worden, maar ook voor de mate waarin grondrechten binnen cyberspace gewaarborgd blijven. Van belang is op te merken dat 'bewoners' van cyberspace steeds tegelijk bewoners zijn van het territorium van een nationale staat en altijd binnen de jurisdictie vallen van een of meer staten. Daarmee valt het handelen in cyberspace in beginsel ook binnen het bereik van eventueel toepasselijk inter- of supranationaal recht. Het geweldmonopolie dat ten grondslag ligt aan de nationale rechtsorde lijkt echter afwezig in cyberspace; het gaat hier om een transnationale ruimte (te onderscheiden van inter- en supranationale rechtsordes).

---

6 A.H. Klip & A.S. Massa, Communicerende Grondslagen Van Extraterritoriale Rechtsmacht, Den Haag: WODC 2010.

7 J.P. Barlow, *A Declaration of the Independence of Cyberspace* (Zwitserland Davos, 1996) beschikbaar via: projects.eff.org/~barlow/Declaration-Final.html. en D.G. Post, 'Anarchy State and the Internet', *Journal of Online Law*, 1995 artikel 3, beschikbaar via: papers.ssrn.com/sol3/papers.cfm?abstract_id=943456.

8 L. Lessig, *Code and Other Laws of Cyberspace,* New York: Basic Books, 1999.

9 J. Zittrain, *The Future of the Internet--And How to Stop It*, New Haven: Yale University Press, 2008.

10 M. Mueller, 'The New Cyber-Conservatism: Goldsmith/Wu and the Premature Triumphalism of the Territorial Nation-State' (bespreking van J. Goldsmith & T. Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford: Oxford University Press 2006) *Internet Governance Project*, paper IGP06-003, juni 2006, beschikbaar via: internetgovernance.org/pdf/MM-goldsmithWu.pdf.

Dat kan enerzijds betekenen dat degene met de slimste applicaties, het meeste geld, het grootste rekenvermogen in beginsel de dienst uitmaakt, en anderzijds dat verschillende staten hun geweldmonopolie proberen in te zetten binnen hetzelfde domein. Dit leidt volgens sommigen tot een nieuwe versie van het wilde westen, waar de sheriff zich moet handhaven in een krachtenveld waar wet en recht al gauw inwisselbaar zijn voor meer effectieve instrumenten van rechtshandhaving (hetgeen wij dan meestal eigenrichting noemen), terwijl hij bovendien andere sheriffs tegenover zich vindt die ook rechtsmacht claimen. De afwezigheid van een 'bovensheriff' impliceert de afwezigheid van het geweld*monopolie*.[11]

De vergelijking dringt zich op met de eerste grote uitdaging voor het stelsel van soevereine staten dat zich aan het eind van de middeleeuwen ontwikkelde. Die uitdaging betrof rechtsmachtconflicten op volle zee, door Hugo de Groot beschreven in zijn *Mare Liberum* van 1609.[12] Oorspronkelijk geschreven als hoofdstuk twaalf van het manuscript *De iure praedae* (het recht op de buit), beoogde dit korte geschrift de positie van de Republiek en de VOC ten aanzien van de handelsvaart veilig te stellen tegenover Spanje en Portugal, voor zover zij een monopolie en zelfs eigendom claimden ten aanzien van de zee. De stelling van De Groot was dat de zee geen territorium is waarover staten soevereiniteit, laat staan eigendomsrechten, *kunnen* uitoefenen. In plaats daarvan gold volgens De Groot het natuurrecht, zoals hij dat in zijn latere *De iure belli ac pacis* (1625) nader uitwerkte bij zijn leer van het maatschappelijk verdrag. Dat verdrag zou ten grondslag zou liggen aan de interne soevereiniteit die het natuurrecht inperkt en grotendeels vervangt door het positieve recht. In paragraaf 3 gaan wij nader in op de idee dat grensoverschrijdende handhaving in cyberspace niet valt binnen de jurisdictie van de nationale soevereiniteit, maar bepaald wordt door natuurrechtelijke normering.

Grensoverschrijdende digitale toegang tot computernetwerken op afstand

Extraterritoriale jurisdictie kan betrekking hebben op drie verschillende dimensies van de rechtsmacht van een staat: de wetgevende, rechtsprekende en handhavende dimensie. In de Lotuszaak van 1927 stelde het Permanent Internationaal Gerechtshof in Den Haag vast dat staten met betrekking tot wetgeving in beginsel extraterritoriale rechtsmacht hebben tenzij dit verboden is, terwijl het Hof met betrekking tot handhaving meende dat staten geen enkele bevoegdheid hebben handhavende rechtsmacht uit te oefenen op het territorium van andere staten, tenzij het

---

11 J. Sternberg, 'Legal Dilemmas in Transnational Cyberspace', in A. Braga (red.) *CMC, Identidades e Género: Teoria e Método*, Covilhã: Universidade da Beira Interior 2005 p. 213-233.

12 H. De Groot, *De Vrije Zee. Een Uiteenzetting over Het Recht Van De Nederlandsers Om Handel Te Drijven in Oost-Indie*, Den Haag: Jongbloed 2009 (*Mare Liberum* 1609, vertaald door A. Eyffinger). Zie ook: H.J.M. Nellen, *Hugo De Groot. Een Leven in Strijd Om De Vrede 1583-1645,* Amsterdam: Balans 2007.

internationaal recht daarvoor op basis van gewoonte of verdrag toestemming geeft.[13] Het standpunt dat staten vrij zijn extraterritoriale wetgevingsjurisdictie te vestigen is omstreden, zowel in de doctrine als in de praktijk van staten.[14] Alleen in geval van universele jurisdictie voor zeer ernstige misdaden (tegen de menselijkheid, genocide) lijkt zich enige consensus af te tekenen dat staten universele jurisdictie kunnen vestigen, zelfs als zij geen concrete relatie hebben met daders en slachtoffers. In het verlengde daarvan is al eens gepleit voor universele jurisdictie voor cyberterrorisme;[15] wij gaan daar verder niet op in, maar merken op dat de *caveats* rond de inzet van het strafrecht voor de bestrijding van internationaal terrorisme ook hier van toepassing zijn.[16] Onze bijdrage beperkt zich tot de extraterritoriale handhavingsjurisdictie in cyberspace. De inzet van het Hof inzake handhavingsjurisdictie lijkt intussen minder omstreden: de 'default' is dat zonder toestemming van het gastland geen handhaving is toegestaan.[17]

De vraag die in deze bijdrage centraal staat is wanneer en onder welke voorwaarden een staat de bevoegdheid heeft om zich grensoverschrijdende digitale toegang te verschaffen tot computersystemen op afstand. De bevoegdheid om toegang te verkrijgen 'op afstand' lijkt van doorslaggevend belang te zijn bij effectieve bestrijding van cybercriminaliteit, wanneer die op grote schaal de vertrouwelijkheid en integriteit van persoonsgegevens schendt en de beschikbaarheid van computersystemen in gevaar brengt. Met name wanneer computers zijn gehackt en – zonder dat de eigenaar/gebruiker het merkt – worden bestuurd door de software van personen of organisaties die aldus op grote schaal spam, kinderporno of malware verspreiden is voor het opsporen van de malware en de daders toegang op afstand noodzakelijk.[18] De problematiek van

---

13 PCIJ 7 september 1927, France v. Turkey, *PCIJ Reports*, Series A, no. 10 (SS Lotus).

14 F.P.E. Wiemans, *Onderzoek Van Gegevens in Geautomatiseerde Werken,* Nijmegen: Wolf Legal Publishers, 2004, p. 106-113 en A.H. Klip & A.S. Massa, *Communicerende Grondslagen Van Extraterritoriale Rechtsmacht* Den Haag:WODC 2010. Met betrekking tot cybercriminaliteit geven sommige staten een zeer ruime toepassing aan hun strafwetgeving. Zie bijvoorbeeld Artikel 9 Computer Crimes Act Malaysia 1997, no. 563, laatste versie 2006: '(1)The provisions of this Act shall, in relation to any person, whatever his nationality or citizenship, have effect outside as well as within Malaysia, and where an offence under this Act is committed by any person in any place outside Malaysia, he may be dealt with in respect of such offence as if it was committed at any place within Malaysia. (2) For the purposes of subsection (1), this Act shall apply if, for the offence in question, the computer, program or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time'.

15 K. Gable, 'Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent', *Vanderbilt Journal of Transnational Law* 2010-43 nr. 1, p. 57–118.

16 M. Van der Woude, *Wetgeving in Een Veiligheidscultuur. Totstandkoming Van Antiterrorismewetgeving in Nederland Bezien Vanuit Maatschappelijke En (rechts)politieke Context,* Den Haag: Boom Juridische Uitgevers, 2010.

17 Met 'gastland' doelen wij op het territorium waar de extraterritoriale handhaving plaats zou moeten vinden. Zie inzake het verbod op extraterritoriale handhaving voor Nederland art. 539a lid 3 Sv volgens welke extraterritoriale strafvordering 'slechts [mag] worden uitgeoefend, voor zover het volkenrecht en het interregionale recht dit toelaten'. Zie ook: P. de Hert, 'De strafvordelijke voorstellen inzake computercriminaliteit', *Delikt en Delikwent* 1993, No. 1 p 7-28.

18 P.L. Bellia, 'Chasing Bits Across Borders', *University of Chicago Legal Forum* 2001 p. 35–101. Zie ook S.M. Young, 'Verdugo in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases', *Michigan Telecommunications and Technology Law Review* 2004-10, 139. Zie ook J. Goldschmidt, 'The Internet and the Legitimacy of Remote Cross-Border Searches' *The University of Chicago Legal Forum* 2001 nr. 1, p. 103–119. Zie ook K. Wang 'Using a Local Search Warrant to Acquire Evidence Stored Overseas via the Internet' in K.P.Chow and S. Shenoi (red.), *Advances in Digital Forensics VI,* vol. 337, IFIP Advances in Information and Communication

grensoverschrijdende toegang tot computernetwerken op afstand hangt enerzijds samen met het feit dat digitaal bewijs snel verloren kan gaan of gewist kan worden en anderzijds met het feit dat een digitale aanval op kritische infrastructuur om zeer snelle actie vraagt. Daar komt bij dat zelfs lokale digitale aanvallen een internationale dimensie kunnen hebben en bijstand kunnen vereisen van de diverse landen via wiens computersystemen de aanval werd 'gerout'. Tot slot merken wij op dat het voor opsporingsambtenaren niet steeds duidelijk zal zijn waar de gegevens dan wel computersystemen zich bevinden waartoe zij zich toegang hebben verschaft.[19] Met het toenemende gebruik van cloud computing zal de vooronderstelling dat men zoekt in systemen die zich op het territorium van de opsporende staat bevinden steeds hachelijker worden. Zelfs de veronderstelling dat een opsporingsambtenaar weet binnen welke staat het computersysteem zich bevindt dat zij onderzoekt dreigt onwerkbaar te worden. Dat impliceert dat extraterritoriale jurisdictie voor toegang op afstand de facto universele handhavingsjurisdictie betreft.

Het vraagstuk van extraterritoriale handhavingsjurisdictie in cyberspace is veelomvattend en de kwestie van toegang op afstand tot computersystemen is ook los van extraterritoriale toepassing omstreden, nu daarbij bestanden worden doorzocht en/of controle wordt verkregen over computersystemen van zowel verdachten als derden (potentiële verdachten en potentiële slachtoffers; in geval van cybercriminaliteit in de cloud is de categorie van derden vrijwel niet te begrenzen).[20]

Wij beperken ons tot een overzicht van de dynamiek van het Europeesrechtelijke kader (paragraaf 2) en stellen in het verlengde daarvan de vraag hoe zo'n extraterritoriale toepassing zich verhoudt tot de interne en externe soevereiniteit (paragraaf 3), en sluiten af met de vraag naar de implicaties voor de bescherming van fundamentele rechten (paragraaf 4).

Europeesrechtelijk kader

De Raad van Europa en het Cybercrime Verdrag

Midden jaren negentig boog de Raad van Europa zich over mogelijke harmonisering van online strafvorderlijke bevoegdheden. Deze wachten nog steeds op wetgeving op Europees niveau. Het comité van ministers van de Raad van Europa schreef destijds over grensoverschrijdende digitale

---

Technology, Boston: Springer 2010, p. 37–48.

19 F.P.E. Wiemans, *Onderzoek Van Gegevens in Geautomatiseerde Werken,* p. 154-155.

20 Zie hierover M.E. Koning, 'Van teugelloos 'terughacken' naar 'digitale toegang op afstand'', Privacy & Informatie 2012-2, p. 46-52. Het gaat ons hier om digitale toegang op afstand als opsporingsbevoegdheid en niet om de inzet van deze bevoegdheid voor het waarschuwen van slachtoffers. Dat laatste staat of gespannen voet met de privacy van die slachtoffers en lijkt bovendien weinig effectief: www.opgelicht.nl/nieuws/detail/waarschuwing-melding-op-uw-beeldscherm-zogenaamd-van-de-politie/10/.

toegang op afstand:[21]

> In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.

De criteria voor grensoverschrijdende toegang tot opgeslagen computergegevens zijn uitgewerkt in het Cybercrime Verdrag van 2001 (CCV), dat overigens ook buiten Europa de toon zet.[22] Staten hebben middels het CCV twee uitzonderingen op de Lotus-regel afgesproken door elkaar wederzijds toestemming te verlenen om in die twee gevallen handhavend op te treden op elkaars grondgebied.[23] De eerste uitzondering betreft de toegang tot publiekelijk toegankelijke computergegevens, zogeheten open bronnen (art. 32 sub a CCV). Open bronnen moeten worden begrepen als die welke zonder specifieke toegangsprocedures beschikbaar zijn. We tekenen daarbij aan dat het uitgangspunt in Nederland niet is dat justitie alles mag dat niet expliciet is verboden, hetgeen onder meer betekent dat het stelselmatig vergaren van informatie over personen – ook als dat afkomstig is uit open bronnen – alleen is toegestaan als is voldaan aan de voorwaarden van 126j Sv.[24] De tweede uitzondering betreft de transnationale netwerkzoeking die voortbouwt op een nationale netwerkzoeking (art. 19 lid 2 CCV). Wanneer een vermoeden bestaat dat bij de doorzoeking van een computer de gezochte gegevens zijn opgeslagen in een ander computersysteem dat rechtmatig via de initieel doorzochte computer kan worden bereikt, ontstaat de bevoegdheid om ook het andere systeem te doorzoeken.[25] Wanneer het andere computersysteem zich buiten het territorium van de opsporende partij bevindt is op grond van art. 32 sub b CCV de rechtmatige en vrijwillige instemming nodig van de persoon die gerechtigd is de gegevens via het computersysteem aan de partij te verstekken. Kaspersen, toenmalig voorzitter van de voorbereidende werkgroep voor het opstellen van de aanbeveling uit 1995 en de conventie zelf, legt de bepaling uit door 'persoon' te lezen als burger.[26] Het betreft volgens hem de medewerking van een burger met rechtmatige toegang tot de data, voor zover die gerechtigd is de informatie openbaar te maken. De burger mag dus niet gebonden zijn aan wettelijke of contractuele geheimhouding.[27] Staten kunnen eventueel toegang met een wettelijke verplichting afdwingen maar een burger kan

---

21 Recommendation R(95) 13 *Concerning Problems of Criminal Procedure Law Connected with Information Technology,* punt 17.

22 *Convention on Cybercrime* Nr. 185 Council of Europe.

23 Wanneer wij in het vervolg spreken van 'toegang zonder toestemming van het gastland' doelen wij op specifieke toestemming voor een bepaalde opsporingshandeling door de staat waar de extraterritoriale handhaving plaats vindt, niet de generieke toestemming die bij verdrag is geregeld.

24 W.Ph Stol, E.R. Leukfeldt & H. Klap, 'Cybercrime en Politie', *Justitiële Verkenningen* 2012 no. 1, p. 29-30.

25 Art. 125j Sv, zie F.P.E. Wiemans, *Onderzoek Van Gegevens in Geautomatiseerde Werken,* p. 152-162 over doorzoeking over de landsgrenzen (in beginsel niet toegestaan) en de gevolgen van aldus onrechtmatig verkregen bewijs.

26 H.W.K. Kaspersen, ' Jurisdiction in the Cybercrime Convention', in: E.J. Koops & S. Brenner (red.), *Cybercrime and Jurisdiction : a Global Survey,* Den Haag: West Nyack 2006, p. 21.

27 H.W.K. Kaspersen, ' Jurisdiction in the Cybercrime Convention', p. 21.

niet meer rechten weggeven dan zij zelf heeft.

Ten tijde van de CCV-onderhandelingen zijn meer variaties op grensoverschrijdende toegang tot opgeslagen computergegevens besproken.[28] De verdragspartijen konden buiten de twee hierboven besproken situaties niet tot overeenstemming komen. Kaspersen schrijft hierover: 'The time was not ripe for such a far reaching instrument'.[29] In de CCV ligt het accent daarom op wederzijdse bijstand, zoals geregeld in art. 29 en 30 (voorlopige voorzieningen voor data retentie), 31-34 (toegang tot opgeslagen gegevens, real-time verzameling en interceptie) en 35 (een 24/7 netwerk contactpunt voor snelle interventies). Nadeel van deze rechtshulpverplichtingen is de inherente vertraging, die in geval van cybercriminaliteit al gauw fataal is.[30] Binnen de context van de Raad van Europa blijft grensoverschrijdende toegang tot opgeslagen computergegevens dan ook voorwerp van debat. De opmars van cloud computing vergroot de behoefte aan nieuwe bevoegdheden, nu daarbij gegevens, software en infrastructuur op data servers buiten het computersysteem van de eindgebruiker worden opgeslagen en beheerd, terwijl de locatie van deze data servers buiten het territorium van de staat kan liggen waar de eindgebruiker zich bevindt. Het onderwerp 'digitale toegang op afstand' maakt deel uit van het internationaal cybercriminaliteitsonderzoeksproject van de Raad van Europa[31] en in juni 2012 staat de jaarlijkse CCV Conferentie (Octopus) volledig in het teken van *Transborder access to data and jurisdiction in the context of cloud computing*.[32]

Het CCV voorziet in minimale verplichtingen en laat staten vrij meer specifieke verplichtingen aan te gaan. Artikel 39 lid 2 CCC geeft bijvoorbeeld ruimte om bi- en/of multilaterale afspraken te maken. Van deze mogelijkheid kan echter niet naar willekeur gebruik worden gemaakt: partijen moeten voldoen aan de doelstellingen en beginselen van het Verdrag.[33] In art. 15 CCV worden een aantal minimale grondrechtelijke en rechtstatelijke waarborgen voor procesrechtelijke bevoegdheden en procedures genoemd. De bevoegdheden en procedures zijn onderworpen aan de voorwaarden en waarborgen uit het nationale recht, dat passende bescherming dient te bieden aan fundamentele vrijheden en rechten, waarbij in ieder geval de beschermingsniveaus gelden van het Europees Verdrag van de Rechten van de Mens (EVRM) en het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten. Bijzonder gewicht wordt toegekend aan het proportionaliteitsvereiste tussen de voorgenomen maatregel, het beoogde doel en de ernst van de

28 *Convention on Cybercrime* Nr. 185 Council of Europe, *Explanatory Report* par. 193.
29 H.W.K. Kaspersen, ' Jurisdiction in the Cybercrime Convention', p. 20.
30 P.L. Bellia, 'Chasing Bits Across Borders', p. 58.
31 Zie de website van de Raad van Europa: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp.
32 Octopus Conference - Cooperation against Cybercrime - 6-8 June 2012 Council of Europe, Strasbourg, France.
33 *Convention on Cybercrime* Nr. 185 Council of Europe, *Explanatory Report* par. 312.

schending. Nationale voorwaarden omvatten daarnaast rechterlijk of in ieder geval onafhankelijk toezicht indien de aard van de betrokken procedure of bevoegdheid dit vereist, de gronden voor toekenning van de bevoegdheid en een beperking van de reikwijdte en de duur. Het mag duidelijk zijn dat het hier gaat om de eisen die bijvoorbeeld art. 8 EVRM stelt aan een gerechtvaardigde inperking van het recht op privacy.

De Europese Unie

Slechts 19 van de 27 EU lidstaten hebben zich bij het CCV aangesloten.[34] De bestrijding van cybercriminaliteit is een 'topprioriteit' binnen de EU.[35] In onder andere de EU-interne veiligheidsstrategie en de digitale agenda wordt de dreiging van cybercriminaliteit benadrukt.[36] De Europese Unie kan sinds het verdrag van Lissabon Richtlijnen uitvaardigen op het gebied van cybercriminaliteit.[37] In het kader van het Stockholm verdrag heeft de EU zich het volgende ten doel gesteld:[38]

> The Union should also clarify the rules on jurisdiction and the legal framework applicable to cyberspace within the Union, including how to obtain evidence in order to promote cross-border investigation.

De Commissie heeft zich in beginsel verbonden tegen 2014 maatregelen (bijvoorbeeld wetgeving) voor te stellen inzake jurisdictie voor grensoverschrijdende digitale opsporingsbevoegdheden op afstand.[39] Hoewel nog geen wetgeving is voorgesteld hebben het Parlement, de Raad en de Commissie in het verleden wel aangegeven aan welke voorwaarden een eventuele bevoegdheid zou moeten voldoen. Zo nam de Raad bij het opstellen van het CCV in 1999 een gemeenschappelijke positie in.[40] Hij stelde dat een extraterritoriale computerdoorzoeking overwogen kon worden in geval van uitzonderlijke omstandigheden, of noodtoestand, na een evenwichtige afweging van soevereiniteit, fundamentele rechten en opsporingsbelangen.[41] In 2000 heeft de Commissie binnen de eigen kaders van de EU de grensoverschrijdende dimensie van cybercriminaliteitsopsporing nog eens aangesneden:[42]

---

34 Bron: www.coe.int. Laatstelijk berekend: 26 april 2012. EU lidstaten het verdrag niet hebben getekend: Oostenrijk, België, Tsjechië, Griekenland, Ierland, Luxemburg, Polen en Zweden.

35 Zie de website van de EU inzake cybercriinaliteit: ec.europa.eu/home-affairs/policies/crime/crime_cybercrime_en.htm.

36 COM/2010/673 *De EU-internetveiligheidsstrategie in actie: vijf stappen voor een veiliger Europa* en COM/2010/245 *A Digital Agenda for Europe.*

37 Art. 83 *Geconsolideerde versie van het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie* 2010/C 83/01.

38 *The stockholm programme — an open and secure europe serving and protecting citizens* 2010/c 115/01, p. 23.

39 COM/2010/171 *Een ruimte van vrijheid, veiligheid en recht voor de burgers van Europa Actieplan ter uitvoering van het programma van Stockholm* p. 39.

40 JBZ/1999/364 *Gemeenschappelijk standpunt van 27 mei 1999 door de Raad aangenomen op grond van artikel 34 van het Verdrag betreffende de Europese Unie inzake onderhandelingen in de Raad van Europa over het verdrag inzake cybercriminaliteit.*

41 JBZ/1999/364, art. 1 lid 7.

42 COM/2000/890 *De informatiemaatschappij veiliger maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden - eEurope 2002*, p. 22.

> Issues become more complicated if, while searching a computer or simply pursuing an investigation, a law-enforcement authority finds itself accessing or needing to access data located in one or more different countries. Important sovereignty, human rights and law-enforcement interests are at stake and need to be balanced.

In de derde pijler heeft de EU een aantal aan cybercriminaliteit gerelateerde kaderbesluiten genomen die nu door Richtlijnen worden of zijn vervangen. Het betreft onderwerpen als de bestrijding van fraude en vervalsing van andere betaalmiddelen dan contanten (JBZ 2001/413, 28 mei 2001), de bestrijding van kinderpornografie (JBZ 2004/68 22 december 2003),[43] en de bescherming tegen aanvallen op informatiesystemen (JBZ 2005/222 24 februari 2005).[44] Geen van deze kaderbesluiten biedt echter de mogelijkheid tot grensoverschrijdende digitale toegang op afstand. De lijn van de Raad van Europa wordt voortgezet, waar men als gezegd voornamelijk inzet op verregaande samenwerking en het reeds bestaande 24/7 netwerk van contactpunten voor cybercriminaliteit (in Nederland onder meer de KLPD).

In 2007 nam de Europese Commissie een aanloop naar de wijziging van het werkingsverdrag van de EU en gaf richtsnoeren voor een algemeen beleid voor de bestrijding van cybercriminaliteit.[45] Zij merkt hierbij op dat het ontbreken of het onvoldoende gebruiken van rechtstreekse structuren voor grensoverschrijdende operationele samenwerking een zeer zwak punt blijft op het gebied van vrijheid, veiligheid en recht.[46] De Raad werkte de richtsnoeren van de Commissie verder uit en noemt *remote computer searches* als een van de relevante beleidsonderwerpen waar consensus over bereikt moet worden.[47] De Raad komt met de volgende – niet bijster vernieuwende - conclusie: 'De EU moet computerdoorzoekingen op afstand bevorderen, indien het nationaal recht daarin voorziet, zodat de onderzoeksdiensten snel toegang hebben tot de informatie, een en ander met instemming van het gastland.'[48]

In de parlementaire Aanbeveling 'Versterking van de veiligheid en van de fundamentele vrijheden op het internet' van 2009 werd de Commissie verzocht na te denken over een brede cybercriminaliteitsbestrijdingsstategie.[49] Het Parlement adviseerde de Raad om de lidstaten te verzoeken erop toe te zien dat, indien het nationaal recht daarin voorziet, computerdoorzoekingen op afstand worden uitgevoerd op basis van een geldig computerdoorzoekingsbevel van de bevoegde

---

43 Inmiddels vervangen door Richtlijn 2011/93/EG van het Europees Parlement en de Raad van 13 december 2011 *ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie* (*PbEU* 2011 L 37/25).

44 Nu besproken in het parlement: COM/2010/517 *Voorstel voor een Richtlijn van het Europees parlement en de Raad over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ van de Raad.*

45 COM/2007/267 *Naar een algemeen beleid voor de bestrijding van cybercriminaliteit.*

46 COM 2007/267, par. 3.1.

47 Council of the EU 13567/08 p. 5 en Council of the EU 15569/08 p. 5.

48 Council conclusions of 27 November 2008 *on a concerted work stategy and pratical measures against cybercrime* (2009/C 62/05) Zie ook de draft: Council of the EU 11784/08 p. 4.

49 Aanbeveling van het Europees Parlement van 26 maart 2009 aan de Raad *betreffende de versterking van de veiligheid en van de fundamentele vrijheden op het internet* (2008/2160(INI)).

rechterlijke instanties. Tevens adviseerde het Parlement dat de Raad vast zou stellen dat vereenvoudigde procedures voor het uitvoeren van computerdoorzoekingen op afstand onaanvaardbaar zijn, vanwege strijd met de beginselen van de rechtsstaat en het recht op bescherming van de privésfeer.[50] Het Parlement stelde als voorwaarden dat voorafgaand aan digitale toegang op afstand een onafhankelijk oordeel van de bevoegde rechter is vereist waarin de omvang en duur van de bevoegdheid worden omschreven.

In meer recente wetgeving, voorstellen en documenten wordt een bevoegdheid voor digitale toegang op afstand niet meer aangesneden.[51] In de mededeling van begin 2012 over de aanpak van criminaliteit in het digitale tijdperk worden de grenzen van de nationale jurisdictie benoemd als een belemmerende factor voor cybercriminaliteitsbestrijding.[52] In dezelfde mededeling wordt de oprichting van een Europees Centrum voor de bestrijding van cybercriminaliteit aangekondigd. Dit centrum zal fungeren als informatieknooppunt, expertisecentrum, onderzoeksondersteuning en spreekbuis van de justitiële cybercrime-onderzoekers en gerechtelijke instanties binnen de EU. De lijn uit het CCV (van verregaande samenwerking, bijvoorbeeld door middel van de 24/7 contactpunten) wordt vooralsnog doorgezet.

Conclusie Europeesrechtelijk kader

Het mag duidelijk zijn dat de bevoegdheid tot grensoverschrijdende digitale toegang op afstand noch door het CCV noch door het recht van de EU aan de deelnemende staten wordt opgelegd. Het scheppen van een dergelijke bevoegdheid binnen het nationale recht is echter niet verboden. De nationale bepaling dient in dat geval passende bescherming te bieden voor de fundamentele vrijheden en rechten, in ieder geval op de beschermingsniveaus van het EVRM en het IVBPR. Conform de beperkingen van grondrechten in het EVRM gaat het daarbij om de bekende eisen van (1) de noodzakelijkheid van de bevoegdheid in een democratische samenleving, (2) een grondslag in het recht, (3) een legitiem doel en (4) proportionaliteit tussen de voorgenomen maatregel, het beoogde doel en de ernst van de schending. De eis van een grondslag in het recht betekent dat de betreffende bepaling de gronden voor toepassing, de reikwijdte en duur omschrijven, alsmede de eis

---

50 Ibid.

51 COM/2009/149 Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's *betreffende de bescherming van kritieke informatie-infrastructuur - "Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht"* en COM/2009/262 Mededeling van de Commissie aan het Europees Parlement en de Raad *Een ruimte van vrijheid, veiligheid en recht ten dienste van de burger* en COM/2010/673 en COM/2011/163 *Mededeling betreffende de bescherming van kritieke informatie-infrastructuur 'Bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid' en* COM/2010/517.

52 COM/2012/140 *De aanpak van criminaliteit in het digitale tijdperk – Oprichting van een Europees Centrum voor de bestrijding van cybercriminaliteit.*

van een onafhankelijk oordeel van de bevoegde rechter. De bevoegdheid mag daarnaast alleen grensoverschrijdend worden toegepast in uitzonderlijke omstandigheden, wanneer sprake is van toestemming van het gastland. Ten slotte dient daarbij een evenwichtige afweging tussen soevereiniteit, fundamentele rechten en de relevante opsporingsbelangen te worden gemaakt. Het CCV laat de mogelijkheid open om hier bi- en/of multilaterale afspraken over te maken. Het feit dat hier over een afweging van soevereiniteit wordt gesproken suggereert dat de eis van 'toestemming van het gastland' in geval van noodtoestand toch wordt gerelativeerd.

Mare Liberum, Cyberspace Liberum?

De eis van een evenwichtige afweging tussen soevereiniteit, fundamentele rechten en relevante opsporingsbelangen raakt de kern van de zaak. Het lijkt een toverformule die het probleem eerder op hoog abstractieniveau samenvat dan dat er een oplossingsrichting mee wordt geboden. Over de metafoor van de weegschaal schreven Leijten en Waldron behartenswaardige caveats.[53] De term 'afweging' is in zekere zin een Trojaans paard, dat een hele serie verzwegen vooronderstelllingen meebrengt die echter niet zonder meer van toepassing zijn. De schijn van precisie (wat zijn de kosten van inbreuken, hoe bereken je het voordeel van veiligheid), de suggestie dat minder vrijheid automatisch tot meer veiligheid leidt (de trade-off), het meestal verzwegen feit dat de illusie van veiligheid voor de één vaak ten koste gaat van daadwerkelijk verlies aan vrijheden voor de ander (ongelijke distributie), de vergelijking van ongelijke grootheden die worden opgeteld en afgetrokken (belangen tegenover rechten). Met betrekking tot die laatste vooronderstelling moeten we vaststellen dat soevereiniteit enerzijds zowel fundamentele rechten als opsporingsbelangen anderzijds geen gelijke grootheden zijn. Individuele rechten en de met opsporing gediende veiligheid veronderstellen *beide* een soevereine institutie die in staat is haar wil op te leggen, en langs die weg *zowel* strafvorderlijke maatregelen *als* de inperking daarvan af te dwingen. De effectuering van fundamentele rechten en opsporingsbelang zijn dus ook beide *afhankelijk van* een staat die op basis van zijn interne en externe soevereiniteit zowel grondrechtenbescherming als cyberveiligheid kan bieden, waarbij de samenhang tussen beide goed in het oog moet worden gehouden. Grondrechten en opsporingsbelang kunnen dus niet tegen soevereiniteit worden afgewogen. Cyberveiligheid voor de burger is immers ook een kwestie van grondrechtenbescherming en vice versa, zoals het Duitse Federale Constitutionele Hof besloot in 2008: geheime toegang tot een computer systeem in het kader van de opsporing vereist een concrete verdenking van de schending van een belangrijk rechtsbelang en een met waarborgen omklede

53 J. Waldron, 'Security and Liberty: The Image of Balance', *Journal of Political Philosophy* 2003-11, no. 2 p. 191–210. Zie ook J.C.M. Leyten, 'Afweging En De Mythe Van De Weegschaal', *Nederlands Juristen Blad* 1997 p. 636–637.

procedure, waarbij rechterlijke machtiging nodig is.[54] Burgers moeten veilig zijn voor de grootmacht van hun overheden en beschermd worden tegen cybercriminaliteit.

Dit geeft eigenlijk al aan dat op volle zee of in cyberspace, waar geen sprake is van een boven alle partijen staande soevereine institutie; *zowel* de grondrechtenbescherming *als* de opsporing van strafbare feiten afhangen van het feitelijk vermogen van een partij om de naleving van rechtsnormen af te dwingen. Daarmee vertoont de normering van cyberspace gelijkenis met het door Hugo de Groot geponeerde natuurrecht, dat de verhoudingen bepaalt bij gebreke van statelijke doorzettingsmacht. Zijn versie van het natuurrecht is interessant voor cyberspace omdat hij in zijn *Mare Liberum* een lans breekt voor het natuurrecht als uitgangspunt voor het zeerecht, en zich verzet tegen de overgang van natuurrecht naar soevereiniteit op zee. In combinatie met zijn *De iure belli ac pacis* pleit hij ervoor de grenzen van de interne soevereiniteit en het daarmee verbonden positieve recht te erkennen. Voor interstatelijke conflicten ontwikkelde hij vanuit zijn natuurrechtelijk kader de idee van het oorlogs*recht* dat geldt tussen staten (het *ius ad bellum* en het *ius in bello*). Ingeval van het zeerecht, kwalificeert hij de zee als een *res nullius,* die zich echter niet leent voor *occupatio* (inbezitneming). Een ware *res communis* die steeds beschikbaar moet blijven voor alle personen en naties die haar willen bevaren of en dus ook geen *res publica* voor zover daarmee wordt gedoeld op het private bezit van een bepaalde staat. Voor zover private partijen proberen te profiteren van de afwezigheid van een geweldmonopolie, zijn alle staten bevoegd tot handhaving. Piraterij op zee is om die reden een van de weinige voorbeelden van universele handhavingsjurisdictie: alle staten mogen piraten opsporen en berechten. Wanneer staten echter proberen een monopolie te vestigen en daarmee andere staten het vrije verkeer op zee ontzeggen, kan dit als een oorlogshandeling worden opgevat, die eigenrichting legitimeert.[55] Dat geeft De Groot de kans te onderscheiden tussen kapers en piraten. Hij schreef zijn pleidooi voor de vrijheid van de zee onder meer om militair ingrijpen (kaapvaart) te legitimeren bij de bescherming van de koopvaardij van de VOC.[56] Kern van zijn pleidooi was de verwerping van de handelsmonopolies van Spanje en Portugal op de scheepvaartroute naar de Oost. Tegelijkertijd legitimeerde hij ook de universele jurisdictie jegens piraten, die zich aan iedere vorm van normering onttrokken.[57] Kapers handelen op basis van het oorlogsrecht dat toestaat de vijand bij wijze van wraak te beroven (oorlogsbuit), piraten handelen buiten enige vorm van recht en zijn alleen uit op eigen gewin (private buit).

---

54 Bundesverfassungsgericht 27 februari 2008, 1 BvR 370/07, 1 BvR 595/07.

55 H. De Groot, *De Vrije Zee. Een Uiteenzetting over Het Recht Van De Nederlandsers Om Handel Te Drijven in Oost-Indie*, Den Haag: Jongbloed 2009 (*Mare Liberum* hoofdstuk XIII, 1609, vertaald door A. Eyffinger).

56 De Groot rechtvaardigt zo het motto van de VOC: 'coophandel met force'. Cf. J. Thumfart, 'On Grotius's Mare Liberum and Vitoria's De Indis, Following Agamben and Schmitt', *Grotiana* 2009-30, no. 1, p. 76.

57 H. De Groot, *De Vrije Zee. Een Uiteenzetting over Het Recht Van De Nederlandsers Om Handel Te Drijven in Oost-Indie*, Den Haag: Jongbloed 2009 (*Mare Liberum* hoofdstuk V, 1609, vertaald door A. Eyffinger), p. 139-140.

Het natuurrechtelijk uitgangspunt voor *Cyberspace Liberum* ten aanzien van cybercriminaliteit die profiteert van de afwezigheid van een geweldmonopolie, zou universele handhavingsjurisdictie zijn. Tenzij daarover andere afspraken zijn gemaakt. Dit gaat duidelijk in tegen de uitgangspunten van de extraterritoriale handhavingsjurisdictie, zoals die in het internationale recht zijn geconsolideerd. Daar lijkt de 'default' te zijn dat extraterritoriale handhaving verboden is, tenzij daarover andere afspraken zijn gemaakt. *Cyberspace Liberum* zou daarnaast ook betekenen dat geen enkele staat zich de uitsluitende jurisdictie over cyberspace kan en mag toe-eigenen, hetgeen impliceert dat staten alleen kunnen handelen op basis van gemaakte afspraken of gerechtvaardigde eigenrichting.

Doorzoeken op afstand: yes we can?

Cyberspace Liberum is geen rechteloze ruimte waar alles geoorloofd is, noch een ruimte waar alleen het recht van de sterkste geldt. Het lijkt er wel op dat het verbod van extraterritoriale handhavingsjurisdictie ten aanzien van ernstige vormen van cybercriminaliteit die zich aan iedere vorm van normering onttrekken, alleen geldt voor staten die zich hiertoe hebben verbonden. De verdragspartijen van het CCV zijn in ieder geval aan het verbod gebonden, hetgeen impliceert dat grensoverschrijdende toegang op opstand tot computersystemen buiten de in het verdrag geregelde gevallen illegaal is – tenzij middels rechtshulp of per verdrag toestemming van het gastland is verkregen. Voor zover deze opsporingshandelingen desondanks plaatsvinden, is de vraag is of we deze illegale acties willen legaliseren, zodat de uitoefening aan voorwaarden gebonden kan worden, dan wel strikte toepassing van territoriale handhavingsjurisdictie blijven eisen.

België, dat geen partij is bij het CCV, heeft zich in art. 88ter Sv de bevoegdheid toegekend om een zoeking in een informaticasysteem onder bepaalde voorwaarden uit te breiden tot een zoeking op afstand in systemen waartoe de gebruiker toegang had. In het derde lid stipuleert de wetgever ten aanzien van gegevens die bij deze zoeking op afstand gevonden worden:[58]

> Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden ze enkel gekopieerd. In dat geval deelt de onderzoeksrechter dit, via het openbaar ministerie, onverwijld mee aan het ministerie van Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald.

Hier wordt zonder meer unilateraal universele handhavingsjurisdictie gevestigd. Een pleidooi voor soortgelijke jurisdictie is vanuit de VS gevoerd, voordat zij partij werden bij het CCV (ratificatie in 2007). Bellia achtte toegang op afstand bij gebreke van internationale samenwerking in beginsel gerechtvaardigd.[59] Goldschmidt meende dat deze interventie is toegestaan wanneer justitiële of

58 M. Bockstaele e.a., *De zoeking doorzocht*, Antwerpen: Maklu 2009, p. 76.
59 P.L. Bellia, 'Chasing Bits Across Borders', p. 59.

politiële samenwerking niet mogelijk is, bijvoorbeeld omdat er geen bevoegdheid is in het gastland, de technische capaciteit ontbreekt of omdat handhaving in het gastland te lang duurt terwijl bewijs met een druk op de knop kan worden vernietigd, verwijderd of geanonimiseerd. Ook weigering tot medewerking door het gastland, was voor Goldschmidt reden het recht in eigen hand te nemen.[60]

Een belangrijke vraag is wat het rechtsgevolg is van de overtreding van het verbod van extraterritoriale toegang. Young beargumenteerde bijvoorbeeld dat degene wiens privacy wordt geschonden door de toegang op afstand, geen aanspraak kan maken op de bescherming van het derde en/of vierde Amendement op de Amerikaanse grondwet (privacy en due process), wanneer zij geen banden heeft met de VS.[61] Wiemans, die vaststelde dat Nederland geen bevoegdheid tot extraterritoriale doorzoeking kent op basis van 125j Sv, onderzocht de gevolgen van illegale extraterritoriale doorzoeking voor het bewijs.[62] Hij maakt daarbij een onderscheid tussen de schending van soevereiniteit van het gastland en de schending van de privacy van degene wiens computersysteem is doorzocht. De soevereiniteitsschending kan op zich reden zijn voor bewijsuitsluiting, dan wel getoetst worden aan de *Schutznorm*: is de verdachte getroffen in het belang dat het volkenrechtelijke verbod op extraterritoriale handhavingsjurisdictie beoogt te beschermen?

Onze zorg betreft echter niet alleen de verdachte. Het gaat er ook om dat burgers in het algemeen bedacht moeten zijn op het feit dat opsporingsambtenaren van andere staten inkijkoperaties kunnen plegen op hun computersystemen, waarbij onduidelijk is hoe die privacy schendingen zijn genormeerd, of burgers hierover bericht ontvangen, waar zij zich kunnen beklagen en of zij een ‘effective remedy’ hebben tegen de inkijkende staat. Ook wanneer de bevoegdheid tot extraterritoriale toegang op afstand wel rechtmatig is, zijn deze vragen relevant. *Cyberspace Liberum* trekt zowel commerciële ‘scheepvaart’ als ‘piraterij’, ‘kaapvaart’ en ‘oorlogsschepen’ aan, die intussen niet altijd gemakkelijk van elkaar onderscheiden kunnen worden. Daarom is van groot belang dat eventuele universele handhavingsjurisdictie aan strikte, overzichtelijke en controleerbare voorwaarden wordt gebonden die burgers greep geven op wat hun eigen en andere overheden kunnen bekijken en doorzoeken in cyberspace. Voor zover dat niet mogelijk is moeten overheden zich onthouden van het scheppen en uitoefenen van dit type bevoegdheden en de strijd aanbinden met staten die zich illegaal toegang verschaffen tot extraterritoriale computersystemen.

---

60 J. Goldschmidt, 'The Internet and the Legitimacy of Remote Cross-Border Searches'. Zie ook K. Wang, 'Using a Local Search Warrant to Acquire Evidence Stored Overseas via the Internet' die met enkele creatieve oplossingen komt bij gebreke van toestemming of bijstand van het gastland (bijvoorbeeld toestemming achteraf).

61 S.M. Young, 'Verdugo in Cyberspace'.

62 F.P.E. Wiemans, *Onderzoek Van Gegevens in Geautomatiseerde Werken,* p. 156-163.