Het Trojaanse politiepaard

Hacken in het opsporingsonderzoek

Een onderzoek naar het bestaan van een wettelijke basis in het Wetboek van Strafvordering voor hacken in het opsporingsonderzoek en – bij afwezigheid van een dergelijke basis – naar de mogelijke invoering van hacken door de politie ter aanvulling van het huidige wettelijke kader omtrent digitale opsporingsmethoden.

Scriptie strafrecht
augustus 2012

Door: Anne Winters
Studentnummer: 2095912

Begeleider: mr. R.H. Hermans

VRIJE UNIVERSITEIT AMSTERDAM

Faculteit der Rechtsgeleerdheid

Voorwoord

Voor u ligt mijn scriptie geschreven ter afsluiting van de opleiding Rechtsgeleerdheid, afstudeerrichting strafrecht, aan de Vrije Universiteit Amsterdam.

Deze scriptie is niet zomaar tot stand gekomen. Ik wil hierbij iedereen bedanken die in meerdere of mindere mate heeft bijgedragen aan de totstandkoming van deze scriptie. Een bijzonder woord van dank gaat uit naar mr. Hermans voor de geboden hulp en begeleiding bij het schrijven van dit onderzoek.

Anne Winters
Augustus 2012

Inhoudsopgave

Lijst van gebruikte afkortingen

AA	Ars Aequi
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
art.	artikel
BVerfG	Bundesverfassungsgericht
D66	Democraten 66
DD	Delikt en Delinkwent
diss.	dissertatie
e.a.	en andere
ECRM	(voormalige) Europese Commissie voor de Rechten van de Mens
EHRM	Europees Hof voor de Rechten van de Mens
e.v.	en verder
EVRM	Europees Verdrag voor de Rechten van de Mens
GG	Grundgesetz
HR	Hoge Raad
ICT	Informatie- en communicatietechnologie
IP	Internet Protocol
IRT	Interregionaal Recherche Team
IT	informatietechnologie
jo.	juncto
JV	Justitiële verkenningen
KLPD	Korps landelijke politiediensten
LJN	Landelijk Jurisprudentie Nummer
MIVD	Militaire Inlichtingen en Veiligheidsdienst
m.nt.	met noot
NJ	Nederlandse Jurisprudentie
NJB	Nederlands Juristenblad
nr.	nummer
NTBR	Nederlands Tijdschrift voor Burgerlijk Recht
NTD	Notice-and-Take-Down
o.a.	onder andere(n)
p.	pagina
P&I	Privacy & Informatie
PvdA	Partij van de Arbeid
PVV	Partij Voor de Vrijheid
red.	redactie
Rb.	Rechtbank
SP	Socialistische Partij
Sr	Wetboek van Strafrecht
Stcrt.	Staatscourant
Stb.	Staatsblad van het Koninkrijk der Nederlanden
Sv	Wetboek van Strafvordering
TNO	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek
Trb.	Tractatenblad van het Koninkrijk der Nederlanden
Tw	Telecommunicatiewet
USB-stick	Universal Serial Bus-stick
VoIP	Voice-over-Internet-Protocol
Wet BOB	Wet bijzondere opsporingsmethoden
Wiv	Wet op de inlichtingen- en veiligheidsdiensten 2002
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum

Inleiding

Op 31 augustus 2011 bericht het Openbaar Ministerie dat door de Dienst Nationale Recherche van het KLPD op het internet grote hoeveelheden kinderpornografisch materiaal zijn aangetroffen op anonieme ontmoetingsplaatsen en diep verborgen websites. De Dienst Nationale Recherche had deze ontdekking gedaan in het kader van het onderzoek naar het (internationale) netwerk van de hoofdverdachte in de Amsterdamse zedenzaak[1] Robert M.

In het onderzoek kwam naar voren dat Robert M. kinderporno had verspreid via verborgen plaatsen, zogenoemde *hidden services*[2], op het internet. Deze verborgen omgevingen zaten verscholen in het *Tor*-netwerk, een wereldwijd netwerk dat het mogelijk maakt om anoniem te surfen op het internet. Op de *hidden services* werden websites, forums en andere geheime ontmoetingsplaatsen aangetroffen, waar kinderpornografische foto's en video's werden uitgewisseld. Tevens kon in deze digitale omgeving door bezoekers in chatkanalen worden gecommuniceerd over het misbruiken van kinderen en de productie en verspreiding van kinderporno.

Onder verantwoordelijkheid van het Landelijk Parket van het Openbaar Ministerie en met toestemming van de rechter-commissaris bij de rechtbank Rotterdam zijn de rechercheurs van de Dienst Nationale Recherche twaalf *hidden services* binnengegaan na de beveiliging te hebben doorbroken.[3] De politie heeft daarbij het anonimiseringsnetwerk *Tor* gehackt om de websites te vinden.[4] Vervolgens is een aantal verborgen sites voor pedofielen *offline* gehaald en is het beeldmateriaal op die pagina's, nadat kopieën werden gedownload en veiliggesteld voor nader onderzoek, gewist. In totaal zijn door middel van het hacken van het *Tor*-netwerk meer dan 220.000 afbeeldingen en video's met kinderporno aangetroffen en verwijderd.[5]

Voor de opsporingsdiensten is op grond van de huidige wetgeving geen enkele andere bevoegdheid voorhanden waarmee dit strafbare en schadelijke materiaal had kunnen worden verwijderd. Alleen door computervredebreuk te plegen, geven deze verborgen websites hun geheimen prijs en kan er opsporing plaatsvinden, aldus Prins.[6]

De aanpak van de opsporingsdiensten in deze zaak is op zijn minst opmerkelijk te noemen. Hacken in het opsporingsonderzoek berust namelijk niet op een expliciete grondslag in de wet. Het is de vraag tot hoever de bevoegdheden van de politie op het gebied van

---

[1] De Amsterdamse zedenzaak is een omvangrijke zedenzaak, waarbij (vermoedelijk) seksueel misbruik heeft plaatsgevonden op onder andere verschillende kinderdagverblijven in Amsterdam. Robert M., hoofdverdachte in de zedenzaak, wordt verdacht van het veelvuldig seksueel misbruiken van zeer jonge kinderen en het bezit van een grote hoeveelheid kinderporno. Zijn partner Richard van O. wordt verdacht van medeplichtigheid aan het misbruik van Robert M. Beide verdachten zijn op 21 mei 2012 veroordeeld; Rb. Amsterdam 21 mei 2012, *LJN* BW6148 en Rb. Amsterdam 21 mei 2012, *LJN* BW6149. Zowel Robert M. en zijn partner als het Openbaar Ministerie hebben inmiddels hoger beroep aangetekend; http://nos.nl/artikel/375119-uitspraak-tegen-robert-m.html en http://nos.nl/artikel/378811-robert-m-en-om-in-hoger-beroep.html.

[2] Het gebruik van hidden services is bij uitstek geschikt voor degenen die – om wat voor reden dan ook – buiten beeld wensen te blijven van politie en justitie. Criminelen kunnen 'onder de radar' blijven opereren, omdat de websites op het *Tor*-netwerk de anonimiteit van de gebruikers ervan op het internet kunnen waarborgen. In beginsel geldt: wie het adres van de verborgen plaatsen kent, kan bij het kinderpornografisch materiaal. Wie er niet bekend mee is, kan de strafbare inhoud van de webpagina's niet bereiken; De Winter 2012.

[3] Zie http://www.om.nl/onderwerpen/verkeer/@156657/kinderporno-anonieme/.

[4] De Winter 2012.

[5] http://www.om.nl/onderwerpen/verkeer/@156657/kinderporno-anonieme/.

[6] Prins 2012, p. 48.

internetgerelateerde opsporingshandelingen reiken. Om deze vraag te kunnen beantwoorden, moeten de grenzen van het huidige wettelijke kader digitale opsporingsbevoegdheden onder de loep worden genomen. Wellicht dat hacken in de opsporingsfase kan worden afgeleid van een van die bevoegdheden uit dat kader. Wanneer afleiding niet mogelijk is, wil ik onderzoeken of de introductie van hacken als opsporingsmethode in het Wetboek van Strafvordering wenselijk is. De hierboven behandelde casus illustreert de obstakels die kunnen ontstaan bij de opsporing van internetgerelateerde criminaliteit. Berust de stelling van Prins op waarheid en vormt hacken door de politie inderdaad de enige mogelijkheid tot het opsporen van strafbaar gedrag op de computer en op het internet of kan cybercriminaliteit met de bestaande methoden in voldoende mate worden aangepakt? De onderzoeksvraag die in deze scriptie centraal staat, luidt daarom als volgt:

> Bestaat in het Wetboek van Strafvordering een wettelijke basis voor hacken in het opsporingsonderzoek en zo niet, is het wenselijk en noodzakelijk om een dergelijke basis te creëren?

Daartoe zal literatuur, jurisprudentie en wetgeving worden onderzocht. Voor de beantwoording van de onderzoeksvraag verdient een aantal juridische kwesties eerst de aandacht. Het eerste hoofdstuk van dit onderzoek behandelt het theoretische kader, waarbij de aanleiding van dit onderzoek zal worden geschetst. Daarbij komt de ontwikkeling van cybercrime aan bod en de wet- en regelgeving op dit gebied. Tevens belicht ik het begrip hacken en onderzoek ik of en in hoeverre hacken in Nederland strafbaar is gesteld.

Het tweede hoofdstuk is toegespitst op hacken als opsporingsbevoegdheid. Weergegeven wordt wat de ontwikkelingen hieromtrent zijn bij opsporingsautoriteiten en in de politiek. Vervolgens besteed ik aandacht aan verschillende hackmethoden en aan een voorbeeld van hacken in de praktijk. Ten slotte neem ik een kijkje over de grens. Hacken vindt namelijk al wel toelaatbaar plaats in Duitsland.

Enkele praktische obstakels die kunnen worden opgeworpen tegen de inzet van hacken in de opsporingsfase behandelt het derde hoofdstuk van dit onderzoek. Daarbij besteed ik tevens aandacht aan de gevolgen van het grensoverschrijdende karakter van de digitale wereld voor hacken door opsporingsautoriteiten.

In het vierde hoofdstuk komt hacken in het opsporingsonderzoek in relatie tot het fundamentele recht op privacy aan bod. In dit kader zal worden beargumenteerd in hoeverre ICT-systemen een onderdeel van het privéleven van burgers vormen. Vervolgens zal worden onderzocht of inbreuk mag worden gemaakt op dit recht op privacy.

Het vijfde hoofdstuk van dit onderzoek belicht het huidige wettelijke kader omtrent digitale opsporing. Alle ICT-gerelateerde bevoegdheden uit ons strafvorderlijk wetboek zullen de revue passeren. Omdat enkelen er vanuit gaan dat hacken op basis van enkele bestaande methoden mogelijk is, acht ik een dergelijke opsomming noodzakelijk.

Het zesde hoofdstuk vormt de kern van dit onderzoek, alwaar aandacht zal worden besteed aan de noodzakelijkheid en wenselijkheid van hacken in het opsporingsonderzoek. In dit gedeelte beoordeel ik of hacken kan worden gebaseerd op een van de in hoofdstuk vijf opgesomde bevoegdheden en maak ik een opsomming van de eisen die aan een eventuele in te voeren hackbepaling moeten worden gesteld.

Tot slot zal in de conclusie mijn onderzoeksvraag worden beantwoord.

Hoofdstuk 1 Theoretisch kader

Onder invloed van technologie, in het bijzonder de opkomst van het internet, is onze samenleving aan verandering onderhevig.[7] Datzelfde geldt voor het criminele milieu. Waar voorheen de traditionele strafbare delicten, zoals diefstal, verkrachting en moord het criminele circuit bepaalden, spelen de criminelen van nu in op de huidige informatiemaatschappij met als gevolg een scala aan nieuwe (digitale) misdrijven. Niet alleen is er een aantal nieuwe delicten ontstaan, ook wordt bij de uitvoering van conventionele strafbare feiten (zoals diefstal en oplichting) door criminelen in toenemende mate gebruikgemaakt van de computer en het internet. Als maatregel tegen dit probleem hebben politie en justitie kenbaar gemaakt hacken als opsporingsmethode in een opsporingsonderzoek te willen toepassen en zelfs al toe te passen.[8] Voordat er vastgesteld kan worden of dergelijk optreden van de strafvorderlijke overheid wettelijk gezien toelaatbaar kan worden geacht, moet mijns inziens eerst uiteen worden gezet waar partijen in dit kader tegenaan lopen. Hieromtrent onderzoekt paragraaf 1.1 waarom de opsporingsautoriteiten hacken in de opsporingsfase noodzakelijk achten en hoe deze wens is ontstaan. Vanwege de complexe aard van het onderwerp schetst deze paragraaf tevens de opzet van het gehele onderzoek, waarbij de hoofdlijnen zullen worden aangestipt. In dit theoretische kader acht ik het daarnaast van belang om te analyseren wat hacken is, of hacken in Nederland strafbaar is en welke verschijningsvormen er bestaan (§ 1.3). Het KLPD wil het hacken van computers en netwerken onder meer inzetten bij de aanpak van cybercrime.[9] Wat het fenomeen cybercrime inhoudt en wat er op dit moment bestaat aan wet- en regelgeving op dit gebied behandelt paragraaf 1.2.

1.1 Een korte introductie

Door de voortschrijdende informatie- en communicatietechnologie is het vergaren en verspreiden van informatie en onderlinge communicatie een stuk eenvoudiger geworden.[10] De wereld van elektronische communicatie kenmerkt zich door snelle innovaties, waardoor een keur aan nieuwe gebruiksmogelijkheden ontstaat.[11] In toenemende mate wordt op dit moment gebruikgemaakt van online communicatie, (ver)koop via internet en elektronisch bankieren. Met zijn laagdrempelige toegang en wereldwijde bereik biedt het internet onbegrensde mogelijkheden. Burgers, bedrijven en overheden worden steeds afhankelijker van het World Wide Web.[12] ICT, en het internet in het bijzonder, laat zich daarom typeren als een alomtegenwoordige, vitale infrastructuur voor vrijwel alle maatschappelijke en economische processen.[13]

[7] Oerlemans 2011a, p. 907.
[8] Laan 2011.
[9] Laan 2011.
[10] Van der Hulst & Neve 2008, p. 31.
[11] Helmus, Smulders & Van der Zee 2006, p. 3.
[12] Van der Hulst & Neve 2008, p. 31.
[13] Helmus, Smulders & Van der Zee 2006, p. 3.

De onbegrensde mogelijkheden van ICT en internet en het intensieve gebruik ervan door de maatschappij, hebben echter ook een keerzijde.[14] In het criminele circuit is het besef ontstaan dat de kwetsbaarheden die zijn ontstaan door de voortschrijdende ontwikkeling van de ICT-sector kunnen worden misbruikt voor criminele doeleinden en dat daarmee veel geld te verdienen valt. Daarbij speelt het ontbreken van barrières van tijd en ruimte op het internet en de optie van anonimiteit voor de cybercriminelen wellicht ook een rol.[15]

De mogelijkheden van het gebruik van ICT en internet hebben het criminele circuit een nieuwe dynamiek gegeven. Behalve dat ICT bestaande criminaliteit (zoals diefstal, kinderporno en oplichting) faciliteert en digitaliseert[16], zijn er ook geheel nieuwe verschijningsvormen van criminaliteit ontstaan, zoals hacken.[17] In dit onderzoek zullen beide vormen van criminaliteit met een digitaal karakter worden behandeld onder de noemer *cybercrime.*

Cybercrime is als criminaliteitsvorm volop in beweging. Als reactie daarop heeft de Nederlandse wetgever – mede onder invloed van de Europese wet- en regelgeving op dit gebied – de afgelopen twee decennia getracht een wettelijk kader te scheppen dat aansluit bij de technologische ontwikkelingen in de samenleving. Zo zijn er nieuwe definities en strafbepalingen in het Wetboek van Strafrecht geïntroduceerd, zoals artikel 80sexies Sr (begrip 'geautomatiseerd werk') en artikel 138ab Sr (computervredebreuk), en voorzag de wetgever in nieuwe bepalingen met betrekking tot de vervolging en opsporing van strafbare feiten met een digitaal karakter.[18] Die laatste bepalingen staan in dit onderzoek centraal.

Cybercrime is een criminaliteitsvorm waarbij de technologische ontwikkelingen razendsnel gaan. Daardoor kan het gebeuren dat tegen de tijd dat een wetswijziging gestalte krijgt, deze alweer aan revisie toe is.[19] Het gevaar bestaat dat de wettelijke bepalingen omtrent de vervolging en opsporing van cybercrime niet meer aansluiten bij de digitale stand van zaken en dat cybercrime op die manier onvoldoende kan worden bestreden.[20] Er moeten steeds geavanceerdere opsporingsbevoegdheden worden toegepast om cybercrime te kunnen opsporen en een halt toe te roepen. De binnen het strafrecht algemeen bekende 'wedloopgedachte' is derhalve ook binnen dit gedeelte van het strafrecht van toepassing. Specifieker geformuleerd is in dit kader sprake van een *digitale* wedloop tussen

[14] GOVCERT.NL 2010, p. 11.
[15] Van der Hulst & Neve 2008, p. 31.
[16] Door het digitaliseren van bestaande misdrijven kunnen digitale varianten van deze delicten ontstaan. In dit kader kan men denken aan grooming (art. 248e Sr) als digitale vorm van het verleiden van een minderjarige tot ontucht (art. 248a Sr), althans bij grooming wordt via een computer een ontmoeting voorgesteld met het oogmerk tot het plegen van ontuchtige handelingen. Ook vormt de opzettelijke vernieling van een geautomatiseerd werk (art. 161sexies Sr) een variant van de reguliere strafbaarstellingen van vernieling (o.a. art. 161 en 161bis Sr) Daarnaast wordt in Nederland regelmatig gediscussieerd over de invoering van een nieuwe vorm van diefstal (art. 310 Sr) op ICT-vlak, namelijk identiteitsdiefstal. Van diefstal van identiteit is sprake wanneer iemand een naam van iemand anders aanneemt op het internet. Een voorbeeld hiervan is het aanmaken van een *Twitter*account met andermans naam en zich met de *tweets* voordoen voor die ander. Hierbij dient onderscheid te worden gemaakt met identiteitsfraude, waarbij naast het verkrijgen van de identiteit van iemand anders ook wederrechtelijke gedragingen worden gepleegd; *Kamerstukken II* 2011/12, 5 maart 2012, Antwoord op Kamervragen van de PVV Kamerleden Elissen en Van Bemmel, Kooiman van de SP en de D66 leden Berndsen en Schouw van de minister van Justitie, kenmerk: 222096, 2012Z00283 en 2012Z00353.
[17] Van der Hulst & Neve 2008, p. 32.
[18] Van der Linden & Baardman 2011, p. 68.
[19] KLPD, Dienst Nationale Recherche 2010, p. 172.
[20] Van der Linden & Baardman 2011, p. 68.

cybercriminelen en opsporingsteams.[21] Dit verschijnsel kan worden geïllustreerd aan de hand van het onderwerp dat centraal staat in dit onderzoek, namelijk hacken. Hacken is het heimelijk en op afstand – via internet – binnendringen van een computer(systeem) of netwerk, althans van een geautomatiseerd werk en wordt in toenemende mate door criminelen gedaan.[22] Ik neem deze definitie van Oerlemans als vertrekpunt in dit onderzoek, omdat hiermee een zeer complex en technisch fenomeen is vervat in een mijns inziens voor juristen te hanteren formulering die bovendien werkbaar is met de betrekking tot het onderwerp van dit onderzoek, te weten hacken door opsporingsautoriteiten. Hacken is immers niet alleen een criminaliteitsvorm in opkomst, maar wordt ook door politie en justitie al jaren gezien als hét opsporingsmiddel in de strijd tegen cybercrime en overige (internetgerelateerde) criminaliteit.[23] Hacken wordt zelfs in de praktijk reeds toegepast.[24]
Het is maar de vraag of een dergelijke innovatieve opsporingsmethode wel past binnen het huidige wettelijke kader van het strafvorderlijk wetboek. Het is immers zeer goed mogelijk dat hacken een inbreuk maakt op de persoonlijke levenssfeer van betrokkenen, zoals onder meer bedoeld in artikel 10 Grondwet en artikel 8 EVRM. Na de IRT-affaire heeft onze wetgever ervoor gekozen opsporingsmethoden die een ernstige inbreuk maken op de rechten en vrijheden van burgers expliciet vast te leggen.[25] Met de Wet BOB kregen 'bijzondere' opsporingsmethoden deze uitdrukkelijke wettelijke basis.[26] Wat hieromtrent vaststaat is dat een dergelijke *expliciete* basis met betrekking tot hacken door de politie in ieder geval ontbreekt.[27] In geen enkele regeling of ander parlementair stuk wordt hacken in het opsporingsonderzoek uitdrukkelijk aangeduid. Dat betekent in ieder geval dat hacken ook niet als bevoegdheid in het Wetboek van Strafvordering wordt genoemd.

Enkelen achten het in dit kader mogelijk dat een bevoegdheid tot hacken kan worden afgeleid van andere – reeds bestaande – wettelijke digitale opsporingsmethoden, zodat hacken op basis van die strafvorderlijke bepalingen is gelegitimeerd. Of deze stelling standhoudt, zal worden beoordeeld in paragraaf 6.2. Dit onderzoek zal derhalve antwoord geven op de vraag of een wettelijke basis voor hacken door de politie in het Wetboek van Strafvordering reeds bestaat en zo niet, of het wenselijk is een dergelijke basis te creëren. Voordat aan de beantwoording van deze vragen kan worden toegekomen, acht ik het van belang om in dit theoretische kader uiteen te zetten wat het fenomeen hacken inhoudt en hoe cybercriminaliteit zich de laatste jaren heeft ontwikkeld.

---

[21] Van der Linden & Baardman 2011, p. 72.
[22] Oerlemans 2011a, p. 903.
[23] Zie bijvoorbeeld Proos 2008.
[24] Zie Rb. Rotterdam 26 april 2010, *LJN* BM2520 en Hof 's-Gravenhage 27 april 2011, *LJN* BR6836.
[25] Het IRT (interregionaal rechercheteam) Noord Holland/Utrecht was een interregionaal samenwerkingsverband van een aantal politiekorpsen. Het team maakte gebruik van de criminele burgerinfiltrant en liet bovendien grote hoeveelheden softdrugs door. Het doel daarvan was te kunnen doordringen tot in de top van enkele criminele organisaties. Daarbij moet men in het oog houden dat de Politiewet en de Wet BOB op dat moment nog niet bestonden. Mede door een verschil van mening over de gebruikte bijzondere opsporingsmethoden werd het IRT in 1993 opgeheven. Het gekrakeel wat ontstond na de opheffing van het team is de boeken ingegaan als de IRT-affaire en vormde bovendien de aanleiding voor een parlementair onderzoek naar de in Nederland gebruikte opsporingsmethoden onder voorzitterschap van Maarten van Traa; Buruma 2000, p. 548 e.v.
[26] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 12.
[27] Boek 2000, p. 592.

1.2 De ontwikkeling van cybercrime

In de vorige paragraaf is al kort het begrip cybercrime geïntroduceerd. Cybercrime is het containerbegrip voor ICT-gerelateerde criminaliteit. Daaronder vallen de traditionele vormen van criminaliteit waarbij gebruik wordt gemaakt van computers, ICT en in het bijzonder het internet. Een veelgebezigde term voor deze vorm van criminaliteit waarbij ICT als middel wordt ingezet om delicten te faciliteren, is *low tech crime*.[28] Bij low tech criminaliteit gaat het derhalve om criminaliteitsvormen die, althans in hun 'oorspronkelijke' vorm, ook zonder tussenkomst van ICT kunnen worden gepleegd, maar door het gebruik van ICT een nieuwe uitvoering hebben gekregen. Voorbeelden zijn fraude en oplichting via het internet, stalking via internet en het verspreiden van illegale inhoud op het internet (zoals kinderporno).[29]

De criminaliteit die zich exclusief in virtuele omgevingen afspeelt, ook wel bekend onder de naam *high tech crime*, valt tevens onder het overkoepelende begrip cybercrime.[30] Het gaat om *nieuwe* vormen van criminaliteit met een sterk technisch, virtueel karakter die zijn ontstaan door en niet kunnen bestaan zonder ICT. ICT wordt gebruikt als instrument, maar de digitale instrumenten, computers of gegevens zijn ook doelwit van de criminele activiteiten. Voorbeelden van high tech crime zijn het verspreiden van spam, het vernielen of wijzigen van elektronische gegevens via kwaadaardige software en het ongeautoriseerd inbreken in computersystemen (hacken).[31]

Het onderscheid tussen cybercrime en high tech en low tech criminaliteit vloeit voort uit de literatuur.[32] Een ander onderscheid dat in dit kader regelmatig wordt gebruikt is het onderscheid tussen cybercrime en computercriminaliteit als onderdelen van de overkoepelende term high tech crime. Computercriminaliteit verwijst naar de criminaliteit die zich afspeelt op het internet en cybercrime naar de traditionele delicten met een ICT-component.[33] De begrippen zijn verwarrend en wijken bovendien teveel af van de internationaal binnen politie en justitie gebruikte terminologie om bruikbaar te zijn.[34] Daarom zal ik in dit onderzoek het eerste onderscheid hanteren, waarbij de term cybercrime wordt gehanteerd als overkoepelend begrip. Het gaat dan zowel om de traditionele delicten met een digitaal karakter (low tech crime), als de criminaliteit waarbij ICT expliciet als doelwit kan worden aangemerkt (high tech crime). De definitie van cybercrime luidt als volgt:

> 'Cybercrime is het gebruik van ICT voor het plegen van criminele activiteiten tegen personen, eigendommen, organisaties of elektronische communicatienetwerken en informatiesystemen.'[35]

[28] Van der Linden & Baardman 2011, p. 65.
[29] GOVCERT.NL 2010, p. 29.
[30] Van der Linden & Baardman 2011, p. 64.
[31] Van der Hulst & Neve 2008, p. 39 e.v.
[32] Van der Linden & Baardman 2011, p. 64.
[33] Van der Hulst & Neve 2008, p. 38 e.v.
[34] KLPD, Dienst Nationale Recherche 2010, p. 16.
[35] Van der Hulst & Neve 2008, p. 33. De auteurs hanteren in hun rapport als een van de weinige het begrip high tech crime als overkoepelend begrip. Ik geef de voorkeur aan cybercrime als containerbegrip voor ICT-gerelateerde criminaliteit. Daarom heb ik de definitie van Van der Hulst & Neve op dit punt aangepast. Mijns inziens is de definitie als zodanig namelijk zeer bruikbaar in dit onderzoek.

Cybercrime ontwikkelt zich bij de gratie van technologische vooruitgang. De technologie en de mate waarin de maatschappij verweven raakt met die technologie bepalen welke vorm en omvang deze criminaliteit aanneemt.[36] In 2009 had negentig procent van de Nederlandse bevolking een internetverbinding, regelde vijfenzeventig procent zijn bankzaken via internet en deed eenzelfde percentage wel eens aankopen online. De fysieke en de digitale wereld raken door het forse gebruik van internet steeds meer met elkaar verweven. De ICT is kwetsbaar; zowel hardware als software zijn niet immuun voor misbruik.[37] Dat betekent dat naarmate de afhankelijkheid van ICT toeneemt, de risico's van het misbruik ervan zullen toenemen. Technologische ontwikkelingen worden in de regel dan ook gevolgd door ontwikkelingen in de criminaliteit.[38] Een strafrechtelijk kader dat voortdurend wordt geüpdatet en gelijke pas houdt met de technologische ontwikkelingen in de samenleving is daarom essentieel.[39] Hierover volgt in de volgende subparagraaf meer.

1.2.1 De ontwikkeling van cybercrimewet- en regelgeving

Nederland voerde in 1993 zijn eerste omvangrijke computergerelateerde wetgeving in met de Wet computercriminaliteit I.[40] Het gebruik van ICT gaf aanleiding om het strafrecht op diverse punten aan te passen, zowel op strafvorderlijk als op strafrechtelijk gebied.[41] Dat betekende dat naast de strafbaarstelling van de belangrijkste vormen van computercriminaliteit de wet ook een uitvoerige regeling van ICT-gerelateerde opsporingsbevoegdheden bevatte.[42] In 1998 zag de toenmalige minister van Justitie aanleiding om het wetsvoorstel computercriminaliteit II bij het parlement in te dienen.[43] Dit hing samen met de opkomst van het internet en de overheidsregulering die deze zou vereisen.[44] Met de komst en onder invloed van Europese regelgeving, zoals het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, beter bekend als het Cybercrimeverdrag[45], werd het wetsvoorstel ingehaald door Europese ontwikkelingen en daarom ingrijpend gewijzigd.[46] Met het – op initiatief van de Raad van Europa opgestelde – Cybercrimeverdrag verplichtten de aangesloten staten zich tot het nemen van (wetgevende) maatregelen ter voorkoming van cybercrime en ten behoeve van een adequate opsporing daarvan.[47] Uiteindelijk is de (aangepaste) Wet computercriminaliteit II op 1 september 2006 in werking getreden.[48] Zowel het materiële als het formele strafrecht werd met deze wet aangepast aan de nieuwe ontwikkelingen in de informatietechnologie.[49]

---

[36] Van der Linden & Baardman 2011, p. 66.
[37] KLPD, Dienst Nationale Recherche 2010, p. 8.
[38] Van der Linden & Baardman 2011, p. 66.
[39] Van der Linden & Baardman 2011, p. 68.
[40] *Kamerstukken II* 1989/90, 21 551, nr. 1-3; *Stb*. 1993, 33.
[41] KLPD, Dienst Nationale Recherche 2010, p. 172.
[42] Koops 2012a, p. 12.
[43] KLPD, Dienst Nationale Recherche 2010, p. 172.
[44] Van der Linden & Baardman 2011, p. 68.
[45] *Trb.* 2002, 18.
[46] Koops 2012a, p. 12.
[47] Van der Linden & Baardman 2011, p. 68.
[48] *Stb.* 2006, 299 en 300.
[49] KLPD, Dienst Nationale Recherche 2010, p. 173.

1.2.1.1 Conceptwetsvoorstel 'versterking bestrijding computercriminaliteit'

Niet veel later kwam men weer tot de conclusie dat het door de voortschrijdende ontwikkelingen op het terrein van ICT noodzakelijk was een aantal wetswijzigingen door te voeren ter bescherming van de persoonlijke levenssfeer, vertrouwelijke communicatie en computergegevens. Met het in juli 2010 ingediende conceptwetsvoorstel 'versterking bestrijding computercriminaliteit' is aan deze noodzaak gevolg gegeven. De snelle ontwikkelingen op het terrein van technologie, internet en computercriminaliteit roepen de vraag op of de huidige juridische instrumenten nog voldoende zijn toegesneden om computercriminaliteit effectief te kunnen bestrijden, aldus de memorie van toelichting bij het conceptwetsvoorstel.[50]

De belangrijkste wijziging die het conceptwetsvoorstel aandraagt is de creatie van een nieuwe bevoegdheid van de officier van justitie tot het afgeven van een bevel tot Notice-and-Take-Down op grond van de voorgestelde artikelen 125p en 125q Sv. Met deze maatregel wordt het mogelijk gemaakt om strafbare informatie op het internet ontoegankelijk te maken.[51] Verder worden drie wetswijzigingen voorgesteld. De eerste en tweede aanpassing zien op de strafbaarstelling van het wederrechtelijk overnemen van computergegevens uit een niet-openbaar werk (artikel 139c lid 1 Sr (nieuw)) en op het beschikken over of bekend maken van die gegevens (artikel 139e Sr (nieuw)).[52] De derde wijziging betreft de verruiming van de strafbaarstellingen van het met een technisch hulpmiddel afluisteren, aftappen of opnemen van vertrouwelijke communicatie (artikelen 139a, 139b en 139c Sr (nieuw)).[53] Thans zijn personen die heimelijk – zonder dat de andere gespreksdeelnemers daarvan weten – vertrouwelijke communicatie opnemen alleen strafbaar als het gaat om communicatie tussen anderen. Met het voorstel worden ook personen strafbaar die stiekem communicatie opnemen waaraan zij zelf deelnemen.[54]

Hoewel er op het gebied van de strafbaarstelling van cybercrime meer mogelijk wordt met het conceptwetsvoorstel, vraag ik me af of het in voldoende mate zal bijdragen aan de opsporing en bestrijding van cybercrime. Een van de knelpunten in de huidige wet- en regelgeving bij de aanpak van deze digitale criminaliteitsvorm heeft betrekking op de bestaande onduidelijkheid en complexiteit van die wet- en regelgeving. Er is daarom een grote behoefte aan uitleg ontstaan over de toepassing van de huidige (digitale) opsporingsbevoegdheden.[55] Het conceptwetsvoorstel voorziet hierin mijns inziens onvoldoende. Andere knelpunten die de opsporing van cybercrime en aanverwante criminaliteit frustreren, zijn de technieken die sporen van criminelen kunnen maskeren of verwijderen en daarnaast de ten gevolge van de komst van het internet ontstane jurisdictieproblemen.[56] Met name het toenemende gebruik van ingewikkelde versleuteltechnieken resulteert in belemmeringen in het opsporingsonderzoek.[57] Deze moeilijkheden en de grensoverschrijdende problematiek worden mijns inziens met de komst

[50] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 2.
[51] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 3.
[52] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 5.
[53] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 10 e.v.
[54] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 1 e.v.
[55] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 2-3.
[56] Oerlemans 2010, p. 152.
[57] Oerlemans 2011a, p. 906.

van de nieuwe wetgeving op cybercrimegebied nauwelijks aangepakt. Oerlemans is in dat kader tevens van mening dat de knelpunten in de opsporing van cybercrime niet worden geadresseerd.[58] Wellicht dat hacken door de opsporingsautoriteiten voornoemde obstakels in het opsporingsonderzoek wel kan bestrijden.

1.3 Hacken

De schaduwzijde van de vrijwel onbegrensde mogelijkheden van ICT en internet komt tot uitdrukking in de ontwikkeling van cybercriminaliteit. In dit onderzoek en in de volgende paragraaf in het bijzonder staat een specifieke verschijningsvorm binnen dit criminaliteitsspectrum centraal: het hacken van computersystemen en -netwerken.

1.3.1 De ontwikkeling van hacken

Ondanks allerlei beveiligingsmaatregelen is het mogelijk dat mensen inbreken op ICT-netwerken en systemen zonder daartoe de bevoegde autorisatie te hebben. Men noemt dit fenomeen hacken, in de Nederlandse juridische terminologie ook wel aangeduid als computervredebreuk.[59]

De term hacken stamt uit de jaren zestig van de vorige eeuw. Een hacker was toentertijd een positieve beschrijving van iemand die bekwaam was in het ontwikkelen van creatieve en effectieve oplossingen voor technische problemen. Een voorbeeld hiervan was het met goede bedoelingen doorbreken van de beveiliging van een systeem om zo de al dan niet aanwezige veiligheidslekken aan te tonen. Hacken was toen eigenlijk niets meer dan het innovatieve gebruik van technologie. Meestal ging het om het ‘onderzoeken’ van andermans computersystemen, louter uit nieuwsgierigheid.[60]

Waar hacken voorheen het aantonen van veiligheidslekken in systemen als doelstelling had, zijn hackers tegenwoordig steeds meer financieel gemotiveerd en is er sprake van een trend van *hacking for fame* naar *hacking for fortune*.[61] Hacken beoefent men niet meer alleen als ‘hobby’, maar wordt steeds vaker met criminele bedoelingen en motieven gedaan. Om die reden wordt ook wel gesproken van *crackers* (criminele hackers). Dit onderscheid wordt in de praktijk echter nauwelijks gehanteerd.[62] Ook in dit onderzoek zal ik enkel de term hacken gebruiken.

1.3.1.1 Hacktechnieken

Uit de literatuur is af te leiden dat een hackpoging doorgaans aan drie criteria voldoet:

> ‘1. Het is ongeoorloofd;
> 2. Het is eenvoudig, maar doordacht;
> 3. Het getuigt van een hoge mate van technische onderlegdheid en expertise.’[63]

[58] Oerlemans 2010, p. 152.
[59] Van der Hulst & Neve 2008, p. 67.
[60] Leukfeldt, Domenie & Stol 2010, p. 17.
[61] Van der Hulst & Neve 2008, p. 68 e.v.
[62] Leukfeldt, Domenie & Stol 2010, p. 17.
[63] Van der Hulst & Neve 2008, p. 69.

Bij een poging tot het inbreken op systemen kan onderscheid worden gemaakt in verschillende technieken die – vaak in combinatie – worden toegepast. Niet zelden maken hackers gebruik van de kwetsbaarheid van een ICT-systeem waarlangs een computer kan worden binnengedrongen. Tevens kan worden gedacht aan het binnendringen van een systeem onder een valse hoedanigheid, bijvoorbeeld met een gestolen inlognaam en wachtwoord op een e-maildienst, zoals *Hotmail* of *Gmail*.[64] Hackers komen dikwijls aan wachtwoorden door simpelweg te raden. In de privésfeer worden (nog steeds) de namen van partner, kinderen of huisdieren veelvuldig gebruikt als wachtwoord. Ook simpele wachtwoorden als 'password' en 'x' worden nog gehanteerd.[65] Het kraken van een wachtwoord kan ook op een veel professionelere manier, namelijk via een zogenaamde *brute force-aanval*.[66] Hierbij worden op automatische wijze alle mogelijke varianten van wachtwoorden achter elkaar uitgeprobeerd, totdat de toegang wordt verschaft tot de computer.[67]

Het plaatsen van malware[68] is ook een manier om een geautomatiseerd systeem binnen te dringen. Door een computer te besmetten met een kwaadaardig softwareprogramma wordt via een 'achterdeur' toegang verschaft tot deze computer. Een vorm van deze malware wordt heel toepasselijk een 'Trojaans paard' genoemd, omdat het softwareprogramma dikwijls ongemerkt op de computer van het slachtoffer verblijft. Nadat op afstand de toegang is verschaft tot de computer van het slachtoffer heeft de hacker verschillende mogelijkheden, zoals het wijzigen van de instellingen van de computer, het kopiëren van gegevens of het registreren van toetsaanslagen.[69]

Een andere techniek die veelvuldig door hackers wordt toegepast om op systemen te kunnen inbreken, is het gebruik van zogenaamde *botnets*[70].[71] Een botnet is een verzameling of een netwerk van door virus besmette computers die op afstand via een *command-and-control-server* door een hacker of een derde kunnen worden aangestuurd.[72] Een computer wordt onderdeel van een botnet door de gebruiker ervan te lokken naar een besmette website. Via deze website kan malware wordt geïnstalleerd, zodat er door de hacker gegevens kunnen worden ingezien op de computer van de gebruiker en er kan worden meegekeken naar welke handelingen de gebruiker uitvoert.[73] Botnets kunnen op deze manier onder meer worden ingezet voor identiteitsfraude[74] op het internet of de verspreiding van kinderporno.[75] Ze

[64] Oerlemans 2011a, p. 889.
[65] KLPD, Dienst Nationale Recherche 2010, p. 36 e.v.
[66] Oerlemans 2011a, p. 889.
[67] KLPD, Dienst Nationale Recherche 2010, p. 36 e.v.
[68] Malware (afkorting van 'malicious software') is het containerbegrip voor computerprogramma's die zonder toestemming van de eigenaar of beheerder draaien op een computer en het systeem iets laten doen naar de wens van de buitenstaander. Computers kunnen op uiteenlopende manieren worden besmet met malware, bijvoorbeeld via het openen van e-mailberichten, door het bezoeken van websites of door het klikken op advertenties. Er zijn verschillende soorten malware, zoals spyware, adware, traditionele virussen en moderne virussen, ook wel Trojaanse paarden genoemd; Van der Hulst & Neve 2008, p. 73.
[69] Oerlemans 2011a, p. 889.
[70] Het woord botnet is een samenvoeging van de woorden 'robot' en 'netwerk'.
[71] Van der Hulst & Neve 2008, p. 69.
[72] Oerlemans & Koops 2011, p. 1181.
[73] GOVCERT.NL 2010, p. 24.
[74] Van identiteitsfraude is sprake wanneer persoonlijk identificerende gegevens of vertrouwelijke informatie van mensen wordt misbruikt om hen vervolgens mee op te lichten. Het verkrijgen van identiteitsgegevens is meestal geen doel op zich, maar dient om andere criminele delicten mogelijk te maken, zoals het plunderen van

vormen daarnaast de infrastructuur van veel soorten internetcriminaliteit.[76] De botnets worden vanwege hun flexibiliteit en veelzijdigheid gezien als het 'Zwitsers zakmes' van cybercriminelen.[77] Het gebruik van botnets komt ook in Nederland voor. In 2010 haalde de High Tech Crime Unit van het KLPD het criminele computernetwerk Bredolab neer.[78]

1.3.2 Strafbaarstelling van hacken

Sinds de invoering van de Wet computercriminaliteit I, in maart 1993, valt hacken in Nederland onder de werking van het strafrecht.[79] De strafbaarstelling van hacken of computervredebreuk is vormgegeven naar analogie met huisvredebreuk.[80] Huisvredebreuk is strafbaar gesteld in artikel 138 Sr:

> 'Hij die in de woning of het besloten lokaal of erf, bij een ander in gebruik, wederrechtelijk binnendringt of, wederrechtelijk aldaar vertoevende, zich niet op de vordering van of vanwege de rechthebbende aanstonds verwijdert, wordt gestraft met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie.'[81]

Het wederrechtelijk binnendringen van de omschreven plaatsen[82] staat centraal in deze delictsomschrijving. Bij binnendringen denkt men aan een persoon die zich begeeft in een ruimte.[83] Van binnendringen is echter ook al sprake, wanneer slechts een deel van een persoon de woning in komt. Zo merkte de Hoge Raad de enkele aanwezigheid van een arm in een woning aan als binnendringen.[84] Van belang is in ieder geval dat de betrokkene in directe verbinding staat met de ruimte, aldus Oerlemans & Koops.[85]

Hetzelfde geldt in zekere zin voor computervredebreuk, dat strafbaar is gesteld in artikel 138ab Sr. Bij computervredebreuk gaat het alleen niet om het wederrechtelijk binnendringen van een woning, besloten lokaal of erf, maar om het wederrechtelijk binnendringen van een computer.[86] Artikel 138ab Sr stelt als volgt:

> 'Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een

---

betaalrekeningen of het onder een valse naam aanvragen van creditcards, bankrekeningen en hypotheken. Een techniek die op dit moment veelvuldig wordt gebruikt is het versturen van informatieverzoeken per e-mail (spam) waarin mensen op geraffineerde wijze wordt verzocht een (nagemaakte) bedrijvenwebsite te bezoeken (bijvoorbeeld een bankinstelling) om persoonsgegevens in te vullen. Deze vorm van misleiding noemt men ook wel *phishing* ; Van der Hulst & Neve 2008, p. 59.

[75] Van der Hulst & Neve 2008, p. 69 e.v.

[76] GOVCERT.NL 2010, p. 49.

[77] GOVCERT.NL 2011, p. 32.

[78] Van der Kroft 2011.

[79] *Stb.* 1993, 33.

[80] Ten Voorde 2010, p. 805.

[81] Artikel 138 lid 1 Sr.

[82] Artikel 138 Sr beoogt het ongestoorde genot of gebruik van deze plaatsen te beschermen (zie ook artikel 12 Grondwet). Met betrekking tot de woning is het beslissende criterium dat het moet gaan om een plaats waar mensen hun privaat huiselijk leven leiden. Het moet – met betrekking tot de overige ruimtes – in ieder geval gaan om een niet voor het publiek of niet voor openbare dienst bestemde plaatsen; Seuters 2009, p. 136.

[83] Oerlemans & Koops 2011, p. 1182.

[84] HR 7 februari 1956, *NJ* 1956, 147.

[85] Oerlemans & Koops 2011, p. 1182 e.v.

[86] Oerlemans & Koops 2011, p. 1182.

> geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:
> a. door het doorbreken van een beveiliging,
> b. door een technische ingreep,
> c. met behulp van valse signalen of een valse sleutel, of
> d. door het aannemen van een valse hoedanigheid.'[87]

Ook voor computervredebreuk geldt dat er een directe verbinding moet zijn tussen de betrokkene en het geautomatiseerde werk of een deel daarvan.[88] De Hoge Raad heeft hieromtrent onlangs een opmerkelijke uitspraak gedaan. De verdachte in deze zaak had gedurende een bepaalde periode een virus verspreid, dat bekend is geworden onder de naam *Toxbot*. Het Toxbot-virus had onder meer een zogenaamde 'keylogger-functionaliteit', waarmee toetsaanslagen konden worden opgenomen en heimelijk konden worden doorgestuurd.[89] Deze functionaliteit wordt in het bijzonder gebruikt voor het afvangen van gebruikersnamen en wachtwoorden. Met de gebruikersnamen en wachtwoorden van het slachtoffer kan een hacker vervolgens bij gegevens die normaal gesproken zijn afgeschermd.[90] De Hoge Raad stelt dat door de infectie met het Toxbot-virus wordt binnengedrongen in een computer.[91] Met andere woorden: het (doen) verspreiden of (doen) installeren van een virus levert hacken (computervredebreuk) op. Volgens Oerlemans & Koops is dit zeer opmerkelijk, aangezien de wetgever verschillende strafbaarstellingen heeft ingevoerd voor hacken en voor virusverspreiding (artikel 350a lid 3 Sr). De auteurs stellen dat er bij virusverspreiding niet per definitie een directe verbinding hoeft te zijn tussen de dader en de computer, zoals dat voor computervredebreuk wel is vereist. Bij virusverspreiding stuurt de betrokkene in de meeste gevallen een virus ongericht de wereld in en staat hij vervolgens niet als zodanig in verbinding met de computers die worden geïnfecteerd, aldus Oerlemans en Koops.[92] Er is derhalve pas sprake van computervredebreuk, indien de dader door het verspreiden van een virus met de geïnfecteerde computers communiceert. Het verspreiden van en computers infecteren met zo'n virus als zodanig voldoet niet aan de strafrechtelijke criteria van computervredebreuk.

1.3.2.1 Onderscheid tussen huisvredebreuk en computervredebreuk

Zoals hiervoor reeds is vermeld, is bij de strafbaarstelling van computervredebreuk aansluiting gezocht bij huisvredebreuk. Dat komt onder meer tot uitdrukking in het vereiste van een directe verbinding tussen de dader en de woning of bij computervredebreuk tussen de betrokkene en het geautomatiseerde werk. De analogie tussen beide artikelen stopt ten aanzien van het object van wederrechtelijk binnendringen. Voor huisvredebreuk is vereist dat het moet gaan om het betreden van een ruimte met een niet-openbaar of besloten karakter. Voor het binnendringen van geautomatiseerde werken geldt deze verbijzondering niet. Het maakt voor de strafbaarheid van computervredebreuk derhalve niet uit of het gaat om computers in de privésfeer of computers die voor het publiek beschikbaar zijn gesteld. De wetgever heeft

[87] Artikel 138ab lid 1 Sr.
[88] Oerlemans & Koops 2011, p. 1183.
[89] HR 22 februari 2011, *LJN* BN9287.
[90] Oerlemans & Koops 2011, p. 1182.
[91] HR 22 februari 2011, *LJN* BN9287.
[92] Oerlemans & Koops 2011, p. 1183.

duidelijk geen onderscheid gemaakt tussen persoonlijke en onpersoonlijke geautomatiseerde werken. Dit onderscheid is wel relevant ten aanzien van hacken door opsporingsautoriteiten, zoals ik zal betogen in paragraaf 6.2.4.2.1.

1.3.2.2 Overige strafbare voorwaarden van computervredebreuk

Voor computervredebreuk, en voor binnendringen in het bijzonder, is derhalve een directe verbinding tussen de betrokkene en de computer vereist. Wat verder met betrekking tot het binnendringen van belang kan worden geacht, is dat het moet gaan om het *opzettelijk en wederrechtelijk* binnendringen van een *geautomatiseerd werk*.[93] Het laatste begrip is gedefinieerd in artikel 80sexies Sr. Hier wordt onder verstaan:

> 'een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen.'[94]

De memorie van toelichting schaart onder meer computers en netwerken van aan elkaar verbonden computers onder dit begrip.[95] Toegespitst op de eenentwintigste eeuw voegt Oerlemans hier laptops en smartphones aan toe.[96] Het Hof 's-Gravenhage is van mening dat een router – het apparaat dat onder meer de koppeling tussen een internetverbinding en de op de router aangesloten computer verzorgt – niet als een geautomatiseerd werk kan worden gekwalificeerd.[97] Wat artikel 138ab Sr wel beschermt naast het medium, zoals de computer, laptop of smartphone, zijn de gegevens die op het geautomatiseerde werk zijn opgeslagen.[98]

Zoals is vermeld, is voor computervredebreuk verder vereist dat het geautomatiseerde werk *opzettelijk en wederrechtelijk* moet worden binnengedrongen. Dat wil zeggen dat het opzet moet zijn gericht op het binnendringen én dat het binnendringen wederrechtelijk moet zijn. Iemand die niet wederrechtelijk in andermans computer binnendringt, is volgens de huidige redactie van artikel 138ab Sr derhalve niet strafbaar.[99] Van binnendringen is in ieder geval sprake indien de toegang tot het systeem wordt verworven op de in artikel 138ab lid 1 sub a tot en met d Sr genoemde manieren.[100] De zinsnede 'in ieder geval' geeft aan dat de opsomming niet limitatief is. De wetgever heeft daarmee de mogelijkheid open willen laten dat ook wanneer geen sprake is van de in sub a tot en met sub d genoemde kunstgrepen, er toch aan de wettelijke vereisten van computervredebreuk kan zijn voldaan.[101]

Een hacker kan nadat hij is binnengedrongen ook nog andere strafbare handelingen verrichten, zoals het verwerken of overdragen van de gegevens, waartoe hij aldus toegang heeft verkregen. Op grond van 138ab lid 2 Sr geldt dergelijk handelen als strafverzwarende omstandigheid.[102] Een hacker kan ook opzettelijk dan wel door schuld een geautomatiseerd

---

[93] Artikel 138ab lid 1 Sr.
[94] Artikel 80sexies Sr.
[95] *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 6.
[96] Oerlemans 2011a, p. 889.
[97] Hof 's-Gravenhage 9 maart 2011, *LJN* BP7080.
[98] Ten Voorde 2010, p. 805.
[99] Leukfeldt, Domenie & Stol 2010, p. 19.
[100] Artikel 138ab lid 1 sub a, b, c, d Sr.
[101] Leukfeldt, Domenie & Stol 2010, p. 19.
[102] Artikel 138ab lid 2 Sr.

werk vernielen op grond van artikel 161sexies en artikel 161septies Sr.[103] Deze laatste twee artikelen zijn gericht op de strafbaarstelling van het in gevaar brengen van de algemene veiligheid.[104] Ten slotte bestaan er strafbepalingen voor de vernieling van gegevens door opzet of schuld (artikel 350a respectievelijk 350b Sr), het aftappen of opnemen van gegevens (artikel 139c Sr), het plaatsen van opname-, aftap- of afluisterapparatuur (artikel 139d Sr) en het bezitten en bekendmaken van wederrechtelijk verkregen gegevens (artikel 139e Sr).[105]

De strafbaarstelling van computervredebreuk heeft daarnaast ook een andere verschijningsvorm, namelijk het binnendringen in een geautomatiseerd werk met het oogmerk (a) zichzelf of een ander te bevoordelen door gebruik te maken van de verwerkingscapaciteit van het geautomatiseerde werk of (b) om zich toegang te verschaffen tot het geautomatiseerde werk van een derde.[106]

1.4 Conclusie

Cybercrime – het containerbegrip voor ICT-gerelateerde criminaliteit – heeft de laatste jaren een hoge vlucht genomen. Zo wordt bij het plegen van traditionelere delicten steeds vaker gebruikgemaakt van computers, ICT en in het bijzonder het internet. Stalking, diefstal en fraude hebben op deze manier een geheel nieuwe uitvoering gekregen. Ook is er – door de voortschrijdende informatie- en communicatietechnologie en de ontwikkeling van internet – een geheel nieuw palet aan criminele activiteiten ontstaan met een sterk technisch, virtueel karakter. Het gaat om nieuwe strafbare gedragingen, die niet kunnen bestaan zonder ICT. Een voorbeeld hiervan is hacken. Hacken is het op elektronische wijze, zonder daartoe de bevoegde autorisatie te hebben, binnendringen van ICT-netwerken en systemen en wordt vaak met financiële motieven gedaan. Hacken is in Nederland met de Wet computercriminaliteit I strafbaar gesteld onder de noemer computervredebreuk (artikel 138ab Sr). Het inbreken op computers, laptops en smartphones kan op verschillende manieren worden gedaan. Zo wordt er onder meer gebruikgemaakt van kwaadaardige softwareprogramma's die – dikwijls ongemerkt – de toegang verschaffen tot computers. Een andere techniek die veelvuldig door hackers wordt gebruikt om op systemen te kunnen inbreken, is het gebruik van botnets. Nu staat in dit onderzoek niet het hacken door criminelen centraal, maar het hacken door politie en justitie bij de aanpak van cybercriminaliteit. Het op afstand binnendringen van systemen in de opsporingsfase staat in het volgende hoofdstuk centraal.

[103] Art 161sexies en art 161septies Sr.
[104] Leukfeldt, Domenie & Stol 2010, p. 19.
[105] Artikel 350a, 350b, 139c, 139d, 139e Sr.
[106] Artikel 138ab lid 3 Sr.

Hoofdstuk 2 Hacken als opsporingsmethode

In het voorgaande hoofdstuk stond onder meer de ontwikkeling van cybercrime en de wet- en regelgeving op dit gebied centraal. Deze nieuwe criminaliteitsvorm komt tegenwoordig overal voor en vindt plaats over de gehele linie van het criminele circuit. Dat heeft implicaties voor het opsporingsbeleid en leidt tot de conclusie dat iedere agent in de toekomst zal moeten beschikken over enige basiskennis inzake deze nieuwe misdaadvorm. Ook klassieke delicten hebben immers steeds vaker een cybercrimeaspect.[107] Dit leidt mijns inziens tot de conclusie dat de opsporings*technieken* ook moeten worden aangepast aan onze veranderende maatschappij. Daar vormt hacken een voorbeeld van.

In het vorige hoofdstuk lag de focus op hacken als specifiek strafbaar feit binnen de overkoepelende criminaliteitsvorm cybercrime. In de volgende hoofdstukken en in het komende hoofdstuk in het bijzonder zal niet zozeer het binnendringen van geautomatiseerde werken door verdachten centraal staan, maar het hacken als opsporingsmethode. Daarbij behandelt paragraaf 2.1 de ontwikkeling van hacken in het opsporingsonderzoek en zet paragraaf 2.2 uiteen waar bij hacken door opsporingsautoriteiten aan kan worden gedacht. Oerlemans trekt in dat kader de conclusie dat hacken niet moet worden gezien als één afgebakende opsporingsmethode, maar als een verzameling van allerlei toepassingen op dat gebied.[108] In de literatuur beweert men dat hacken op dit moment al plaatsvindt, ook al is niet duidelijk of voor deze methode een wettelijke basis kan worden gevonden. Een voorbeeld van hacken in de praktijk komt aan bod in paragraaf 2.2.1.4. Ook neem ik in dit hoofdstuk een kijkje over de grens. Hacken door politie en justitie is namelijk op dit moment al wel toegestaan in Duitsland (§ 2.3).

2.1 De ontwikkeling van hacken als opsporingsmethode

Met de Wet computercriminaliteit I is tegemoetgekomen aan de snelle ontwikkelingen op het terrein van de informatie- en communicatietechnologie. De Nederlandse wetgever creëerde bevoegdheden op het gebied van het onderzoek van geautomatiseerde werken en formuleerde specifieke strafbepalingen rond de wederrechtelijke toegang tot computers en het misbruik van gegevens. Met de invoering van de Wet computercriminaliteit II zijn het formele en het materiële recht verder in overeenstemming gebracht met de ontwikkelingen op het gebied van de informatietechnologie op dat moment.[109] Met betrekking tot het strafvorderlijke kader heeft dit geresulteerd in de totstandkoming van een op het verzamelen van digitale informatie gericht arsenaal aan opsporingsmethoden, waaronder de doorzoeking ter vastlegging en inbeslagneming van gegevens en het opnemen van vertrouwelijke communicatie.[110]

Steeds vaker klinken bij politie en justitie geluiden dat ook het hacken – en het online doorzoeken als onderdeel daarvan – door opsporingsautoriteiten mogelijk zou moeten worden

[107] Leukfeldt, Domenie & Stol 2010, p. 254 e.v.
[108] Oerlemans 2011a, p. 891.
[109] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 2.
[110] Ministerie van Veiligheid en Justitie 2011, p. 43.

gemaakt.[111] Ook in de politiek wordt al jaren over het invoeren van een dergelijke mogelijkheid gesproken. In de praktijk wordt deze opsporingsmethode zelfs al gehanteerd.[112] Een korte beschrijving van de ontwikkelingen binnen de politiek en politie en justitie met betrekking tot de opsporingsmethode hacken is hier daarom op zijn plaats. Daarbij dient te worden opgemerkt dat hacken het overkoepelende begrip vormt voor iedere vorm van het heimelijk en op afstand via internet binnendringen van een geautomatiseerd werk.[113] Binnen dat overkoepelende begrip valt onder meer de online doorzoeking.[114]

2.1.1 Ontwikkelingen in de politiek en bij opsporingsautoriteiten

In mei 2008 werd de online doorzoeking voor het eerst concreet behandeld in de politiek, toen door de Tweede Kamer een motie werd aangenomen van de Kamerleden Teeven en Heerts om het 'virtueel doorzoeken' voor de opsporing van terroristische misdrijven en misdrijven in georganiseerd verband mogelijk te maken.[115] Niet veel later bleken ook de opsporingsautoriteiten interesse te hebben in de online doorzoeking als opsporingsmethode. Uit onderzoek dat in opdracht van het ministerie van Justitie werd uitgevoerd, was namelijk gebleken dat het extreem gecompliceerd was geworden criminele activiteiten op het internet te traceren. Dat zou samenhangen met het feit dat het voor criminelen betrekkelijk eenvoudig was geworden te voorkomen dat hun sporen konden worden gevolgd. Het criminele milieu zou daarbij gebruikmaken van software die berichten versleutelt en sporen uitwist.[116] De online doorzoeking zou in die gevallen een oplossing kunnen bieden, doordat het op die manier mogelijk zou worden om op afstand een geautomatiseerd werk binnen te dringen teneinde bewijsmateriaal te verzamelen. In het voornoemde onderzoek van het ministerie van Justitie werd tevens het creëren van een bevoegdheid tot het grensoverschrijdend veiligstellen van gegevens door middel van een online doorzoeking in internationaal verband aanbevolen.[117] Juridisch gezien lijkt het hanteren van deze bevoegdheid met een internationaal karakter op dit moment niet houdbaar. De uitoefening van strafvorderlijke bevoegdheden is gebaseerd op het geweldsmonopolie van de staat en als zodanig territoriaal gebonden.[118] Het aanwenden van strafvorderlijke bevoegdheden in het buitenland – zoals het grensoverschrijdend hacken – is daarom uit den boze.[119] Voor het verkrijgen van in het buitenland opgeslagen bestanden moet Nederland rechtshulp zoeken.[120] Dit lijkt een vrij helder en duidelijk verhaal. Het een en ander wordt echter gecompliceerd door het feit dat digitale grenzen zeer lastig te trekken zijn. Internet is per definitie grenzeloos en beperkt zich niet tot één land.[121]

---

[111] Zie pleidooi van officier van justitie Lodewijk van Zwieten voor het mogelijk maken van grensoverschrijdend hacken op 25 oktober 2010 in 'Nieuwsuur', NOS Nederland 2. Dit tv-fragment is te vinden via: http://nieuwsuur.nl/video/193776-de-strijd-tegen-cybercrime.html.
[112] Oerlemans 2011a, p. 888.
[113] Oerlemans 2011a, p. 903.
[114] Oerlemans 2011a, p. 893.
[115] *Kamerstukken II* 2007/08, 28 684, nr. 144.
[116] *Kamerstukken II* 2008/09, 28 684, nr. 232, p. 2-3.
[117] *Kamerstukken II* 2008/09, 28 684, nr. 232, p. 3.
[118] Baaijens-van Geloven 2001, p. 355.
[119] Klip 2000, p. 140.
[120] Koops 2012a, p. 17.
[121] Oerlemans 2011a, p. 893.

In november 2010 wordt de online doorzoeking opnieuw besproken in de Tweede Kamer. De minister van Veiligheid en Justitie zegt in dit kader toe hacken als opsporingsmethode 'in beginsel' binnen de nationale wetgeving te realiseren en daartoe voorstellen te doen.[122] Met het eerder behandelde en na de toezegging van de minister verschenen conceptwetsvoorstel 'versterking bestrijding computercriminaliteit' is hieraan echter geen gevolg gegeven.[123] Blijkbaar worden de huidige opsporingsbevoegdheden voldoende geacht in de strijd tegen cybercrime.[124] Hier valt mijns inziens wat tegen in te brengen, zoals ik zal betogen in hoofdstuk 6.

Eind januari 2011 worden over hacken in het opsporingsonderzoek weer Kamervragen gesteld aan de minister van Veiligheid en Justitie. Nu over het gebruik van zogenaamde *spysoftware* door de Nederlandse opsporingsautoriteiten. De minister bevestigt in februari 2012 dat de overheid in het bezit is van software die geïnstalleerd kan worden op de computer van een verdachte en waarmee in het kader van een opsporingsonderzoek toegang kan worden verkregen tot die computer en of gegevens daarvan kunnen worden overgenomen. De minister verklaart dat de software slechts wordt gebruikt binnen de grenzen van het huidige Wetboek van Strafvordering en zich dientengevolge beperkt tot het opnemen van vertrouwelijke communicatie op grond van artikel 126l Sv. Over de vraag of hacken in dit kader ook al plaatsvindt, laat de minister zich ook deze keer niet uit.[125] Dat wil zeggen dat door de verklaring van de minister niet duidelijk is geworden of de spysoftware ook *op afstand* wordt geplaatst in plaats van het installeren van de software op verdachtes computer na het betreden van zijn woning zonder toestemming. Dit laatste – zo wordt beargumenteerd – wordt op grond van de huidige wetgeving wel mogelijk geacht.[126] Het is maar de vraag of dit ook geldt voor het plaatsen van de software op afstand. Oftewel, is het hacken of online doorzoeken reeds op grond van de huidige wetgeving mogelijk? Daarover volgt in relatie tot het opnemen van vertrouwelijke communicatie in paragraaf 6.2.2 meer. Eerst acht ik het noodzakelijk om te bepalen wat hacken door opsporingsautoriteiten precies inhoudt.

2.2 Hacken in het kader van de opsporing

Zoals reeds is vermeld, is het internet geen virtuele wereld waar alleen brave burgers vertoeven. Ook criminelen maken er veelvuldig gebruik van. Het internet levert derhalve werk op voor de wetshandhavers. De computer en vergelijkbare machines zijn een bron van informatie over de misdaden die worden gepleegd op of met behulp van deze apparaten of in de wereld die deze creëren.[127] De vraag is hoe de opsporingsautoriteiten de beschikking krijgen over deze informatie. Het hacken van computers van verdachte personen zou daarbij buitengewoon handig zijn. Bij hacken wordt heimelijk en op afstand – via het internet – een

[122] *Kamerstukken II* 2010/11, 25 november 2010, Antwoord op Kamervragen van PvdA Kamerlid Recourt van de minister van Veiligheid en Justitie, kenmerk: 2010Z15331.
[123] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10.
[124] Oerlemans 2010, p. 148.
[125] *Kamerstukken II* 2011/12, 7 februari 2012, Antwoord op Kamervragen van de D66 Kamerleden Schouw en Berndsen van de minister van Veiligheid en Justitie, aanhangselnummer 1374, p. 1 e.v.
[126] Oerlemans 2011a, p. 902.
[127] Boek 2000, p. 589.

geautomatiseerd werk binnengedrongen.[128] Op deze geautomatiseerde werken zijn mogelijk sporen van criminele daden te vinden, terwijl in de e-mailboxen communicatie over strafbare feiten of strafbare communicatie als zodanig kan worden aangetroffen.[129]

Hacken vindt derhalve plaats op afstand. Dat wil zeggen dat het niet noodzakelijk is dat opsporingsautoriteiten fysiek in de computer van de verdachte inbreken.[130] Een besloten plaats, zoals een woning, hoeft dus niet te worden binnengetreden.[131] Een goede hack zal bovendien door de betrokkene meestal niet worden opgemerkt. Zo kunnen de opsporingsautoriteiten zonder veel risico op ontdekking veel te weten komen over bepaalde strafbare feiten, zonder dat de onderzochte personen dit merken.[132] Hacken vormt daarom een bijzonder indringende opsporingsmethode, niet alleen doordat het binnendringen heimelijk gebeurt, ook omdat de computer zich heeft ontplooid – zoals Koops & Prinsen het mooi formuleren – tot de spiegel van de persoonlijke levenssfeer.[133]

Hacken moet daarnaast niet worden beschouwd als één afgebakende opsporingsmethode, maar als een verzameling van opsporingsmethoden die in verschillende mate inbreuk maken op de grondrechten van de betrokkene, aldus Oerlemans.[134] Eerder werd al kort aangegeven dat de online doorzoeking in de literatuur wordt gezien als een specifieke vorm van hacken. Aan de volgende toepassingen kan met betrekking tot hacken als overkoepeld begrip tevens worden gedacht:

> ‘I) Het ‘inkijken’ van een computer teneinde vast te stellen welke eigenschappen van een geautomatiseerd werk heeft en welke bestanden zich op een computer en aangesloten apparaten bevinden;
> II) het op afstand kopiëren van gegevens (doorzoeken) op een geautomatiseerd werk;
> III) het afvangen van toetsaanslagen, waaronder wachtwoorden, van de betrokkene die van het geautomatiseerde werk gebruik maakt;
> IV) het *real time* monitoren van netwerkverkeer op een geautomatiseerd werk door middel van een technische voorziening; en
> V) het beïnvloeden van een geautomatiseerd werk, zoals het aanpassen van instellingen, aanzetten van webcams of microfoons en saboteren of uitschakelen van een geautomatiseerd werk.’[135]

2.2.1 Van vijf manieren naar drie methoden naar één overkoepelend begrip

De vijf toepassingen of manieren van hacken in het opsporingsonderzoek die hiervoor zijn opgesomd, kunnen worden ingekaderd in drie methoden die onder het overkoepelende begrip hacken kunnen worden gerangschikt. Deze drie methoden zijn de online doorzoeking, het plaatsen van een technische voorziening op een geautomatiseerd werk en het beïnvloeden van een dergelijk systeem. Optie I en II kunnen volgens Oerlemans onder de online doorzoeking worden geschaard en optie III en IV zien op het plaatsen van een technische voorziening op een geautomatiseerd werk.[136] Met de online doorzoeking kunnen die gegevens of bestanden

[128] Oerlemans 2011a, p. 903.
[129] Boek 2000, p. 589.
[130] Proos 2008.
[131] Oerlemans 2010, p. 148.
[132] Boek 2000, p. 590.
[133] Koops & Prinsen 2005, p. 627.
[134] Oerlemans 2011a, p. 891 e.v.
[135] Oerlemans 2011a, p. 891 e.v.
[136] Oerlemans 2011a, p. 893.

worden bemachtigd, die zijn vastgelegd of opgeslagen op de computer en met het plaatsen van een technische voorziening op een dergelijk medium kan computerverkeer of -gebruik *real time* worden gemonitord. Deze laatste mogelijkheid heeft tot gevolg dat, met bepaalde software die door de politie is geïnstalleerd op de computer van de betrokkene, communicatie kan worden afgevangen, die wordt verstuurd met of ontvangen op het geautomatiseerde werk. Het gaat in deze gevallen derhalve niet om informatie die op de computer of op het netwerk is opgeslagen, maar om vluchtig(e) communicatie of gegevensverkeer. Met dit onderscheid wordt aangesloten bij het onderscheid in bevoegdheden in het Wetboek van Strafvordering tussen opgeslagen en stromende gegevens, waarbij de online doorzoeking ziet op opgeslagen gegevens en het plaatsen van een technische voorziening op stromend gegevensverkeer.[137]

De derde en laatste methode van hacken ziet op het beïnvloeden van een geautomatiseerd werk. Steenbruggen is – verwijzend naar de huidige Duitse wetgeving waarin de bevoegdheid van de online doorzoeking reeds is vastgelegd – in dit kader in zijn noot van mening dat onder de online doorzoeking ook het beïnvloeden van een computer zou moeten worden verstaan.[138] Ik prefereer optie V echter te beschouwen als een losstaande methode binnen de bevoegdheid hacken als overkoepelend opsporingsbegrip, omdat de methode in beginsel niet ziet op de vergaring van gegevens, zoals de online doorzoeking en het plaatsen van een technische voorziening dat wel doen, maar in essentie betrekking heeft op het op afstand besturen van een geautomatiseerd werk. Het inzetten van een dergelijke methode heeft mijns inziens een potentieel andere inbreuk op het recht op privacy tot gevolg dan de overige twee methoden.

In de volgende subparagrafen zullen de drie aangehaalde methoden nog eens afzonderlijk aan bod komen. Eerst wil ik benadrukken dat er in de literatuur over het onderscheid tussen de online doorzoeking en het plaatsen van een technische voorziening op een geautomatiseerd werk geen volledige consensus bestaat. Zo is Koning van mening dat dit onderscheid tussen bijvoorbeeld het kopiëren of bekijken van gegevens op de computer (de online doorzoeking) en het afvangen van toetsaanslagen (het plaatsen van een technische voorziening) niet werkbaar is. De auteur stelt dat een dergelijke tweesplitsing de technische realiteit ontkent.[139] Daarmee doelt ze op het feit dat beide toepassingen in de praktijk niet altijd strikt gescheiden (kunnen) blijven. Zo zal een online doorzoeking in veel gevallen tevens het plaatsen van een technische voorziening behoeven en zal het computersysteem in veel gevallen ook moeten worden gemanipuleerd om sporen van de doorzoeking te wissen.[140] Hoewel het onderscheid tussen de online doorzoeking en het plaatsen van een technische voorziening op een geautomatiseerd werk *in de praktijk* waarschijnlijk moeilijk te hanteren is, zal ik het – waar noodzakelijk in dit onderzoek – toch gebruiken. Daarbij zal ook het beïnvloeden van een computersysteem of netwerk afzonderlijk worden benaderd. Vanwege het ingewikkelde en technische karakter van hacken, acht ik het in dit hoofdstuk van belang om de verschillende vormen van hacken gescheiden van elkaar te behandelen. Ik sluit me aldus aan bij Oerlemans en Buermeyer.[141] Daaraan wil ik toevoegen dat het onderscheid

[137] Oerlemans 2011a, p. 893.
[138] BVerfG 27 februari 2008, 'Online-Durchsuchung', m.nt. W.A.M. Steenbruggen, *Mediaforum* 2008, 5, p. 232.
[139] Koning 2012, p. 52.
[140] Koning 2012, p. 52.
[141] Zie Oerlemans, 2011a, p. 892 en Buermeyer 2007, p. 160-161.

tussen de online doorzoeking en het plaatsen van een technische voorziening tevens wordt gemaakt in de Wet op de inlichtingen- en veiligheidsdiensten 2002. Inlichtingen- en veiligheidsdiensten hebben op grond van artikel 24 Wiv 2002 de bevoegdheid om binnen te dringen in geautomatiseerde werken. Waar het onderscheid tussen de methoden niet relevant is, zal het niet worden gemaakt en zal het begrip hacken als overkoepelende term worden gebruikt.

2.2.1.1 De online doorzoeking

Zoals hierboven is vermeld, moeten de 'inkijkoperatie' in een geautomatiseerd werk en het doorzoeken ervan op afstand, respectievelijk optie I en II, als online doorzoeking worden gekwalificeerd.[142] Met de online doorzoeking worden op afstand via internet gegevens op een persoonlijk geautomatiseerd werk van de verdachte bekeken of eigenschappen van dit systeem beoordeeld. Om de doorzoeking mogelijk te maken, dient het geautomatiseerde werk eerst in juridische zin te worden gehackt.[143] Dat wil zeggen dat opsporingautoriteiten computervredebreuk (artikel 138ab Sr) dienen te plegen om de computer van de verdachte toegankelijk te maken voor de online doorzoeking.

De doorzoeking als zodanig is een rechtsfiguur die ons huidig strafvorderlijk wetboek reeds in verschillende verschijningsvormen kent. Zo heeft de wetgever de doorzoeking van plaatsen ter aanhouding (artikel 55a Sv), ter inbeslagneming (artikelen 96b, 96c en 97 Sv) en ter vastlegging van gegevens (artikel 125i Sv) gecreëerd. Het doorzoeken van plaatsen zal altijd als steunbevoegdheid worden toegepast.[144] Dat wil zeggen dat de doorzoeking geen opsporingsdoel als zodanig is, maar dat dit dwangmiddel de uitoefening van een andere bevoegdheid (zoals de vastlegging van gegevens of de inbeslagneming van voorwerpen) dient te ondersteunen. Met andere woorden, door de hantering van de doorzoeking als steunbevoegdheid wordt de inzet van andere strafvorderlijke bevoegdheden mogelijk gemaakt.[145] In dit kader rijst de vraag of de *online* doorzoeking ook dient te worden aangemerkt als steundwangmiddel in het (digitale) opsporingskader. Ik ben die mening wel toegedaan. Mijns inziens valt er in dit kader een parallel te trekken met de doorzoeking ter vastlegging van gegevens ex artikel 125i Sv. De kern van dit dwangmiddel ligt in de bevoegdheden tot het doorzoeken van een plaats ter vastlegging van de (aangetroffen) gegevens en kan ertoe leiden dat onderzoek wordt gedaan naar gegevens, inzage wordt verkregen in gegevens en maakt het kopiëren van gegevens, die op een computersysteem zijn opgeslagen, mogelijk.[146] De overeenkomsten tussen deze bevoegdheid en de online doorzoeking zijn groot. Met de laatste methode kunnen immers ook opgeslagen gegevens worden bekeken en gekopieerd. Het een en ander vindt echter – in tegenstelling tot de doorzoeking ter vastlegging van gegevens – *op afstand* plaats. Dit neemt niet weg dat het doel en uitgangspunt van beide bevoegdheden hetzelfde is, namelijk het verzamelen of vorderen van (incriminerend) materiaal op geautomatiseerde werken. De online doorzoeking dient

[142] Oerlemans 2011a, p. 891 e.v.
[143] Zie blog Jan-Jaap Oerlemans over het mogelijk maken van hacken als opsporingsmethode op 29 oktober 2011. De blog is te vinden via: http://oerlemansblog.weblog.leidenuniv.nl/2011/10/.
[144] Kronenberg & De Wilde 2010, p. 203.
[145] Corstens 2011, p. 478.
[146] *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 11.

daarom analoog aan de overige doorzoekingsbevoegdheden als steunbevoegdheid te worden gekwalificeerd.

Zoals hiervoor reeds is vermeld, kunnen politie en justitie met de online doorzoeking gegevens bekijken, die op een in een opsporingsonderzoek betrokken computer te vinden zijn. Oerlemans stelt in dit kader dat deze opsporingsmethode tevens ziet op het onderzoeken van gegevens in de persoonlijke webmail van de verdachte.[147] De rechtbank Rotterdam heeft zich al uitgesproken over deze vorm van opsporen en heeft hieromtrent bepaald dat het een opsporingsambtenaar niet vrij staat om zonder toestemming van de gebruiker in een *Hotmail*-inbox te kijken, omdat daarmee een ernstige inbreuk wordt gemaakt op de persoonlijke levenssfeer van die gebruiker.[148] Deze uitspraak bewijst dat de opsporingsautoriteiten reeds gebruikmaken van hacken in het opsporingsonderzoek. In deze zaak had de politie na toestemming van de officier van justitie met een verkregen inlognaam en wachtwoord op afstand in een e-mailaccount gekeken. De Rotterdamse rechter was van mening dat er voor deze handelswijze geen wettelijke basis bestaat en daarmee als ontoelaatbaar moest worden beschouwd.[149] Hierbij moet worden opgemerkt dat het door de Nederlandse wetgever wel mogelijk is gemaakt om op een andere manier kennis te nemen van de inhoud van berichten op een e-mailaccount. De officier van justitie moet dan in de daarvoor in aanmerking komende gevallen, na een verkregen machtiging van de rechter-commissaris, een vordering daartoe doen als bedoeld in artikel 126ng lid 2 Sv.[150] Overigens werd in de voornoemde zaak in hoger beroep bepaald dat er geen sprake was van enig vormverzuim tijdens het voorbereidend onderzoek jegens de verdachte, omdat de verdachte had verklaard dat het vermelde *Hotmail*-adres niet bij hem in gebruik was en dat hij het e-mailadres bovendien niet kende.[151] Deze uitspraak doet verder niets af aan de vaststelling dat hacken door de politie reeds geschied.

2.2.1.2 Het plaatsen van een technische voorziening op een geautomatiseerd werk

Optie III en IV van de hierboven opgesomde toepassingen van hacken als opsporingsmethode zijn in essentie te vergelijken met een opsporingsbevoegdheid uit het huidige Wetboek van Strafvordering, namelijk het opnemen van vertrouwelijke informatie.[152] Met dit in artikel 126l Sv geregelde dwangmiddel gaat het erom dat met behulp van apparatuur als richtmicrofoons en bugs stromende communicatie kan worden afgevangen. Informatie die iemand in zijn eigen computer invoert, kan met deze bevoegdheid derhalve niet worden opgenomen.[153]

Het plaatsen van een technische voorziening op een geautomatiseerd werk als vorm van hacken ziet – net als de bevoegdheid ex artikel 126l Sv – op het (direct) afluisteren van beschermd gespreksverkeer. De technische voorziening wordt in deze context ook wel

[147] Zie blog Jan-Jaap Oerlemans over het mogelijk maken van hacken als opsporingsmethode op 29 oktober 2011. De blog is te vinden via: http://oerlemansblog.weblog.leidenuniv.nl/2011/10/.
[148] Rb. Rotterdam 26 april 2010, *LJN* BM2520.
[149] Rb. Rotterdam 26 april 2010, *LJN* BM2520.
[150] Artikel 126ng lid 2 Sv.
[151] Hof 's-Gravenhage 27 april 2011, *LJN* BR6836.
[152] Oerlemans 2011a, p. 893.
[153] Corstens 2011, p. 433.

spyware genoemd.[154] Het plaatsen van spyware met als doel het opnemen van vertrouwelijke communicatie wordt op dit moment reeds door het strafvorderlijk wetboek mogelijk gemaakt via artikel 126l Sv.[155] Het is toegestaan om na het betreden van bijvoorbeeld een woning software (spyware) op de computer van de verdachte te plaatsen om toetsaanslagen of muisklikken te registreren.[156] Dit standpunt is – zoals hiervoor reeds is vermeld – bevestigd door de minister van Veiligheid en Justitie. Waar het met betrekking tot hacken als opsporingsmethode echter over gaat, is dat men wenst dat het plaatsen van spyware ook *op afstand* mag plaatsvinden.[157] Daarvoor zal doorgaans de computer van de verdachte moeten worden gehackt. De vraag rijst of een dergelijke opsporingsmethode wetmatig is.

2.2.1.3 Het beïnvloeden van een geautomatiseerd werk

Door een computer(systeem) of netwerk te hacken, krijgt men in principe de toegang tot de gehele inhoud van dat systeem of netwerk. Dit heeft tot gevolg dat al het gegevensverkeer en opgeslagen data op de geautomatiseerde werken voor opsporingsautoriteiten toegankelijk worden.[158] Deze vrije doorgang brengt tevens met zich mee dat politie en justitie het systeem volledig kunnen overnemen en kunnen besturen en daarmee ook op afstand kunnen beïnvloeden. Op die wijze zouden de opsporingsdiensten een microfoon of webcam op de computer kunnen activeren, geluid- of beeldopnames kunnen maken en deze vervolgens kunnen beluisteren of bekijken. Met name het aanzetten van een webcam gaat mijns inziens, vanwege onder meer het recht op bescherming van de persoonlijke levenssfeer, zeer ver en mogelijk zelfs te ver. Daar kan tegen in worden gebracht dat de wetgever de invoering van een bevoegdheid tot het stelselmatig observeren van personen wel noodzakelijk heeft geacht. Ter wille van de opsporing of in de daaraan voorafgaande fase kan de politie bepaalde personen, objecten en situaties gadeslaan teneinde informatie te verzamelen. Zo kan (stelselmatige) observatie inhouden dat men vanuit een bepaalde ruimte met een videocamera bekijkt wie een bepaald pand in- en uitgaan.[159] Het permanent waarnemen door middel van een camera van wat zich *in* de woning afspeelt, is echter niet toegestaan.[160] Het op afstand aanzetten van een webcam op een computer in een huis lijkt – vanwege onder andere de (te) grote inbreuk op de vrijheid van het individu – daarom tevens uitgesloten.

Zoals reeds is vermeld, maakt het binnendringen op een geautomatiseerd werk praktisch alles mogelijk op dat apparaat. Zo kunnen instellingen op een computer of netwerk worden aangepast en kan het systeem worden uitgeschakeld. De Bredolab-ontmanteling – waarover in de volgende subparagraaf meer volgt – is een voorbeeld van het op afstand uitschakelen van een geautomatiseerd werk.

2.2.1.4 Hacken door opsporingsautoriteiten in de praktijk

Hacken als opsporingsmethode wordt in de praktijk al incidenteel toegepast. Zo behandelde ik in de inleiding van dit onderzoek het binnendringen van het anonimiseringsnetwerk *Tor*

[154] Oerlemans 2011a, p. 893.
[155] Verbeek, De Roos & Van den Herik 2000, p. 155.
[156] Koops & Buruma 2007, p. 118.
[157] Oerlemans 2011a, p. 903.
[158] Interview R. Prins en J.J. Oerlemans op 5 juni 2012 ten burele van Fox-IT te Delft.
[159] Corstens 2011, p. 446.
[160] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 71.

teneinde kinderpornografisch materiaal op het internet te wissen en noemde ik in paragraaf 2.2.1.1 de zaak waarin de opsporingsautoriteiten met een verkregen inlognaam en wachtwoord op afstand de e-mailberichten van de verdachte bekeken. Een andere in dit kader relevante zaak is bekend onder de naam Bredolab.[161] Bredolab was een crimineel computernetwerk dat in oktober 2010 onder veel mediabelangstelling werd ontmanteld.[162] Dit zogenoemde botnet – zie paragraaf 1.3.1.1 voor meer informatie over een botnet – bestond uit een netwerk van op afstand bestuurbare computers. De rechtmatige gebruikers van de computers, de slachtoffers, wisten niet dat een ander de controle over het besturingssysteem van hun computers had genomen door middel van een computervirus. Het botnet werd via command-and-control-servers door de verdachte ingezet voor allerlei activiteiten, waaronder het onderscheppen van creditcardgegevens en het versturen van spam.[163] Deze command-and-control-servers bevonden zich in Nederland, zodat de ontmanteling van het botnet door het Team High Tech Crime van het KLPD werd uitgevoerd. Onderdeel van deze ontmantelingsactie was het aftappen van het verkeer van en naar de Bredolab command-and-control-servers. De tapstroom leverde een cruciale sleutel op die de weg vrijmaakte om alle beveiliging en versleuteling op de servers te doorbreken. Eenmaal binnen werden de handelingen van de botnetbestuurder op de servers onderzocht en gemonitord. Op deze manier werd ongeveer gedurende tien weken over de schouder van de verdachte meegekeken. In principe zou het verbreken van het communicatiekanaal tussen de Bredolab-servers en de computers van de slachtoffers vervolgens voldoende zijn geweest om het botnet op te rollen. De high tech crime-unit van het KLPD en het Openbaar Ministerie kozen echter voor een andere aanpak. Het KLPD nam alle command-and-control-servers van binnenuit over en kreeg op deze manier de controle over het botnet in handen. Via dit botnet werd een waarschuwing naar de geïnfecteerde computers van de slachtoffers gezonden, die verscheen als een willekeurige internetpagina die op de computers werd geopend. Op deze manier werden de slachtoffers op de hoogte gesteld van de virusbesmetting door Bredolab en de ontmanteling daarvan.[164]

De Bredolab-ontmanteling is mijns inziens – naast de Rotterdamse uitspraak en de *Tor*-zaak – het definitieve bewijs dat de opsporingsdiensten momenteel al gebruikmaken van hacktechnieken in het opsporingsonderzoek. In de eerste plaats is het KLPD door middel van de afgevangen sleutels op de servers van de verdachte binnengedrongen, waardoor zijn handelingen heimelijk zijn onderzocht. Daarnaast werd de controle over het gehele botnet overgenomen en verwierven de opsporingsdiensten op die manier de volledige toegang tot de geïnfecteerde computers van de slachtoffers, zodat een waarschuwingsbestand kon worden verstuurd.[165] Uiteindelijk werd de hoofdverdachte van het botnet op verzoek van Nederland in Armenië gearresteerd.[166] Duidelijkheid over of het handelen van het KLPD in de Bredolab-ontmanteling juridisch houdbaar is, is er (nog) niet. Zinn, senior advisor bij het Team High Tech Crime van het KLPD, verklaart in BN de Stem in dit kader: ‘Het enige dat ons kan

[161] GOVCERT.NL 2011, p. 6.
[162] Zie beschrijving Bredolab-botnet en ontmanteling op 25 oktober 2010 in ‘Nieuwsuur’, NOS Nederland 2. Dit tv-fragment is te vinden via: http://nieuwsuur.nl/video/193776-de-strijd-tegen-cybercrime.html en Laan 2011.
[163] Koning 2012, p. 46.
[164] Koning 2012, p. 47.
[165] Koning 2012, p. 47.
[166] Koops 2012a, p. 21.

overkomen, is dat de rechter het zo verkregen bewijs niet toelaat in een rechtszaak'.[167] Het woord hierover is dus aan de Nederlandse rechter. Tot op heden heeft die rechter in deze zaak nog geen uitspraak gedaan. Vanwege de arrestatie van de verdachte in Armenië zal rechterlijke toetsing van het optreden van de strafvorderlijke overheid hoogstwaarschijnlijk uitblijven.

2.3 Hacken in Duitsland

In Duitsland heeft men ook enige ervaring op het gebied van hacken door politie en justitie.[168] Men discussieert daar al jaren over de wenselijkheid van een dergelijke vergaande opsporingsmethode.[169] Het voor recherchedoeleinden met behulp van spyware uitlezen van harde schijven op afstand heeft daardoor in ons buurland een hoge vlucht genomen.[170] In 2006 werd in dat kader een wet aangenomen die opsporingsautoriteiten de bevoegdheid gaf computers van verdachten heimelijk en op afstand (via een internetverbinding) te doorzoeken.[171] Om de toegang te verkrijgen tot een computer kon gebruik worden gemaakt van een technologie die het mogelijk maakte om op afstand te infiltreren in computers of netwerken van burgers en bedrijven, zonder dat de gebruiker ervan merkte dat de infiltratie plaatsvond.[172] Enerzijds werden door de Duitse wetgever derhalve maatregelen ontwikkeld die het mogelijk maakten om via een technische weg de inhoud van communicatie die via een computer werd gefaciliteerd te onderzoeken, anderzijds werden maatregelen gecreëerd die infiltratie en doorzoeking konden realiseren.[173] In de officiële documenten spreekt men van *Remote Forensic Software*, maar in de volksmond wordt de heimelijk geïnstalleerde software ook wel *Polizeitrojaner* genoemd of – wanneer het gaat om het gebruik op federaal niveau door het Bundeskriminalamt – hanteert men de term *Bundestrojaner.*[174] Hierop voortbordurend noem ik een dergelijk softwareprogramma in het Nederlandse opsporingsonderzoek een 'Trojaans politiepaard'.

Vijf burgers dienden een klacht in tegen de Duitse wet bij het Bundesverfassungsgericht.[175] Het Bundesverfassungsgericht is de hoogste constitutionele rechter in Duitsland en wordt in dat kader ook wel de 'hoeder van de Grondwet' genoemd. Deze rechter heeft de bevoegdheid om de grondwettelijkheid van normen te beoordelen en ze, wanneer dat nodig blijkt, nietig te verklaren.[176] Naar aanleiding van de klacht van enkele burgers besloot het BVerfG hiertoe ook en achtte de regeling omtrent de Online-Durchsuchung in strijd met de Duitse Grondwet. De wet bevatte onvoldoende procedurele waarborgen om de grondrechten van de betrokkene(n) te beschermen. Een heimelijke infiltratie van een ICT-systeem was naar het oordeel van het Bundesverfassungsgericht alleen

[167] Laan 2011.
[168] De Hert, De Vries & Gutwirth 2009, p. 200.
[169] Oerlemans 2011a, p. 890 e.v.
[170] De Hert, De Vries & Gutwirth 2009, p. 200.
[171] Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006 (GVB1 NW, S. 620).
[172] Buermeyer 2007, p. 158 e.v.
[173] BVerfG 27 februari 2008, 'Online-Durchsuchung', m.nt. W.A.M. Steenbruggen, *Mediaforum* 2008, 5, p. 232.
[174] De Hert, De Vries & Gutwirth 2009, p. 205 e.v.
[175] Groothuis & de Jong 2010, p. 278.
[176] De Hert, De Vries & Gutwirth 2009, p. 201.

toegestaan indien er aanwijzingen waren voor een concreet gevaar voor een belangrijk rechtsgoed, zoals gevaar voor het leven of de vrijheid van een persoon of staatsbelang (bij terroristische misdrijven) en mocht dientengevolge slechts als laatste redmiddel worden ingezet. Ook oordeelde de rechter dat voor infiltratie een rechterlijke machtiging was vereist, evenals een notificatieverplichting.[177]

2.3.1 De ontwikkeling van een nieuw Duits IT-grondrecht

Wat zeer opvallend was aan de uitspraak, was dat het Bundesverfassungsgericht de op dat moment bestaande grondwettelijke bescherming voor de inbreuk onvoldoende vond.[178] De rechter riep daarom een nieuw grondrecht in het leven, althans leidde het af van het *allgemeine Persönlichkeitsrecht*[179], zoals vastgelegd in de Duitse Grondwet.[180] Dit nieuwe IT-grondrecht op *der Vertraulichkeit und Integrität informationstechnischer Systeme*, in het Nederlands de vertrouwelijkheid en integriteit van een persoonlijk informatietechnisch systeem, wordt gezien als de grootste mijlpaal sinds 1983 – toen het Hof ook een nieuw grondrecht (het recht op informationele zelfbeschikking) afleidde uit het algemene persoonlijkheidsrecht. Dit recht vormt derhalve een bruikbaar instrument om gaten in de Duitse Grondwet op te vullen.[181]

Het begrip *informationstechnischer Systeme* is vergelijkbaar met het Nederlandse begrip geautomatiseerd werk voor zover het voor persoonlijk gebruik dient.[182] Het BVerfG noemt in dat kader apparaten waar persoonlijke gegevens op staan, zoals een computer of de luxe mobiele telefoon met persoonlijke gegevens en agenda.[183]

Met de uitspraak over de Online-Durchsuchung heeft de hoogste Duitse constitutionele rechter zich niet principieel uitgesproken tegen het gebruik van ingrijpende en uitgebreide surveillancetechnologie, maar wel aangegeven dat zulke maatregelen proportioneel en constitutioneel verantwoord moeten worden ingezet.[184] Het BVerfG heeft met deze uitspraak een bijzondere stap gezet door een grondrecht te creëren dat past bij de huidige informatiemaatschappij.[185] Naar aanleiding van deze ontwikkelingen in Duitsland kan de vraag worden gesteld of een dergelijk grondrecht op de vertrouwelijkheid en integriteit van ICT-systemen wellicht in Nederland ook zou moeten worden ingevoerd. In ons land heeft het gebruik van informatiesystemen en in het bijzonder van computers immers ook voor de persoonlijke ontwikkeling van het individu een grote betekenis gekregen.[186] Daarbij moet wel worden aangetekend dat de Duitse wijze van het ontwikkelen van een nieuw grondrecht in

---

[177] BVerfG 27 februari 2008, 'Online-Durchsuchung', m.nt. W.A.M. Steenbruggen, *Mediaforum* 2008, 5, p. 228, r.o. 247 e.v.
[178] Oerlemans 2011a, p. 896.
[179] Het allgemeine Persönlichkeitsrecht (algemene persoonlijkheidsrecht) wordt afgeleid uit twee artikelen waarmee het Grundgesetz (Grondwet) begint: art. 1 lid 1 GG (bescherming van de menselijke waardigheid) en art. 2 lid 1 GG (het recht om vrij de eigen persoonlijkheid te kunnen ontplooien; De Hert, De Vries & Gutwirth 2009, p. 202.
[180] Groothuis & De Jong 2010, p. 278.
[181] De Hert, De Vries & Gutwirth 2009, p. 200.
[182] Oerlemans 2011a, p. 897.
[183] BVerfG 27 februari 2008, 'Online-Durchsuchung', m.nt. W.A.M. Steenbruggen, *Mediaforum* 2008, 5, p. 225, r.o. 202.
[184] De Hert, De Vries & Gutwirth 2009, p. 200.
[185] Oerlemans 2011a, p. 897.
[186] Groothuis & De Jong 2010, p. 283.

Nederland niet mogelijk is. Rechterlijke toetsing van wetgeving aan de Grondwet is immers ons land niet toegestaan.

2.4 Conclusie

Binnen politie en justitie en in de politiek wordt al tijden gediscussieerd over het construeren van de mogelijkheid van hacken in de opsporingsfase. In de praktijk is hacken door de politie zelfs al toegepast. Zo heeft de politie met een verkregen inlognaam en wachtwoord op afstand de e-mailinbox van een verdachte bekeken, is de Dienst Nationale Recherche de *Tor*-server binnengedrongen en is het KLPD in de Bredolab-ontmanteling heimelijk binnengedrongen op de servers van de verdachte. Het woord is nu aan de Nederlandse rechter of dergelijk handelen van opsporingsdiensten toelaatbaar kan worden geacht.

Wat hieromtrent in ieder geval vaststaat is dat hacken een bijzonder indringende opsporingsmethode vormt. Enerzijds omdat de computer een bron is van privacygevoelige informatie, anderzijds omdat het hacken heimelijk en op afstand plaatsvindt. Hierdoor kan het inzetten van deze methode tijdens de opsporing als een potentiële inbreuk worden gezien op de persoonlijke levenssfeer van de betrokkene.

Daarnaast moet hacken niet worden beschouwd als één afgebakende opsporingsmethode, maar als een verzameling van verschillende toepassingen. Zo wordt er in de literatuur onderscheid gemaakt tussen de online doorzoeking en het plaatsen van een technische voorziening op een geautomatiseerd werk en voeg ik daar het beïnvloeden van een dergelijk systeem aan toe.

Nederland is binnen Europa niet het enige land dat hackt in het opsporingsonderzoek. In Duitsland heeft men ook enige ervaring op het gebied van hacken door politie en justitie. De hoogste constitutionele rechter in ons buurland heeft in dat kader zelfs een nieuw grondrecht op de vertrouwelijkheid en integriteit van een ICT-systeem gecreëerd. Wellicht dat in Nederland dergelijke wetgeving omtrent hacken ook zou moeten worden ingevoerd. De informatie- en communicatietechnologie heeft in Nederland immers ook een hoge vlucht genomen.

Hoofdstuk 3 Belemmeringen ten aanzien van hacken in het opsporingsonderzoek

In het vorige hoofdstuk is hacken als opsporingsmethode geïntroduceerd. Daarbij is onder meer aangegeven dat de inzet van dit middel ingrijpende gevolgen voor de persoonlijke levenssfeer van betrokkene kan hebben. In dit hoofdstuk zullen niet zozeer deze indringende consequenties op het recht op privacy centraal staan, maar de belemmeringen die voor de opsporingsautoriteiten ontstaan bij het inzetten van hacken in de opsporingsfase. Zo kent de opsporing van cybercrime, aanverwante computercriminaliteit en misdaden met een digitaal karakter een groot jurisdictieprobleem.[187] Dit hangt samen met de grensoverschrijdende aard van het internet. Waar de opsporingsautoriteiten in dit kader tegenaan zouden kunnen lopen en welk beginsel aan de barrières in de opsporingsfase ten grondslag ligt, komt aan bod in paragraaf 3.2. In paragraaf 3.1 zal ik daarnaast enkele praktische belemmeringen noemen, die kunnen ontstaan door een dergelijk complex en breed inzetbaar middel als hacken te hanteren in de opsporingfase. Ten aanzien van deze praktische obstakels zal ik tevens enkele aanbevelingen doen.

3.1 Praktische belemmeringen

Zoals in het vorige hoofdstuk is uiteengezet, kunnen de verschillende vormen van hacken in grofweg drie categorieën worden ingedeeld: de online doorzoeking, het plaatsen van een technische voorziening op een geautomatiseerd werk en het beïnvloeden van een dergelijk werk. Ten aanzien van iedere vorm van hacken kan in de praktijk een aantal belemmeringen ontstaan, die de volgende subparagrafen behandelt.[188]

3.1.1 Complexe ontwikkeling van de gewenste software

Fox noemt als obstakel dat het lastig is software met de benodigde functionaliteiten te ontwerpen die zich in *elk* geautomatiseerd werk kan nestelen.[189] Om een computersysteem te kunnen binnendringen is het – zoals in paragraaf 1.3.1.1 te lezen valt – soms noodzakelijk om bepaalde software (malware) te installeren. Door de computer van de betrokkene te besmetten met een dergelijk programma wordt een toegang verschaft tot deze computer. Vanaf dat moment is het mogelijk om het geautomatiseerde werk te beïnvloeden door bijvoorbeeld de instellingen aan te passen of een microfoon aan te zetten. Tevens kan het geautomatiseerde werk vanaf dat ogenblik online worden doorzocht.

In principe is een dergelijk kwaadaardig softwareprogramma (Trojaans politiepaard) gericht op één bepaald besturingssysteem, zoals *Mac OS X* van *Apple Computer*. Dit hangt samen met het feit dat ieder besturingssysteem een specifiek daartoe behorende programma-firewall heeft.[190] Met betrekking tot *Windows* van *Microsoft* komt daar tevens een kenmerkende virusscanner bij. De verscheidenheid aan systemen met verschillende

[187] Oerlemans 2010, p. 152.
[188] Oerlemans 2011a, p. 892.
[189] Fox 2007, p. 829.
[190] Oerlemans 2011a, p. 892.

beveiligingsmechanismen vormt een belemmering voor de opsporingdiensten bij het binnendringen van computers.

Overigens zijn er aanwijzingen dat de voor het opsporingsonderzoek benodigde software voor het meest gebruikte besturingssysteem, namelijk *Windows* van *Microsoft*, wel voor handen is.[191] Blijkbaar is het dus mogelijk om specifieke hacksoftware voor politie en justitie te ontwikkelen, aldus Oerlemans.[192] Om het hacken van computers met andere besturingssystemen te realiseren, dient er tevens voor deze systemen speciale software te worden ontworpen.

3.1.2 Aantasting van de betrouwbaarheid van het bewijsmateriaal

Een ander gevaar dat schuilt in het gebruik van hacken in de opsporingsfase, is de aantasting van de betrouwbaarheid van het verzamelde bewijs. Het bewijsmateriaal dient daarom niet anders dan met verantwoord digitaal forensisch onderzoek op een geautomatiseerd werk te worden vergaard. Daarbij is het van belang dat de originele gegevens – zoals die zijn aangetroffen op de computer – ter controle kunnen worden vergeleken met de gegevens die als bewijsmateriaal in een zaak worden gepresenteerd.[193] Men kan op deze manier nagaan of er niet met de verzamelde gegevens is geknoeid.

Om mogelijke aantasting van het bewijs te voorkomen, acht ik het van belang dat er expertise en specialisatie op het gebied van cybercrime en de werking en het gebruik van digitale apparaten wordt opgebouwd bij opsporingsinstanties. Op deze manier kan het criminele circuit, dat de laatste jaren steeds vaker gebruikmaakt van de computer en het internet, op dat gebied worden bijgebeend. De Dienst Nationale Recherche, organisatieonderdeel van het KLPD, pleit hieromtrent voor de oprichting van gespecialiseerde cybercrime opsporingsteams.[194] Het Team High Tech Crime, ingesteld in 2007 als afdeling binnen het KLPD, is hier een voorbeeld van.[195] Dit team van jonge cyberrechercheurs is opgericht na klachten uit het bedrijfsleven en het parlement over de amateuristische wijze waarop de regionale politiediensten omgingen met criminele inbraken in bedrijfscomputers.[196] De oprichting van deze gespecialiseerde unit in 2007 lijkt een goede stap in de richting bij de aanpak van cybercrime en overige computer- en internetgerelateerde criminaliteit. Toch wordt ook nu nog steeds gewaarschuwd voor het gebrek aan kennis bij politie en justitie.[197] De opsporingsdiensten zullen zich door de digitalisering van de samenleving moeten blijven aanpassen (met kennis, bevoegdheden en apparatuur) op een andere technologische omgeving. Het een en ander zorgt er tevens voor dat de politie zich zal moeten conformeren aan de verandering van de aard van de criminaliteit. Ook klassieke delicten hebben immers steeds vaker een digitale dimensie.[198]

---

[191] Lake 2011.
[192] Oerlemans 2011a, p. 892.
[193] Oerlemans 2011a, p. 893.
[194] KLPD, Dienst Nationale Recherche 2010, p. 183.
[195] KLPD, Dienst Nationale Recherche 2010, p. 152.
[196] Laan 2011.
[197] Stol, Leukfeldt & Klap 2012, p. 25.
[198] Stol, Leukfeldt & Klap 2012, p. 26 e.v.

Naast de waarschuwing voor het tekort aan kennis bij politie en justitie, heeft men bij het KLPD ook zorgen over het gebrek aan capaciteit. Zinn, senior advisor van het Team High Tech Crime, zegt hierover in de BN de Stem:

> 'Wij kunnen met dertig rechercheurs maar vier grote zaken per jaar draaien. De politiek wil dat dit er twintig worden'.[199]

Niet alleen de kennis bij de opsporingsautoriteiten over internetgerelateerde criminaliteit zal derhalve moeten worden opgeschroefd, maar ook de uitbreiding van capaciteit door de oprichting van (meer) gespecialiseerde cybercrime opsporingsteams zal mijns inziens leiden tot een betere aanpak van deze specifieke vorm van criminaliteit.

Hieraan kan worden toegevoegd dat er in algemene zin meer bewustwording moet komen voor de problematiek en de knelpunten op het gebied van ICT-gerelateerde criminaliteit. Cybercrime is 'booming' en dat dient tot uitdrukking te komen in de erkenning van de hierdoor ontstane complicaties in de opsporing en vervolging van delicten binnen dit rechtsgebied en de (schadelijke) gevolgen voor de computergebruikende samenleving in zijn geheel.

3.1.3 Misbruik van de bevoegdheid tot hacken

Een ander bezwaar dat kan worden opgeworpen tegen het gebruik van hacken in het opsporingsonderzoek heeft betrekking op het feit dat er een risico bestaat dat relatief gemakkelijk misbruik kan worden gemaakt van deze bevoegdheid. Zo kan tijdens de opsporinghandelingen betrekkelijk eenvoudig incriminerend materiaal op de computer van de verdachte worden geplaatst. Het is derhalve van groot belang dat naderhand kan worden nagegaan welke handelingen precies zijn verricht op het geautomatiseerde werk.[200] In dit kader zou men er bijvoorbeeld voor kunnen kiezen om de handelingen van de opsporingsambtenaren op de computer van de betrokkene op te nemen of te monitoren en vast te leggen. Dat kan worden bewerkstelligd door bijvoorbeeld de werkplek van de dienstdoende opsporingsambtenaar onder de tap te zetten of door op gezette tijden scherm- of video-opnames te maken.[201]

Tevens zou ten aanzien van hacken in de opsporingsfase een verbaliseringsplicht moeten gelden, zoals dat ook het geval is in het reguliere opsporingsonderzoek.[202] Dat wil zeggen dat opsporingsambtenaren op grond van de wet verplicht zijn tot het ten spoedigste opmaken van een proces-verbaal van het door hen opgespoorde strafbare feit of van hetgeen door hen tot opsporing is verricht of bevonden.[203] Deze verbaliseringsplicht geldt eveneens ten aanzien van het verrichten van digitale opsporingshandelingen. Ook van heimelijk verrichte handelingen op een computer op afstand – van hacken dus – zal mijns inziens ter controle een proces-verbaal moeten worden gemaakt. Dit wordt bevestigd door Corstens, die stelt dat de verbaliseringplicht geldt, indien er activiteiten worden verricht die zich laten

---

[199] Laan 2011.
[200] Oerlemans 2011a, p. 892.
[201] Interview R. Prins en J.J. Oerlemans op 5 juni 2012 ten burele van Fox-IT te Delft.
[202] Corstens 2011, p. 257.
[203] Zie artikel 152 Sv.

kwalificeren als opsporing.[204] Het monitoren en registreren van de handelingen van de opsporingsambtenaar op het geautomatiseerde werk zal bijdragen aan het vervullen van deze plicht.

3.1.4 Reikwijdte van hacken als opsporingsmethode

Ten slotte vormt de enorme reikwijdte van hacken als opsporingsmethode een mogelijk bezwaar tegen de hantering ervan.[205] Hacken heeft verschillende mogelijke toepassingen, die elk inbreuk maken op verschillende aspecten van de persoonlijke levenssfeer. Dit geldt in het bijzonder voor het beïnvloeden van een geautomatiseerd werk. Zo kan een computer bijvoorbeeld worden in- en uitgeschakeld, kunnen diverse instellingen worden gewijzigd en kan een microfoon op de computer worden aangezet. Het aantal hackmogelijkheden is derhalve zeer groot en de gevolgen van het inzetten van die mogelijkheden zijn daarom lastig te overzien.[206] Ik acht het daarom van belang dat goed wordt ingekaderd wat er op het gebied van digitale opsporing mag en wat er op dit gebied niet mag. Datzelfde geldt met betrekking tot hacken in het opsporingsonderzoek als specifieke bevoegdheid binnen het (generale) digitale opsporingskader.

Tot zover enkele praktische belemmeringen die zich kunnen vormen door hacken in een opsporingsonderzoek toe te passen. Een wellicht nog groter obstakel dat kan ontstaan in de opsporingsfase heeft betrekking op het kenmerkende wijdverbreide karakter van de digitale wereld.

3.2 Grensoverschrijdend karakter van de digitale wereld

De mogelijkheden van het plegen van grensoverschrijdende strafbare feiten hebben de laatste jaren een hoge vlucht genomen als gevolg van de verhoogde mobiliteit van mensen. Dat geldt in het bijzonder binnen de Europese Unie, waar het principe van het vrije verkeer van mensen, goederen en diensten zijn schaduwzijde heeft in het wegvallen van de grenzen voor criminele activiteiten.[207] Ook de ontwikkeling van de computer en het internet hebben geresulteerd in een grensoverschrijdend crimineel milieu.[208] Waar klassieke misdaad, zoals drugscriminaliteit of wapen- en mensensmokkel, nog altijd fysiek van aard is met mensen en objecten die de grens overgaan, speelt cybercriminaliteit zich af in *cyberspace*. Zoals Koops het mooi formuleert: ‘daarbij gaan alleen bits en bytes de grens over’. Internet als locus delicti kent diverse eigenschappen die computergerelateerde criminaliteit tot een specifiek probleem maken: het is wereldwijd, gedeterritorialiseerd, flexibel en snel ontwikkelend.[209]

Doordat internet per definitie grenzeloos is, zijn internetdiensten daardoor in principe overal te bereiken. Gevolg hiervan is dat gegevens op geautomatiseerde werken in beginsel over de hele wereld te benaderen zijn.[210] Ditzelfde geldt voor criminele gegevens of gegevens over crimineel gedrag. Computergerelateerde criminaliteit is derhalve intrinsiek

[204] Corstens 2011, p. 256.
[205] Oerlemans 2011a, p. 893.
[206] Oerlemans 2011a, p. 893.
[207] Beijer e.a. 2004, p. 195.
[208] Prins 2012, p. 49 e.v.
[209] Koops 2012a, p. 9.
[210] Oerlemans 2011a, p. 893.

grensoverschrijdend en kent daardoor minder natuurlijke drempels dan de hierboven aangehaalde klassieke vormen van internationale misdaad.[211] Zo speelt een cyberincident zich zelden enkel af op Nederlands grondgebied. Dader en slachtoffer verblijven vaak wel in ons land, maar de gebruikte server bevindt zich in de meeste gevallen in het buitenland.[212] Het wijdverbreide karakter van cyberdelicten vormt een enorme belemmering in het opsporingsonderzoek naar dergelijke criminaliteit. Gegevens die zich op servers of computers in het buitenland bevinden, zijn in beginsel niet te bereiken, omdat strafvorderlijk optreden op het grondgebied van een vreemde staat niet is toegestaan behoudens gegeven toestemming of verdragsrechtelijke basis.[213] Deze extraterritoriale opsporingsproblematiek kan worden geïllustreerd aan de hand van het veelgebruikte *cloud computing*.

3.2.1 Cloud computing

Een *cloud* is een virtuele omgeving waarop via internet hardware[214], software of gegevens beschikbaar kunnen worden gesteld. Verschillende gebruikers met computers kunnen op aanvraag gebruikmaken van de data en hard- en software die op de server van de externe dienstverlener (cloud) zijn geplaatst. Deze hardware, software en data staan derhalve niet op de computers van de gebruikers zelf, maar op machines in de cloud. Ook is het mogelijk om als gebruiker zelf data in de cloud op te slaan.[215] Via bijvoorbeeld *Dropbox* of *iCloud* kan een gebruiker gegevens vastleggen of bewaren op het web. In het licht van dit onderzoek kan dan bijvoorbeeld worden gedacht aan het opslaan van correspondentie die als zodanig strafbaar is of van bepaalde documenten over criminele activiteiten in de cloud. De opkomst van cloud computing stelt politie en justitie voor een aantal interessante uitdagingen. Het doorzoeken van een computer in het kader van een opsporingsonderzoek levert namelijk in de meeste gevallen niet de gewenste criminele gegevens of correspondentie op. Deze staan namelijk in de cloud.[216] Opsporingsautoriteiten kunnen er dan belang bij hebben deze informatie te bekijken, bijvoorbeeld middels het zetten van een hack. Deze aanpak wordt volgens Prins gecompliceerd, doordat men gegevens kan verspreiden over verschillende clouds waardoor de herkomst van de data moeilijk te herleiden is. Een andere belemmering voor politie en justitie met betrekking tot het gebruik van clouds hangt samen met het al dan niet gebruikmaken van een cloudprovider. Wanneer iemand zijn gegevens via een dergelijke publieke aanbieder op het internet vastlegt in een cloud hebben de opsporingsautoriteiten de mogelijkheid deze data op te vragen bij deze cloudprovider. Steeds vaker wordt echter gebruikgemaakt van particuliere of eigen (anonieme) clouds die voor politie en justitie veel moeilijker te ontdekken en te benaderen zijn.[217] Een ander probleem dat samenhangt met het gebruik van een cloud is dat deze vaak verspreid staat over meerdere landen. Data en informatie worden

[211] Koops 2012a, p. 9.
[212] Prins 2012, p. 46.
[213] Sjöcrona & Orie 2002, p. 81.
[214] Alle fysieke onderdelen van een computer en de randapparatuur die verbonden kan worden met een computer noemt men hardware. Hardware kan op aanvraag via het internet beschikbaar worden gesteld door een cloudprovider. Op deze manier kunnen gebruikers virtueel de beschikking krijgen over onder meer servers, netwerkapparatuur, opslagcapaciteit en werkstations, terwijl deze apparaten eigendom blijven van de cloudprovider; Cuijpers e.a. 2011, p. 6.
[215] Crielaard 2011.
[216] KLPD, Dienst Nationale Recherche 2010, p. 137.
[217] Interview R. Prins en J.J. Oerlemans op 5 juni 2012 ten burele van Fox-IT te Delft.

tijdens het produceren ervan continu opgeslagen in de cloud – en dus niet op de harde schijf van de gebruikte computer – waarbij het heel goed mogelijk is dat verschillende bitjes (bepaalde eenheden van informatie) zich in verschillende landen bevinden.[218] Het grensoverschrijdend hacken van computers die gebruikmaken van een cloud kan dan in de opsporingsfase noodzakelijk worden geacht. Los van de vraag of hacken thans al dan niet een basis in de wet heeft, rijzen er omtrent deze extraterritoriale vorm van hacken enkele problemen.

3.2.2 De Rotterdamse zaak

Het internet zorgt ervoor dat gegevens overal ter wereld kunnen worden opgeslagen. Voor politie en justitie kan dit een enorme belemmering vormen in het opsporingsonderzoek. Ze hebben daarom kenbaar gemaakt hacken ook graag grensoverschrijdend toe te willen passen en zelfs al toe te passen.[219] De vraag is of dat op grond van de huidige wetgeving is geoorloofd. Het een en ander kan worden geïllustreerd aan de hand van de Rotterdamse rechtszaak die eerder al in paragraaf 2.2.1.1 werd behandeld. In deze zaak kwamen – via een informant – de inlognaam en wachtwoord van een e-mailaccount van de verdachte terecht bij de politie. Op deze *Hotmail*-account, welke wordt aangeboden door de Amerikaanse computersoftwareproducent *Microsoft*, kon mogelijk bewijsmateriaal over drugssmokkel worden gevonden. De officier van justitie vorderde dientengevolge de e-mailgegevens van *Microsoft* uit de Verenigde Staten. Dit proces nam enorm veel tijd in beslag, waarop de desbetreffende officier besloot een opsporingsambtenaar te instrueren de e-mailaccount te openen om de inhoud van de berichten op die account na te gaan. Uit die berichten werd vervolgens inderdaad afgeleid dat er een drugsoverdracht zou plaatsvinden in de Rotterdamse haven, zodat de verdachte daar kon worden gearresteerd.[220] In het vorige hoofdstuk werd al aangehaald dat de rechtbank oordeelde dat dergelijk handelen van een opsporingsambtenaar – bestaande uit het inloggen op een e-mailaccount en het kennisnemen van de berichten daarop zonder toestemming van de betrokkene – op grond van onze huidige wetgeving niet geoorloofd is. Voor deze paragraaf is van belang dat de rechter tevens benadrukte dat extraterritoriale toepassing van deze opsporingsmethode, voor zover hacken als bestaande opsporingmethode betiteld mag worden, ook niet toelaatbaar is.[221]

Toch is het uitlezen van berichten op een buitenlandse e-mailaccount onder bepaalde voorwaarden wel geoorloofd.[222] Er dient in dat geval een rechtshulpverzoek te worden gedaan aan de justitiële autoriteiten van het desbetreffende land voor het verkrijgen van die berichten op grond van artikel 126ng lid 2 Sv.[223]

---

[218] Prins 2012, p. 49.
[219] *Kamerstukken II* 2010/11, 25 november 2010, Antwoord op Kamervragen van PvdA Kamerlid Recourt van de minister van Veiligheid en Justitie, kenmerk: 2010Z15331, p. 1.
[220] Rb. Rotterdam 26 maart 2010, *LJN* BM2520.
[221] Rb. Rotterdam 26 maart 2010, *LJN* BM2520.
[222] Oerlemans 2011a, p. 894.
[223] Artikel 126ng lid 2 Sv.

3.2.3 Extraterritoriale toepassing van opsporingsbevoegdheden

De uitspraak van de rechtbank Rotterdam is in overeenstemming met de doctrine van extraterritoriale toepassing van opsporingsbevoegdheden.[224] Aan deze doctrine ligt onder meer het soevereiniteitsbeginsel ten grondslag. Fundamenteel uitgangspunt van dit beginsel is respect voor de soevereiniteit van een andere staat, zodat de ene staat niet zo maar de werking en toepassing van zijn strafbepalingen naar het grondgebied van de andere mag uitbreiden, maar daarvoor toestemming nodig heeft van de bevoegde autoriteiten aldaar.[225] Strafprocessueel gezien brengt dit mee, dat opsporingsambtenaren alleen binnen de grenzen van de staat, die hen heeft aangesteld, tot handelen (in dit geval opsporen) bevoegd zijn, tenzij er sprake is van goedkeuring van de aangezochte staat.[226]

Goedkeuring om opsporingshandelingen in het buitenland te kunnen verrichten, kan ad hoc of bij verdrag worden verkregen en wordt verleend voor bepaalde, omschreven situaties en onder bepaalde voorwaarden.[227] Tevens kan men voor een concreet geval toestemming krijgen door middel van het indienen van een rechtshulpverzoek, waarvan de inwilliging afhangt van de voorwaarden van het toepasselijke rechtshulpverdrag of de nationale wetgeving.[228] Een van Nederland uitgaand rechtshulpverzoek is overigens niet afhankelijk van het bestaan van een verdragsbasis met een aangezochte staat.[229]

Toch heeft ons land een aantal verdragen ondertekend, waarin bepalingen zijn opgenomen die verband houden met het verlenen van wederzijdse rechtshulp.[230] De procedures die voortvloeien uit deze verdragen nemen vaak veel tijd in beslag en zijn niet efficiënt. Daarenboven leiden de verschillen in de nationale wettelijke bepalingen omtrent opsporing tot belemmeringen in de samenwerking.[231] In lijn met de conclusies die zijn getrokken door de Europese Raad in Tampere[232], die betrekking hebben op samenwerking door lidstaten in de vorm van wederzijdse erkenning, heeft de Europese Commissie daarom een voorstel gepresenteerd voor een Kaderbesluit inzake een Europees bewijsverkrijgingsbevel ter verkrijging van voorwerpen, documenten en gegevens voor gebruik in strafprocedures. Een dergelijk Europees bewijsverkrijgingsbevel ziet op het vergaren van bewijs in strafzaken in andere lidstaten en zal bijdragen aan een snellere, meer

---

[224] Oerlemans 2011a, p. 894.
[225] Beijer e.a. 2004, p. 200.
[226] Reijntjes 2012, p. 146.
[227] Zie tevens HR 18 mei 1999, *NJ* 2000, 107.
[228] Beijer e.a. 2004, p. 200.
[229] Beijer e.a. 2004, p. 201.
[230] De voor Nederland belangrijkste verdragen die specifiek handelen over wederzijdse rechtshulp, zijn de volgende multilaterale overeenkomsten: het Europees Rechtshulpverdrag van 1959 (ERV), met Aanvullend Protocol van 1978 (AP/ERV); het Benelux Uitleverings- en Rechtshulpverdrag (BUV); de Schengen-uitvoeringsovereenkomst (SUO), die inmiddels deel uitmaakt van het Unie-recht; het EU rechtshulpverdrag, met protocol. Specifieke verdragen over wederzijdse rechtshulp zijn er overigens ook in bilaterale vorm tussen Nederland en bijvoorbeeld Australië, Canada en Duitsland; Reijntjes, Mos & Sjöcrona 2008, p. 249.
[231] Voorstel voor een kaderbesluit van de Raad betreffende het Europees bewijsverkrijgingsbevel ter verkrijging van voorwerpen, documenten en gegevens voor gebruik in strafprocedures, COM(2003) 688 definitief, p. 4.
[232] In 1999, tijdens de Europese Raad in Tampere onder voorzitterschap van Finland, werd geconcludeerd dat Europa geleid moest worden naar een nieuwe vorm van justitiële samenwerking in de vorm van wederzijdse erkenning. Deze vorm van samenwerking zou eerder de ruimte van vrijheid, veiligheid en rechtvaardigheid realiseren dan de vormen van samenwerking die tot dat moment bestonden. Onder wederzijdse erkenning wordt in dit verband verstaan erkenning van juridische beslissingen die in een lidstaat zijn genomen en worden erkend door de autoriteiten van een andere lidstaat die daar dan ook onmiddellijk, of vrijwel onmiddellijk, uitvoering aan kunnen geven; Reijntjes, Mos & Sjöcrona 2008, p. 295.

doeltreffende justitiële samenwerking in deze zaken.[233] Met het bevel kan zo spoedig mogelijk bewijsmateriaal dat zich in een lidstaat bevindt en dat nodig is in een strafrechtelijke procedure in een andere lidstaat worden verkregen.[234] Bestaande procedures inzake wederzijdse rechtshulp worden met de implementatie[235] van het kaderbesluit in de nationale wetgeving van lidstaten vervangen.[236] Onderlinge bijstand tussen lidstaten wordt daardoor bijna een vanzelfsprekendheid en de mogelijkheid om zich eraan te onttrekken wordt steeds kleiner.[237] Voor nu gelden ten aanzien van het opsporingsonderzoek – behoudens enkele uitzonderingen, zoals de implementatie van het Kaderbesluit inzake tenuitvoerlegging van beslissingen tot bevriezing van voorwerpen of bewijsstukken in artikel 552jj tot en met 552vv Sv – nog steeds de bestaande procedures inzake rechtshulp.[238]

Voordat een verzoek om rechtshulp aan een andere staat kan worden gedaan, moeten eerst de voor de toepassing van een bepaalde opsporingsbevoegdheid in ons land geldende procedures en wettelijke voorschriften zijn gevolgd.[239] Daarbij geldt tevens dat Nederland alleen een aangezochte staat kan verzoeken om een specifieke bijzondere opsporingsbevoegdheid in dat land uit te oefenen, voor zover de uitoefening daarvan ook in ons land is toegestaan.[240] De uitoefening van opsporingshandelingen in andere staten moet derhalve in overeenstemming zijn met ons Wetboek van Strafvordering.[241] Grensoverschrijdend hacken met toestemming van een andere staat kan derhalve slechts plaatsvinden, indien hacken in Nederland een wettelijke basis heeft.

3.2.3.1 Het toestemmingsvereiste

Zonder een verdragsrechtelijke basis of toestemming van de aangezochte staat zijn de mogelijkheden van grensoverschrijdende toepassing van hacken als opsporingsmethode theoretisch gezien beperkt. Oerlemans is in dit kader echter van mening dat het vereiste van toestemming slechts relatief is. Dit hangt volgens hem samen met de aard van het internet. Hij stelt dat door een computer van een verdachte te hacken allerlei gegevens op afstand kunnen worden bekeken en toestemming van de betreffende staat daarom praktisch gezien niet meer noodzakelijk is.[242] De auteur doelt met zijn uitspraak op het feit dat staten pas ‘een probleem’ van de schending van hun soevereiniteit kunnen maken, als ze een strafvorderlijke handeling van een andere staat opmerken. Als Nederlandse opsporingsambtenaren zich op het grondgebied van een andere staat begeven om daar vervolgens een infiltratie- of observatietraject te starten, is de kans op ontdekking door die staat groot. Het heimelijk

[233] Voorstel voor een kaderbesluit van de Raad betreffende het Europees bewijsverkrijgingsbevel ter verkrijging van voorwerpen, documenten en gegevens voor gebruik in strafprocedures, COM(2003) 688 definitief, p. 2.
[234] Reijntjes, Mos & Sjöcrona 2008, p. 297.
[235] Het voorstel betreffende de implementatie is op 12 juni 2012 aangenomen door de Tweede Kamer. Het voorbereidend onderzoek door de Eerste Kamercommissie voor Veiligheid en Justitie zal in dit kader plaatsvinden op 11 september 2012; http://www.eerstekamer.nl/wetsvoorstel/32717_implementatie_kaderbesluit.
[236] Voorstel voor een kaderbesluit van de Raad betreffende het Europees bewijsverkrijgingsbevel ter verkrijging van voorwerpen, documenten en gegevens voor gebruik in strafprocedures, COM(2003) 688 definitief, p. 5.
[237] Reijntjes 2012, p. 150.
[238] Voorstel voor een kaderbesluit van de Raad betreffende het Europees bewijsverkrijgingsbevel ter verkrijging van voorwerpen, documenten en gegevens voor gebruik in strafprocedures, COM(2003) 688 definitief, p. 4.
[239] Aanwijzing opsporingsbevoegdheden 2012, § 4.3.
[240] Beijer e.a. 2004, p. 201.
[241] Baaijens-van Geloven 2001, p. 367 e.v.
[242] Oerlemans 2011a, p. 895.

inzetten van hacken als opsporingsmethode zal – vanwege dit geheime karakter en vanwege het feit dat de activiteiten vanuit ons land kunnen worden ontplooid – daarentegen voor de andere staat lastiger te ontdekken zijn. Het toestemmingsvereiste is in het geval van hacken derhalve van relatieve aard. Staten kunnen immers geen toestemming geven voor opsporingsactiviteiten van een ander land op hun grondgebied, als ze daar geen weet van hebben. Dit neemt niet weg dat de soevereiniteit van de andere staat wel degelijk wordt geschonden, als geautomatiseerde werken op het territorium van die staat door ons land op afstand worden binnengedrongen zonder toestemming of verdragsrechtelijke basis. Er vindt immers Nederlands opsporingsonderzoek plaats op het grondgebied van een andere staat, ook al is het fysiek betreden van andermans territorium niet noodzakelijk.[243]

Grensoverschrijdend hacken is mijns inziens ook om een andere reden nauwelijks toegestaan. Die reden hangt samen met de betwiste grondslag van deze methode in de wet. Hiervoor kwam reeds naar voren dat een specifieke bijzondere opsporingsbevoegdheid in het buitenland slechts mag worden uitgeoefend, indien dat in Nederland ook is toegestaan. Tot op heden is echter (nog) niet duidelijk of hacken in een opsporingsonderzoek is geoorloofd. Wat hieromtrent in ieder geval vaststaat, is dat een *expliciete* wettelijke basis voor hacken in de opsporingsfase in ons land ontbreekt. Wellicht dat een bevoegdheid tot hacken kan worden afgeleid van bestaande wettelijk verankerde bijzondere opsporingsmethoden. Wanneer het op afstand binnendringen van computers op grond van een andere opsporingsmethode mogelijk wordt geacht, kan het – met toestemming of met een verdragsrechtelijke basis – misschien ook grensoverschrijdend plaatsvinden.

3.2.4 Grensoverschrijdend hacken

Zoals ook uit de uitspraak van de Rotterdamse rechter volgt, is strafvorderlijk optreden op het grondgebied van een vreemde staat ook niet toegestaan voor opsporingsmethoden met een digitaal karakter.[244] Dat wil zeggen dat Nederlandse opsporingsambtenaren op computernetwerken slechts onderzoek mogen doen voor zover de Nederlandse rechtsmacht reikt. De politie mag dus geen onderzoek doen wanneer de betrokken computers zich buiten Nederland bevinden of wanneer er zodanige aanwijzingen zijn dat er een gerede kans is dat dit het geval is.[245] Hiermee wordt overigens niet gedoeld op de specifieke opsporingsmethode hacken, maar op de virtuele opsporingsmethoden die op dit moment wel een expliciete basis in de wet hebben. Mocht hacken ook toegestaan zijn op grond van onze huidige wet of mocht deze opsporingsmethode in de toekomst een duidelijke wettelijke grondslag krijgen, dan is de

[243] Naar analogie met het arrest van de Hoge Raad, het *Azewijnse paard*, waar wordt bepaald dat men zeer goed in een andere staat verblijvend in Nederland een misdrijf kan plegen. Men kan door middel van een instrument handelen op een andere plaats dan waar men zich op dat moment bevindt. Niet de plaats waar de dader zich bevindt, maar de plaats van het delict is derhalve bepalend; HR 6 april 1915, *NJ* 1915, 427. Deze uitspraak is mijns inziens nog steeds actueel. Met betrekking tot het onderwerp van dit onderzoek wil ik hem echter omdraaien en van toepassing verklaren op het opsporingsonderzoek. Niet de plaats vanuit waar de politie hackt (Nederland) is relevant, maar de locatie van de computer die wordt binnengedrongen (in een andere staat).

[244] Kaspersen 2007, p. 166.

[245] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 36. De locatie van computers kan via het internet worden bepaald met een IP-adres. Met een dergelijk adres kan in beginsel op de wijk of straat nauwkeurig worden geconstateerd waar het geautomatiseerde werk zich bevindt, dus ook of de computer zich in het buitenland bevindt of niet. Men noemt het bepalen van de werkelijke geografische locatie van de computer de wetenschap van geolocatie. Door anonimiseringstechnieken kan het IP-adres echter op een zodanige manier worden verborgen of veranderd, dat de locatie van de computer niet of nauwelijks te bepalen is; Oerlemans 2011a, p. 904.

doctrine van extraterritoriale toepassing van opsporingsmethoden hierop ook van toepassing. Het wordt voor opsporingsambtenaren dan zeer moeilijk om criminele gegevens of gegevens over criminaliteit door middel van het zetten van een hack te bemachtigen. Gegevens worden tegenwoordig immers overal ter wereld verspreid en opgeslagen en zijn niet louter verbonden aan de computer waarop ze zijn geproduceerd. De opsporingsautoriteiten zien zich hierdoor genoodzaakt ook computers of servers te onderzoeken die zich bevinden in het buitenland. In het voorgaande is echter uiteengezet dat grensoverschrijdende uitoefening van opsporingshandelingen slechts is toegestaan, indien er een verdragsrechtelijke basis voor is of indien er rechtshulp is toegekend. Zoals uit de Rotterdamse zaak blijkt, kosten rechtshulpverzoeken over het algemeen veel tijd en is bij sommige zaken veel haast geboden. Dit komt door de vluchtigheid van de gegevens: criminelen wisselen geregeld van infrastructuur, waarbij alle opgeslagen data van de vorige server worden gewist. Bovendien kan bij een rechtshulpverzoek slechts die informatie worden verstrekt waar de verzoekende partij om vraagt. Als meer informatie voorhanden is, kan deze niet automatisch worden meegeleverd.[246] Om die informatie toch te kunnen benaderen, is het daarom verleidelijk voor politie en justitie hacken grensoverschrijdend toe te passen.[247] Zonder rechtshulp of verdrag zijn dergelijke activiteiten echter niet toelaatbaar. Indien de betrokken verdachte door deze wijze van handelen in zijn belangen wordt geschaad, zal waarschijnlijk strafvermindering of mogelijk zelfs uitsluiting van het langs deze weg verkregen materiaal als bewijs volgen.[248] Wanneer niet duidelijk is waar de computer zich bevindt, in Nederland of in het buitenland, en de gegevens bovendien te goeder trouw zijn vergaard, dan mogen ze wel als bewijsmateriaal worden gebezigd.[249]

Naast mogelijke strafvermindering of bewijsuitsluiting zal Nederland ook rekening moeten houden met het ontstaan van politieke spanningen naar aanleiding van de inbreuk op de soevereiniteit van het betrokken land. Bovendien ontwikkelt na grensoverschrijdende toepassing van hacken door Nederland zich het risico dat andere landen hetzelfde op geautomatiseerde werken in ons land zullen doen.[250]

3.3 Conclusie

In de praktijk wordt hacken als opsporingsmethode al incidenteel toegepast. Dit terwijl een expliciete wettelijke bevoegdheid op dit moment ontbreekt. Hieruit kan worden afgeleid dat de (introductie van een) mogelijkheid van hacken in het opsporingsonderzoek door de opsporingsautoriteiten wel wordt gewenst. Opsporingactiviteiten zijn in beginsel enkel toelaatbaar binnen de grenzen van een land. Met andere woorden, strafvorderlijk optreden op het grondgebied van een vreemde staat is niet toegestaan, tenzij deze staat toestemming geeft voor dergelijk handelen of er sprake is van een verdragsrechtelijke basis. Dat wil zeggen dat Nederlandse opsporingsambtenaren slechts onderzoek mogen doen op computers en servers voor zover de Nederlandse rechtsmacht reikt. Criminele gegevens of strafbare communicatie

[246] KLPD, Dienst Nationale Recherche 2010, p. 166.
[247] Oerlemans 2011a, p. 895.
[248] Zie *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 36 en *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 23.
[249] Oerlemans 2011a, p. 895 e.v. met verwijzing naar *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 23.
[250] Wiemans 2004, p. 157.

als zodanig op buitenlandse informatiesystemen zijn daardoor in principe onbereikbaar. Vanwege de grenzeloze aard van het internet worden nu juist deze gegevens overal ter wereld verspreid en opgeslagen en zijn ze derhalve vaak niet verbonden aan de computer waarop ze zijn geproduceerd. Deze grensoverschrijdende verspreiding van gegevens zorgt voor complicaties in het opsporingsonderzoek.

Politie en justitie dienen daarnaast te waken voor het gevaar van misbruik van de bevoegdheid tot hacken. Tevens kan de enorme reikwijdte van deze methode voor problemen zorgen. Juridische inkadering van de digitale bevoegdheden acht ik onder meer met het oog op de rechten en vrijheden van degenen die betrokken zijn in het opsporingsonderzoek in dit kader dan ook zeer noodzakelijk. Tevens ben ik van mening dat bij opsporingsautoriteiten de benodigde expertise en specialisatie dient te worden opgebouwd om mogelijke aantasting van de betrouwbaarheid van het bewijsmateriaal te voorkomen. Daarbij zal ook de capaciteit van opsporingsteams gespecialiseerd in cybercrime uitgebreid dienen te worden.

Hoofdstuk 4 Hacken en het recht op privacy

In het vorige hoofdstuk is uiteengezet dat de grensoverschrijdende aard van de digitale wereld zorgt voor grote belemmeringen in het (digitale) opsporingsonderzoek. Tevens kleven er enkele praktische obstakels aan de opsporingsmethode hacken. Het sterkste argument tegen de uitvoering van hacken in het opsporingsonderzoek hangt echter samen met de beschermwaardigheid van het recht op een privéleven. In dit hoofdstuk zal dat recht dan ook centraal staan. Daarbij zal ik verantwoorden hoe ICT-systemen en privacy zich tot elkaar verhouden (§ 4.1) en of dergelijke systemen kunnen worden gekwalificeerd als een te respecteren dimensie van de persoonlijke levenssfeer (§ 4.3). Tevens besteed paragraaf 4.1.1 aandacht aan de inhoud van het recht op een privéleven uit artikel 10 Grondwet en artikel 8 EVRM. Daarbij rijst in het kader van dit onderzoek de vraag of een verdachte in een opsporingsonderzoek wel een recht op privacy toekomt (§ 4.2). Vervolgens beoordeelt paragraaf 4.4 of hacken kan resulteren in een inbreuk op het privéleven. Het recht op privacy is geen absoluut recht. In paragraaf 4.5 zal ik behandelen op grond waarvan een inbreuk op artikel 8 EVRM is gepermitteerd.

4.1 ICT-systemen en het recht op privacy

De integriteit en vertrouwelijkheid van computersystemen is heden ten dage een essentiële voorwaarde voor het persoonlijk en maatschappelijk functioneren van burgers.[251] Deze vaststelling geldt natuurlijk ook met betrekking tot de ‘criminele burger’. Het gebruik van informatietechnologie, en dan in het bijzonder personal computers en smartphones, heeft voor de persoonlijke ontwikkeling van individuen een belangrijke betekenis gekregen.[252] Tegenwoordig *kan* – zoals men het pleegt uit te drukken – niemand meer zonder mobiele telefoon, internet of computer. Dit resulteert in het feit dat naast de gegevens, zakelijk of privé, die een individu normaal gesproken vastlegt op zijn computer of smartphone, nu ook gegevens te vinden zijn over onder meer zijn gedrag, bezoek aan websites, tijdstippen waarop en locaties waar vanuit wordt gehandeld en de maatschappelijke context waarbinnen hij door middel van zijn computer optreedt.[253] Tevens worden ‘fysieke’ activiteiten steeds vaker verplaatst naar het internet. Zo wordt het internet meer en meer gebruikt als alternatief voor ‘lijfelijk’ winkelen en bankieren.[254] Het op afstand en zonder medeweten van de betrokkene binnendringen op en ingrijpen in computersystemen en dergelijke in het kader van een opsporingsonderzoek kan voor het persoonlijke leven van de betrokken burger hierdoor ingrijpende gevolgen hebben.[255] Dat geldt in het bijzonder voor zijn privacy. Na toegang tot een ICT-systeem maakt de techniek immers alles mogelijk. De inbreuk op het privéleven is potentieel zeer groot.[256]

[251] Groothuis & De Jong 2010, p. 282.
[252] Groothuis & De Jong 2010, p. 282.
[253] Groothuis & De Jong 2010, p. 282.
[254] GOVCERT.NL 2010, p. 13.
[255] Groothuis & De Jong 2010, p. 282.
[256] Koning 2012, p. 46.

4.1.1 Bescherming van het recht op privacy

Op grond van artikel 10 Grondwet en artikel 8 EVRM heeft iedereen recht op eerbiediging van zijn of haar persoonlijke levenssfeer of privacy.[257] De persoonlijke levenssfeer omvat tal van terreinen, welke zeer uitlopend van aard zijn en waarvan sommige volop in ontwikkeling zijn.[258] Sommige van deze deelterreinen genieten zelfstandige verdragsrechtelijke of grondwettelijke bescherming.[259]

Uitgangspunt van beide bepalingen is dat de overheid uitsluitend beperkingen kan stellen aan de persoonlijke levenssfeer in gevallen die bij of krachtens de wet zijn bepaald.[260] Het gaat derhalve om het recht een eigen leven te leiden met zo weinig mogelijk inmenging van buitenaf. Korter geformuleerd, het recht om met rust te worden gelaten.[261]

De memorie van toelichting bij artikel 10 Grondwet omschrijft de persoonlijke levenssfeer als de reeks situaties waarin de mens onbevangen zichzelf wil zijn.[262] Een voorbeeld van wat onder die privacy valt, kan met betrekking tot dit onderzoek van belang worden geacht. De memorie van toelichting noemt in dat kader namelijk bepaalde vormen van communicatie, zoals een telefoongesprek of briefwisseling, welke tot de privésfeer kunnen worden gerekend.[263] Vertaald naar deze tijd zou deze vaststelling mijns inziens tevens moeten gelden voor e-mail, fax- en chatverkeer. In dat kader kan bijvoorbeeld worden gedacht aan correspondentie via het VoIP-programma[264] *Skype* of via de op mobiele telefonie gerichte berichtenapplicatie *WhatsApp*. Wat hieromtrent in ieder geval vaststaat, is dat de inhoud van het grondrecht toegespitst op de eenentwintigste eeuw voornamelijk in de wetgeving en rechtspraak zijn nadere omlijning zal moeten vinden.[265]

Zowel in de Nederlandse Grondwet als op Europees niveau wordt het privéleven van onderdanen beschermwaardig geacht. De Hoge Raad heeft in dat kader bepaald dat de inhoud van de privacyregelgeving in Nederland onder meer dient te worden bepaald door artikel 8 EVRM en derhalve dient aan te sluiten bij de ontwikkelingen over de grens.[266] Mede als gevolg van deze uitspraak staat artikel 8 EVRM in de komende analyse centraal.

4.1.1.1 Het recht op privacy ex artikel 8 EVRM

Het EHRM heeft nooit getracht een definitie van privacy te geven.[267] Het Hof stelde zelfs dat het onmogelijk en onnodig was en is om een uitputtende definitie van het begrip privacy te

---

[257] Zie artikel 10 Grondwet en artikel 8 EVRM.
[258] *Kamerstukken II* 1975/76, 13 872, nr. 3, p. 40.
[259] Zie bijvoorbeeld het recht op bescherming van persoonsgegevens in artikel 8 Handvest van de grondrechten van de Europese Unie en het recht op eerbiediging van de communicatie via brief, telefoon en telegraaf in artikel 13 Grondwet. Daarbij dient met betrekking tot dit onderzoek opgemerkt te worden dat digitale communicatie, zoals chat en e-mailverkeer, niet wordt beschermd door artikel 13 Grondwet; Ministerie van Veiligheid en Justitie 2011, p. 8.
[260] Ministerie van Veiligheid en Justitie 2011, p. 8.
[261] Burkens e.a. 2006, p. 128.
[262] *Kamerstukken II* 1967/68, 9 419, nr. 3, p. 3.
[263] *Kamerstukken II* 1975/76, 13 872, nr. 3, p. 40.
[264] VoIP- (Voice-over-Internet-Protocol) verkeer is telefoonverkeer via een internetverbinding. Het via internet voeren van een (vertrouwelijk) telefoongesprek wordt vaak met behulp van het programma *Skype* gedaan; Van Tuil 2012.
[265] Knigge & Kwakman 2001, p. 161
[266] HR 9 januari 1987, *NJ* 1987, 928.
[267] Blom 2001, p. 142.

geven.[268] Toch kan aan de hand van enkele uitspraken van het EHRM een aantal punten worden geformuleerd, die bescherming genieten onder artikel 8 EVRM. Zo omvat het recht op een privéleven in ieder geval het recht op een eigen identiteit, lichamelijke en geestelijke integriteit en bescherming tegen vergaring en gebruik van informatie.[269]

Het Europese rechtscollege achtte het daarnaast van belang om naar aanleiding van een aantal aan hem voorgelegde zaken enkele criteria te formuleren voor de beantwoording van de vraag of in concreto al dan niet sprake was van een schending van het recht op privacy.[270] Of sprake was van een dergelijke inbreuk, diende vervolgens van geval tot geval te worden bepaald.

Het recht op privacy heeft in ieder geval betrekking op het streven van een individu om zijn leven in vrijheid naar zijn zin in te richten en om in dit (persoonlijk) leven gevrijwaard te blijven van ongewenste inmenging, vooral van de kant van de overheid.[271] Voor de overheid is daarbij naast deze negatieve verplichting ook een positieve verantwoordelijkheid neergelegd. Met betrekking tot de opsporingsfase houdt de negatieve verplichting in dat opsporingsambtenaren aan de ene kant bepaalde handelingen achterwege dienen te laten om de privésfeer van burgers te respecten en aan de andere kant heeft de positieve verantwoordelijkheid tot gevolg dat de overheid het diezelfde burgers dient mogelijk te maken van het recht op privacy te kunnen genieten.[272] Daarbij verliest een individu zijn beschermwaardigheid onder het EVRM niet (meteen), als hij zichzelf of zijn eigendommen in een meer publieke omgeving brengt.[273] Hieruit kan mijns inziens de conclusie worden getrokken dat iemand zijn recht op privacy ook niet direct verliest, als degene zich begeeft op het openbare en publieke internet om op die manier bijvoorbeeld persoonlijke gegevens te verspreiden of op te slaan.

4.2 De verdachte en zijn recht op privacy

Nu het recht op privacy in algemene zin kort is geïntroduceerd, rijst de vraag of dit recht kan worden beïnvloed door het feit of een verdachte rekening moet houden met politiële of justitiële belangstelling voor zijn persoon. Het gaat hier in dit onderzoek immers om het recht op privacy in relatie tot hacken in het opsporingsonderzoek naar een verdachte. Komt een verdachte in dit verband wel een recht op privacy toe? Geniet het belang van een verdacht persoon bij niet-schending van zijn persoonlijke levenssfeer rechtens wel bescherming?[274]

In een uitspraak van de Hoge Raad werd deze vraag negatief beantwoord. In deze zaak werden in het kader van een gerechtelijk vooronderzoek diverse telefoongesprekken afgeluisterd, waarin de verdachte sprak met andere personen die al werden verdacht van grootschalige heroïnehandel over leveranties van drugs en betaling daarvan. De verdachte in deze zaak hield zijn telefoongesprekken niet via de aansluiting in zijn woning, maar hij gebruikte openbare telefoontoestellen. Het Arnhemse Hof had eerder in deze zaak geoordeeld

[268] EHRM 16 december 1992, nr. 13710/88, § 29 (*Niemietz/Duitsland*).
[269] Blom 2001, p. 142.
[270] Knigge & Kwakman 2001, p. 155.
[271] Blom 2001, p. 142.
[272] Blom 2001, p. 142.
[273] EHRM 28 januari 2003, nr. 44647/98 (*Peck/Verenigd Koninkrijk*).
[274] Corstens 1995, p. 546.

dat de verdachte er op bedacht had moeten zijn dat de politie bijzondere belangstelling voor hem zou kunnen hebben, omdat hij veelvuldig gebruikmaakte van deze openbare telefoons en niet van zijn persoonlijke verbinding. Het zou een feit van algemene bekendheid zijn dat betrokkenen bij heroïnehandel een sterke voorkeur hebben om bij hun communicatie met leveranciers het openbare telecommunicatienetwerk te benutten om afluisteren door de justitiële autoriteiten zoveel mogelijk te voorkomen. De Hoge Raad liet dit oordeel van het Hof in Arnhem in stand.[275] De verdachte had er in deze omstandigheden rekening mee moeten houden dat de politie opsporingsactiviteiten tegen hem zou kunnen ontplooien, hij kan daardoor geen redelijke verwachting meer hebben dat de politie hem ongemoeid laat en hij kan dus achteraf geen recht op bescherming meer inroepen. Dat recht heeft hij door zich zo (openlijk) strafbaar te gedragen zelf opgegeven. Dit oordeel van Nederlands hoogste rechter kan worden geplaatst in een rijtje arresten waarin het recht op bescherming van de persoonlijke levenssfeer werd beperkt tot de redelijke verwachting daarop in de gegeven omstandigheden.[276] Deze benadering wordt ook de *reasonable expectation of privacy*-doctrine genoemd.[277]

4.2.1 Reasonable expectation of privacy-doctrine

In een uitspraak van het EHRM komt deze problematiek ook uitvoerig aan bod, maar zonder het begrip *reasonable expectation* uitdrukkelijk te hanteren. In deze zaak werd het optreden van een pseudokoper niet in strijd geacht met artikel 8 EVRM, omdat de dader van het drugsdelict wel *had* moeten weten dat hij het risico kon lopen een undercoveragent tegen te komen.[278] Een inbreuk op de privacy van iemand is volgens het Hof blijkbaar afhankelijk van het bewustzijn dat degene heeft dat hij bezig is een strafbaar feit te plegen. De vraag of er sprake is van een inbreuk op privacy wordt derhalve afhankelijk gesteld van de 'redelijke verwachting' van de betrokkene.[279]

Met de *Halford*-zaak wordt de reasonable expectation of privacy-doctrine vervolgens voor het eerst opgenomen in het dictum.[280] Deze uitspraak is verstrekkend. Centraal staat de vraag of een betrokkene er in bepaalde omstandigheden op mag vertrouwen dat zijn gesprekken niet worden afgeluisterd.[281] Uit de doctrine vloeit voort dat iemand die zich met criminele activiteiten bezighoudt, er rekening mee dient te houden dat bijvoorbeeld zijn telefoon kan worden afgeluisterd.[282] Het is mogelijk dat het afvangen van die telefoongesprekken door de opsporingsinstanties dan vervolgens niet zal worden gezien als een inbreuk op de privacy van die personen, doordat de verdachten de redelijke verwachting hadden moeten hebben dat dergelijk onderzoek kon plaatsvinden.[283]

---

[275] HR 18 mei 1999, *NJ* 2000, 104.
[276] Blom 2001, p. 145.
[277] Oerlemans 2011a, p. 897.
[278] EHRM 15 juni 1992, nr. 12433/86 (*Lüdi/Zwitserland*).
[279] Blom 2001, p. 146.
[280] EHRM 25 maart 1997, nr. 44787/98 (*Halford/Verenigd Koninkrijk*).
[281] Als deze vraag over de aanwezigheid van de redelijke verwachting bij de betrokkene is beantwoord, komt pas de vraag aan de orde wie heeft afgeluisterd en of daar op dat moment een wettelijke bevoegdheid voor was; Blom 2001, p. 147.
[282] Corstens 1995, p. 547.
[283] Lensing 1994, p. 1016.

Met betrekking tot het hacken van criminele computers zou langs dezelfde weg kunnen worden geredeneerd. Zo zou bijvoorbeeld een verdachte die gebruikmaakt van een server, die voornamelijk wordt ingezet voor illegale activiteiten, geen reasonable expectation of privacy meer hebben. Het binnendringen op een geautomatiseerd werk door de politie zou dan zelfs kunnen worden gerechtvaardigd met een beroep op de algemene opsporingsbevoegdheid uit artikel 2 Politiewet 1993 en artikel 141 Sv, aldus Oerlemans.[284]

4.2.2 Relativering reasonable expectation of privacy-doctrine

Uit de hierboven aangehaalde uitspraak van het Europese Hof in de zaak *Lüdi* kan worden afgeleid dat het recht op privacy niet kan worden ingeroepen door degene die een strafbaar feit aan het voorbereiden dan wel aan het plegen is. De verdachte moet er dan immers van uitgaan dat de politie bepaalde opsporingsmethoden tegen hem inzet, waardoor hij zich achteraf niet meer kan beroepen op de bescherming van zijn privéleven, omdat hij zelf (door zijn handelen) dit recht op het spel heeft gezet.[285] Zo ver gaat men in Nederland niet. In ons land wordt ervan uitgegaan dat degene die strafbare feiten pleegt of voorbereidt zijn recht op privacy behoudt. Het een en ander heeft wel gevolgen voor de omvang van dit recht en de juridische consequenties die een inbreuk op het recht op een privéleven moet hebben.[286] In de hierboven behandelde uitspraak oordeelde het Arnhemse Hof, dat er ten aanzien van de observaties sprake was van een niet-noemenswaardige inbreuk op de privacy van de verdachte, waarvoor artikel 2 Politiewet 1993 – de algemene taakstelling voor opsporingshandelingen in combinatie met artikel 141 en 142 Sv – een voldoende wettelijke basis bood, omdat de verdachte zich bezighield met de handel in heroïne.[287]

Overigens lijkt men ook op Europees niveau enigszins te zijn teruggekomen op de uitspraken in *Lüdi* en *Halford*. Zo heeft het EHRM in *A.* en in *Peck* geoordeeld dat ondanks dat er strafbare feiten waren gepleegd in deze zaken, er toch sprake was van een schending van het privacyrecht en dat de overheid de bescherming van dit recht had moeten waarborgen.[288]

De kentering in Europa is een goede zaak. De reasonable expectation of privacy-doctrine als beperking van het recht op een privéleven is niet noodzakelijk en bovendien ongewenst. Men gaat er in deze benadering van uit dat grond- en mensenrechten niet voor iedere burger gelden. De overheid zou alleen de rechten van ‘brave’ burgers dienen te respecteren. Dit uitgangspunt is verkeerd. Grond- en mensenrechten zijn in beginsel geschreven om de overheid te verbieden de vrijheidssfeer van de burger binnen te treden.[289] Hierop kan onder (strenge) voorwaarden een uitzondering worden gemaakt. Daar is lid 2 van artikel 8 EVRM een voorbeeld van. Ook artikel 10 Grondwet kan in bepaalde gevallen worden begrensd. Beide artikelen hoeven daarom niet ook nog eens te worden beperkt door de redelijke verwachting (reasonable expectation). In artikel 10 Grondwet en 8 EVRM zelf wordt immers aangegeven op welke gronden het recht op privacy mag worden beknot.

---

[284] Oerlemans 2011a, p. 898.
[285] Blom 2001, p. 152.
[286] Blom 2001, p. 152 e.v.
[287] HR 18 mei 1999, *NJ* 2000, 104.
[288] EHRM 23 november 1993, nr. 14838/89, § 34 (*A./Frankrijk*) en EHRM 28 januari 2003, nr. 44647/98 (*Peck/Verenigd Koninkrijk*).
[289] Vande Lanotte & Haeck 2005, p. 3.

4.3 ICT-systemen als onderdeel van het recht op privacy

In het voorgaande is vastgesteld dat de computer heden ten dage een grote rol speelt in het persoonlijke leven van zijn gebruiker. Veel privacygevoelige gegevens worden erin opgeslagen of verspreid. Het in het kader van een opsporingsonderzoek binnendringen van een computer verschaft de toegang tot deze soms zeer persoonlijke gegevens. Hierdoor rijst de vraag of dergelijke ICT-systemen bescherming genieten onder de huidige privacywetgeving.

Het EHRM heeft de personal computer in ieder geval (nog) niet expliciet gekwalificeerd als een te respecteren dimensie van de persoonlijke levenssfeer. Ook de verdragstekst van het EVRM rept met geen woorden over het vertrouwelijke karakter van een dergelijk systeem.[290] Duitsland heeft in dit kader wel een recht in het leven geroepen dat de integriteit en vertrouwelijkheid van een geautomatiseerd werk beschermd. Ons buurland heeft een belangrijke stap gezet door een grondrecht te creëren dat past bij onze huidige gedigitaliseerde maatschappij en gaat daarmee op dit punt aanzienlijk verder dan het EHRM.

Dat het EHRM niet expliciet heeft aangegeven dat de computer onder de beschermingsomvang van het EVRM valt, betekent niet dat er in de Europese jurisprudentie geen aanknopingspunten zijn te vinden voor de bescherming van de vertrouwelijkheid en integriteit van computersystemen. Zo bepaalde het Hof in verschillende zaken dat de noodzaak tot het treffen van passende beschermingsmaatregelen in het recht van lidstaten des te groter is wanneer bepaalde privacygevoelige gegevens langs de geautomatiseerde weg worden verwerkt. De volgende rechtsoverweging komt in al die uitspraken voor:

> 'The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes.'[291]

Ditzelfde uitgangspunt werd in een andere zaak, de *Liberty*-uitspraak, van het Europese rechtscollege bevestigd. Het EHRM oordeelde in dit kader over de praktijk van *strategic monitoring*.[292] Hier wordt het met behulp van satellietschotels en andere ICT-toepassingen systematisch onderscheppen en monitoren van telecommunicatieverkeer onder verstaan.[293] Het Hof bepaalde dat het, in de context van het onderscheppen en afluisteren van communicatie, van groot belang is dat er duidelijke en gedetailleerde wetgeving is, vooral omdat de beschikbare technologie voor het gebruik van het onderschepte berichtenverkeer steeds geavanceerder wordt.

Uit deze Straatsburgse jurisprudentie komt het beeld naar voren van overheden die vergaande en steeds toenemende technische mogelijkheden hebben om inbreuk te maken op

---

[290] Groothuis & De Jong 2010, p. 280.
[291] EHRM 4 december 2008, nr. 30562/04, § 103 (*S. en Marper/Verenigd Koninkrijk*), EHRM 17 december 2009, nr. 5335/06, § 61 (*Bouchacourt/Frankrijk*), EHRM 17 december 2009, nr. 16428/05, § 62 (*Gardel/Frankrijk*) en EHRM 17 december 2009, nr. 22115/06, § 53 (*M.B./Frankrijk*).
[292] EHRM 1 juli 2008, nr. 58243/00 (*Liberty e.a./Verenigd Koninkrijk*).
[293] Groothuis & De Jong 2010, p. 280 e.v.

de integriteit van door burgers gebruikte ICT-systemen.[294] Het Hof eist in de uitspraken waarborgen van die overheden om de burgers tegen deze inbreuken te beschermen. In die zin vormen de uitspraken een stap in de richting van de erkenning van de beschermwaardigheid van (gegevens op) geautomatiseerde werken. Twee waarborgen worden in het kader van de bescherming van individuen cruciaal geacht: doelbinding, het bepalen dat met opsporingsbevoegdheden vergaarde informatie alleen voor strafvordering kan worden gebruikt, en controle, het vormgeven van adequaat toezicht op de uitoefening van bevoegdheden. Alleen met expliciete en effectieve rechtswaarborgen kan de toenemende macht van de overheid ten opzichte van de burger in goede banen worden geleid, aldus Koops & Prinsen.[295]

Dat het Europese Hof informatiesystemen nog niet expliciet onder de beschermingsomvang van het EVRM heeft gebracht, is mijns inziens geen goede zaak. Het EHRM schiet op dit gebied dan ook tekort. De rol die ICT-systemen, zoals smartphones en computers, op dit moment vervullen en het gebruik ervan voor de persoonlijke ontwikkeling maken het goed verdedigbaar dat deze systemen onder de beschermingsomvang van het begrip privéleven uit dit artikel zouden moeten vallen.[296] Ook al kan men naar aanleiding van de hierboven beschreven recente uitspraken van het EHRM spreken van een beginnende rechtsontwikkeling op Europees niveau in de richting van erkenning van dit concept, een uitdrukkelijke vermelding ervan zou beter passen in onze huidige gedigitaliseerde maatschappij. Wellicht dat artikel 8 EVRM als aanknopingspunt zou kunnen dienen voor een met het Duitse IT-grondrecht vergelijkbare bescherming van ICT-systemen. Duitsland zou daarmee als grote inspiratiebron voor de rest van Europa kunnen dienen.[297]

4.4 Hacken als inbreuk op het recht op privacy

Mijns inziens kan worden vastgesteld dat door te hacken in de opsporingsfase inbreuk kan worden gemaakt op de persoonlijke levenssfeer van de betrokkene. Met betrekking tot de huidige wettelijke opsporingsmethoden kan immers ook worden gesteld dat de toepassing ervan in het kader van de strafrechtelijke handhaving dikwijls leidt tot een inbreuk op het recht op privacy.[298] Sterker nog, het recht op bescherming van de persoonlijke levenssfeer is in praktisch elk opsporingsonderzoek in het geding.[299] Daarbij geldt dat naarmate de toegepaste opsporingsbevoegdheid zwaarder wordt, de inbreuk op het recht op een privéleven ingrijpender wordt.[300]

Hacken is er onder meer op gericht om informatie over personen of criminele activiteiten te verzamelen, op te slaan en aan elkaar te koppelen. Het recht op bescherming van de persoonlijke levenssfeer komt daarbij in het geding. Dat komt doordat een ICT-systeem in de huidige gedigitaliseerde samenleving in het privéleven van een persoon een aanzienlijke rol speelt. Mensen gaan ervan uit dat de integriteit van dit persoonlijke

[294] Groothuis & De Jong 2010, p. 281.
[295] Koops & Prinsen 2005, p. 21.
[296] Koning 2012, p. 48.
[297] De Hert, De Vries & Gutwirth 2009, p. 211.
[298] Blom 2001, p. 139.
[299] Knigge & Kwakman 2001, p. 154.
[300] Schermer 2003, p. 35.

computersysteem is gewaarborgd. Men vertrouwt erop dat derden in beginsel niet zonder toestemming van de eigenaar van de computer kunnen kennis nemen van wat er op die computer staat. Het betekent volgens Oerlemans ook dat burgers veronderstellen dat vertrouwelijke documenten niet kunnen worden ingezien en dat er niet kan worden 'meegeluisterd' met vertrouwelijke communicatie via computers. Het voeren van deze privégesprekken kan onder meer plaatsvinden via e-mail, VoIP of chat.[301] Bij hun internetactiviteiten houden mensen er dus geen rekening mee dat de politie overal kan meekijken. In elk geval bestaat er geen verwachting bij burgers dat de politie op grotere schaal gegevens verzamelt en met slimme technische middelen met elkaar in verband brengt.[302] Dat de opsporingsautoriteiten dit type onderzoek uitvoert, is wel duidelijk. Het feit dat hacken of daaraan verwante digitale opsporingsactiviteiten voor burgers vaak niet kenbaar is en het feit dat geautomatiseerde werken heden ten dage een substantieel onderdeel vormen voor personen in hun privéleven, zorgen voor een inbreuk op het recht op privacy.

Ook Boek is van mening dat men door hacken inbreuk op de privacy van de betrokkene maakt. Dit hangt volgens de auteur samen met het heimelijke karakter ervan.[303] Het binnendringen is in principe niet kenbaar voor de betrokkene en deze heeft daardoor geen kans om daadwerkelijk met het betreden van zijn computer in te stemmen. Het feit dat hacken een geheime opsporingsmethode is, kan zelfs zorgen voor een *aanzienlijke* inbreuk op de persoonlijke levenssfeer. Juist omdat de bevoegdheid wordt uitgeoefend op een voor de betrokkenen niet kenbare wijze. De geheime toepassing is echter een wezenskenmerk van hacken, anders kan het niet effectief en efficiënt worden toegepast.[304] Ook de ECRM heeft bevestigd dat het heimelijke gebruik van een opsporingsmethode een inbreuk op het recht op privacy impliceert.[305]

Het feit dat tegenwoordig steeds vaker gebruik wordt gemaakt van servers gelegen in het buitenland of van het eerder aangehaalde *cloud computing* doet overigens niets af aan de inbreuk op het privéleven die wordt gemaakt door het binnendringen van dergelijke systemen. De geautomatiseerde werken bevinden zich in deze voorbeelden buiten de directe fysieke atmosfeer van de gebruiker in een meer publieke omgeving. Ondanks de afstand tussen de betrokkene en het systeem is het gebruik ervan hetzelfde. Ook servers en clouds zouden dientengevolge onder de beschermingsomvang van artikel 8 EVRM moeten geraken, aldus Koning. Net als bij gewone computers wordt er immers inbreuk gemaakt op het recht op privacy van de gebruikers door op deze systemen heimelijk binnen te dringen en eventuele handelingen te monitoren.[306]

Dat hacken in de opsporingsfase leidt tot een inbreuk op de privacy van de betrokkene blijkt wanneer men een vergelijking maakt met enkele huidige digitale opsporingsbevoegdheden. Zo stelt Oerlemans dat de inbreuk bij hacken in het opsporingsonderzoek enigszins te vergelijken is met de inbreuk die wordt gemaakt bij onder meer het tappen van telecommunicatie (artikelen 126m en 126t Sv), het opnemen van vertrouwelijke communicatie (artikelen 126l en 126s Sv) of de bevoegdheid tot de

[301] Oerlemans 2011a, p. 898.
[302] Koops 2012b, p. 42.
[303] Boek 2000, p. 592.
[304] Verbeek, De Roos & Van den Herik 2000, p. 133.
[305] ECRM 9 mei 1989, nr. 12175/86, § 27 en § 31 (*Hope Hewitt en Harman/Verenigd Koninkrijk*).
[306] Koning 2012, p. 49.

doorzoeking ter vastlegging van gegevens (artikelen 125i en 125j Sv).[307] Bij de toepassing van deze bijzondere opsporingsmethoden wordt inbreuk gemaakt op het privéleven van de betrokken burger.[308] Ook het EHRM heeft bevestigd dat het aftappen van telecommunicatie en het opnemen van vertrouwelijke communicatie onder omstandigheden als een schending van artikel 8 EVRM kan worden beschouwd.[309] Dat komt mede door het geheime karakter van beide methoden.[310] Daaruit volgt mijns inziens de conclusie dat de uitoefening van de opsporingsmethode hacken ook zal resulteren in een inbreuk op de persoonlijke levenssfeer. Het recht op privacy is echter niet absoluut. Wanneer aan een aantal in artikel 8 lid 2 EVRM omschreven voorwaarden wordt voldaan, is een inbreuk gepermitteerd.[311]

4.5 Artikel 8 lid 2 EVRM

Naast het Europese mensenrechtenverdrag voorziet artikel 10 Grondwet tevens in een mogelijkheid om geoorloofd inbreuk te maken op het recht op privacy.[312] De regeling van die inbreuken verschilt.[313] Zo eist de Grondwet bij de beperking van artikel 10 een wet in formele zin.[314] Op artikel 8 EVRM mag inbreuk worden gemaakt, wanneer aan de volgende cumulatieve voorwaarden van lid 2 van dit artikel is voldaan.[315] Ten eerste moet met de inzet van de opsporingsmethode een legitiem doel worden nagestreefd. De inbreuk moet daarnaast voorzienbaar zijn bij wet en ten derde noodzakelijk zijn in een democratische samenleving.[316] De volgende subparagrafen gaan nader in op deze voorwaarden.

4.5.1 Het legitieme doel

Een inbreuk op het recht op een privéleven is geoorloofd, indien er onder andere sprake is van een legitiem doel. De verschillende doelcriteria zijn uitputtend opgenomen in artikel 8 lid 2 EVRM.[317] Beperkingen van het privacyrecht van overheidswege zijn alleen toegestaan, indien deze noodzakelijk zijn ter bescherming van bepaalde belangen, waaronder de nationale en de openbare veiligheid, het economisch welzijn van een land, de bescherming van de gezondheid en goede zeden, de bescherming van de rechten en vrijheden van anderen en het voorkomen van wanordelijkheden en strafbare feiten.[318] Het EHRM pleegt overigens in zijn jurisprudentie weinig aandacht te besteden aan de omlijning en reikwijdte van deze doelen.[319] In het kader van dit onderzoek is in ieder geval helder dat de opsporingsmethode hacken het voorkomen van strafbare feiten tot doel heeft en dientengevolge met dit doel zal worden ingezet. In enkele gevallen zal ook de nationale veiligheid dergelijk ingrijpen door de

[307] Oerlemans 2011a, p. 898.
[308] Blom 2001, p. 139.
[309] Zie onder meer EHRM 12 mei 2000, nr. 35394/97 (*Khan/Verenigd Koninkrijk*) en EHRM 1 juli 2008, nr. 58243/00 (*Liberty e.a./Verenigd Koninkrijk*).
[310] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 11.
[311] Blom 2001, p, 141.
[312] Koning 2012, p. 48.
[313] Corstens 1995, p. 551.
[314] Zie artikel 10 lid 1 Grondwet.
[315] Koning 2012, p. 48.
[316] Artikel 8 lid 2 EVRM.
[317] Koning 2012, p. 48.
[318] Ministerie van Veiligheid en Justitie 2011, p. 8.
[319] Koning 2012, p. 48.

opsporingsautoriteiten rechtvaardigen.[320] De legitimiteitstoets ex artikel 8 lid 2 EVRM kan daarmee worden gepasseerd.[321]

4.5.2 Voorzienbaarheid bij wet

Het tweede criterium van artikel 8 lid 2 EVRM behelst de voorzienbaarheid bij wet en is gekoppeld aan drie cumulatieve toetsstenen: (i) de maatregel moet in de nationale wetgeving zijn vastgelegd (*basis in domestic law*), (ii) ze moet voldoende toegankelijk zijn voor het publiek (het vereiste van *accessibility*)[322] en (iii) ze moet voldoen aan de voorzienbaarheid (het vereiste van *foreseeability*).[323]

Het EVRM eist derhalve dat een beperking van het recht op een privéleven *in accordance with the law* (voorzienbaar bij de wet) dient te zijn.[324] De Nederlandse rechtstaat eist met het strafvorderlijk legaliteitsbeginsel ook een expliciete wettelijke grondslag voor ingrijpend optreden van de overheid. Het legaliteitsvereiste vloeit dus eigenlijk voort uit twee afzonderlijke eisen, namelijk uit onze rechtstaatgedachte en dus uit artikel 8 lid 2 EVRM (de beperkende maatregel moet *in accordance with the law* zijn) Voordat de voornoemde voorwaarden (i, ii, en iii) voortvloeiend uit dit vereiste van artikel 8 lid 2 EVRM zullen worden behandeld, zal ik eerst hét basisprincipe in het Nederlandse Wetboek van Strafvordering doornemen, namelijk het strafvorderlijk legaliteitsbeginsel.

4.5.2.1 Het strafvorderlijk legaliteitsbeginsel

Het eerste artikel van het Wetboek van Strafvordering bepaalt:

> 'Strafvordering heeft alleen plaats op de wijze bij de wet voorzien.'[325]

In dit artikel is het strafvorderlijk legaliteitsbeginsel verwoord.[326] Dit grondbegrip bepaalt dat overheidsoptreden dat inbreuk maakt op de rechten en vrijheden van zijn onderdanen, alleen is toegestaan binnen de grenzen van de wettelijke bevoegdheidsbepaling.[327] Het legaliteitsbeginsel heeft als doelstelling de overheid in haar optreden te binden aan democratisch vastgestelde regels ter bescherming van willekeurige aantasting van de rechten en vrijheden van burgers.[328] Zo bezien fungeert de wet als waarborg voor de vrijheid van het individu.[329] De grondslag van het strafvorderlijk legaliteitsbeginsel is derhalve de rechtszekerheid van de burger. Deze mag niet worden overgeleverd aan de willekeur van de met strafrechtstoepassing belaste instanties, zoals de rechter en bestuurlijke instellingen. Het primaat ligt bij de wetgever. Dat wil zeggen dat andere machten in de staat zich moeten

---

[320] In de in paragraaf 2.2.1.4 behandelde Bredolab-ontmanteling werd het gebruikte botnet door het Openbaar Ministerie gekwalificeerd als een gevaarlijk netwerk, dat de nationale veiligheid kon bedreigen; Koning 2012, p. 49.
[321] Oerlemans 2011a, p. 899.
[322] EHRM 2 augustus 1984, nr. 8691/79 (*Malone/Verenigd Koninkrijk*).
[323] Koning 2012, p. 48.
[324] Hofman 1995, p. 73.
[325] Zie artikel 1 Sv.
[326] Corstens 2011, p. 13.
[327] Cleiren 1992, p. 25.
[328] Knigge & Kwakman 2001, p. 182.
[329] Cleiren 2011, p. 9.

onthouden van het scheppen van strafvorderlijke bepalingen, het aanwijzen van bevoegde (rechterlijke) organen en het vaststellen van regels omtrent procedures.[330] De Hoge Raad heeft dit standpunt bevestigd, waarbij deze stelt dat het eigenmachtig in het leven roepen van een procesgang door de rechter onverenigbaar is met het legaliteitsbeginsel.[331]

De rechtszekerheid speelt eveneens een grote rol bij de bepalingen die inbreuken op rechten en vrijheden van burgers toestaan, zoals de opsporingsbevoegdheden uit het Wetboek van Strafvordering. De organen van strafrechtsrechtspleging behoren niet te morrelen aan de grenzen die de wetgever via die bepalingen heeft getrokken. Er moet van worden uitgegaan dat de wetgever die grenzen weloverwogen heeft vastgesteld, aldus Corstens. Interpretatievrijheid bij dwangmiddelen is derhalve gering.[332] Dit kwam onlangs nog naar voren in een uitspraak van de Hoge Raad, waarin werd bepaald dat artikel 1 Sv tot restrictieve interpretatie van de voorschriften inzake de toepassing van strafvorderlijke dwangmiddelen noopt.[333] Een strikte uitleg van de bewoordingen van een wettelijke bepaling staat soms echter op gespannen voet met de behoefte om een bepaald, wenselijk geacht resultaat te bereiken.[334] In zekere zin is daar met betrekking tot hacken in de opsporingsfase op dit moment ook sprake van. De politie ziet zich immers genoodzaakt om geautomatiseerde werken op afstand binnen te dringen, terwijl een uitdrukkelijke wettelijke basis voor dergelijk handelen ontbreekt.

Andere opsporingsmethoden die een serieuze inbreuk maken op de rechten en vrijheden van de betrokkene zijn na de IRT-affaire wel expliciet vastgelegd. De tot dan toe betrekkelijke ongereguleerdheid van deze methoden had, zo bleek, tot misstanden in de opsporing geleid.[335] De Hoge Raad oordeelde hieromtrent in *Zwolsman* dat opsporingsbevoegdheden die resulteren in een ernstige inbreuk op de grondrechten van betrokkenen een expliciete wettelijke basis in de zin van artikel 1 Sv behoeven.[336] Met de invoering van de Wet BOB kwam die basis.[337] Deze wet heeft als uitgangspunt dat de opsporing integer en beheersbaar dient te zijn en dat slechts op basis van daartoe specifiek bij de wet gegeven bevoegdheden inbreuk mag worden gemaakt op de fundamentele rechten van de burger, waaronder en in het bijzonder het recht op privacy.[338] Het strafvorderlijk legaliteitsbeginsel fungeert derhalve niet alleen als waarborg voor de vrijheid van het

[330] Corstens 2011, p. 13.
[331] HR 4 maart 1994, *NJ* 1994, 475.
[332] Corstens 2011, p. 23.
[333] HR 15 april 2011, *NJ* 2012, 345. Overigens dient men zich te realiseren dat de Hoge Raad zich niet altijd zo strikt opstelt als in dit arrest het geval is. Nederlands hoogste rechtscollege laat in enkele zaken behoorlijk veel ruimte voor strafvorderlijk optreden waaraan geen specifiek wettelijk voorschrift ten grondslag ligt. Dat optreden wordt dan toelaatbaar geacht op grond van artikel 2 Politiewet 1993 in combinatie met de artikelen 141 en 142 Sv; zie noot Borgers bij HR 15 april 2011, *NJ* 2012, 345. In HR 20 december 2011, *NJ* 2012, 159 en in HR 20 december 2011, *NJ* 2012, 160 is door de politie gebruikgemaakt van een opsporingsmethode die niet of niet specifiek in een wettelijke regeling was vastgelegd. Toch kwalificeerde de Hoge Raad de gearrangeerde 'pseudo-verkoop' van voor drugshandel bestemde grondstoffen en de inzet van een politiefunctionaris die dienst deed als 'stand-in' bij een oplichtingsactie niet als onrechtmatig; zie noot Schalken bij HR 20 december 2011, *NJ* 2012, 160.
[334] Corstens 2011, p. 23.
[335] Beijer e.a. 2004, p. 27.
[336] HR 19 december 1995, *NJ* 1996, 249 (*Zwolsman*).
[337] Oerlemans 2011a, p. 899.
[338] Beijer e.a. 2004, p. 28 e.v.

individu, maar vormt tevens de bevoegdheidsgrondslag voor strafvorderlijk optreden.[339] Opsporing – en berechting en tenuitvoerlegging – heeft dus slechts plaats op wettelijk geregelde wijze.

In de memorie van toelichting bij de invoering van de Wet BOB werd aangegeven dat het niet mogelijk was een regeling te maken voor alle in de toekomst denkbare opsporingsactiviteiten die zouden kunnen resulteren in een inbreuk op het privéleven.[340] Hieruit kan de conclusie worden getrokken dat de wetgever moet anticiperen op noodzakelijke opsporingsactiviteiten die dat wel doen en deze een wettelijke basis moet geven. Het is immers aan de wetgever – en dus niet aan de rechter – om 'gaten' in het strafprocesrecht te dichten.[341] Eerder in paragraaf 3.1.2 citeerde ik Zinn, senior advisor van het Team High Tech Crime van het KLPD, al over het gebrek aan capaciteit in de opsporing naar cybercrime. Over de lacunes in ons Wetboek van Strafvordering met betrekking tot de opsporing van computergerelateerde criminaliteit en hacken in deze fase zegt hij in BN de Stem het volgende:

> 'Wij proberen dingen uit, waarvan wij niet weten of de rechter het goed vindt. Ons jonge team zou eens een keer op zijn bek moeten gaan, zodat er jurisprudentie komt over wat wij wel en niet mogen in de strijd tegen hackers.'[342]

De wetgevende overheid zal zijn best moeten doen te voorkomen dat het 'falen' van de opsporingsautoriteiten het enige in dit kader adequate leermiddel vormt. Daarmee wordt een situatie vermeden, waarin politie en justitie moedwillig letterlijk en figuurlijk de grenzen overgaan teneinde jurisprudentie over hacken als opsporingsmethode af te dwingen.[343] Indien men wil voorkomen dat de strafvorderlijke overheid tegen de grenzen van het legaliteitsbeginsel oploopt, zijn korte en heldere communicatielijnen tussen enerzijds de werkvloer van het Openbaar Ministerie en anderzijds het wetgevingsapparaat van groot belang. De adequate reactie op signalen omtrent tekortkomingen in de regelgeving is het initiëren van wetgeving. Die reactie is in elk geval te prefereren boven handelend optreden, terwijl men zich bewust is van het feit dat dergelijk optreden kan uitmonden in gerechtelijke procedures.[344]

4.5.2.2 Artikel 8 lid 2 EVRM

Naast het strafvorderlijk legaliteitsbeginsel vloeit de eis van een wettelijke grondslag dus ook voort uit artikel 8 lid 2 EVRM. Zoals is vermeld, moet bij gepermitteerde inmenging in de privacy onder meer sprake zijn van een *basis in domestic law* (i). In de arresten *Kruslin* en *Huvig* is deze subvoorwaarde uitgebreid aan de orde gekomen. In deze gevallen werden telefoongesprekken door de politie afgeluisterd zonder dat er sprake was van een expliciete bevoegdheid tot het aftappen van telefoonlijnen in de Franse wetgeving. Een algemene bevoegdheid tot het inzetten van dwangmiddelen bestond wel. Het EHRM besloot in deze

[339] Cleiren 2011, p. 9.
[340] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 12.
[341] Oerlemans 2011a, p. 900.
[342] Laan 2011.
[343] Oerlemans 2011a, p. 900.
[344] Zie noot Borgers bij HR 15 april 2011, *NJ* 2012, 345.

zaken dat er wel sprake was een wettelijke bevoegdheid tot tappen. Het Hof oordeelde dat onder een *basis in domestic law* niet alleen een wet in formele zin kon vallen, maar ook lagere wetgeving. Daarnaast bepaalde het EHRM dat het recht op privacy zelfs mag worden beperkt door jurisprudentie en ongeschreven recht.[345]

De rechtsgrond voor inmenging moet daarnaast ook voldoende *accessible* (ii) zijn. De inmenging zelf dient bovendien *foreseeable* (iii) te zijn.[346] Beide kwaliteitseisen vloeien voort uit de *rule of law*, waaraan de rechtstaatidee ten grondslag ligt en waarmee dus wordt beoogd de burger te beschermen tegen willekeurig overheidsoptreden.[347] Op grond van deze vereisten moet de burger in staat zijn om op de hoogte te raken van de toepasselijke regels en moeten deze regels voldoende inzicht bieden in de voorwaarden en omstandigheden waaronder de inbreuk is toegelaten.[348]

4.5.2.2.1 Vereisten van toegankelijkheid (ii) en voorzienbaarheid (iii) ex artikel 8 lid 2 EVRM

Ten aanzien van de specifieke toegankelijkheidsvoorwaarde eist het EHRM dat de burger op de hoogte moet kunnen zijn van de regels die in dat geval van belang en toepasselijk zijn.[349] Daarbij dient het van toepassing zijnde recht in ieder geval te zijn gepubliceerd.[350]

Met betrekking tot de eis van voorzienbaarheid wordt gedoeld op het feit dat er voldoende informatie moet worden verstrekt over de reikwijdte en de wijze van uitoefening van de inmenging.[351] Omdat het gebruik van vage termen onontkoombaar is[352], bestaat de voorzienbaarheid in het strafrecht uit een voldoende mate van helderheid en niet uit absolute duidelijkheid.[353] De norm moet derhalve met voldoende precisie worden geformuleerd.[354] Afhankelijk van de aard van de inbreuk op de privacy (de ernst van de inbreuk en de gevolgen daarvan) stelt het Europese Hof zware of minder zware eisen aan de materiële precisie van de vereiste wettelijke grondslag.[355] Daarbij acht het EHRM het van belang dat de effecten van de maatregel door de burger kunnen worden ingeschat, zodat het gedrag hierop kan worden aangepast.[356] Het vereiste van voorzienbaarheid kan daarbij natuurlijk niet zover gaan, dat de betrokkene van tevoren te horen dient te krijgen wanneer bijvoorbeeld zijn communicatie door de autoriteiten zal worden onderschept, zodat hij zijn gedrag hierop kan afstemmen.[357] Het EHRM eist derhalve wel strenge, heldere en gedetailleerde wetgeving in het geval de inbreuk plaatsvindt ter voorkoming van strafbare feiten.[358] Naarmate de inbreuk op de

---

[345] EHRM 24 april 1990, nr. 11801/85, § 29 (*Kruslin/Frankrijk*) en EHRM 24 april 1990, nr. 11105/84, § 27 (*Huvig/Frankrijk*).
[346] EHRM 26 april 1979, nr. 6538/74, § 49 (*The Sunday Times/Verenigd Koninkrijk*).
[347] Knigge & Kwakman 2001, p. 156.
[348] Baaijens-van Geloven & Simmelink 2002, p. 489.
[349] Vande Lanotte & Haeck 2005, p. 717.
[350] ECRM 30 maart 1989, nr. 10461/83 (*Chappell/Verenigd Koninkrijk*).
[351] Vande Lanotte & Haeck 2005, p. 717.
[352] EHRM 24 mei 1988, nr. 10737/84, § 29 (*Müller e.a./Zwitserland*).
[353] EHRM 24 april 1990, nr. 11105/84, § 26 (*Huvig/Frankrijk*).
[354] Hofman 1995, p. 73.
[355] EHRM 2 augustus 1984, nr. 8691/79 (*Malone/Verenigd Koninkrijk*).
[356] EHRM 1 juli 2008, nr. 58243/00 (*Liberty e.a./Verenigd Koninkrijk*).
[357] EHRM 2 augustus 1984, nr. 8691/79, § 67 (*Malone/Verenigd Koninkrijk*).
[358] EHRM 24 april 1990, nr. 11801/85 (*Kruslin/Frankrijk*) en EHRM 30 juli 1998, nr. 27671/95 (*Valenzuela/Spanje*).

persoonlijke levenssfeer ernstiger is, wordt een nauwkeuriger en meer gedetailleerde, specifieke regeling in de wet nodig geacht.[359] Dat geldt tevens wanneer er in de opsporingsfase gebruik wordt gemaakt van geavanceerde technologie.[360] Dat zou in het bijzonder dus ook gelden voor hacken door de politie. Om te kunnen binnendringen in een computer dienen immers allerlei ingewikkelde software- en hardwarematige programma's te worden benut.

Ten slotte heeft het Hof ten aanzien van de eis van voorzienbaarheid bepaald dat een (privacy)beperkende maatregel in overeenstemming dient te zijn met de algemene beginselen van de rechtsstaat en daarmee waarborgen dient te bevatten tegen willekeur en misbruik.[361] Dit heeft tot gevolg dat er voldoende garanties dienen te worden geformuleerd tegen het misbruik van de heimelijke opsporingsmethode hacken.[362] De regeling moet voldoende duidelijkheid verschaffen over de omstandigheden waarin en de voorwaarden waaronder het dwangmiddel mag worden ingezet door opsporingsautoriteiten.[363] Vanwege het geheime karakter dienen daarbij hoge eisen te worden gesteld aan de gedetailleerdheid van de nationale wettelijke regeling omtrent deze ingrijpende opsporingsmethode.[364] Baaijens-van Geloven & Simmelink wijzen er in dit kader op dat er, om de benodigde duidelijkheid te creëren, bepaalde eisen in de wettelijke hackbepaling moeten worden ingepast, zoals de aanduiding van categorieën personen tegen wie de bevoegdheid kan worden uitgeoefend, de bepaling van de tijdsduur van de uitoefening van de bevoegdheid, de wijze van verslaglegging, de aanduiding van bevoegde instanties, bijzondere voorzieningen ter bescherming van geheimhouders en de betrokkenheid van een rechter bij de inbreukmakende opsporingshandelingen.[365]

Men kan hieruit concluderen dat een grondslag in de wet voor hacken als opsporingsmethode – los van de vraag of hacken door de politie wenselijk kan worden geacht – noodzakelijk is. Eerder werd in dit kader al aangegeven dat enkele rechtsgeleerden van mening zijn dat hacken in de opsporingsfase kan worden gebaseerd op sommige bestaande opsporingsbepalingen in ons Wetboek van Strafvordering. Anderen zijn van mening dat door de aanzienlijke potentiële inbreuk op de persoonlijke levenssfeer een meer expliciete wettelijke basis voor hacken in het opsporingsonderzoek is vereist. Of deze opsporingsmethode van huidige wettelijke opsporingsbevoegdheden kan worden afgeleid of dat een uitdrukkelijke basis in de wet voor hacken onontbeerlijk is, behandelt paragraaf 6.2.

4.5.3 Noodzakelijkheid in een democratische samenleving

Het laatste criterium van het recht op een privéleven is de noodzakelijkheid van de inbreuk in een democratische samenleving. Dit vereiste vormt dikwijls het scharnierpunt in de overwegingen van het EHRM, wanneer aan de overige vereisten – is sprake van een inbreuk

[359] Knigge & Kwakman 2001, p. 158.
[360] EHRM 24 april 1990, nr. 11801/85 (*Kruslin/Frankrijk*) en EHRM 30 juli 1998, nr. 27671/95 (*Valenzuela/Spanje*).
[361] EHRM 26 september 1995, nr. 17851/91, § 48 (*Vogt/Duitsland*).
[362] Baaijens-van Geloven & Simmelink 2002, p. 491 met verwijzing naar EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland*) en EHRM 2 augustus 1984, nr. 8691/79 (*Malone/Verenigd Koninkrijk*).
[363] Oerlemans 2011a, p. 900 e.v.
[364] Baaijens-van Geloven & Simmelink 2002, p. 491.
[365] Baaijens-van Geloven & Simmelink 2002, p. 497.

op het grondrecht, is deze inbreuk bij wet voorzien en is zij getroffen met een legitiem doel? – is voldaan.

De vraag, of een aangebrachte beperking al dan niet noodzakelijk is in een democratische samenleving, vraagt vooral beoordeling van de concrete feiten en de toepasselijke regelgeving in het betreffende geval.[366] Wel heeft het EHRM in een aantal uitspraken getracht te benoemen wat de noodzakelijkheid binnen het criterium precies inhoudt. Zo is het begrip in ieder geval niet synoniem aan nodig, wenselijk of nuttig.[367] Andere principes die het Hof in dit verband heeft ontwikkeld, zijn de volgende:

> '- the Contracting States enjoy a certain but not unlimited margin of appreciation in the matter of the imposition of restrictions, but it is for the Court to give the final ruling on whether they are compatible with the Convention (…);
> - the phrase 'necessary in a democratic society' means that, to be compatible with the Convention, the interference must, *inter alia*, correspond to a 'pressing social need' and be 'proportionate to the legitimate aim pursued' (…);
> - those paragraphs of Articles of the Convention which provide for an exception to a right guaranteed are to be narrowly interpreted.'[368]

Voorafgaande aan dit arrest oordeelde het Europese Hof in *The Sunday Times* ook al dat er met betrekking tot het vereiste ex artikel 8 lid 2 EVRM sprake moet zijn van een *pressing social need* en dat de beperkende maatregel in redelijke verhouding dient te staan tot het te dienen doel.[369] Met deze laatste voorwaarde wordt gedoeld op de belangafweging tussen het effect van de inmenging op recht en rechtsbeleving van de burger en het nagestreefde legitieme doel.[370] Oftewel, er dient voldaan te zijn aan de proportionaliteitseis.[371] Ook dient gewicht te worden toegekend aan de subsidiariteit en dient te worden beoordeeld of de redenen die de nationale autoriteiten aandragen ter rechtvaardiging van de gepleegde inbreuk relevant en sufficiënt zijn.[372] Staten wordt bij de belangenafweging een zekere beoordelingsvrijheid, *margin of appreciation*, toegekend om de effectiviteit, proportionaliteit en noodzakelijkheid van de maatregel te beoordelen.[373] Dat wil zeggen dat het EHRM zich dus niet onnodig met het nationale recht zal dienen te bemoeien.[374]

Wat in een democratische samenleving nodig is, staat overigens niet voor alle tijden vast.[375] Het criterium ex artikel 8 lid 2 EVRM heeft daarmee een fluctuerend karakter. Zo kan het in tijden en omstandigheden, waarin de criminaliteit sterk oprukt en vanuit de overheid alle zeilen moeten worden bijgezet, zo zijn dat om met enige kans op succes de rechtsorde te kunnen handhaven, inbreuken op de privacy van betrokkenen in meerdere mate geoorloofd

[366] Hofman 1995, p. 78.
[367] EHRM 7 december 1976, nr. 5493/72 (*Handyside/Verenigd Koninkrijk*).
[368] EHRM 25 maart 1983, nr. 5947/72, § 97 (*Silver e.a./Verenigd Koninkrijk*).
[369] EHRM 26 april 1979, nr. 6538/74 (*The Sunday Times/Verenigd Koninkrijk*).
[370] Koning 2012, p. 48.
[371] Blom 2001, p. 141.
[372] EHRM 25 maart 1983, nr. 5947/72, § 97 (*Silver e.a./Verenigd Koninkrijk*).
[373] Koning 2012, p. 48.
[374] Knigge & Kwakman 2001, p. 158.
[375] Hofman 1995, p. 78.

zijn dan in situaties waarin dat niet het geval is.[376] Daarbij voegt het Hof ten aanzien van het tappen van telefoongesprekken in *Malone* toe:

> 'However, the exercise of such powers, because of its inherent secrecy, carries with it a danger of abuse of a kind that is potentially easy in individual cases and could have harmful consequences for democratic society as a whole (…). This being so, the resultant interferences can only be regarded as 'necessary in a democratic society' if the particular system of secret surveillance adopted contains adequate guarantees against abuse.'[377]

Deze garanties tegen misbruik moeten vooral worden gezocht in de controleerbaarheid van de genomen maatregelen.[378] Met betrekking tot hacken creëert deze toetsbaarheid mogelijk een belemmering. Het binnendringen van geautomatiseerde werken vindt immers heimelijk plaats. Dit geheime karakter vormt bovendien de kracht van deze verregaande opsporingsmethode. De controleerbaarheid is echter een voorwaarde voor het kunnen aanwenden van rechtsmiddelen tegen een inbreuk op een grondrecht.[379]

Toch kan het hacken in de opsporingsfase – onder voorwaarden – wel noodzakelijk worden geacht. Dit hangt onder meer samen met de problemen die ontstaan door anonimiteit en versleuteling.

4.5.3.1 Anonimiteit

Computers waar mensen gebruik van maken, kunnen via het internet worden geïdentificeerd met een IP-adres. Met een dergelijk adres kan in beginsel precies worden vastgesteld waar het geautomatiseerde werk zich bevindt. Tevens is in de meeste gevallen de service provider bekend die het IP-adres aan het apparaat heeft toegekend. Bij deze dienstverlener kunnen vervolgens identificerende gegevens over klanten worden gevorderd. Weliswaar bestaat de kans dat het IP-adres leidt naar een gehackte computer of server, maar ook in die gevallen levert het de opsporingsautoriteiten wel een spoor op om vervolgens op door te kunnen rechercheren. Waar politie en justitie nu in hun opsporingsonderzoek juist tegenaan lopen, is het feit dat in het criminele milieu steeds vaker gebruik wordt gemaakt van allerlei anonimiseringstechnieken.[380] Anonimiteit wordt in dat kader gedefinieerd als:

> 'het ontbreken van een bekende naam, identiteit en bron, waarbij de 'naam' een persoon identificeert, de 'identiteit' zijn persoonlijke eigenschappen omvat en de 'bron' zijn locatie op het netwerk vastlegt.'[381]

Doel van de anonimiseringsvaardigheden is het IP-adres zo aan te passen, dat de locatie van de verdachte lastiger – zo niet onmogelijk – is vast te stellen.[382] Voor criminelen die voor hun activiteiten van netwerken gebruikmaken, is anonimiteit uiteraard een prioriteit.[383]

---

[376] Hofman 1995, p. 78.
[377] EHRM 2 augustus 1984, nr. 8691/79, § 81 (*Malone/Verenigd Koninkrijk*).
[378] Hofman 1995, p. 79.
[379] Hofman 1995, p. 79.
[380] Oerlemans 2011a, p. 904.
[381] Van den Eshof e.a. 2002, p. 21.
[382] Oerlemans 2011a, p. 904.
[383] Van den Eshof e.a. 2002, p. 21.

Om toch aan de (identificerende) gegevens van de betrokkene te geraken, zou hacken een uitkomst kunnen bieden. Zo zou – wanneer er toch enige informatie over de identiteit van de verdachte bekend is – kunnen worden geprobeerd om met behulp van malware (Trojaans politiepaard) het geautomatiseerde werk binnen te dringen. Met een eenvoudige handeling zou dan vervolgens het niet-afgeschermde IP-adres van de computer kunnen worden vastgesteld. Vervolgens zou de opsporingsambtenaar een stap verder kunnen gaan en bijvoorbeeld op afstand schermopnames kunnen maken. Op die manier kan bruikbaar bewijsmateriaal worden verzameld van bijvoorbeeld kinderpornografisch materiaal of illegale communicatie. Ook zouden bestanden en documenten op de computer kunnen worden gekopieerd.[384] Hetzelfde geldt voor bestanden op externe aangesloten apparaten, servers of harde schijven. Tevens kunnen vluchtige gegevens op deze manier worden veiliggesteld.[385]

Met het hacken in de opsporingsfase worden dus heimelijk en op afstand nieuwe mogelijkheden tot opsporing gecreëerd en problemen ten aanzien van anonimiteit omzeild.[386]

4.5.3.2 Versleuteling

Cryptografie (of 'versleuteling' of 'encryptie') betreft het versleutelen van een boodschap zodanig dat zij onleesbaar wordt.[387] Er wordt dus leesbare data (*plaintext*) omgevormd in onleesbaar materiaal (*ciphertext*) door middel van een wiskundig algoritme.[388] Slechts degenen die de sleutel kennen, die benodigd is voor het ontsleutelen van de boodschap, kunnen deze weer lezen.[389] Vaak wordt overigens ook een wachtwoord gebruikt om de sleutel te beveiligen.[390] Essentieel aan cryptografie is dat het om een omkeerbare bewerking moet gaan. Dat wil zeggen dat een bericht met een bepaalde sleutel gecodeerd en gedecodeerd kan worden. Dezelfde sleutel wordt derhalve gebruikt om het bericht te versleutelen, als om het weer leesbaar te maken. Het meest eenvoudige voorbeeld van versleuteling is het verwisselen van letters in een boodschap door andere letters, die op een regelmatige afstand in het alfabet staan. Zo wordt de A een D, de B een E, de C een F en zo verder.[391] In het algemeen zijn versleutelingstechnieken veel moeilijker te ontcijferen.[392]

Cryptografie is ongekend populair, zeker waar gecommuniceerd wordt over publieke netwerken.[393] Deze techniek heeft dan ook brede toepassing gekregen en is daarmee een essentieel onderdeel geworden van informatiebeveiliging. Cryptografie heeft niet alleen positieve kanten. Het criminele circuit kan dit middel immers ook aanwenden.[394] Een groot voordeel van deze techniek is namelijk dat het de privacy kan waarborgen. Criminelen kunnen hun berichtgeving versleutelen en daardoor op een betrekkelijk eenvoudige manier veilig met elkaar communiceren.[395] Hun gespreksverkeer wordt door deze werkwijze derhalve

[384] Oerlemans 2011a, p. 904 e.v.
[385] Fox 2007, p. 828.
[386] Oerlemans 2011a, p. 905.
[387] Van den Eshof e.a. 2002, p. 65.
[388] Oerlemans 2011a, p. 905.
[389] Van den Eshof e.a. 2002, p. 65.
[390] Oerlemans 2011a, p. 905.
[391] Van den Eshof e.a. 2002, p. 65.
[392] Van den Eshof e.a. 2002, p. 66.
[393] Van den Eshof e.a. 2002, p. 65.
[394] Koops 2000, p. 10.
[395] Van den Eshof e.a. 2002, p. 67.

vergemakkelijkt. Gegevens op geautomatiseerde werken kunnen daarnaast ook worden gecodeerd. Onderzoek in computers heeft ten gevolge daarvan weinig zin als de verzamelde gegevens blijken te zijn versleuteld.[396]

Voor opsporingsautoriteiten zorgen deze virtuele handelswijzen voor veel problemen.[397] In de fysieke wereld is elke kluis immers door de politie open te maken. In de virtuele wereld is dat niet altijd het geval. Door gebruik te maken van sterk cryptografische programma's kan een crimineel al zijn digitale sporen (bijvoorbeeld van kinderporno) ontoegankelijk maken voor de opsporingsautoriteiten. Zo kan een gebruiker met een cryptografisch programma twee wachtwoorden aanmaken, een voor de politie en een voor de gebruiker zelf. Wanneer de opsporingsambtenaren het wachtwoord achterhalen en gebruiken, krijgen ze onschuldig materiaal te zien. Wanneer het andere (geheime) wachtwoord wordt gebruikt, worden de criminele gegevens zichtbaar.[398] Met behulp van deze techniek wordt de inhoud op een gegevensdrager (USB-stick, externe en interne harde schijf) voor derden dus onleesbaar gemaakt. Versleuteling van dergelijke gegevensdragers met moderne versleutelingssoftware is voor opsporingsdiensten onkraakbaar. De versleutelcodes zijn, mits de gebruiker zorgvuldig met het systeem omgaat, zo complex dat ze de facto niet voor de politie te kraken zijn.[399] Indien het bewijsmateriaal niet eerder is veiliggesteld, de verdachte weigert de sleutel vrijwillig af te staan en de sleutel niet op een andere manier te ontfutselen is, kan het heel goed zijn dat het bewijsmateriaal nooit kan worden bemachtigd.[400]

Niet alleen kan een gebruiker bepaalde data op een gegevensdrager versleutelen, ook is het dus mogelijk om communicatieverkeer onbegrijpelijk te maken, zodat dergelijke correspondentie niet meer af te vangen is met een (internet)tap.[401] Een bekend voorbeeld hiervan is dat de communicatie via het programma *Skype* niet of zeer moeilijk kan worden afgeluisterd.[402] Internettaps worden bovendien steeds minder effectief door de groei van de hoeveelheid gegevens die over de tap gaat en het aantal apparaten dat van een internetverbinding gebruikmaakt. Het gevolg hiervan is dat de opsporingsautoriteiten niet meer alle benodigde communicatie kunnen onderscheppen. Men noemt dit verschijnsel ook wel het 'Going Dark Problem'.[403] De kluwen of opeenhoping van informatie is in dat geval zo ingewikkeld (en groot), dat zij niet meer te ontwarren is.

4.5.3.2.1 Hacken als oplossing voor de versleutelingsproblematiek

Resumerend mondt criminele versleuteling voor opsporingsautoriteiten uit in een juridisch en een praktisch probleem. Juridisch gezien kan de politie de verdachte niet dwingen tot het afgeven van zijn pas- of wachtwoord, omdat dit in strijd is met het nemo tenetur-beginsel[404].[405] Met de Wet computercriminaliteit I is overigens de mogelijkheid gecreëerd een

[396] Koops 2000, p. 10.
[397] Van den Eshof e.a. 2002, p. 67.
[398] Prins 2012, p. 50.
[399] Koops 2000, p. 11.
[400] Oerlemans 2011a, p. 906.
[401] Buermeyer 2007, p. 160.
[402] *Kamerstukken II* 2008/09, 28 684, nr. 232, p. 3.
[403] Oerlemans 2011a, p. 905.
[404] Dit beginsel, dat nergens uitdrukkelijk in de Nederlandse wet staat, houdt in dat een persoon niet actief hoeft mee te werken aan zijn eigen veroordeling, noch daartoe verplicht dan wel gedwongen kan worden en dat hij tot die veroordeling voor onschuldig wordt gehouden (de onschuldpresumptie); Meijer 2009, p. 415. Daaruit volgt

bevel tot ontsleuteling uit te vaardigen.[406] Vanwege het nemo tenetur-principe kan het bevel derhalve slechts gericht worden aan niet-verdachten.[407] De vraag rijst of een dergelijk bevel dan in de praktijk nog wel van waarde is. Praktisch gezien zijn de versleutelde bestanden daarnaast meestal – qua versleuteling – van zo'n hoog niveau dat zij niet te kraken zijn.[408] Het een en ander heeft gevolgen voor de opsporingsfase. Indien de politie een versleuteld bestand aantreft op internet, zal het in de praktijk moeilijk zijn om vast te stellen of het illegaal materiaal betreft: het bestand is immers onleesbaar. Indien de versleuteling van voldoende kwaliteit is, is het praktisch onmogelijk om deze te ontcijferen. Vervolgens zal het dan tevens moeilijk zijn om het bestand aan een bepaalde verdachte te koppelen.[409] De noodzaak van een maatregel tegen versleuteling wordt des te evident bij ernstige ICT-gerelateerde incidenten zoals kinderpornografie, waarbij criminelen zich in toenemende mate inspannen kinderporno met cryptografietechnieken te verbergen.[410]

Hacken zou het ontstaan van voornoemde problemen kunnen voorkomen. Zo kan door het plaatsen van spyware op de computer van de verdachte internetverkeer bij de bron worden doorgestuurd. Op die manier wordt als het ware een tap op de bron gezet, waardoor het probleem van versleuteling kan worden omzeild.[411] Tevens kunnen tijdens het op afstand en heimelijk binnendringen van de computer van de gebruiker – en de inzet van bepaalde technieken, zoals *keyboard sniffers* – cryptografische sleutels worden opgevangen en wordt daarmee ook de toegang verschaft tot het criminele materiaal.[412] Met behulp van een dergelijke *keyboard sniffer* kunnen stiekem alle toetsenbordaanslagen worden geregistreerd, inclusief wachtwoorden waarvan de betrokkene gebruikmaakt.[413] Vervolgens kunnen de gegevens op de computer met de afgevangen wachtwoorden weer leesbaar worden gemaakt.
Ook op grond van de huidige wetgeving kan na het betreden van bijvoorbeeld een woning een apparaatje op het toetsenbord worden geplaatst dat toetsaanslagen afvangt. Het voordeel van het registreren van toetsaanslagen door middel van het zetten van een hack is dat de opsporingsambtenaar achter zijn bureau kan blijven zitten, zelfs al is de verblijfplaats van de verdachte onbekend. Bovendien bestaat er wellicht minder kans op ontdekking.[414] Op deze manier vormt het hacken van computers een mogelijke oplossing voor het versleutelingsprobleem en kan daarmee in combinatie met de anonimiseringsproblematiek de noodzakelijkheid van deze opsporingsmethode worden aangetoond.

---

in dit kader dat het onder dwang aan de politie moeten afstaan van een wachtwoord resulteert in een schending van dit principe. Overigens is het nemo tenetur-beginsel door het EHRM onder meer erkend in de uitspraken *Murray/Verenigd Koninkrijk*, 8 februari 1996, nr. 18731/91 en *Saunders/Verenigd Koninkrijk*, 17 december 1996, nr. 19187/91.

[405] Van den Eshof e.a. 2002, p. 67 e.v.
[406] *Stb.* 1993, 33.
[407] Koops 2000, p. 20.
[408] Van den Eshof e.a. 2002, p. 67 e.v.
[409] Van den Eshof e.a. 2002, p. 68.
[410] Oerlemans 2011a, p. 906.
[411] Oerlemans 2011a, p. 907.
[412] Prins 2012, p. 50.
[413] Van den Eshof e.a. 2002, p. 69.
[414] Oerlemans 2011a, p. 907.

4.6 Conclusie

ICT-systemen zijn heden ten dage essentieel geworden voor het persoonlijk en maatschappelijk leven van burgers. Allerhande gegevens, zowel zakelijk als privé, worden voortdurend geproduceerd, opgeslagen en verspreid met behulp van deze systemen. Het van buitenaf, en zonder medeweten van de betrokkene, binnendringen van dergelijke geautomatiseerde werken in de opsporingsfase kan resulteren in aanzienlijke inbreuk op het privéleven. Dezelfde redenering gaat op voor de verdachte, ondanks het feit dat diegene strafbare feiten pleegt of voorbereidt. Het uitoefenen van opsporingsbevoegdheden tegen deze persoon leidt in praktisch alle gevallen tot een zekere inbreuk op de persoonlijke levenssfeer. Dat is met betrekking tot hacken door de politie niet anders. Inbreuken op de privacy van de verdachte zijn gerechtvaardigd, mits aan de cumulatieve vereisten ex artikel 8 lid 2 EVRM wordt voldaan. Ten eerste dient er met de inzet van hacken als opsporingsmethode een legitiem doel te worden nagestreefd. Daar lijkt in het kader van dit onderzoek aan te zijn voldaan, namelijk het voorkomen van strafbare feiten. Tevens dient de maatregel noodzakelijk te zijn in een democratische samenleving. Om de necessiteit van hacken in het opsporingsonderzoek te kunnen aantonen, heb ik verwezen naar de ontwikkeling van de anonimiserings- en versleutelingstechnieken in het criminele circuit. De derde en laatste voorwaarde uit artikel 8 lid 2 EVRM behelst de voorzienbaarheid bij wet. Dit vereiste heeft tot gevolg dat de opsporingsmaatregel hacken in de wet moet zijn vastgelegd, dat de maatregel voldoende toegankelijk moet zijn voor het publiek en dat ze moet voldoen aan de voorzienbaarheid. Korter geformuleerd, het Europese verdrag eist strenge, heldere en gedetailleerde wetgeving. Nu zijn enkelen van mening dat hacken als opsporingsbevoegdheid kan worden afgeleid van reeds bestaande wettelijke opsporingsmethoden. Of deze stelling standhoudt, kan pas worden geconstateerd nadat deze huidige in de wet verankerde methoden zijn onderzocht. Behandeling van dit ICT-opsporingsframe vindt in het volgende hoofdstuk plaats.

Hoofdstuk 5 Het huidige wettelijke kader omtrent digitale opsporing

In beginsel mag en kan de politie, net als ieder ander, het internet gebruiken als een voor iedereen toegankelijke informatiebron.[415] Als bij deze vorm van virtueel surveilleren geen inbreuk wordt gemaakt op de rechten en vrijheden van burgers, biedt artikel 2 Politiewet 1993 daarvoor in combinatie met artikel 141 Sv een voldoende geschikte wettelijke grondslag. Een verdenking van een strafbaar feit is derhalve niet noodzakelijk. Wanneer er wel een (digitaal) misdrijf wordt gepleegd, beschikt justitie over diverse bevoegdheden in het Wetboek van Strafvordering. Daarbij geldt in beginsel: wat offline geldt, moet ook online gelden. Dat wil zeggen dat de waarborgen en regels omtrent opsporingsbevoegdheden die in de fysieke wereld gelden, in principe tevens van kracht moeten zijn op het internet.[416] Slechts de ICT-gerelateerde varianten van de opsporingsbevoegdheden zal dit hoofdstuk doornemen. Daarbij zal een onderscheid worden gemaakt tussen de methoden met betrekking tot stromende gegevens en die omtrent opgeslagen gegevens (§ 5.2). Vervolgens besteed paragraaf 5.3 kort de aandacht aan enkele andere ICT-gerelateerde opsporingsbevoegdheden. Paragraaf 5.4 behandelt aansluitend de inkijkoperatie. De inkijkoperatie lijkt naar haar aard niet geschikt te zijn voor toepassing in een digitale omgeving, omdat in het artikel wordt gedoeld op een fysieke plaats.[417] Boek betoogt echter dat het besloten plaatsbegrip wel kan worden opgerekt naar virtuele ruimtes.[418] Daarom acht ik behandeling van deze methode in dit hoofdstuk van belang. De auteur gaat zelfs verder en beargumenteert dat de bevoegdheid tot hacken kan worden afgeleid van artikel 126k Sv.[419]

Hacken is op dit moment in ieder geval al wel toegestaan voor inlichtingen- en veiligheidsdiensten, zoals paragraaf 5.5 betoogt. Ten slotte zullen de toekomstige vernieuwingen voor het digitale opsporingskader worden doorgenomen naar aanleiding van de formulering van het conceptwetsvoorstel ‘versterking bestrijding computercriminaliteit’ (§ 5.6).

5.1 Het opsporingsonderzoek in het algemeen

Opsporing is ‘het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen’.[420] Vanuit ICT-perspectief is juist deze fase van belang.[421] Zoals in het vorige hoofdstuk is behandeld, staat het legaliteitsbeginsel centraal bij strafvordering en opsporing. Dit strafvorderlijke beginsel ex artikel 1 Sv vereist een wet in formele zin voor de uitoefening van opsporingsmethoden.[422]

[415] Stol, Leukfeldt & Klap 2012, p. 28.
[416] Schermer 2003, p. 52.
[417] Schermer 2003, p. 53.
[418] Boek 2000, p. 592.
[419] Boek 2000, p. 592.
[420] Artikel 132a Sv.
[421] Koops & Buruma 2007, p. 77.
[422] Corstens 2011, p. 14.

Ook uit het EVRM en aanverwante jurisprudentie vloeit de eis van een grondslag in de wet voor inbreukmakende activiteiten door de overheid voort.

In dit kader rijst de vraag wanneer de wet voorziet in een opsporingsmethode. Deze vraag is niet eenvoudig te beantwoorden. De wet beschrijft namelijk bevoegdheden en bevat geen systematische weergave van opsporingsmethoden. Wie wil weten van welke opsporingsmethoden de politie zich in het opsporingsveld bedient en daarbij zou afgaan op hetgeen het Wetboek van Strafvordering daarover zegt, krijgt een zeer vertekend beeld.[423] Bezwaarlijk is dat niet. Het is onmogelijk en onnodig om met betrekking tot iedere strafvorderlijke bevoegdheid uitputtend in de wet vast te leggen hoe een dergelijke bevoegdheid in de praktijk dient te worden aangewend. Zo is in ons strafvorderlijk wetboek de bevoegdheid tot het opnemen van vertrouwelijke communicatie wel terug te vinden, maar kan men tevergeefs zoeken naar aanwijzingen op welke manier deze bevoegdheid in het opsporingsonderzoek moet worden gehanteerd. Dat komt doordat naarmate de tijd verstrijkt en de technologie evolueert steeds weer zal blijken dat de wettelijk verankerde bevoegdheid op alternatieve wijze of met behulp van andere (technische) middelen kan worden toegepast.

Omtrent de opsporingsfase geldt in beginsel het volgende: opsporingsactiviteiten kunnen op grond van de algemene opsporingsbevoegdheid zoals vastgelegd in de artikelen 2 Politiewet 1993 en 141 en 142 Sv in overeenstemming met het strafvorderlijk legaliteitsbeginsel worden gehanteerd, voor zover zij redelijkerwijs noodzakelijk zijn voor de opsporing.[424] De concrete toepassing wordt genormeerd door enkele algemene rechtsbeginselen, zoals de proportionaliteit, subsidiariteit en het verbod van willekeur.[425]

Wanneer de inzet van een opsporingsmethode de verdachte burger in zijn grond- of mensenrechten beperkt, feitelijk is dat vrijwel altijd het geval, volstaat de algemene wettelijke grondslag voor opsporingsactiviteiten niet meer en dient voor de inzet ervan een expliciete wettelijke grondslag te bestaan.[426] Als uitvloeisel van de IRT-affaire en de daaropvolgende parlementaire enquête opsporingsmethoden in de jaren negentig is deze basis in de wet tot stand gekomen met de Wet BOB[427]. Veel – en voor ICT de meest relevante – bevoegdheden zijn daarmee vastgelegd in het Wetboek van Strafvordering.[428] Daardoor geldt nu het principe: als het niet nadrukkelijk is toegestaan, dan mag het niet.[429]

5.2 Opgeslagen en stromende gegevens

In dit hoofdstuk zullen enkele ICT-gerelateerde opsporingsbevoegdheden worden beschreven en geanalyseerd. Deze bevoegdheden zijn door het toegenomen gebruik van computersystemen van een steeds groter belang.[430] De wetgever maakt in het digitale

[423] Corstens 2011, p. 246.
[424] Beijer e.a. 2004, p. 30.
[425] Boek 2000, p. 591.
[426] HR 19 december 1995, *NJ* 1996, 249 (*Zwolsman*).
[427] *Stb*. 1999, 245.
[428] Koops & Buruma 2007, p. 78.
[429] Stol, Leukfeldt & Klap 2012, p. 28.
[430] Deze artikelen zijn gecreëerd in het kader van de invoering van de Wet computercriminaliteit I en II (*Stb.* 1993, 33 en *Stb.* 2006, 299 en 300).

strafvorderlijke kader een onderscheid tussen opgeslagen en stromende gegevens. Soms volgt dit onderscheid uit de wettekst zelf, soms uit de achterliggende ratio.[431]

Het onderzoek van opgeslagen (bedrijfsmatig vastgelegde) gegevens richt zich tot personen waarvan vermoed wordt dat zij toegang tot deze gegevens hebben. Dat kunnen telecommunicatieaanbieders zijn, maar het onderzoek kan ook worden gericht tot natuurlijke personen met wie de verdachte bijvoorbeeld een bijzondere betrekking heeft.[432] Voor onderzoek van opgeslagen gegevens op geautomatiseerde werken bestaat een apart regime, wat grotendeels parallel loopt aan de traditionele opsporingsbevoegdheden van het uitleveringsbevel en de doorzoeking. In dit kader zullen de vorderingsmogelijkheden van gegevens (§ 5.2.1) worden behandeld en de digitale doorzoeking (§ 5.2.2). Paragraaf 5.2.2.1 besteed aandacht aan de netwerkzoeking. Daarbij beschrijf ik ook het ontsleutel- en bevriezingsbevel (§ 5.2.2.2 en § 5.2.3).

Het onderzoek van stromende gegevens – dat wil zeggen de gegevens in transport – betreffen de aftapbevoegdheden (§ 5.2.4) en het opnemen van vertrouwelijke communicatie (§ 5.2.5).[433] Het zijn bevoegdheden die betrekking hebben op de verplaatsing van communicatiegegevens over de openbare telecommunicatie-infrastructuur en de wijze waarop en de voorwaarden waaronder politiediensten deze stromende gegevens mogen verzamelen.[434] Waar het gaat om stromende gegevens worden in de wet de termen ‘worden verwerkt of overgedragen’ gehanteerd. Het stromende karakter ziet in wezen op de overbrenging of overdracht van gegevens van geautomatiseerd werk A naar geautomatiseerd werk B.[435]

Het onderscheid tussen opgeslagen en stromende gegevens is in ons Wetboek van Strafvordering niet van een heel groot belang.[436] Toch ben ik van mening dat het kan helpen de grenzen en beperkingen van de strafvorderlijke bevoegdheden te verhelderen. Daarom zal ik de differentiatie in dit onderzoek hanteren.

5.2.1 Het vorderen van opgeslagen gegevens

Het opvragen van gegevens is geregeld in de artikelen 126nc Sv en verder.[437] Om gegevens te kunnen vorderen is de inzet van aparte bevoegdheden noodzakelijk naast de traditionele bevoegdheden voor een uitleveringsbevel, omdat gegevens geen ‘goed’[438] zijn en dus niet op

[431] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 26.
[432] Smits 2006, p. 9.
[433] Koops & Buruma 2007, p. 79.
[434] Smits 2006, p. 8.
[435] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 28.
[436] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 29.
[437] Overigens is het opvragen van gegevens bij communicatieaanbieders geregeld in de artikelen 126n, 126na en 126ng Sv.
[438] De door de minister van Justitie in 1985 ingestelde Commissie computercriminaliteit (Commissie-Franken) heeft bepaald dat computergegevens om een aantal redenen niet kunnen worden vereenzelvigd met het strafrechtelijke vermogensobject ‘goed’. Een van de argumenten was toentertijd dat gegevens ‘multipel’ zijn. Dat wil zeggen dat vele mensen tegelijkertijd de beschikking kunnen hebben over dezelfde gegevens. Dit gegeven staat haaks op de kenmerken van een ‘goed’. Daarnaast zijn gegevens in beginsel het product van geestelijke arbeid, terwijl goederen het product zijn van fysieke arbeid; Kaspersen 2007, p. 21 e.v. De Hoge Raad zag zich onlangs nog voor de vraag gesteld ‘of *virtuele objecten* kunnen worden aangemerkt als een ‘goed’ in de zin van artikel 310 Sr’; HR 31 januari 2012, *LJN* BQ9251. Het ging in deze zaak om diefstal van een virtueel amulet en masker in het online computerspel *RuneScape.* In dit spel kunnen spelers hun online alter ego (*avatar*) opdrachten en handelingen laten verrichten, waaronder het verzamelen van objecten (*items*). De verdachten in deze zaak hadden het slachtoffer gedwongen om in te loggen op zijn account, zodat een van de

basis van de artikelen 96a of 105 Sv (het bevel tot uitlevering van een voorwerp) kunnen worden gevorderd. De opsporingsautoriteiten kunnen, in volgorde van oplopende zwaarte, identificerende, 'andere' en gevoelige gegevens opvragen, alsmede toekomstige gegevens, bij allerlei personen en instanties.[439] De bevoegdheid tot het opvragen van gegevens komt toe aan de officier van justitie. In sommige gevallen is een voorafgaande machtiging van de rechter-commissaris vereist.[440]

Tevens kan de officier van justitie op grond van artikel 126n Sv de verstrekking van verkeersgegevens en gebruikersgegevens vorderen aan aanbieders van communicatiediensten.[441] Op deze manier is het mogelijk om onder meer nummergegevens van de beller en de gebelde, datum, tijdstip en duur van de verbinding en locatiegegevens te verzamelen, aldus artikel 2 Besluit vorderen gegevens telecommunicatie.[442] Overigens hoeven deze gevorderde gegevens niet een verdachte van een misdrijf te betreffen: in beginsel kunnen van iedereen gegevens worden opgevraagd.[443] Van deze mogelijkheid wordt overigens veel gebruikgemaakt, omdat verkeersgegevens zeer interessant zijn in het beginstadium van een opsporingsonderzoek om verbanden in kaart te brengen en om uit te vinden wie nader onderzoek zou kunnen behoeven.[444]

5.2.2 Opgeslagen gegevens: de doorzoeking

Politie en justitie zijn bij het vorderen van opgeslagen gegevens afhankelijk van de medewerking van derden, zoals communicatieaanbieders. De opsporingsautoriteiten hebben echter ook de bevoegdheid om zelf onderzoek te doen in systemen en bestanden.[445] Dergelijk onderzoek op computersystemen kan op grond van artikel 125i Sv geschieden in het kader van het doorzoeken van een plaats ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn opgeslagen of vastgelegd.[446] Van een reguliere doorzoeking is in dit kader derhalve geen sprake. Deze doorzoekingsbevoegdheden strekken immers tot de inbeslagneming van voorwerpen en stukken, hetgeen niet mogelijk is voor gegevens, omdat deze niet als 'goed' kunnen worden gekwalificeerd.[447] Wel is de doorzoeking ter vastlegging

---

verdachten de *items* van het slachtoffer virtueel kon overhandigen aan de *avatar* van een medeverdachte; Spierings & Pesselse 2012, p. 195. De Hoge Raad bepaalde dat een dergelijke virtueel *item* kan worden aangemerkt als een 'goed' in de zin van artikel 310 Sr. Bij deze overweging wordt aansluiting gezocht bij de volgende vereisten: de objecten zijn overdraagbaar, vertegenwoordigen waarde en over de objecten had het slachtoffer de feitelijke en exclusieve heerschappij. Deze beschikkingsmacht is door het handelen van de verdachten verloren gegaan. Virtuele objecten fungeren in het maatschappelijk verkeer kortom als vermogensobject en zijn mitsdien aan te merken als een voor diefstal vatbaar goed. De Hoge Raad heeft daarbij bevestigd dat computergegevens (nog steeds) niet kunnen worden aangemerkt als 'goed', vanwege het feit dat deze gegevens een multiple karakter hebben; HR 31 januari 2012, *LJN* BQ9251. Gegevens ontberen de wezenlijke eigenschap van een goed, namelijk dat degene die de feitelijke macht heeft over een goed deze noodzakelijkerwijs verliest indien een ander zich de feitelijke macht erover verschaft; HR 3 december 1996, *NJ* 1997, 574. De categorieën 'goed' en 'gegevens' lijken elkaar derhalve uit te sluiten.

[439] Koops & Buruma 2007, p. 81.
[440] Zie onder meer artikel 126nd lid 4 Sv en artikel 126nf Sv.
[441] Zie artikel 126n Sv.
[442] *Stb.* 2004, 394.
[443] Koops & Buruma 2007, p. 85.
[444] Koops & Buruma 2007, p. 86.
[445] Koops & Buruma 2007, p. 90.
[446] *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 28.
[447] *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 11-13.

van gegevens mogelijk onder dezelfde voorwaarden als de reguliere doorzoeking.[448] Wanneer de doorzoeking heeft plaatsgevonden en er in dit kader gegevens zijn vastgelegd, dienen de betrokkenen (de verdachte, de verantwoordelijke voor de gegevens en de rechthebbende van de plaats waar de doorzoeking plaatsvond) daarvan op de hoogte te worden gesteld. In kader van een doorzoeking ter vastlegging van gegevens geldt derhalve een notificatieplicht.[449]

5.2.2.1 De netwerkzoeking

De doorzoeking kan op grond van artikel 125j Sv vanaf de plaats waar de doorzoeking plaatsvindt, worden voortgezet in een *elders* aanwezige computer, mits de personen die op de plek van doorzoeking wonen, plegen te werken of te verblijven, met toestemming van de rechthebbende tot zo'n computersysteem elders toegang hebben. Opsporingsautoriteiten hebben derhalve de bevoegdheid om via het geautomatiseerde werk van de aanvankelijke doorzoeking een ander geautomatiseerd werk op afstand te doorzoeken. Dit type onderzoek, in jargon de netwerkzoeking genoemd, is slechts toegestaan, indien de eigenaar van de computer waarop de netwerkzoeking betrekking heeft, de andere computereigenaar heeft toegelaten op zijn geautomatiseerde werk. Er dient derhalve sprake te zijn van enige vorm van toestemming.

Dit toestemmingsvereiste ziet ten eerste op een noodzakelijke juridische band tussen degene bij wie de oorspronkelijke doorzoeking plaatsheeft en de computer elders.[450] Dat wil zeggen dat beide computers op enigerlei wijze aan elkaar verbonden dienen te zijn, bijvoorbeeld middels een netwerkverbinding. Wat hieromtrent in ieder geval geldt, is dat de persoon op wie de doorzoeking in eerste instantie betrekking heeft, de rechtmatige toegang moet hebben tot het geautomatiseerde werk elders. Ten tweede blijkt uit artikel 125j Sv dat er sprake dient te zijn van een feitelijke band tussen de degene bij wie de oorspronkelijke doorzoeking wordt verricht en de locatie waar die doorzoeking plaatsvindt.[451] Het kan derhalve niet zo zijn dat een netwerkzoeking wordt gedaan vanaf de laptop van een toevallige bezoeker of vanaf de smartphone van een dienstdoende schoonmaker. Er dient in dit kader dus sprake te zijn van dubbele binding, aldus Koops & Buruma.[452] Aan beide behandelde vereisten moet aldus worden voldaan.

De uitvoering van een netwerkzoeking kan problematisch zijn. Zo moet de persoon bij wie de oorspronkelijke doorzoeking wordt verricht – zoals is vermeld – de rechtmatige toegang tot de computer elders hebben. Daarmee is niet gezegd dat deze persoon ook de toestemming van de rechthebbende van het geautomatiseerde werk elders heeft om *alle* opgeslagen gegevens op die computer te benaderen. In principe geldt dat wanneer er geen toestemming is gegeven, ook justitie geen toegang tot de bestanden op de computer elders heeft.[453]

Een ander probleem dat speelt bij de inzet van de netwerkzoeking heeft – net als bij hacken door de politie – betrekking op het grensoverschrijdende karakter van de digitale wereld. In verband met het territorialiteitsbeginsel is Nederland bij opsporingsactiviteiten

[448] Koops & Buruma 2007, p. 91.
[449] Wiemans 2004, p. 184 e.v.
[450] Koops & Buruma 2007, p. 94.
[451] Koops & Buruma 2007, p. 94.
[452] Koops & Buruma 2007, p. 94.
[453] Wiemans 2004, p. 151.

gebonden aan landsgrenzen.[454] Dit uitgangspunt is vanwege de grenzeloze aard van het internet echter enigszins achterhaald. Niettemin is strafvorderlijk optreden op het territorium van een vreemde staat niet toegestaan. Netwerkzoekingen mogen dientengevolge slechts plaatsvinden op computers die zich ophouden op ons grondgebied. Het is echter lang niet altijd duidelijk in welk land de gegevens zich op het geautomatiseerde werk bevinden.[455] Daarmee is de mogelijke inzet van de methode beperkt.

5.2.2.2 Het ontsleutelbevel

Bij een doorzoeking zal het regelmatig voorkomen dat een computer beveiligd is. In paragraaf 4.5.3.2 kwam reeds naar voren dat criminelen om hun privacy te waarborgen veelvuldig gebruikmaken van allerlei ingewikkelde versleuteltechnieken. Daarnaast wordt cryptografie steeds vaker standaard ingebouwd in allerlei computerprogramma's.[456] De doorzoekende autoriteit kan, wanneer sprake is van een dergelijk beveiligd geautomatiseerd werk of van versleutelde gegevens op dat werk, degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van beveiliging, bevelen de toegang te verschaffen tot de desbetreffende computer of de gegevens op grond van artikel 125k Sv.[457] Deze bevoegdheid heeft slechts betrekking op het onderzoek ter gelegenheid van een doorzoeking naar gegevens die zijn *opgeslagen* in een geautomatiseerd werk. Dit heeft tot gevolg dat een ontsleutelbevel zowel bij een doorzoeking ter vastlegging van gegevens, als bij een netwerkzoeking kan worden gegeven.[458] Artikel 125k Sv ziet dus niet op het onderzoek naar stromend gegevensverkeer.[459]

Bij een traditionele doorzoeking ter inbeslagneming kan de bevoegdheid overigens niet (meer) worden uitgeoefend, terwijl ook daar zeer regelmatig beveiligde computers – eventueel ter inbeslagname – worden aangetroffen.[460] Koops pleit hieromtrent dan ook om het toepassingsbereik van artikel 125k Sv uit te breiden, zodat ten aanzien van iedere beveiligde computer een decryptiebevel kan worden gegeven.[461]

Zoals is vermeld, kan het bevel worden gericht aan de persoon die beschikt over de benodigde kennis of technieken om te kunnen ontsleutelen. In verband met het nemo-teneturbeginsel kan het decryptiebevel echter niet worden gegeven aan een verdachte in de opsporingsfase.[462] Het verplichten van de verdachte tot medewerking aan ontsleuteling gaat te ver, omdat hiermee de verklaringsvrijheid en het zwijgrecht van deze verdachte in het geding komt.[463] De vraag rijst in hoeverre een dergelijk bevel dan in de praktijk nog bruikbaar is, nu het terecht niet tegen een verdachte kan worden ingeroepen. Ik ben van mening dat het effect van een bevel tot decryptie gering is als het niet aan een verdachte mag worden gericht. De verdachte is immers meestal de enige met kennis van de ontsleutelwijze, omdat hij hoogstwaarschijnlijk degene is die de encryptie – om welke reden dan ook – heeft

[454] Koops & Buruma 2007, p. 94.
[455] Koops & Buruma 2007, p. 94.
[456] Koops 2000, p. 11.
[457] Zie artikel 125k Sv.
[458] Koops 2007, p. 126.
[459] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 24.
[460] Koops & Buruma 2007, p. 95.
[461] Koops 2010, p. 2466.
[462] Artikel 125k lid 3 Sv.
[463] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 26.

aangebracht. Vreemd genoeg wordt deze gedachte in dit kader impliciet bevestigd door de memorie van toelichting, waarin wordt gesteld dat het bij de meeste gevallen van ontsleutelen neerkomt op het vertellen van een slechts in het geheugen van de verdachte opgeslagen code of wachtwoord.[464]

In een ander geval kan het bevel wellicht wel van betekenis zijn. Voor zover een netwerkbeheerder of een aanbieder van een telecommunicatienetwerk kennis draagt van de door een klant toegepaste encryptietechnieken, kan deze worden verplicht die kennis ter beschikking van justitie te stellen.[465]

5.2.3 Het bevriezingsbevel

In paragraaf 3.2.4 is het vluchtige karakter van gegevens op geautomatiseerde werken reeds kort aangestipt. Met name in grensoverschrijdende zaken – waar een rechtshulpverzoek noodzakelijk is ter vergaring van data – zorgt dit aspect dikwijls voor problemen in het opsporingsonderzoek. Ten gevolge hiervan heeft Nederland ter veiligstelling van gegevens bij de Wet computercriminaliteit II als steunmaatregel een bevriezingsbevoegdheid ingevoerd in artikel 126ni Sv.[466] Als er aanwijzingen zijn dat gegevens bijzonder vatbaar zijn voor verlies of wijziging, kan de officier van justitie bevelen dat deze voor een (eenmalig verlengbare) periode van maximaal negentig dagen worden bewaard in de oorspronkelijke vorm. Aansluitend aan de bevriezing kan justitie dan in relatieve rust maatregelen nemen om de gegevens op de gewenste manier te verkrijgen, zoals nadat een officieel rechtshulpverzoek tot ‘uitlevering’ van de gegevens is toegewezen.[467] Ook deze bevoegdheid kan niet worden ingezet tegen de verdachte.[468] Ook in dit geval vraag ik me af wat de kracht van een dergelijk bevel in de praktijk dan is.

5.2.4 Stromende gegevens: de (internet)tap

In het voorgaande gedeelte van dit hoofdstuk lag de nadruk op het statische karakter van de gegevens in relatie tot de digitale opsporingsbevoegdheden. Het ging derhalve om activiteiten in de opsporingsfase ter verkrijging van opgeslagen data op geautomatiseerde werken. Het tappen van communicatie ziet juist op gegevens ‘in transport’, de zogenaamde stromende gegevens. In dit kader geldt voor opgeslagen berichten – bijvoorbeeld in de e-mailinbox van de gebruiker – dus een ander wettelijk kader (vorder- en doorzoekingsbevoegdheden), dan voor de communicatie die onderweg is (tapmogelijkheden).[469] Met betrekking tot het onderwerp van dit onderzoek zal ik me omtrent de tapbevoegdheden voornamelijk richten op de internettap.

Tappen, behorend tot de bevoegdheden in een besloten plaats, is op basis van de artikelen 126m en 126t Sv mogelijk voor ‘niet voor het publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst’.[470] Artikel 126la Sv definieert zo’n aanbieder als ‘de natuurlijke persoon

[464] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 26.
[465] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 24.
[466] Koops & Buruma 2007, p. 97.
[467] Koops 2003, p. 8.
[468] Artikel 126ni lid 1 Sv.
[469] Koops & Buruma 2007, p. 98.
[470] Zie artikel 126m Sv.

of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst'.[471] Een van de gevolgen van deze bepaling is dat het aftappen van interne netwerken van bijvoorbeeld bedrijven en ministeries of thuisnetwerken niet mogelijk is, vanwege het gedeelte 'in de uitoefening van een beroep of bedrijf' in de strafvorderlijke bepaling. Via dergelijke netwerken kan – zonder gebruik te maken van een internetaansluiting – tussen computers onderling worden gecommuniceerd of kunnen gegevens worden uitgewisseld.

Via de artikelen 126m en 126t Sv kunnen naast vaste of mobiele telefoongesprekken tevens elektronische post, chatverkeer en webcamerabeelden worden afgetapt.[472] Het maakt sinds 2006 niet uit of dergelijke vormen van communicatie in beslotenheid plaatsvinden.[473] Vanwege de ingrijpendheid van de opsporingsbevoegdheid is naast de beslissing van de officier van justitie tot het inzetten van een tap, ook de machtiging van de rechter-commissaris nodig.[474] Ook bij afgetapte gegevens kan een decryptiebevel worden gegeven op grond van artikel 126m lid 6 Sv. Deze medewerkingsplicht geldt opnieuw niet voor de verdachte.[475]

Het aftappen van communicatie is een bijzonder populaire opsporingsmethode. Waar voorheen met behulp van de telefoontap allerlei relevante informatie over criminele activiteiten werd verzameld, vindt er op dit moment een kentering plaats bij de inzet van deze opsporingsbevoegdheid.[476] In 2010 werd 22.006 keer een tapbevel afgegeven. Dat is ten opzichte van het jaar ervoor een daling van elf procent.[477] Deze terugloop vindt zijn oorzaak in het feit dat de telefoontap steeds minder direct bewijs oplevert. Dit wordt ten dele veroorzaakt doordat het criminele circuit bewust rekening houdt met de mogelijkheid dat er kan worden getapt en dat men op grond hiervan niet meer vrijuit praat over de telefoon en dientengevolge mogelijk alternatieve communicatievormen zoekt. Een voorbeeld hiervan is communiceren via internet met VoIP.[478] Eerder werd in paragraaf 4.5.3.2 al gerefereerd aan het feit dat communicatie via *Skype*, een van de beter bekende VoIP-programma's, door versleutelingstechnieken niet of nauwelijks kan worden afgeluisterd. Een dergelijke manier van het voeren van gesprekken belemmert het opsporingsonderzoek daarom in grote mate.

Toch wordt de internettap steeds vaker ingezet. Met behulp van deze bevoegdheid kunnen alle gegevens worden onderschept die van en naar een bepaald IP-adres lopen. Het gaat dan voornamelijk om communicatie via het internet.[479] Indien specifiek verkeer er niet wordt uitgefilterd, komt al het internetverkeer mee dat vanuit een bepaalde IP-adres wordt gegenereerd, zoals zoektermen die in *Google* worden ingetypt, chatberichten die onversleuteld over en weer worden verstuurd en *YouTube*-fragmenten die via internet worden bekeken.[480] Obstakels in het opsporingsonderzoek ten gevolge van het grensoverschrijdende karakter van het internet – *Google* en *YouTube* zijn immers van Amerikaanse origine – zijn er

[471] Artikel 126la Sv.
[472] Koops & Buruma 2007, p. 99.
[473] *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 25 e.v. en 29.
[474] Artikel 126m lid 5 Sv.
[475] Zie artikel 126m lid 6 jo. lid 7 Sv.
[476] Odinot & De Jong 2012, p. 10.
[477] Odinot e.a. 2012, p. 81.
[478] Odinot & De Jong 2012, p. 10.
[479] Odinot & De Jong 2012, p. 13.
[480] Oerlemans 2012, p. 21.

in principe niet. Een internettap wordt geplaatst op een Nederlands IP-adres.[481] Hier is dus geen sprake van strafvorderlijk optreden op het grondgebied van een andere staat.

De internettap kan tevens worden beperkt tot het onderscheppen van binnenkomende e-mailberichten. Een dergelijke bevoegdheid wordt in het jargon de e-mailtap genoemd.[482] E-mail is goed te tappen bij een aanbieder. Hieromtrent rijzen echter wel weer territoriale complicaties. Veel internetgebruikers hebben namelijk een e-mailaccount bij webmaildiensten zoals *Hotmail*, *Gmail* of *Yahoo!*, waarvan de aanbieder een buitenlands bedrijf is. In dat geval is een internationaal rechtshulpverzoek nodig om inzage in deze communicatie te krijgen.[483]

Communicatie via smartphones kan overigens ook met behulp van de internettap worden opgenomen, waardoor bijvoorbeeld boodschappen die via de populaire berichtenapplicatie voor mobiele telefoons *WhatsApp* standaard onversleuteld worden verstuurd daarmee voor de opsporingsautoriteiten zichtbaar worden.[484] Voor het enkel aftappen van telefoongesprekken op deze populaire mobiele telefoons hoeft uitsluitend een telefoontap te worden gebruikt.[485]

De inzet van internettaps is door de toenemende afhankelijkheid van mensen van communicatie via het World Wide Web explosief gestegen. Vooral het groeiend aantal smartphones blijkt een belangrijke drijfveer te zijn achter de toenemende inzet van deze opsporingsmethode.[486] In 2005 werden nog maar zevenentwintig tapbevelen uitgevaardigd.[487] Dat aantal is in 2010 gestegen naar 1.704 IP-taps (zowel internet- als e-mailtaps).[488] Op het moment van schrijven (augustus 2012) zijn nog geen cijfers over 2011 bekend.

5.2.4.1 Beperkingen internettap

Toch is de inzet van de internettap aan enkele beperkingen gebonden. Een van die restricties heeft betrekking op de vraag *aan wie* de aftaplast kan worden opgelegd.[489] Artikel 126m lid 1 Sv bepaalt dat de officier van justitie een opsporingambtenaar kan bevelen bepaalde communicatie af te vangen.[490] Wanneer het echter gaat om het aftappen van *openbare* communicatie dient het aftapbevel ingevolge artikel 126m lid 3 Sv te worden gericht aan een aanbieder van een openbaar telecommunicatienetwerk of een aanbieder van een openbare telecommunicatiedienst in de zin van artikel 1.1 onder ee en ff van de Telecommunicatiewet, tenzij dat technisch niet mogelijk is of het belang van strafvordering zich daartegen verzet.[491] Aanbieders van openbare telecommunicatie zijn op basis van artikel 13.2 Tw verplicht hun medewerking te verlenen aan een dergelijk bevel.[492] Het is in dit kader echter (nog) niet duidelijk wat onder een *openbare* telecommunicatiedienst dient te worden

[481] Odinot e.a. 2012, p. 75.
[482] Odinot e.a. 2012, p. 155.
[483] Odinot e.a. 2012, p. 52.
[484] Oerlemans 2012, p. 22.
[485] Odinot e.a. 2012, p. 155.
[486] Odinot & De Jong 2012, p. 13.
[487] Zie http://www.nbip.nl/nieuws/nbip-heeft-tachtig-deelnemers/.
[488] *Kamerstukken II* 2010/11, 32 710, nr. 1, p. 67.
[489] Oerlemans 2012, p. 28.
[490] Zie art. 126m lid 1 Sv.
[491] Zie art. 126m lid 3 Sv.
[492] Artikel 13.2 Tw.

verstaan. Evident is in ieder geval dat diensten die uitsluitend beschikbaar zijn voor leden van een 'besloten gebruikersgroep' geen openbare telecommunicatiediensten zijn.[493]

Ook over het begrip telecommunicatie*dienst* bestaat thans nog veel onduidelijkheid. Zo is het bijvoorbeeld de vraag of de programma's *Skype*, *Gmail* of *Hotmail* onder dit begrip kunnen worden geschaard.[494] Onder een telecommunicatiedienst wordt een 'voor het publiek beschikbare dienst die geheel of gedeeltelijk bestaat in het overbrengen van signalen via een elektronisch communicatienetwerk, voor zover deze dienst niet bestaat uit het verspreiden van programma's' verstaan.[495] Oerlemans lijkt er in ieder geval vanuit te gaan dat aan deze communicatieaanbieders geen taplast kan worden gegeven. Zo maakt *Skype* gebruik van een bestaande telecommunicatie-infrastructuur en verzorgt daarbij niet grotendeels het overbrengen van signalen.[496] Met betrekking tot *Gmail* en *Hotmail* heeft Hirsch Ballin als toenmalige minister van Justitie bevestigd dat ze niet als aanbieders van een openbare telecommunicatiedienst in de zin van de Telecommunicatiewet kunnen worden aangemerkt.[497]

Zelfs al neemt men wel aan dat dergelijke aanbieders van telecommunicatie verplicht kunnen worden tot het medewerken aan een tapbevel, dan speelt bij voorgaande voorbeelden ook het probleem dat ze in het buitenland zijn gevestigd.[498] Opsporingsactiviteiten buiten Nederlands grondgebied zijn in beginsel zonder rechtshulpverzoek niet toegestaan.[499]

Tevens leiden technologische ontwikkelingen tot een beperking van de effectiviteit van de internettap.[500] Hiervoor noemde ik al kort het probleem van versleuteling. Ook al kan op grond van artikel 126m lid 6 Sv een decryptiebevel worden uitgevaardigd en ligt deze plicht tot ontsleuteling volgens de memorie van toelichting ook nog eens besloten in de taplast[501], het verkeer kan in veel gevallen niet worden ontcijferd. Dat komt doordat communicatie vaak door tussenliggende diensten wordt versleuteld en deze instanties in de meeste gevallen niet aan een taplast hoeven te voldoen. Daar komt bij dat deze diensten zich meestal in het buitenland bevinden.[502]

Hoewel er diverse beperkingen kleven aan de internettap, is wel te verwachten dat deze opsporingsbevoegdheid in toenemende mate zal worden ingezet. Ook al kan niet alle inhoudelijke communicatie worden afgevangen, opsporingsautoriteiten kunnen wel uit de kenmerken van het gegevensverkeer relevante informatie afleiden. Deze zogeheten verkeersgegevens kunnen als bewijsmateriaal dienen, omdat ze informatie kunnen geven over gedragingen van verdachten en aanknopingspunten kunnen bieden voor verder onderzoek.[503]

---

[493] Zie in dit kader Rb. Rotterdam 27 maart 2009, *LJN* BH9324.
[494] Oerlemans 2012, p. 25.
[495] Zie artikel 1.1ff Tw.
[496] Oerlemans 2012, p. 25.
[497] *Kamerstukken II* 2007/08, 31 145, nr. 9, p. 6.
[498] Oerlemans 2012, p. 27.
[499] Daarbij moet met betrekking tot aftappen wel worden opgemerkt dat er binnen de Europese Unie enige afspraken zijn gemaakt omtrent rechtshulp; Oerlemans 2012, p. 27.
[500] Oerlemans 2012, p. 28 e.v.
[501] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 24.
[502] Oerlemans 2012, p. 29.
[503] Oerlemans 2012, p. 37 e.v.

5.2.5 Stromende gegevens: het opnemen van vertrouwelijke communicatie

Het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel, ook wel direct afluisteren genoemd, is als wettelijke bevoegdheid geïntroduceerd in artikel 126l Sv.[504] Voor misdrijven in georganiseerd verband is artikel 126s Sv van toepassing.[505] Deze opsporingsbevoegdheid is een vergaande bevoegdheid en is door de wetgever om die reden met strikte waarborgen omkleed.[506]

Vertrouwelijke communicatie verwijst naar de uitwisseling van berichten tussen twee of meer personen die in beslotenheid plaatsvindt.[507] In dat kader kan worden gedoeld op het geschreven of gesproken woord, zoals een in beslotenheid gevoerd gesprek.[508] De wetgever heeft echter bij direct afluisteren niet alleen aan communicatie in de reële wereld gedacht, zo blijkt uit de memorie van toelichting. Daar wordt beargumenteerd dat de bevoegdheid ook betrekking heeft op bijvoorbeeld niet-openbaar e-mailverkeer.[509] Wat omtrent het begrip vertrouwelijke communicatie vaststaat, is dat er altijd sprake moet zijn van het communiceren met een ander (of met een ander apparaat). Informatie die de betrokkene uitsluitend in zijn computer invoert, kan derhalve niet worden opgenomen.[510]

De bevoegdheid tot het opnemen van vertrouwelijke communicatie omvat meer dan de bevoegdheid tot het opnemen van communicatie op grond van artikel 126m Sv (de telecommunicatietap). Dit betekent dat technische apparatuur mag worden geplaatst waarmee direct kan worden afgeluisterd.[511] Het afvangen van deze communicatie ex artikel 126l en artikel 126s Sv kan tijdens een huiszoeking – het betreden van de woning als steunbevoegdheid – geschieden door het gebruik van richtmicrofoons of het plaatsen van een *bug*, een verborgen microfoontje.[512] Bugs zijn in staat om gesprekken duidelijk op te nemen of uit te zenden naar een bepaalde plaats waar de gesprekken kunnen worden beluisterd of opgenomen.[513] Het verborgen apparaatje kan volgens de memorie van toelichting bijvoorbeeld op een lamp worden geplaatst, maar ook op een toetsenbord of muis van een computer.[514] Op deze manier kunnen toetsaanslagen of muisklikken van de verdachte worden geregistreerd. Dit wordt ook wel *hardwarematige keylogger* genoemd.[515] Met de inzet van de bug kunnen, door het afvangen van toetsaanslagen, gegevens worden onderschept nog voordat ze worden verzonden of door versleuteling onbegrijpelijk zijn geworden.[516] Men kan in dit kader denken aan het onderscheppen van wachtwoorden en encryptiesleutels.[517] Met het opnemen hoeft dus niet te worden gewacht totdat de gegevens deel uitmaken van communicatie.[518] De bevoegdheid opent de mogelijkheid data te onderscheppen nog voor er

---

[504] Koops & Buruma 2007, p. 110.
[505] Zie artikel 126s Sv.
[506] Beijer e.a. 2004, p. 64.
[507] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 36.
[508] Koops & Buruma 2007, p. 110.
[509] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 36.
[510] Corstens 2011, p. 433.
[511] Koops & Buruma 2007, p. 111.
[512] Oerlemans 2011a, p. 902.
[513] Verbeek, De Roos & Van den Herik 2000, p. 25.
[514] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 35.
[515] Oerlemans 2011a, p. 902.
[516] Corstens 2011, p. 433.
[517] Koops & Buruma 2007, p. 111.
[518] Kamerstukken II 1996/97, 25 403, nr. 3, p. 35 e.v.

wordt gecommuniceerd. De eis dat de bevoegdheid beperkt blijft tot gesprek*sverkeer* houdt in deze opvatting dus geen inhoud meer over. De memorie van toelichting stelt in dit verband daarom dat er geen bug kan worden geplaatst op een computer die niet is aangesloten op een netwerk, omdat dan redelijkerwijze bekend kan zijn dat er geen communicatie zal kunnen worden opgenomen.[519] Afgezien van het feit dat elke computer in elk geval potentieel deel uitmaakt van een netwerk, is dit een in de praktijk niet hanteerbaar onderscheid.[520]

5.2.5.1 Softwarematige keylogger

Ondanks dat de memorie van toelichting er met geen woorden over rept, zijn Verbeek, De Roos & Van den Herik van mening dat er tevens gebruik kan worden gemaakt van een *softwarematige keylogger*.[521] De bug is dan in dit geval een vorm van speciale software, waarmee elektronische communicatie in computernetwerken kan worden opgenomen.[522] De auteurs stellen dat de artikelen 126l en 126s Sv voldoende ruimte bieden om een dergelijke bevoegdheid hieronder te brengen.[523] Op deze manier kan tijdens een huiszoeking software op de computer van de verdachte worden geïnstalleerd, waarmee bijvoorbeeld wachtwoorden kunnen worden onderschept.[524]

Ook Koops & Buruma achten het gebruik van de softwarematige keylogger gepermitteerd. Zij stellen dat de politie bij direct afluisteren op grond van artikel 126l Sv een woning mag betreden om op de harde schijf een technisch hulpmiddel te plaatsen dat direct afluisteren realiseert. De auteurs menen, dat het in dit kader mogelijk is om op deze wijze bepaalde software (een Trojaans politiepaard) op de computer te zetten die een 'achterdeur' inbouwt op die computer, zodat justitie vervolgens via een netwerk rechtstreeks kan meekijken wanneer de verdachte gebruiker iets intikt. Dat meekijken dient wel plaats te vinden op grond van het opnemen van vertrouwelijke communicatie, zodat de opsporingsautoriteiten zich zullen moeten beperken tot het ophalen van het versleutelde wachtwoord dat het Trojaanse politiepaard heeft onderschept, of tot onderzoek van de inbox van een e-mailaccount gekoppeld aan de harde schijf.[525]

Zeer recentelijk heeft minister Opstelten in dit kader ook bevestigd dat een technisch hulpmiddel een softwareprogramma op de computer van de verdachte kan zijn.[526]

Groot voordeel van deze opsporingsbevoegdheid ten opzichte van bijvoorbeeld de internettap is dat gegevensverkeer direct op de computer zelf kan worden gekopieerd en met de software kan worden doorgestuurd naar de politie. Op die manier kan communicatie worden afgevangen voordat versleuteling plaatsvindt en daardoor kan het probleem van encryptie worden omzeild. De software kan daarnaast – zoals hiervoor reeds behandeld – ook toetsaanslagen, waaronder wachtwoorden, registreren en doorsturen. Met deze opgevangen wachtwoorden kan eventuele versleuteling ongedaan worden gemaakt.[527]

---

[519] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 35.
[520] Blom 2011, p. 491.
[521] Verbeek, De Roos & Van den Herik 2000, p. 155.
[522] Verbeek, De Roos & Van den Herik 2000, p. 21.
[523] Verbeek, De Roos & Van den Herik 2000, p. 155.
[524] Oerlemans 2011a, p. 902.
[525] Koops & Buruma 2007, p. 118.
[526] *Kamerstukken II* 2011/12, 7 februari 2012, Antwoord op Kamervragen van de D66 Kamerleden Schouw en Berndsen van de minister van Veiligheid en Justitie, aanhangselnummer 1374, p. 1 e.v.
[527] Oerlemans 2012, p. 36.

In principe plegen opsporingsautoriteiten door het gebruik van de softwarematige keylogger op grond van artikel 126l Sv het strafbare feit computervredebreuk. Er wordt immers – met behulp van speciale software – ingebroken op de harde schijf van een betrokkene.[528] Deze manier van hacken kan mijns inziens worden afgeleid van de toegestane methode ex artikel 126l Sv. Dit artikel biedt echter geen grondslag voor het via een netwerk of via internet – dus *op afstand* – binnendringen van een computer, zoals dat op dit moment wel door politie en justitie wordt gewenst.[529] De opsporingsautoriteiten hebben derhalve niet de bevoegdheid om met de softwarematige keylogger afgevangen wachtwoorden in te loggen op de e-mailinbox van een verdachte. Op die manier wordt immers op afstand op een ander geautomatiseerd werk binnengedrongen. Voor die handeling is de politie op grond van artikel 126l Sv in ieder geval niet geautoriseerd.[530] In dit kader rijst de vraag welke manier van opsporen in dit kader de voorkeur heeft: hacken op afstand of op grond van artikel 126l Sv. Daarover volgt in paragraaf 6.2 meer.

5.3 Overige vormen van digitaal rechercheren

Volgens artikel 126g Sv kan de officier van justitie een opsporingsambtenaar bevelen stelselmatig[531] een persoon te volgen of stelselmatig diens aanwezigheid of gedrag waar te nemen.[532] De wetgever heeft het belang van deze bevoegdheid in de digitale wereld niet genoemd.[533] Schermer is in dit kader van mening dat het irrelevant is of bepaald gedrag zich online of offline manifesteert.[534] Deze opmerking is mijns inziens terecht. Zoals ik reeds eerder heb betoogd, spelen geautomatiseerde werken in de huidige gedigitaliseerde samenleving een aanzienlijke rol. Dat komt mede tot uitdrukking in de totstandkoming van allerlei vormen van strafrechtelijk te verwijten gedrag op het internet. Men kan in dit kader denken aan de verspreiding van kinderporno. Het opsporen van dergelijk strafbaar handelen kan middels de bevoegdheid van stelselmatige observatie. Ook Koops en Buruma vinden dat deze opsporingsactiviteit een digitale rol kan spelen. Zo achten de auteurs stelselmatige observatie op het internet soms noodzakelijk.[535] In beginsel kunnen opsporingsambtenaren – net zoals de ‘gewone burger’ – vrijelijk rondkijken op het internet en weergeven wat zich daar afspeelt.[536] Wanneer dergelijk snuffelen op internet stelselmatige vormen gaat aannemen en specifiek op een bepaald persoon wordt geconcentreerd, zal hiervoor een bevel van de officier van justitie op grond van artikel 126g Sv nodig zijn.[537] Op die manier kan immers een ‘min of meer volledig beeld worden geschetst van bepaalde aspecten van iemands leven’, aldus de memorie van toelichting bij de totstandkoming van de Wet BOB.[538]

---

[528] Koops & Buruma 2007, p. 118.
[529] Koops & Buruma 2007, p. 118.
[530] Oerlemans 2011a, p. 903.
[531] Er is sprake van stelselmatigheid indien een ‘min of meer volledig beeld van bepaalde aspecten van iemands leven wordt verkregen.’; *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 26.
[532] Artikel 126g Sv.
[533] Koops & Buruma 2007, p. 113.
[534] Schermer 2003, p. 53.
[535] Koops & Buruma 2007, p. 113.
[536] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 38.
[537] Koops & Buruma 2007, p. 113.
[538] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 26.

Andere digitale opsporingsmethoden zijn het stelselmatig inwinnen van informatie over personen op het internet, politiële infiltratie en pseudo-acties. Een uitgebreide behandeling van deze bevoegdheden is met het oog op het onderwerp van dit onderzoek niet op zijn plaats. De drie vormen van digitaal rechercheren zullen dientengevolge kort worden aangestipt.

Op grond van artikel 126j Sv kan een opsporingsambtenaar op bevel van de officier van justitie stelselmatig, zonder dat kenbaar is dat hij als opsporingsambtenaar optreedt, onder een dekmantel deelnemen aan bijvoorbeeld een nieuwsgroep op internet of chatten met bepaalde gebruikersgroepen (stelselmatige inwinning van informatie).[539] Stol, Leukfeldt & Klap noemen in dit kader als voorbeeld het in kaart brengen van iemands sociale netwerk in cyberspace.[540]

Verwant aan het stelselmatig inwinnen van informatie is de bevoegdheid van politiële infiltratie op grond van artikel 126h Sv. Het gaat bij deze methode om het deelnemen of medewerking verlenen aan een groep van personen waarbinnen, naar redelijkerwijs kan worden vermoed, misdrijven worden beraamd of gepleegd. Het optreden van de infiltrant kan, bijvoorbeeld om zijn geloofwaardigheid niet te verliezen, het plegen van strafbare feiten omvatten. Hij zal immers om niet uit de toon te vallen en om niet te worden ontmaskerd de kleur van het milieu moeten aannemen.[541] Dat kan ook in een digitale omgeving. Zo kan een opsporingsambtenaar onder een valse identiteit op het internet verdachten of derden misleiden of zelfs strafbare feiten plegen.[542]

De pseudokoop of -dienstverlening kan een onderdeel van infiltratie vormen, maar onderscheid zich hiervan, omdat de opsporingsambtenaar zich bij de pseudoactiviteiten laat beperken tot het eenmalig plegen van een strafbaar feit in tegenstelling tot het mogelijk langdurig vertonen van strafbaar gedrag bij infiltratie.[543] Pseudokoop of -dienstverlening kan ook zonder infiltratie plaatsvinden, indien het strafbare feit buiten een criminele groepering om wordt gepleegd.[544] Wanneer via het internet bepaalde goederen worden afgenomen, spreekt men van online pseudokoop.[545]

5.4 De inkijkoperatie

Een van de bevoegdheden in een besloten plaats naast de hiervoor behandelde telecommunicatietap – in opsporingsjargon ook wel de inkijkoperatie genoemd – is in de artikelen 126k en 126r Sv geregeld, waarbij het in artikel 126k Sv om opsporing in klassieke zin gaat, dus na het ontstaan van een verdenking dat een strafbaar feit is gepleegd en in artikel 126r Sv om proactieve opsporing, na verdenking van misdrijven gepleegd in georganiseerd verband.[546] In het laatste geval hoeft er derhalve nog geen concreet strafbaar feit te hebben plaatsgevonden.[547] De bevoegdheid strekt tot het heimelijk binnentreden in een besloten

[539] Koops & Buruma 2007, p. 114.
[540] Stol, Leukfeldt & Klap 2012, p. 30.
[541] Corstens 2011, p. 456.
[542] Schermer 2003, p. 54.
[543] Koops & Buruma 2007, p. 115.
[544] Corstens 2011, p. 457.
[545] Schermer 2003, p. 55.
[546] Boek 2000, p. 592.
[547] Corstens 2011, p. 246.

plaats om aldaar de plaats op te nemen, sporen veilig te stellen of een technisch hulpmiddel te plaatsen ten einde de aanwezigheid of verplaatsing van een goed te kunnen vaststellen.[548]

Met betrekking tot dit onderzoek rijst de vraag of een softwareprogramma (een Trojaans politiepaard) – waarvan het gebruik in principe noodzakelijk is voor het zetten van een hack door opsporingsautoriteiten – moet worden betiteld als een technisch hulpmiddel. De memorie van toelichting behandelt de reikwijdte van het begrip zeer summier.[549] Buruma geeft aan dat een *cookie*[550] als een technisch hulpmiddel kan worden bestempeld, welke opsporingsautoriteiten zouden kunnen inzetten bij de observatie van iemand die zich op het internet begeeft.[551] Boek trekt de conclusie dat een speciaal softwareprogramma waarmee een computer kan worden gehackt daarmee ook als technisch hulpmiddel kan worden aangemerkt.[552] Overigens wordt het gebruik van cookies in de opsporingsfase bemoeilijkt door recente wetswijzigingen op dit gebied. De aangepaste bepalingen in de Telecommunicatiewet bepalen dat cookies alleen mogen worden geplaatst op voorwaarde dat de gebruiker van de randapparatuur daarvoor toestemming heeft gegeven en nadat hij is voorzien van duidelijke en volledige informatie.[553] Dit heeft gevolgen voor de opsporingsautoriteiten. Gegevens van (verdachte) gebruikers zijn immers niet standaard meer beschikbaar voor de politie.

De andere in het kader van de inkijkoperatie relevante voorwaarde – naast het vereiste van een technisch hulpmiddel – ziet op de besloten plaats. Dit begrip verwijst niet naar een woning, maar naar een niet-openbare en niet voor ieder toegankelijke plaats, zoals een kantoor, een loods of een garage.[554] De wetgever heeft de bevoegdheid tot inkijken aldus beperkt tot plaatsen die geen woning zijn. Daartoe werd in de memorie van toelichting aangevoerd dat woningen de plaatsen zijn waar men bij uitstek onbevangen zichzelf kan zijn. De redenen die – met het oog op inkijken – kunnen worden genoemd omtrent het mogelijk maken van het betreden van woningen, wegen niet op tegen het belang van de bescherming van dit huisrecht, aldus de memorie van toelichting.[555] Boek beredeneert dat de harde schijf van een computer ook als besloten plaats kan worden gekwalificeerd. Hij trekt daaruit de conclusie dat hacken onder voorwaarden op grond van artikel 126k Sv is gelegitimeerd. Dit komt op mij als ‘gekunsteld’ over, zoals ik zal betogen in paragraaf 6.2.

---

[548] Artikel 126k lid 1 Sv.
[549] *Kamerstukken II* 1997/98, 25 403, nr. 7, p. 79.
[550] Cookies zijn kleine tekstbestanden die bij het surfen over internet op de computer van de gebruiker worden geplaatst. Cookies maken het mogelijk om de computer waarop het cookie is geplaatst tijdens het surfen of bij een volgend bezoek van een website te herkennen. Met behulp van deze kleine tekstbestanden kunnen allerlei gegevens worden verzameld en onthouden. Daaronder valt tevens het (surf)gedrag van de gebruiker op het internet; Antic 2012, p. 103.
[551] Buruma 1998, p. 182 e.v.
[552] Boek 2000, p. 592.
[553] Antic 2012, p. 104.
[554] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 40 en 77.
[555] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 43.

5.5 Hacken door de inlichtingen- en veiligheidsdiensten

De Wiv 2002 omschrijft de taken en regelt de bevoegdheden van de AIVD en MIVD. De beide diensten hebben een aantal taken in het belang van de nationale veiligheid.[556] Om die nationale veiligheid te kunnen bewaken, heeft de Wiv 2002 in tegenstelling tot het Wetboek van Strafvordering wel een expliciete mogelijkheid geschapen om te kunnen hacken.[557] De AIVD en de MIVD zijn in dit kader bevoegd om al dan niet met gebruikmaking van technische hulpmiddelen, valse signalen, valse sleutels of een valse hoedanigheid, binnen te dringen in geautomatiseerde werken.[558] Tot deze bevoegdheid behoort tevens het ongedaan maken van versleuteling en het overnemen van computergegevens.[559]

5.6 Toekomst naar aanleiding van het conceptwetsvoorstel 'versterking bestrijding computercriminaliteit'

De voortschrijdende ontwikkeling en toepassing van informatietechnologie heeft geresulteerd in de totstandkoming van een aantal opsporingsbevoegdheden, waarmee delicten in een digitale omgeving kunnen worden opgespoord.[560] Toch zorgt de snelle technologische ontwikkeling voor snel verouderde wetgeving. Als gevolg hiervan acht men het noodzakelijk een aantal wetswijzigingen op het gebied van opsporing door te voeren.[561] Deze aanpassingen van het Wetboek van Strafvordering worden met het conceptwetsvoorstel 'versterking bestrijding computercriminaliteit' geadresseerd. Daarbij dient te worden aangetekend dat de wijzigingen niet zien op een uitbreiding van (bijzondere) opsporingsbevoegdheden.[562] Doelstelling van het conceptwetsvoorstel is wel het bieden van een ruimere strafrechtelijke bescherming van computergegevens ter bescherming van de persoonlijke levenssfeer van burgers en van vertrouwelijke communicatie, aldus de memorie van toelichting.[563] In paragraaf 1.2.1.1 werd het voorstel al kort aangestipt.

De belangrijkste wijziging binnen het formele strafrecht is de creatie van een nieuwe bevoegdheid voor de officier van justitie tot het afgeven van een bevel tot Notice-and-Take-Down (NTD) op grond van het voorgestelde artikel 125p Sv.[564] Met een dergelijk bevel kunnen communicatieaanbieders in kennis worden gesteld (de 'notice') van illegaal of onrechtmatig materiaal. Vervolgens kunnen ze worden gedwongen dit materiaal van het internet te verwijderen (de 'take down').[565] Deze wijziging biedt een versterking voor de strafvorderlijke overheid met betrekking tot het ontoegankelijk maken van gegevens op het internet ten opzichte van de huidige situatie. Het grootste probleem wordt hier op het gebied van cybercrime echter niet mee geadresseerd. De achtergrond van de invoering van deze

[556] Ministerie van Veiligheid en Justitie 2011, p. 16.
[557] Boek 2000, p. 593.
[558] Zie artikel 24 lid 1 Wiv 2002.
[559] Zie artikel 24 lid 1 sub b en c Wiv 2002.
[560] Schermer 2003, p. 51
[561] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 2.
[562] Oerlemans 2010, p. 148.
[563] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 2.
[564] Oerlemans 2010, p. 148.
[565] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 4.

bevoegdheid lijkt de bestrijding van kinderporno te zijn, althans het invoeren van een mogelijkheid tot het verwijderen van afbeeldingen van kinderporno van het internet.[566] Het probleem is echter niet zozeer het weghalen van kinderpornografisch materiaal van het web, als wel dat die strafbare informatie of anderszins strafrechtelijk verwijtbare cybergedragingen momenteel vaak niet of nauwelijks te traceren zijn. Dit hangt samen met de problemen omtrent anonimiteit en versleuteling.[567] De creatie van een nieuwe bevoegdheid tot het afgeven van een NTD-bevel lijkt in die zin dus meer van symbolische aard. De bestrijding van kinderporno op het internet is immers een 'hot topic'.[568]

Dat de invoering van een NTD-bevel voornamelijk een symbolisch karakter heeft, neemt niet weg dat de wetgever met betrekking tot het ontoegankelijk maken van gegevens op het internet wel een stap vooruit zet. Op dit moment kan de officier van justitie op grond van artikel 125o Sv op een computer aangetroffen onrechtmatige of strafbare gegevens ontoegankelijk maken en vernietigen.[569] Daarbij gaat het om situaties waarin *bij een doorzoeking* dergelijke gegevens worden aangetroffen. Indien de gegevens voor het publiek toegankelijk zijn en zo worden aangetroffen op het internet, kan de bevoegdheid tot het ontoegankelijk maken niet worden toegepast.[570] Met betrekking tot het verwijderen van strafbaar materiaal op het internet biedt deze regeling dus geen soelaas.

Onze huidige strafwet geeft de officier van justitie wel de mogelijkheid om op grond artikel 54a Sr een bevel tot NTD uit te vaardigen.[571] De formulering van het artikel is echter zodanig belabberd, dat het bevel niet rechtmatig is. Er kleven aan artikel 54a Sr dermate tekstuele, wethistorische, wetsystematische en rechtsbescherming bezwaren, dat het niet kan worden toegepast.[572]

Doordat deze juridische mogelijkheid onbruikbaar is en de bevoegdheid ex artikel 125o Sv niet van toepassing is, bestaat er op dit moment slechts een niet-afdwingbare methode om strafbare of onrechtmatige gegevens van het internet te verwijderen. In dit kader is op basis van vrijwilligheid namelijk een gedragscode 'Notice and Take Down' opgesteld en ondertekend. Deze gedragscode richt zich op groot aantal internetproviders die, wanneer er sprake is van onmiskenbaar onrechtmatige of strafbare inhoud op het internet, ervoor zorgt dat de betreffende inhoud onverwijld wordt verwijderd.[573] De communicatieaanbieders bepalen derhalve zelf of materiaal van het internet ontoegankelijk moet worden gemaakt.[574]

---

[566] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 4.
[567] Zie voor meer informatie over versleuteling en anonimiteit paragraaf 4.5.3.1 en 4.5.3.2.
[568] De overheid heeft zich voor het jaar 2015 tot doel gesteld dat er vijfentwintig procent meer verdachten door de politie voor vervolging bij het Openbaar Ministerie moeten worden aangeleverd. In dat kader dienen er vijfenzeventig extra politiemensen te worden ingezet, dient een landelijke aanpak van kinderporno te worden gerealiseerd en dient een landelijk expertisecentrum voor kinderporno te worden opgericht; zie http://www.rijksoverheid.nl/onderwerpen/kinderporno/bestrijding-kinderporno.
[569] Zie artikel 125o Sv.
[570] Koops & Buruma 2007, p. 96.
[571] Artikel 54a Sr.
[572] Oerlemans 2011b, p. 8.
[573] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 4.
[574] Er mag slechts tot deze conclusie worden gekomen, indien er sprake is van 'onmiskenbare onrechtmatige of strafbare informatie'. Wanneer deze beoordeling aan de internetproviders wordt gelaten, bestaat de kans dat ze uit angst voor procedures of onwetendheid over de strafbaarheid of onrechtmatigheid van het materiaal ook *recht*matig materiaal van het internet verwijderen; Oerlemans 2010, p. 149. Deze huidige regeling kan mogelijk zelfcensuur tot gevolg hebben of kan daarnaast de aanleiding vormen voor aansprakelijkheidsprocedures; Van den Hoven van Genderen 2008, p. 323.

Deze verwijdering van de gegevens ziet op het offline halen van de informatie met behoud van een kopie ten behoeve van strafvordering.[575] Daarnaast kunnen onrechtmatige of strafbare gegevens ook worden gefilterd of geblokkeerd.[576] Wanneer internetproviders of andere aanbieders binnen deze bedrijfstak niet bereid zijn op basis van de gedragscode de gegevens ontoegankelijk te maken, kan de nieuwe bevoegdheid van de officier van justitie dergelijke dienstverleners hiertoe dwingen en daarmee strafbare feiten beëindigen of nieuwe strafbare feiten voorkomen.[577] Om de vordering kracht bij te kunnen zetten is in het voorgestelde 125q Sv voorzien in de mogelijkheid zo nodig een dwangsom op te leggen voor gevallen waarin niet aan de vordering van de officier van justitie wordt voldaan. Deze mogelijkheid wordt als een effectievere spreekwoordelijke 'stok achter de deur' gezien, dan het instellen van strafvervolging, hetgeen mogelijk is op grond van artikel 184 Sr waarin het niet voldoen aan een bevoegd gegeven ambtelijk bevel strafbaar is gesteld.[578] Dat komt mede doordat het laatste meer inspanning, tijd en middelen vergt en bovendien het risico van imagoschade met zich meebrengt, indien de rechter zou oordelen dat de gewraakte inhoud toch niet strafbaar zou zijn, aldus Koops.[579]

5.6.1 Kritiek NTD-bevel

Op het creëren van de mogelijkheid tot het uitvaardigen van een NTD-bevel wordt veel kritiek geuit. Zo vraagt Oerlemans zich af of het wenselijk is om zoveel macht bij het Openbaar Ministerie te leggen.[580] Een dergelijk bevel staat immers op gespannen voet met de vrijheid van meningsuiting. De waarborg van een machtiging van een rechter-commissaris acht hij daarom wenselijk.[581]

Daar wil ik omtrent de rol van het Openbaar Ministerie het volgende aan toevoegen: de nieuwe regeling lijkt te veronderstellen dat het Openbaar Ministerie eerder achter het bestaan van strafbare inhoud op het internet komt dan de providers. Ik vraag me af of deze aanname realistisch is. Weliswaar kunnen de klanten van internetaanbieders strafbare informatie op hun servers plaatsen, de providers zijn wel degene die de servers beheren. Dat impliceert mijns inziens dat zij ook op de hoogte (dienen te) zijn van de (mogelijk strafbare) inhoud van de server.

Een andere beperking van deze wetswijziging ziet op het feit dat met een NTD-bevel alleen de gevolgen van een delict (zoals kinderporno) kunnen worden weggenomen, als dat al lukt. De problemen omtrent anonimiteit en versleuteling compliceren immers het een en ander. Wanneer de gevolgen toch kunnen worden weggenomen, is dit vaak slechts van korte duur. Daders kunnen de informatie namelijk zeer vlot op een alternatieve locatie weer beschikbaar stellen.[582] Daarnaast kunnen monitoringsmogelijkheden ten behoeve van een opsporingsonderzoek verloren gaan, rechtmatig materiaal kan worden verwijderd bij het

[575] Oerlemans 2010, p. 149.
[576] Conceptiewetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 15 met verwijzing naar *Kamerstukken II* 2001/02, 28 197, nr. 3, p. 65.
[577] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 3.
[578] Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10, p. 4 e.v.
[579] Koops 2010, p. 2464.
[580] Oerlemans 2010, p. 150.
[581] Oerlemans 2010, p. 152.
[582] Oerlemans 2010, p. 151.

offline halen van het illegale materiaal en er kan een averechts effect optreden doordat de actie aandacht genereert en daardoor het strafbare materiaal meer aandacht krijgt dan het oorspronkelijk zou krijgen.[583] De invoering van een wetswijziging in deze voorgestelde vorm laat derhalve te wensen over. Toch moet de bevoegdheid tot het afgeven van een NTD-bevel er volgens Oerlemans wel komen. Er zijn zeker situaties te bedenken waar een afdwingbaar bevel wenselijk is, zoals bij het plaatsen van kinderpornografie of spam. Degene die dergelijke informatie op het internet tentoonspreid, kiest zijn internetprovider soms bewust om het feit dat deze bekend staat niet mee te werken met politie en justitie, aldus Oerlemans.[584] Een afdwingbaar bevel omzeilt dergelijke problematiek. Toch is de strijd tegen cybercrime nog lang niet gestreden. Zo worden de problemen met betrekking tot anonimiteit en versleuteling met het conceptwetsvoorstel niet geadresseerd en worden de knelpunten op het gebied van cybercrime (onder meer grensoverschrijdende kwesties en onduidelijke wetgeving) onvoldoende aangepakt.

5.7 Conclusie

Voor de uitoefening van inbreukmakende opsporingsbevoegdheden eist het strafvorderlijke legaliteitsbeginsel en het Straatsburgse kader een grondslag in de wet. Dat is voor hacken door de politie niet anders. Op dit moment voorziet het Wetboek van Strafvordering in diverse op geautomatiseerde werken gerichte opsporingsmethoden. Sommige zien op het onderzoeken van daarin opgeslagen gegevens, andere maken het afvangen of opnemen van data in transport mogelijk. Zo mag de politie bijvoorbeeld e-mail- en chatverkeer onderscheppen met de internettap. Toch is deze methode aan enkele beperkingen gebonden, zoals de vraag aan wie de aftaplast kan worden opgelegd, de gevolgen van het grensoverschrijdende karakter van het internet en het versleutelprobleem. Tevens maakt de wetgever het mogelijk om vertrouwelijke communicatie op te nemen met behulp van een technisch hulpmiddel. Het afvangen van gegevensverkeer via de computer kan met behulp van een bug op het toetsenbord of muis, maar het is ook mogelijk met speciale software, die kan worden geïnstalleerd op het geautomatiseerde werk van de betrokkene. Met een dergelijk computerprogramma kan communicatie wordt afgevangen, voordat versleuteling kan plaatsvinden. Ook kunnen toetsaanslagen, waaronder wachtwoorden, worden geregistreerd, zodat hiermee de encryptie ongedaan kan worden gemaakt. Deze opsporingsactiviteit vertoont veel gelijkenissen met hacken. Er wordt immers met behulp van speciale software binnengedrongen op een computersysteem. Het een en ander vindt alleen niet plaats op afstand, zoals dat bij hacken wel het geval is. Opsporingsambtenaren zullen na het betreden van de woning het computerprogramma handmatig op het geautomatiseerde werk moeten installeren. Inbreken op computers via internet – dus op afstand – is volgens de huidige wetgeving niet mogelijk. Overigens heeft de wetgever voor inlichtingen- en veiligheidsdiensten wel de expliciete mogelijkheid geschapen om te kunnen hacken. Boek is van mening dat hacken door de opsporingsautoriteiten tevens mogelijk is gemaakt, namelijk via de bevoegdheid van de inkijkoperatie. Hij beargumenteert dat het begrip besloten plaats

[583] Oerlemans 2010, p. 152.
[584] Oerlemans 2011b, p. 9 e.v.

uit artikel 126k Sv ook een harde schijf kan omvatten en dat daarmee het heimelijk binnentreden ervan is gelegitimeerd.

In dit hoofdstuk stond het digitale wettelijke kader omtrent opsporingsmethoden centraal. Op het gebied van opsporing van cybercrime is veel mogelijk. De vraag rijst in dit kader of er voldoende mogelijk is. Moet de politie niet meer en ruimere bevoegdheden krijgen in de strijd tegen criminaliteit waar geautomatiseerde werken bij betrokken zijn, zoals de bevoegdheid tot hacken in de opsporingsfase? Of mogen opsporingsautoriteiten dit op grond van de huidige wetgeving al? Daarover volgt in het volgende hoofdstuk meer.

Hoofdstuk 6 Wenselijkheid en noodzakelijkheid van hacken in het opsporingsonderzoek

Ondanks het feit dat de wetgever voor politie en justitie ingrijpende bevoegdheden voor de opsporing van computergerelateerde criminaliteit heeft gecreëerd in het Wetboek van Strafvordering, zien deze autoriteiten zich genoodzaakt om hacken toe te passen in het opsporingsfase. De vraag die in dit hoofdstuk daarom onder meer centraal staat, is of de invoering van een wettelijke bevoegdheid wenselijk kan worden geacht (§ 6.1). Oftewel, moet hacken in het opsporingsonderzoek mogelijk worden gemaakt door de wetgever? Daarbij besteed ik in paragraaf 6.1.1 aandacht aan de vraag of hacken wel iets toevoegt aan het huidige digitale opsporingskader. Vervolgens komt in paragraaf 6.1.2 een aantal argumenten aan bod ten aanzien van de wenselijkheid van de invoering van hacken in de opsporingsfase.
In paragraaf 6.2 behandel ik de noodzakelijkheid van een dergelijke opsporingsbevoegdheid. In dit kader wordt eerst onderzocht of de bevoegdheid tot hacken kan worden afgeleid van enkele bestaande opsporingsmethoden. Wanneer dat niet het geval is, en wanneer de invoering van hacken in de opsporingsfase wenselijk wordt geacht, zal vanwege het legaliteitsbeginsel een (uitdrukkelijke) grondslag in de wet zijn vereist. Bij deze beoordeling trek ik een parallel met de argumentatie in het rapport 'Inzake opsporing' van de parlementaire enquêtecommissie onder leiding van Van Traa (§ 6.2.4.1). Het rapport kwam toentertijd tot stand naar aanleiding van geconstateerde en vermoede uitwassen van ongenormeerde opsporing. Ook op dit moment ontbreekt een uitdrukkelijke basis in de wet voor hacken in het opsporingsonderzoek. In paragraaf 6.2.4.3 behandel ik de eisen die mijns inziens moeten worden gesteld aan een wettelijke bepaling voor hacken door de politie. De cumulatieve voorwaarden ex artikel 8 lid 2 EVRM op grond waarvan de strafvorderlijke overheid met een dergelijke verregaande methode geoorloofd inbreuk mag maken op het recht op privacy, worden als rode draad door dit hoofdstuk behandeld. Overigens kan in dit kader aan de behandeling van de legitieme doelbepaling (§ 4.5.1) voorbij worden gegaan. Het is duidelijk dat de opsporingsmethode hacken het voorkomen van strafbare feiten tot doel heeft en dientengevolge met dit doel zal worden ingezet.

Aan het slot van dit hoofdstuk doe ik enkele aanbevelingen over de opsporingsautoriteiten in het algemeen (§ 6.3).

6.1 Wenselijkheid van hacken in het opsporingsonderzoek

Het internet biedt met betrekking tot het opsporingsonderzoek naast enkele nadelen – zoals de problematiek omtrent versleuteling en anonimiteit – ook een aantal voordelen. Stevens & Koops verwijzen in dit kader naar het feit dat alle gegevens die ooit in een computer zijn ingevoerd in beginsel blijven bewaard. Datgene wat van de computer wordt weggooit – en in *Windows*-termen wordt verwijderd door de 'prullenbak' leeg te maken – blijft aanwezig op de harde schijf en is met weinig moeite en zonder hulp van speciale software of gespecialiseerde kennis weer toegankelijk of leesbaar te maken.[585] Wanneer men wel gebruikmaakt van

[585] Stevens & Koops 2009, p. 672.

dergelijke software is het in enkele gevallen zelfs mogelijk data van een gecrashte harde schijf terug te halen. Geautomatiseerde werken zijn op deze manier een bron van onschatbare informatie over de misdaden die worden gepleegd op of met behulp van deze apparaten of in de wereld die deze creëren.[586]

De vraag rijst hoe de opsporingsautoriteiten de beschikking krijgen over deze data. In hoofdstuk 5 zijn reeds meerdere opsporingsbevoegdheden met een digitaal karakter opgesomd, die gegevens op computer(netwerken) kunnen opnemen, aftappen of bemachtigen. Toch blijft altijd het risico bestaan dat de verdachte, vanwege de belangstelling van de politie naar zijn handelen, bepaalde informatie uitwist. Voor de gemiddelde maar ook voor de iets behendigere verdachte computergebruiker is het echter lastig om alle sporen van afbeeldingen, gegevens of webbezoek op de harde schijf onbereikbaar te maken.[587] Niettemin is het wel degelijk mogelijk. Wil men een bestand definitief van deze harde schijf verwijderen, dan moet speciale wissoftware worden gebruikt die het bestand herhaaldelijk met *bits* en *bytes* overschrijft.[588]

Naast de inzet van bestaande opsporingsmethoden – zoals de internettap en het opnemen van vertrouwelijke communicatie – zou het hacken van computers van criminelen de politie goed van pas kunnen komen. Zij kan een computer hacken om er achter te komen wat er op de harde schijf staat, zoals kinderpornoplaatjes of bestanden die informatie bevatten over de voorbereiding van een criminele daad.[589] Ook kan men geïnteresseerd zijn in het elektronische communicatieverkeer. In beginsel kunnen opsporingsautoriteiten op grond van artikel 126m Sv besluiten dit verkeer af te tappen. Door de wijdverbreide beschikbaarheid van draadloze verbindingen is dit echter niet zo eenvoudig. Tegenwoordig kan via (gratis) WiFi-netwerken[590] (hotspots) bijna overal verbinding worden gemaakt met het internet. Slechts van het IP-adres van de verdachte, kan het verkeer worden afgetapt.[591] Alleen de communicatie over die bepaalde internetlijn kan worden doorgegeven.[592] Als de verdachte vanuit meerdere locaties het internet gebruikt, kan derhalve niet de gehele internetcommunicatie worden afgeluisterd.[593]

Het een en ander wordt nog eens gecompliceerd door het veelvuldige gebruik van *freemail*, zoals *Hotmail* of *Gmail*. Deze gratis e-mailaccounts zijn niet gebonden aan een computersysteem met een bepaald IP-adres, maar zijn te openen vanaf iedere willekeurige locatie met een internetaansluiting. Wanneer de politie is geïnteresseerd in het e-mailverkeer van de verdachte en de e-mailaccount wordt vanaf een andere locatie geopend en gebruikt, valt deze elektronische correspondentie buiten het bereik van de tap. Wellicht dat het hacken van de *inbox* van een dergelijk e-mailadres veel problemen kan oplossen, al loopt de politie in dat geval tegen de grenzen van de soevereiniteit van Nederland aan. De meeste gratis e-mailaccounts zijn immers van Amerikaanse origine.

---

[586] Boek 2000, p. 589.
[587] Stevens & Koops 2009, p. 673.
[588] Stevens & Koops 2009, p. 675.
[589] Boek 2000, p. 590.
[590] WiFi is een techniek waarvan mensen gebruik kunnen maken voor draadloos internet. Apparaten als laptops, smartphones, Ipads en andere draagbare computers kunnen automatisch verbinding maken met een router die het draadloze signaal uitzendt; Oerlemans 2012, p. 30.
[591] Oerlemans 2012, p. 30.
[592] Odinot e.a. 2012, p. 75.
[593] Oerlemans 2012, p. 30.

Niet alleen de explosieve groei van draadloze internetverbindingen en het veelvuldige gebruik van freemail zorgen voor complicaties in het taponderzoek, ook het feit dat het criminele circuit steeds vaker gebruikmaakt van encryptie resulteert in een beperking van de internettap. Met deze methode wordt communicatie immers onzichtbaar gemaakt. Prins stelt dat de enige kans voor opsporingsautoriteiten om nog waardevolle sporen op te doen, bestaat uit het digitaal inbreken op betrokken geautomatiseerde werken van verdachten om hen zo te kunnen monitoren.[594]

6.1.1 Hacken als toevoeging aan het huidige digitale opsporingskader

Door geautomatiseerde werken te hacken in de opsporingsfase kunnen politie en justitie aldus sporen van criminele daden vinden en kan criminele communicatie worden onderschept.[595] Gespreksverkeer kan echter ook worden opgenomen op grond van 126l Sv. In de literatuur wordt zelfs aangenomen dat de opsporingsautoriteiten na het betreden van de woning in het kader van het opnemen van vertrouwelijke communicatie speciale software mogen installeren, welke direct afluisteren mogelijk maakt. In die zin verschilt hacken niet veel van deze in de wet vastgelegde bevoegdheid. Er wordt immers met behulp van een computerprogramma (een Trojaans politiepaard) een ‘achterdeur’ op de computer ingebouwd, waarmee justitie rechtstreeks kan meekijken met de handelingen van de verdachte. Daarmee rijst de vraag in hoeverre hacken als opsporingsmethode nog iets toevoegt aan het huidige wettelijke kader digitale opsporingsbevoegdheden. In hoeverre heeft hacken praktische meerwaarde voor het bestaande tableau van opsporingsbevoegdheden? Oftewel, kan hacken door politie en justitie wenselijk worden geacht, wanneer men de huidige opsporingsmogelijkheden op ICT-gebied in ogenschouw neemt?

Mijns inziens is dat het geval. In vergelijking met het opnemen van vertrouwelijke communicatie op grond van artikel 126l Sv biedt hacken in de opsporingsfase namelijk veel meer mogelijkheden. Zoals in paragraaf 2.2 wordt vermeld, moet hacken niet worden beschouwd als één afgebakende opsporingsmethode, maar als een verzameling van allerlei methoden. Zo kan men zich beperken tot het onderzoeken van de computer om te kijken welke eigenschappen de computer bezit of welke documenten er zijn opgeslagen, maar kan men ook toetsaanslagen afvangen, gegevens kopiëren en zelfs het geautomatiseerde werk beïnvloeden. Dat het binnendringen van geautomatiseerde werken praktisch alles mogelijk maakt op die apparaten, wil mijns inziens nog niet zeggen dat de opsporingsautoriteiten daarmee ook alle vrijheid moeten krijgen om op computers rond te kijken en handelingen te verrichten.

Los van de beantwoording van de vraag in hoeverre hacken mogelijk moet worden gemaakt – moet worden vastgesteld dat via het opnemen van vertrouwelijke communicatie minder gegevens kunnen worden verzameld dan middels hacken. Weliswaar kunnen allerlei vormen van communicatie (zoals chat- en e-mailverkeer) worden afgevangen, op de computer opgeslagen bestanden (zoals kinderporno) kunnen in principe niet worden bekeken. Voorwaarde van het inzetten van de bevoegdheid ex artikel 126l Sv is namelijk dat er sprake moet zijn van communicatie met een ander. Oftewel, het moet gaan om stromend

[594] Prins 2012, p. 48.
[595] Boek 2000, p. 589.

gegevensverkeer. Het afvangen van hetgeen iemand op zijn computer doet of zet – zonder dat deze informatie of dit materiaal wordt verzonden – is bij direct afluisteren niet gepermitteerd. Overigens is dat wel weer mogelijk met de doorzoeking op grond van artikel 125i Sv. De opsporingsautoriteiten hebben hiermee de bevoegdheid om direct onderzoek te doen in computersystemen en bestanden. Dat wil zeggen dat ze tijdens een doorzoeking een daar aangetroffen computer mogen aanzetten en wat zich op dat geautomatiseerde werk bevindt, mogen bekijken. Daarbij is het betreden van de woning van de betrokkene noodzakelijk. Hacken biedt ten opzichte van deze bevoegdheid een voordeel, omdat het op afstand plaatsvindt. De opsporingsambtenaar kan vanaf een andere locatie achter zijn (eigen) computer binnendringen in het geautomatiseerde werk van de betrokkene. Het betreden van een besloten plaats zonder de toestemming van de rechthebbende is derhalve niet noodzakelijk.

De vraag rijst in dit kader of het op afstand handelen (hacken) niet een te prefereren manier van strafvorderlijk optreden is. Hieromtrent is mijns inziens het beginsel van subsidiariteit van belang. Deze eis vloeit onder meer voort uit de jurisprudentie aangaande het criterium ex artikel 8 lid 2 EVRM, de noodzakelijkheid van de inbreuk in een democratische samenleving. Het gaat met betrekking tot de opsporingsfase in relatie tot het subsidiariteitsbeginsel in wezen om de vraag of de inzet van een 'lichtere' opsporingsbevoegdheid niet mogelijk was geweest. Als een bepaalde inbreuk op het privéleven onvermijdelijk is, dient te worden gekozen voor die methode die met de minste inbreuk gepaard gaat.[596] Het is de vraag bij welke bevoegdheid – de doorzoeking ter vastlegging van gegevens of hacken door de politie – dat het geval is. Wat hieromtrent in ieder geval vaststaat, is dat met hacken slechts de toegang wordt verkregen tot het dikwijls persoonlijke geautomatiseerde werk, terwijl om de doorzoeking mogelijk te maken zowel de woning als de computer moeten worden binnengedrongen. Hierdoor lijkt hacken als opsporingsbevoegdheid te resulteren in een lichtere inbreuk op het privéleven. Omdat met de inzet van deze methode praktisch alles op het geautomatiseerde werk mogelijk wordt en de uitoefening heimelijk plaatsvindt, dient het wel met waarborgen te worden omkleed.

6.1.2 Anonimiteit, versleuteling en de aanpak van botnets

De computer en het internet zijn een bron van allerlei informatie over de (criminele) gebruiker ervan en zijn activiteiten. In principe kan men met bepaalde technieken de gegevens van deze gebruiker, zowel zakelijk als privé, boven water krijgen. Zoals reeds in paragraaf 4.5.3 is uiteengezet, wordt het verzamelen van gegevens en het ophalen van gespreksstromen op computernetwerken steeds moeilijker door de problemen die samenhangen met anonimiteit en versleuteling.[597] Aan de hand van deze problematiek kan mijns inziens worden aangetoond dat de invoering van bepaalde vormen van hacken wenselijk kan worden geacht. Ook bij de aanpak van botnets kan het introduceren van een hackbevoegdheid van belang worden geacht.

[596] Vedder e.a. 2007, p. 64.
[597] Oerlemans 2011a, p. 903.

6.1.2.1 Hacken en anonimiteit

In principe dient iedere gebruiker zich te realiseren dat computergebruik het verspreiden van persoonlijke gegevens met zich meebrengt. Toch zijn er diverse technieken ontworpen die een zekere mate van anonimiteit in de virtuele wereld mogelijk maken.[598] In paragraaf 4.5.3.1 heb ik verwezen naar de mogelijkheid van aanpassing van het IP-adres op een zodanige manier dat het lokaliseren van de verdachte praktisch wordt uitgesloten. Anoniem surfen op het internet wordt hierdoor derhalve mogelijk gemaakt.[599] Tevens is het haalbaar om e-mail te anonimiseren. De meest simpele manier is het registreren van een e-mailaccount bij een *freemailprovider*, zoals *Hotmail of Gmail*. Voor het aanmelden bij zo'n provider kan immers een willekeurige (valse) naam of pseudoniem worden gebruikt.[600] Hoewel het gebruik van freemail anonimiteit voor de buitenwereld oplevert, beschikt de provider via het gebruik van een webpagina wel over gegevens van de gebruiker. Het criminele circuit zal daarom van deze mogelijkheid over het algemeen nauwelijks gebruikmaken.

E-mail kan ook worden geanonimiseerd door een *anonymous remailer* te benutten als 'tussenstation' tussen de verzender van de e-mail en de geadresseerde. In plaats van een bericht rechtstreeks naar de geadresseerde te sturen, stuurt de verzender zijn e-mail naar de *remailer*.[601] Deze verwijdert vervolgens alle informatie die de oorspronkelijke verzender zou kunnen identificeren uit het bericht alvorens het naar de geadresseerde door te sturen. Remailers bewaren het IP-adres van de oorspronkelijke verzender soms gedurende enkele maanden. Derden kunnen tijdens die periode de identiteit van de verzender met behulp van de remailer achterhalen. Om te voorkomen dat de identificerende informatie op deze wijze alsnog kan worden ontdekt, wordt vaak gebruikgemaakt van *chained remailing*. Wanneer een bericht door een keten van remailers wordt gestuurd, wordt de kans steeds kleiner dat de identificerende gegevens nog beschikbaar zijn.[602]

Absolute anonimiteit kan men tevens realiseren door een afgeschermd of aangepast IP-adres te combineren met een anonieme remailer. De gebruiker ervan kan achteraf niet worden getraceerd.[603] In principe heeft justitie de bevoegdheid om gebruikersgegevens op te vragen, maar in veel gevallen houdt de provider geen informatie over de gebruiker bij of bevindt deze zich in het buitenland. Om inzage in de gegevens te krijgen, zal de weg van de rechtshulp moeten worden bewandeld.[604] Een andere mogelijkheid is met behulp van speciale software het geautomatiseerde werk binnen te dringen. Op die manier kan het IP-adres worden vastgesteld of kan een stap verder worden gegaan door een 'inkijkoperatie' uit te voeren. Zo kan bruikbaar bewijsmateriaal worden verzameld door beeldschermopnames te maken of bestanden te kopiëren.[605]

Anonimiteit op het internet kan – naast de aanpassing van het IP-adres of de aanwending van een anonieme remailer – tevens worden bewerkstelligd door het gebruik van

[598] Van den Eshof e.a. 2002, p. 21.
[599] Van den Eshof e.a. 2002, p. 27.
[600] Ekker 2006, p. 25.
[601] Van den Eshof e.a. 2002, p. 25.
[602] Ekker 2006, p. 25.
[603] Van den Eshof e.a. 2002, p. 28.
[604] Van den Eshof e.a. 2002, p. 29.
[605] Oerlemans 2011a, p. 904 e.v.

verborgen websites. Daarbij kan men het zogenaamde *Tor-netwerk*[606] benutten. Zoals de inleiding van dit onderzoek reeds aangaf, heeft Robert M., verdachte in de Amsterdamse zedenzaak, op deze wijze via verborgen websites op dit netwerk zeer veel kinderpornografisch materiaal verspreid en gecommuniceerd over het misbruiken van kinderen.[607] Tijdens het opsporingsonderzoek is de politie in deze geheime webpagina's binnengedrongen om het strafbare beeldmateriaal op de sites te verwijderen.[608] Ook hier is derhalve sprake van hacken door politie en justitie. Blijkbaar zagen de opsporingsautoriteiten geen andere mogelijkheid om het materiaal van het internet te wissen.[609] Ook ik ben van mening dat politie en justitie op grond van het huidige Wetboek van Strafvordering niet over de benodigde bevoegdheden beschikken om dergelijke activiteiten op te sporen en aan te pakken. Hacken kan in die gevallen een uitkomst kan bieden, al ontbreekt voor deze vorm van handelen een grondslag in de wet.

6.1.2.2 Hacken en versleuteling

Hacken kan niet alleen het probleem van anonimiteit omzeilen, maar ook de problematiek omtrent versleuteling. Het is extreem gecompliceerd geworden om criminele activiteiten op het internet te traceren, omdat het redelijk eenvoudig is geworden te voorkomen dat sporen kunnen worden gevolgd. Zo kan software worden gebruikt die berichten versleutelt.[610] Niet alleen communicatie kan worden versleuteld, ook gegevens kunnen op geautomatiseerde werken onleesbaar worden gemaakt.[611] Met behulp van bepaalde software in de vorm van een Trojaans politiepaard – dus via een hack – kan internetverkeer van de betrokkene bij de bron worden doorgestuurd. Op die manier kan het probleem van versleuteling worden omzeild. Tevens kunnen toetsaanslagen worden afgevangen, inclusief wachtwoorden, zodat versleutelde gegevens leesbaar kunnen worden gemaakt.[612]

Versleuteling is de afgelopen decennia een substantieel probleem geworden voor opsporingsdiensten. Dit hangt onder meer samen met de schaalvergroting van beschikbare (software)mogelijkheden, het gemak van sleuteluitwisseling en de robuustheid van versleutelsystemen.[613] De noodzaak van de invoering van een maatregel tegen versleuteling wordt evident bij ernstige misdrijven met een digitale component zoals kinderpornografie, waarbij criminelen zich in toenemende mate inspannen kinderporno met encryptietechnieken te verbergen.[614]

Het versleutelprobleem kan worden aangepakt met hacken, maar kan tevens worden omzeild via het opnemen van vertrouwelijke communicatie. Net als bij de doorzoeking ter vastlegging van gegevens is het noodzakelijk om de betrokken computer fysiek te benaderen. Het voordeel van hacken door de politie en justitie is dat het op afstand (en heimelijk) plaatsvindt. Mocht de verblijfplaats van de verdachte en zijn geautomatiseerde werk(en) niet

---

[606] Een *Tor*-netwerk is een wereldwijd netwerk dat het mogelijk maakt om anoniem op internet te surfen; http://www.om.nl/onderwerpen/verkeer/@156657/kinderporno-anonieme/.
[607] Zie http://www.om.nl/onderwerpen/verkeer/@156657/kinderporno-anonieme/.
[608] Prins 2012, p. 48.
[609] Prins 2012, p. 48.
[610] *Kamerstukken II* 2008/09, 28 684, nr. 232, p. 3.
[611] Oerlemans 2011a, p. 906.
[612] Oerlemans 2011a, p. 907.
[613] Koops 2000, p. 58.
[614] Oerlemans 2011a, p. 906.

bekend zijn, dan hoeft dat voor het opsporingsonderzoek geen beletsel te vormen. De opsporingsambtenaar kan achter zijn bureau blijven zitten. Bovendien is bij een 'goede' hack de kans op ontdekking zeer klein. Op die manier kunnen opsporingsautoriteiten derhalve zonder veel risico op ontdekking door de betrokkene veel te weten komen over de mogelijk gepleegde strafbare feiten.[615] Ook hier ontkomt men niet aan de beoordeling van de eis van subsidiariteit, voortvloeiend uit jurisprudentie omtrent artikel 8 lid 2 EVRM. De vraag dient te worden beantwoord of het binnendringen op afstand een te prefereren manier van opsporen is in verhouding tot het opnemen van vertrouwelijke communicatie. Met beide bevoegdheden wordt hetzelfde doel bereikt, namelijk de vergaring van strafbare communicatie als zodanig of communicatie over strafbare feiten. Met beide bevoegdheden kan daarnaast de problematiek van versleuteling worden omzeild en met beide bevoegdheden wordt bovendien door het binnendringen van de computer een vergelijkbare inbreuk op het recht op een privéleven gemaakt. Toch lijkt hacken wel van minder bezwarende aard te zijn. Het binnentreden van bijvoorbeeld een woning is immers niet noodzakelijk. Het op afstand binnendringen van geautomatiseerde werken vormt mijns inziens daardoor een minder ingrijpende methode van opsporen en zou in het opsporingsonderzoek de voorkeur moeten hebben boven het opnemen van vertrouwelijke communicatie.

6.1.2.3 Hacken en de aanpak van botnets

Hacken kan de problemen van versleuteling en anonimiteit aanpakken. Daarnaast kan het middel worden ingezet in de strijd tegen botnets. Zo stelt officier van justitie Van Zwieten, belast met de aanpak van computercriminaliteit, dat een bevoegdheid tot hacken:

> 'een heel effectief middel zou kunnen zijn in de bestrijding van deze criminaliteit. (…) Een groot voordeel van het op afstand kunnen benaderen van computers is dat je rechtstreeks en zonder de vertragende factor van collegiaal overleg die criminele systemen kunt aanpakken, ook ver in het buitenland. Dat je ze derhalve kunt uitschakelen. (…) Daarvoor zou de wet moeten worden aangepast.'[616]

Prins gaat verder en stelt in dit kader dat:

> 'de politie bevoegdheid zou moeten krijgen om computers in het buitenland van criminelen te kunnen overnemen. In feite moeten ze de bevoegdheid krijgen om terug te kunnen hacken. Als ze eenmaal in die computer zitten, kunnen ze twee dingen doen: dat is zo'n botnet met al die kwaadaardige software uitschakelen, maar daarnaast kun je ook heel goed onderzoek doen wie de criminelen zijn die erachter zitten.'[617]

---

[615] Boek 2000, p. 590.

[616] Zie pleidooi van officier van justitie Lodewijk van Zwieten voor het mogelijk maken van grensoverschrijdend hacken op 25 oktober 2010 in 'Nieuwsuur', NOS Nederland 2. Dit tv-fragment is te vinden via: http://nieuwsuur.nl/video/193776-de-strijd-tegen-cybercrime.html.

[617] Zie pleidooi van directeur en medeoprichter van Fox-IT Ronald Prins voor het mogelijk maken van terughacken bij de aanpak van botnets op 23 oktober 2010 in 'Nieuwsuur', NOS Nederland 2. Dit tv-fragment is te vinden via: http://nieuwsuur.nl/video/193369-internetbankieren-niet-100-procent-veilig.html.

Prins geeft daarnaast aan dat de invoering van hacken wenselijk is, omdat het zou kunnen bijdragen aan het verwijderen van strafbare informatie van het internet.[618]

In dit kader wil ik wederom refereren aan een voorwaarde die door het EHRM is gesteld ten aanzien van inbreukmakende activiteiten van de overheid, namelijk de voorwaarde van proportionaliteit. Met deze eis wordt tot uitdrukking gebracht dat bij de beslissing tot toepassing van een bepaalde opsporingsmethode het daardoor getroffen belang in redelijke verhouding dient te staan tot het belang dat met de toepassing wordt gediend.[619] Zoals ik hierboven heb betoogd, kan hacken door de politie de problemen van anonimiteit en versleuteling omzeilen en kan het middel de aanpak van botnets en andere schadelijke (en strafbare) geautomatiseerde werken bewerkstelligen. Deze complicaties belemmeren het opsporingsonderzoek in grote mate. Dat komt onder meer doordat de problemen met de huidige opsporingsbevoegdheden onvoldoende kunnen worden aangepakt. Er is dus sprake van een *pressing social need*. Hacken in het opsporingsonderzoek kan deze complicaties mijns inziens wel bestrijden, al leidt de inzet van de methode tot een aanzienlijke inbreuk op de persoonlijke levenssfeer. Het belang dat echter met hacken kan worden gediend en de winst die ten opzichte van de overige digitale opsporingsmethoden kan worden behaald, wegen hier naar mijn mening onder strenge voorwaarden tegen op. In specifiek omlijnde gevallen kan hacken door de politie daarom in redelijke verhouding staan tot het te dienen doel.

6.2 Noodzakelijkheid van hacken in het opsporingsonderzoek

Koning stelt dat het technisch effect van hacken door de opsporingsautoriteiten op de privacy de totaalsom is van het doorzoeken, aftappen, heimelijk volgen, observeren en infiltreren. Na toegang tot een geautomatiseerd werk maakt de techniek immers alles mogelijk.[620] Hacken maakt met betrekking tot persoonlijk geautomatiseerde werken ontegenzeggelijk inbreuk op de persoonlijke levenssfeer. Met het binnendringen van een geautomatiseerd werk kan van allerlei privacygevoelige informatie worden kennisgenomen.[621] Hacken in de opsporingsfase is echter niet vervat in een uitdrukkelijke wettelijke bepaling. Dit terwijl een grondslag in de wet – vanwege de inbreuk op het fundamentele recht op privacy – wel noodzakelijk wordt geacht.

In dit kader wordt door een enkele auteur en (impliciet) door de strafvorderlijke overheid betoogd dat hacken als opsporingsmethode kan worden afgeleid uit bestaande gelegitimeerde opsporingsmethoden. In de volgende subparagrafen blijkt dat daar veel tegen in kan worden gebracht.

---

[618] Interview R. Prins en J.J. Oerlemans op 5 juni 2012 ten burele van Fox-IT te Delft. Daar wil ik dit kader aan toevoegen dat Prins specialist is op het gebied van cybercrime. Hij is tot op zekere hoogte ook juridisch onderlegd, maar hij is geen jurist. Hij bepleit bepaalde standpunten dan ook meer vanuit een technisch perspectief dan vanuit een rechtswetenschappelijk oogpunt.
[619] Mevis 2009, p. 331.
[620] Koning 2012, p. 46.
[621] Boek 2000, p. 592.

6.2.1 Hacken en de inkijkoperatie

Boek is van mening dat hacken interpretatiegewijs onder een van de wettelijke opsporingsbevoegdheden kan worden geplaatst. Zo beargumenteert hij dat het hacken van een harde schijf van een computer via de inkijkoperatie kan plaatsvinden.[622] Inkijken is te omschrijven als het heimelijk betreden van een bepaalde (besloten) plaats met een strafvorderlijk doel.[623] Artikel 126k lid 1 Sv noemt een drietal gronden voor de uitoefening van dit dwangmiddel. Met betrekking tot dit onderzoek is voornamelijk het plaatsen van een technisch hulpmiddel in een besloten omgeving van belang teneinde de aanwezigheid of verplaatsing van een goed te kunnen vaststellen.[624] Boek is van mening dat een kwaadaardig softwareprogramma – benodigd voor het zetten van een hack – kan worden betiteld als een technisch hulpmiddel. Vervolgens stelt hij daarbij een harde schijf van een computer gelijk aan een besloten plaats waarbinnen de inkijkoperatie kan worden uitgevoerd. De auteur merkt op dat bij een besloten plaats in principe alleen is gedacht aan reële plaatsen, zoals loodsen, erven en garages, maar dat er taalkundig niets in de weg staat de harde schijf ook daaronder te laten vallen.[625] Boeks interpretatiemethode is niet bepaald gangbaar en moet zeker ook in een ander tijdsperspectief worden geplaatst. Met de redenering van de auteur wordt het begrip besloten plaats te ver opgerekt. Hacken resulteert in een zodanige stevige inbreuk op het recht op privacy dat een uitdrukkelijke basis in de wet noodzakelijk moet worden geacht. Ook Schermer is van mening dat de oprekking van het begrip besloten plaats onaanvaardbaar is, omdat een inbreuk op grondrechten altijd een expliciete wettelijke legitimatie dient te hebben en geen legitimatie die wordt verkregen uit een taalkundige slimmigheid.[626] Oerlemans sluit zich hierbij aan.[627] Buruma en Koops wijzen in dit kader tevens op een sterk wetssystematisch argument.[628] In paragraaf 5.5 werd reeds uiteengezet dat de inlichtingen- en veiligheidsdiensten op grond van artikel 24 lid 1 Wiv 2002 de uitdrukkelijke bevoegdheid hebben om binnen te dringen in geautomatiseerde werken in tegenstelling tot politie en justitie. De Wiv 2002 is in dezelfde tijd tot stand gekomen als de Wet BOB. Hieruit kan worden afgeleid dat het de bedoeling van de wetgever is geweest juist de inlichtingen- en veiligheidsdiensten de bevoegdheid tot hacken te geven en daarmee de politie en justitie dus niet.[629]

6.2.2 Hacken en het opnemen van vertrouwelijke communicatie

Boek plaatst daarnaast het hacken van e-mail onder de bijzondere opsporingsbevoegdheid van het opnemen van vertrouwelijke communicatie ex artikel 126l Sv. Met dit middel wordt onder meer het plaatsen van een bug op een toetsenbord mogelijk gemaakt. Hij stelt dat het niet uitmaakt of het toetsenbord van een computer wordt voorzien van een dergelijk microfoontje of de harde schijf.[630] Koops en Buruma gaan hier tot op zekere hoogte in mee en stellen zelfs

---

[622] Boek 2000, p. 592.
[623] Corstens 2011, p. 517.
[624] Corstens 2011, p. 518.
[625] Boek 2000, p. 592 met verwijzing naar *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 40 en 77.
[626] Schermer 2003, p. 53.
[627] Oerlemans 2011a, p. 901.
[628] Koops & Buruma 2008, p. 118.
[629] Koops & Buruma 2008, p. 118.
[630] Boek 2000, p. 592.

dat met artikel 126l Sv voor justitie een grondslag is gecreëerd om te hacken. Zoals is vermeld, mogen opsporingsambtenaren op basis van dit artikel een woning binnentreden om op de harde schijf van een computer een technisch hulpmiddel te plaatsen, dat direct afluisteren mogelijk maakt. Koops en Buruma kwalificeren het inbreken in een computer om iets op de harde schijf te plaatsen als computervredebreuk. In tegenstelling tot wat Boek beweert, biedt artikel 126l Sv echter geen grondslag voor de generieke vorm van hacken, namelijk het *via een netwerk* binnendringen van een computer. Justitie heeft geen bevoegdheid dat laatste te doen.[631] Ik sluit me hierbij aan. De bevoegdheid tot het opnemen van vertrouwelijke communicatie beperkt zich tot het afvangen van correspondentie middels een bug of door middel van het plaatsen van een softwareprogramma op de harde schijf van de computer na het betreden van de woning van de betrokken verdachte. Voor het op afstand plaatsen van dergelijke software biedt het huidige Wetboek van Strafvordering mijns inziens geen ruimte.

6.2.3 Hacken en de internettap

In paragraaf 2.2.1.4 van dit onderzoek kwalificeerde ik de Bredolab-ontmanteling als een van de voorbeelden waarbij politie en justitie gebruik hebben gemaakt van hacktechnieken, ook al ontbrak en ontbreekt hiervoor een uitdrukkelijke wettelijke grondslag. Het Openbaar Ministerie maakte daarom in zijn onderzoek naar het botnet gebruik van zijn tapbevoegdheid ex artikel 126m Sv. Toepassing van dit artikel had het effect dat de opsporingsdiensten middels de afgevangen toegangs- en decryptiesleutels op de servers zijn binnengedrongen, waardoor gedurende ongeveer tien weken heimelijk de handelingen van de verdachte zijn gemonitord en onderzocht.[632] Het in te schatten effect van artikel 126m Sv op het recht op privacy is dat door af te tappen de inhoud van de communicatie, ook al is deze versleuteld, bij opsporingsautoriteiten bekend wordt en mogelijk als bewijs zal dienen.[633] Het effect van de inmenging die heeft plaatsgevonden bij de Bredolab-ontmanteling komt mijns inziens niet overeen met het effect van tappen. Bij de Bredolab-actie zijn de handelingen van de verdachte op zijn computer en op de server heimelijk geobserveerd en onderzocht. Deze opsporingsactiviteiten wijken voor een groot gedeelte af van het aftappen van communicatie op grond van artikel 126m Sv. Dit hangt samen met het feit dat door mee te kijken met de handelingen van de verdachte niet alleen zijn communicatie zichtbaar wordt, maar tevens zijn gehele activiteitenpatroon op het geautomatiseerde werk. Hacken op grond van artikel 126m Sv komt niet door de toetsing aan artikel 8 lid 2 EVRM heen. In casu en met betrekking tot hacken door de politie in het algemeen is ten eerste niet voldaan aan de eis van een wettelijke grondslag. Weliswaar hebben de opsporingsautoriteiten de bevoegdheid om te tappen, het op afstand binnendringen op servers of andere geautomatiseerde werken is op grond van deze bepaling niet toegestaan. Ten tweede is niet tegemoetgekomen aan de voorzienbaarheidseis ex 8 lid 2 EVRM. Daarvoor moet sprake zijn van strenge, heldere en gedetailleerde regels, die in de effecten van de inbreuk voorzien.[634] Artikel 126m Sv voorziet daar met betrekking tot het

[631] Koops & Buruma 2007, p. 118.
[632] Koning 2012, p. 49 e.v.
[633] Koning 2012, p. 50.
[634] Koning 2012, p. 50.

binnendringen van computers niet in, waardoor hacken op grond van dit artikel een schending van het privacyrecht oplevert en dientengevolge niet kan worden toegelaten.

Om hacken door opsporingsautoriteiten geoorloofd plaats te laten vinden, dient – voortbordurend op artikel 8 lid 2 EVRM – in ieder geval sprake te zijn van *basis in domestic law*. Daarover volgt in de volgende paragraaf meer. De rechtsgrond voor inmenging in het privéleven dient daarnaast in voldoende mate toegankelijk en voorzienbaar te zijn. Op grond van deze vereisten moet de burger in staat zijn om op de hoogte te raken van de toepasselijke regelgeving omtrent hacken in de opsporingsfase en moeten deze bepalingen voldoende inzicht bieden in de voorwaarden en omstandigheden waaronder de inbreuk is toegelaten.

6.2.4 Expliciete wettelijke grondslag voor hacken vereist

Zoals ik hiervoor reeds heb betoogd, ben ik van mening dat de extensieve interpretatie van bestaande opsporingsbevoegdheden teneinde hacken mogelijk te maken niet toelaatbaar kan worden geacht. De inkijkoperatie is gecreëerd voor de fysieke en reële wereld. Dat wil zeggen dat de bevoegdheid ziet op het heimelijk betreden van besloten plaatsen, zoals loodsen, erven en garages met als doel die plaats op te nemen, sporen veilig te stellen of een technisch hulpmiddel te plaatsen.[635] Het begrip besloten plaats kan niet – zoals Boek bepleit – worden opgerekt tot de harde schijf van een computer. Hacken is op grond van artikel 126k Sv dan ook niet mogelijk. Hetzelfde geldt met betrekking tot het opnemen van vertrouwelijke communicatie. Met direct afluisteren kan weliswaar via de harde schijf middels de *softwarematige keylogger* correspondentie worden afgevangen, de bevoegdheid ex artikel 126l Sv laat het onderscheppen van communicatie *op afstand* niet toe.[636] Ten slotte kan het hacken door opsporingsautoriteiten ook niet worden afgeleid van de aftapbevoegdheid ex artikel 126m Sv. Met het binnendringen van geautomatiseerde werken wordt de toegang verkregen tot de gehele inhoud van de computer, terwijl de aftapbevoegdheid slechts en uitsluitend ziet op het afvangen van communicatie.[637]

Een soortgelijke discussie als hiervoor is jaren geleden ook al gevoerd. Toen werden door een rechercheteam opsporingsactiviteiten verricht, waarvoor de strafvorderlijke wet geen ruimte bood. Naar aanleiding hiervan werd een parlementair onderzoek naar de in Nederland gebruikte opsporingsmethoden en de controle daarop van belang geacht. Vervolgens achtte men de instelling van een parlementaire enquêtecommissie gewenst, die onder meer de opdracht kreeg om onderzoek te doen naar de feitelijke toepassing, de rechtmatigheid, het verantwoord zijn en de effectiviteit van de opsporingsmethoden.[638] Een van de conclusies van de commissie was dat opsporing moest worden genormeerd. Een vrij politiebedrijf is ongepast, aldus de commissie.[639] De argumenten voor het invoeren van een wettelijke grondslag voor opsporingsactiviteiten toen acht ik nu met betrekking tot de lacune in de wet voor hacken in de opsporingsfase nog steeds van belang. Daarnaast zijn de handvatten die de enquêtecommissie heeft geformuleerd voor de inhoud van de opsporingsbepalingen mijns inziens ook in deze tijd nog bruikbaar.

---

[635] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 40.
[636] *Kamerstukken II* 2011/12, 7 februari 2012, Antwoord op Kamervragen van de D66 Kamerleden Schouw en Berndsen van de minister van Veiligheid en Justitie, aanhangselnummer 1374.
[637] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 39.
[638] Buruma 2001, p. 3.
[639] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 415.

6.2.4.1 De IRT-affaire

Omdat ik de invoering van een grondslag in de wet voor hacken door de politie wenselijk acht en omdat de parlementaire enquêtecommissie gedegen richtlijnen op het gebied van opsporing heeft geformuleerd, wil ik graag een parallel trekken met de argumentatie in het rapport 'Inzake opsporing' van de commissie onder voorzitterschap van Van Traa. Een onderzoek van deze enquêtecommissie werd noodzakelijk geacht met als primaire doel het verkrijgen van informatie met het oog op het normeren van methoden die door politie, bijzondere opsporingsdiensten en justitie werden gehanteerd.[640] Hieraan ten grondslag lag onder meer de IRT-affaire.

Het interregionaal rechercheteam Noord-Holland/Utrecht (IRT) was een samenwerkingverband van politiekorpsen ter bestrijding van de georganiseerde criminaliteit.[641] Het IRT-team deed onderzoek naar enkele criminele organisaties in Nederland. De leiding van het IRT verwachtte niet dat met de gebruikelijke opsporingsmethoden een verband zou kunnen worden aangetoond tussen deze netwerken en de criminele activiteiten die binnen deze netwerken werden ontplooid. Daarom werd nieuw, creatief onderzoek noodzakelijk geacht.[642] Een van de methoden die het team hanteerde, was het bewust doorlaten van drugs onder verantwoordelijkheid van politie en justitie, waarbij gestuurde informanten of beter gezegd burgerinfiltranten behulpzaam waren.[643] Dit alles met als doel een beter inzicht te krijgen in de criminele organisaties.[644] Deze methode, beter bekend als de Delta-methode, heeft mede ten grondslag gelegen aan de opheffing van het IRT-team in 1993.[645] In het rapport 'Inzake opsporing' is aan het licht gekomen dat de Delta-methode als opsporingsmethode onverantwoord en onrechtmatig is.[646] Het doorlaten van grote partijen drugs had geen basis in de wet.

6.2.4.2 Hacken als inbreuk op het recht op privacy

Er is significante gelijkenis tussen de huidige opsporingsproblematiek en de situatie die aanleiding gaf tot de IRT-affaire. Ook nu hebben politie en justitie een vorm van opsporen toegepast, waarvoor (nog) geen uitdrukkelijke grondslag in de wet is.

Ten gevolge van de IRT-affaire en daaropvolgend het rapport van de parlementaire enquêtecommissie is met de Wet BOB een groot aantal opsporingstechnieken van een expliciete wettelijke bevoegdheid voorzien.[647] Ik zie niet in waarom dat in het geval van hacken anders zou moeten zijn. Ook nu wordt door het handelen van politie en justitie het recht op een privéleven van betrokkenen geschonden en is er mijns inziens sprake van enige crisis in de opsporing. De huidige situatie wordt echter niet zozeer getypeerd door eigenstandig opererende politiemensen, maar wel door opsporingswerk dat onterecht wordt gebaseerd op bestaande opsporingsmethoden. Desalniettemin is er mijns inziens wel degelijk

---

[640] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 11.
[641] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 75.
[642] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 85.
[643] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 72.
[644] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 86.
[645] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 72.
[646] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 157.
[647] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 452.

sprake van een 'déjà vu' op opsporingsgebied. Het gevaar van creatieve toepassing van opsporingsmethoden lag toen en ligt nu wederom op de loer.

De commissie Van Traa oordeelde toentertijd dat de inzet van observatiemethoden, het runnen van informanten en het gebruik van politie- en burgerinfiltraten een specifieke wettelijke basis ontbeerde. Daarbij achtte de commissie de artikelen 2 Politiewet 1993 en 141 en 142 Sv als basis voor dergelijk overheidsoptreden te smal.[648] Het rapport gaat verder en stelt:

> 'In de democratische rechtsstaat vraagt elk optreden van bestuur, justitie en politie een zo precies mogelijke wettelijke grondslag. Bij de toepassing van strafrecht en strafvordering binnen de democratische rechtsstaat kan het doel de middelen niet heiligen. De toepassing van proportionaliteit en subsidiariteit moet geschieden binnen de grenzen van wettelijke bevoegdheden en niet daarbuiten.'[649]

Opsporingsmethoden dienen derhalve in een democratische rechtsstaat een expliciete wettelijke basis te hebben. Opsporing mag slechts plaatshebben op de wijze bij wet voorzien. Het een en ander hangt samen met de mogelijke inbreuk op de fundamentele rechten van burgers. Inbreuken op deze rechten behoeven in ieder geval een legitimatie in de wet.[650] Het vereiste van een dergelijke uitdrukkelijke grondslag in de wet hangt tevens samen met het risico op aantasting van de integriteit en beheersbaarheid van de opsporing en enkele andere rechtsstatelijke beginselen.[651] Dat is mijns inziens voor hacken door de opsporingsautoriteiten niet anders. Hacken als opsporingsmethode resulteert immers in een aanzienlijke inbreuk op de persoonlijke levenssfeer van de betrokkene. Omdat de inbreuk niet gering is, vormt artikel 2 Politiewet 1993 en artikel 141 Sv daarom geen geschikte grondslag voor het gebruik van deze opsporingsmethode.[652] Hacken dient in ons wettelijk systeem daardoor te worden ingepast als een bijzondere opsporingsbevoegdheid met adequate waarborgen. Betrokkenen krijgen op die manier inzicht onder welke voorwaarden dergelijke opsporingshandelingen mogen worden verricht.[653] Een preciezere legitimatie in de wet wordt daarnaast tevens verlangt door de toenemende technische verfijning en intensivering van onderzoeksmethoden en -technieken.[654]

6.2.4.2.1 Persoonlijke en onpersoonlijke geautomatiseerde werken

Oerlemans maakt een onderscheid tussen het hacken van persoonlijke computers en geautomatiseerde werken die niet voor privézaken worden gebruikt.[655] Bij het laatste kan men denken aan de servers van een botnet, een server waar vooral illegaal netwerkverkeer (zoals malware en spam) vandaan komt of een server waarop een webpagina of forum met vooral

---

[648] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 429 e.v.
[649] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 447.
[650] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 448.
[651] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 3.
[652] HR 19 december 1995, *NJ* 1996, 249 (*Zwolsman*).
[653] Oerlemans 2011a, p. 901.
[654] Koning 2012, p. 51.
[655] Zie blog Jan-Jaap Oerlemans over het mogelijk maken van hacken als opsporingsmethode op 29 oktober 2011. Deze blog is te vinden via: http://oerlemansblog.weblog.leidenuniv.nl/2011/10/29/hacken-als-opsporingsbevoegdheid.

kinderpornografie op draait.[656] Ik wil daar zelf computers, servers of netwerken die openbaar of voor ieder toegankelijk zijn aan toe willen voegen. Ik trek hieromtrent de parallel met de bevoegdheid van de inkijkoperatie ex artikel 126k Sv. Met deze bevoegdheid kunnen besloten plaatsen worden betreden met een bepaald doel.[657] De memorie van toelichting stelt hieromtrent dat openbare en voor iedereen toegankelijke plaatsen niet onder het begrip besloten plaats vallen.[658] Naar analogie met deze bepaling ben ik van mening dat ten aanzien van openbare en voor iedereen toegankelijke computers andere (lichtere) eisen omtrent hacken in de opsporingsfase kunnen worden gesteld dan met betrekking tot het hacken van persoonlijk geautomatiseerde werken. Voorbeelden van openbare, onpersoonlijke computers zijn de geautomatiseerde werken op een universiteit, in een internetcafé of in een bibliotheek. In dit kader rijst de vraag of op dergelijke computers voor de politie relevante gegevens of communicatie kan worden aangetroffen. Met name in het geval van internetcafés acht ik die kans aanwezig. Net zoals de ietwat verouderde anonieme openbare telefooncel wordt gebruikt als communicatiemiddel in schimmige zaken, verwacht ik dat het internetcafé ook wel eens een geliefde uitwijkplaats zou kunnen zijn voor mensen die liever geen sporen achterlaten.[659] Op de computers in deze cafés kan immers op relatief anonieme wijze een e-mailaccount worden geopend of worden gecommuniceerd.

Oerlemans beargumenteert dat het binnendringen van persoonlijke computers een grotere inbreuk op de privacy met zich meebrengt dan wanneer dit bij onpersoonlijke geautomatiseerde werken gebeurt. Het een en ander heeft volgens hem gevolgen voor de manier waarop de opsporingsbevoegdheid hacken moet worden genormeerd. Inbreken in computers of servers die niet voor privézaken worden gebruikt, resulteert in een lichte inbreuk op de persoonlijke levenssfeer van de betrokkene, waardoor voor die handeling geen uitdrukkelijke bevoegdheid in het strafvorderlijk wetboek is vereist. In dat geval kan volgens Oerlemans worden volstaan met de algemene grondslag voor opsporingsactiviteiten ex artikel 2 Politiewet 1993 en 141 en 142 Sv, eventueel in combinatie met de inzet van andere opsporingsbevoegdheden. Daarbij tekent hij aan dat dit afhankelijk is van het geval en dat er vooral niet te gemakkelijk moet worden overgegaan tot zo'n complexe operatie.[660]

Koning weerlegt de stelling van Oerlemans omtrent servers. De auteur stelt dat het eventuele persoonlijke gebruik ervan in de meeste gevallen lastig op voorhand vast te stellen is. Het gebruik van servers in de privésfeer kan pas worden geconstateerd op het moment dat de inhoud van de servers bekend is; dus na het hacken ervan. Door het op voorhand uitsluiten van de toepasbaarheid van het recht op privacy of de legitimiteit van een beroep op dit recht, zo gaat zij verder, zal de overheid zijn zorgplicht voor grondrechtelijke bescherming verzaken.[661] Koning heeft mijns inziens met betrekking tot servers een punt. Niettemin blijft het onderscheid ten aanzien van andere geautomatiseerde werken (zoals computers) van belang. Soms kan men immers wel van tevoren vaststellen of een computer in de privésfeer

[656] Oerlemans 2011a, p. 897.
[657] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 41.
[658] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 77 e.v.
[659] De Lange 2009.
[660] Zie blog Jan-Jaap Oerlemans over het mogelijk maken van hacken als opsporingsmethode op 29 oktober 2011. Deze blog is te vinden via: http://oerlemansblog.weblog.leidenuniv.nl/2011/10/29/hacken-als-opsporingsbevoegdheid.
[661] Koning 2012, p. 49.

wordt gebruikt – bijvoorbeeld omdat deze zich bevindt in een woning – of dat het geautomatiseerde werk voor iedereen toegankelijk is.

6.2.4.3 Eisen aan een expliciete wettelijke grondslag hacken

Uit het rapport van de parlementaire enquêtecommissie bleek – naast het feit dat de activiteiten van de politie niet genormeerd waren – dat de bevoegdheden en verantwoordelijkheden van politie en justitie bij het hanteren van opsporingshandelingen onduidelijk waren.[662] Ook hier is een vergelijking te trekken met de situatie zoals die op dit moment is. Eerder in dit onderzoek bleek immers al dat het in de praktijk volstrekt onduidelijk is hoe er met hacken in de opsporingsfase dient te worden omgegaan en waar de grenzen van het hanteren van een dergelijke methode liggen. De bevoegdheden van opsporingsambtenaren omtrent hacken dienen daarom expliciet in de wet te worden vastgelegd.[663] Op die manier wordt duidelijkheid gecreëerd voor de opsporingsautoriteiten.[664] Daarbij moet worden voorkomen dat de omschrijving van de bevoegdheden dermate vaag is dat te ruime interpretaties aan deze kunnen worden gegeven.

Niet alleen moet voor politie en justitie duidelijk worden over welke mogelijkheden zij beschikken, ook moet controle van de wijze van uitoefening ervan mogelijk zijn. Er dient daarom uitdrukkelijk te worden vastgelegd met welke methode en op welke manier bepaalde informatie is verkregen of verzameld.[665] Van de inzet van hacken in het opsporingsonderzoek dient daarom uitdrukkelijk verslag te worden opgemaakt.

6.2.4.3.1 Eisen aan een expliciete wettelijke grondslag hacken voortvloeiend uit het opnemen van vertrouwelijke communicatie

Andere eisen of waarborgen die aan hacken door de politie kunnen worden gesteld, hangen samen met de zwaarte van deze bevoegdheid en de heimelijke aard ervan. Mijn inziens is het noodzakelijk, gelet op dit indringende en geheime karakter, om zware voorwaarden en procedurele eisen aan het inzetten van hacken in het opsporingsonderzoek te verbinden. Daarbij wil ik voor een groot gedeelte aansluiten bij de eisen die zijn gesteld bij het creëren van de bevoegdheid tot het opnemen van vertrouwelijke communicatie. Het afvangen van dergelijke communicatie is slechts toegestaan bij zware misdrijven.[666] Dat wil zeggen dat een verdenking van een misdrijf als omschreven in artikel 67 lid 1 Sv (onder andere misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaar of meer is gesteld) is vereist, dat bovendien gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert.[667] Een dergelijke beperking tot zware misdrijven acht ik – vanwege de aanzienlijke inbreuk op de rechten en vrijheden van de betrokken verdachte – tevens met betrekking tot hacken in de opsporingsfase noodzakelijk.

Een bevel tot opnemen van vertrouwelijke communicatie mag daarnaast alleen worden gegeven, indien het onderzoek dit dringend vordert. Alleen de communicatie die kan

---

[662] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 430.
[663] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 448.
[664] Oerlemans 2011a, p. 901.
[665] *Kamerstukken II* 1995/96, 24 072, nr. 10, p. 448.
[666] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 11 e.v.
[667] Zie artikel 126l lid 1 Sv.

bijdragen aan de opheldering en afdoening van het misdrijf en waarvan de opname in dat kader dringend gevorderd wordt, mag worden opgenomen.[668] Steeds geldt derhalve het subsidiariteitsvereiste, waaraan niet is voldaan indien met een andere, minder bezwarende methode kan worden volstaan.[669] Net als bij andere bevoegdheden moet een eventuele hackbevoegdheid derhalve alleen worden ingezet voor delicten waar een lichtere bevoegdheid geen resultaat zal opleveren. Dit hangt samen met de onmiskenbare inbreuk op het recht op een privéleven.[670] In dit kader is de vergelijking met het opnemen van vertrouwelijke communicatie en de doorzoeking ter vastlegging van gegevens interessant. Hiervoor heb ik immers betoogd dat deze bevoegdheden in wezen een zwaarder en ingrijpender karakter hebben dan hacken door de politie. Dit komt doordat voor hacken slechts het binnendringen van een geautomatiseerd werk noodzakelijk is, terwijl voor de doorzoeking en direct afluisteren naast het aanzetten van de computer en het bekijken van de inhoud ervan tevens het betreden van een woning of van een andere besloten plaats is vereist. In die zin wordt bij deze laatste twee bevoegdheden twee maal een ‘ruimte’ binnengegaan die in meer of mindere mate privacygevoelig is.

Toch kunnen de opsporingautoriteiten middels hacken ook bij privégegevens of -correspondentie. Hoewel een geautomatiseerd werk nog niet expliciet onder de beschermingsomvang van het EVRM is gebracht, speelt een dergelijk werk op privacygebied dikwijls een aanzienlijke rol. De inzet van hacken in het opsporingsonderzoek zal dientengevolge met grote zorgvuldigheid moeten worden betracht. Prins is in dit kader ook van mening dat hacken zich dient te beperken tot zeer ernstige misdrijven en alleen mag worden gebruikt als er geen andere mogelijkheid is om de zaak op te lossen. Oerlemans benadrukt hierbij dat er ook andere opsporingsmethoden zijn ontwikkeld om bepaalde informatie te bemachtigen. Hij wijst in het bijzonder op het bevriezingsbevel ex 126ni Sv. Vanwege het vluchtige karakter van gegevens in de digitale wereld kan voor een bepaalde periode worden bevolen dat deze gegevens worden bewaard in de oorspronkelijke vorm.[671] Het feit dat de mogelijkheid tot bevriezing van gegevens bestaat, neemt niet weg dat ik de invoering van hacken noodzakelijk acht. Hacken in de opsporingsfase kan immers ook worden gebruikt bij de aanpak van botnets en het opheffen van anonimiteit.

Naast het feit dat hacken slechts bij zware misdrijven mag worden ingezet en er voldaan moet zijn aan de subsidiariteitseis, acht ik een verplichte rechterlijke machtiging voorafgaand aan de inzet van de opsporingsbevoegdheid van belang. Net als bij het opnemen van vertrouwelijke communicatie dient de toepassing van de hackbevoegdheid aan een termijn gebonden te zijn en dient er te worden voorzien in een meldingsplicht achteraf. Deze plicht maakt het mogelijk voor betrokkenen om zich achteraf over de toepassing van de bevoegdheid te beklagen.[672] Hoewel ik van mening ben dat de bevoegdheid tot het opnemen van vertrouwelijke communicatie in vergelijking met de bevoegdheid tot hacken door opsporingsautoriteiten zwaarder en indringender is, bedreigen beiden het recht op privacy in ernstige mate. Ik ben daarom van mening dat alle criteria voor het uitoefenen van de

[668] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 78.
[669] Corstens 2011, p. 434.
[670] Prins 2012, p. 48 e.v.
[671] Interview R. Prins en J.J. Oerlemans op 5 juni 2012 ten burele van Fox-IT te Delft.
[672] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 11 e.v.

bevoegdheid tot direct afluisteren in een wettelijke bepaling voor hacken door de politie dienen terug te komen. Daarbij wil ik naar aanleiding van het interview met Prins en Oerlemans nog een aantal dingen toevoegen. Daarover volgt in de volgende subparagraaf meer.

6.2.4.3.2 Overige eisen aan een expliciete wettelijke grondslag hacken

Eerder in dit onderzoek werd al duidelijk dat men met het gebruik van een Trojaans politiepaard bij het zetten van een hack de volledige toegang krijgt tot de inhoud van de computer. Prins is daarom van mening dat voorafgaande aan het zetten van een hack specifiek moet worden aangegeven waar naar mag worden gezocht.[673] Net als bij het opnemen van vertrouwelijke communicatie dient de officier van justitie de bevoegdheid te krijgen een bevel tot hacken uit te vaardigen. Dit bevel dient in ieder geval het misdrijf en indien bekend de naam van de verdachte te vermelden. Daarnaast dient het bevel de plaats van het geautomatiseerde werk (IP-adres), de wijze waarop aan het bevel uitvoering dient te worden gegeven en de geldigheidsduur van het bevel te omvatten. Het bevel kan slechts worden gegeven na het verlenen van een schriftelijke machtiging door de rechter-commissaris. De machtiging dient alle onderdelen van het bevel te bevatten.[674] Wanneer het hacken door de politie eenmaal plaatsvindt, dient dit proces met waarborgen te worden omkleed en moet het daarnaast streng worden gecontroleerd.[675] In dit kader dient de officier van justitie ingevolge artikel 126aa Sv de processen-verbaal en andere gegevens die zijn verkregen door de uitoefening van hacken in het opsporingsonderzoek, voor zover die voor het onderzoek in de zaak van betekenis zijn, te voegen bij de processtukken.[676]

Prins pleit ter controle van de inzet van de bevoegdheid tot hacken voor het aflopen van scenario's tijdens het hacken. De officier van justitie en de rechter-commissaris dienen specifiek aan te geven wat er tijdens het binnendringen van geautomatiseerde werken mag en ook wat er niet mag. Vervolgens zullen de activiteiten van de hacker en de opsporingsambtenaar – dit zullen volgens Prins verschillende personen zijn – zorgvuldig moeten worden gemonitord en vastgelegd. Dat kan bijvoorbeeld door hun werkplek onder tap te zetten of op diverse momenten scherm- of video-opnames te maken.[677] Prins' waarborgen lijken mij zeer plausibel. Zeker vanwege het feit dat relatief gemakkelijk misbruik kan worden gemaakt van de bevoegdheid tot hacken.

Nu alle noodzakelijke waarborgen van een wettelijke hackbepaling grotendeels zijn behandeld, wil ik nog enkele opmerkingen maken over de structuur van een dergelijke regeling. Daarbij wil ik graag aanhaken bij de gedachte van Koning over een gelaagd systeem van digitale toegang op afstand.[678] Zoals reeds is vermeld, moet hacken niet worden beschouwd als één afgebakende opsporingsbevoegdheid, maar als een verzameling van methoden die in verschillende mate inbreuk maken op de grondrechten van de betrokken verdachte.[679] Verschillende vormen van hacken raken derhalve verschillende aspecten van het

[673] Interview R. Prins en J.J. Oerlemans op 5 juni 2012 ten burele van Fox-IT te Delft.
[674] Artikel 126l Sv.
[675] Interview R. Prins en J.J. Oerlemans op 5 juni 2012 ten burele van Fox-IT te Delft.
[676] Artikel 126aa Sv.
[677] Interview R. Prins en J.J. Oerlemans op 5 juni 2012 ten burele van Fox-IT te Delft.
[678] Koning 2012, p. 52.
[679] Oerlemans 2011a, p. 891.

recht op bescherming van de persoonlijke levenssfeer.[680] Koning pleit daarom voor een gelaagde structuur van digitale toegang op afstand met inachtneming van doel, technische betekenis, effect op de privacy en de juiste beschermingsniveaus.[681] Hiermee doelt de auteur naar mijn mening op de mogelijkheid in een wettelijke bepaling omtrent hacken onderscheid te maken tussen verschillende methoden van hacken. Zoals ik reeds in paragraaf 2.2.1 heb betoogd, kan hacken als overkoepelend begrip worden onderverdeeld in drie methoden: de online doorzoeking, het plaatsen van een technische voorziening op een geautomatiseerd werk en het beïnvloeden van een dergelijk werk. Iedere methode kan met een ander doel worden ingezet, vindt op een alternatieve manier plaats en heeft een verschillend effect op de privacy. Zo vormt de online doorzoeking een relatief lichte bevoegdheid, omdat hiermee slechts kan worden vastgesteld welke eigenschappen een computer heeft en omdat op grond van deze bepaling de computer kan worden doorzocht. Het plaatsen van een technische voorziening brengt daarentegen een zwaardere inbreuk op de persoonlijke levenssfeer met zich mee, omdat hiermee *real time* communicatie kan worden afgevangen. Omdat de potentiële inbreuk op het privéleven per methode verschilt, maar toch in alle gevallen ernstig is, ben ik van mening dat iedere handeling afzonderlijk zal moeten worden omschreven in de wet en met eigen waarborgen zal moeten worden omkleed. De methoden dienen echter niet te specifiek in een wettelijke bepaling te worden vastgelegd, omdat anders het risico bestaat dat de strafvorderlijke wet zijn soepelheid verliest. Uiteindelijk dient de officier van justitie strikte eisen te stellen aan de uitoefening van een bevoegdheid tot hacken en zullen deze eisen strenger moeten zijn naarmate de inzet van een dergelijke bevoegdheid een potentieel grotere inbreuk op de persoonlijke levenssfeer met zich mee zal brengen. Dit proces moet bovendien worden gecontroleerd en gewaarborgd door de rechter-commissaris.

Het is niet mogelijk een limitatieve opsomming te geven van alle in de toekomst denkbare opsporingsactiviteiten die wellicht ook een inbreuk op de privacy zouden kunnen maken. Er zal in dit systeem waarbij vergaande opsporingsbevoegdheden in de wet worden vastgelegd derhalve regelmatig moeten worden nagegaan of de wet door nieuwe ontwikkelingen moet worden aangepast.[682] Die tijd is wat mij betreft met betrekking tot hacken in de opsporingsfase aangebroken.

6.3 Opbouw van expertise voor hacken in het opsporingsonderzoek

Het uitsluitend invoeren van een wettelijke bevoegdheid tot hacken in het opsporingsonderzoek acht ik onvoldoende. Stol, Leukfeldt & Klap schetsen in dit kader het probleem van het gebrek aan kennis van politie en justitie over de huidige digitale mogelijkheden. De veranderende samenleving vraagt dat opsporingsautoriteiten zich aanpassen en met kennis, nieuwe bevoegdheden en apparatuur inspelen op een andere technologische omgeving.[683] De auteurs zijn van mening dat de politie anno 2012 nog flink wat heeft in te halen op de samenleving die haar omringt. Niet zozeer omdat er geen actie wordt ondernomen (zoals de oprichting van het Team High Tech Crime bij het KLPD en de

[680] Oerlemans 2011a, p. 908.
[681] Koning 2012, p. 52.
[682] Oerlemans 2011a, p, 908.
[683] Stol, Leukfeldt & Klap 2012, p. 26.

start van het Programma Aanpak Cybercrime bij de politie), maar wel omdat de acties nog pril zijn en te veel het karakter hebben van pionierswerk van enkelen. 'Digitaal' is ten onrechte nog geen normaal en integraal onderdeel van de politieorganisatie in volle breedte.[684] Er zal dus moeten worden geïnvesteerd in expertise op ICT-vlak bij de politie. Dat geldt ook voor hacken. De opbouw van deskundigheid op dit gebied is noodzakelijk. Toch blijft hacken een vaardigheid. Prins is in dit kader van mening dat het onmogelijk gaat worden om opsporingsambtenaren op te leiden tot gedegen hackers. Hacken is zeer specialistisch en vergt veel inzicht en vaardigheden. Daarom dient het zijns inziens te worden overgelaten aan 'echte' hackers. Dat is in het verleden reeds gebeurd. De ervaren hacker dringt de systemen binnen en de dienstdoende opsporingsambtenaar bekijkt, beoordeelt en noteert zijn handelingen.

Niet alleen zal er moeten worden geïnvesteerd in ICT-expertise bij de politieorganisatie, ook het rechterlijk apparaat kan op dat gebied niet achterblijven. Rechters-commissarissen, in de toekomst belast met het afgeven van een rechterlijke machtiging tot hacken, moeten volgens Prins meer verstand van zaken krijgen.[685]

6.4 Conclusie

Het criminele circuit maakt volop gebruik van de mogelijkheden op het gebied van ICT. Dit veranderende misdaadklimaat vraagt van politie en justitie dat zij zich blijven aanpassen met kennis, nieuwe bevoegdheden en apparatuur op deze voortschrijdende technologische omgeving. Het huidige digitale opsporingskader schiet in sommige gevallen toch tekort in de aanpak van computergerelateerde criminaliteit. Dat komt doordat het extreem gecompliceerd is geworden criminele activiteiten op het internet te traceren. Het verzamelen van criminele gegevens en het ophalen van gespreksstromen over strafbare feiten op geautomatiseerde werken wordt steeds moeilijker door de problemen die samenhangen met anonimiteit en versleuteling. Tevens wordt het digitale opsporingsonderzoek belemmert door het gebruik van botnets. Ik acht de invoering van hacken in het opsporingsonderzoek wenselijk, doordat het de problematiek omtrent anonimiteit en versleuteling kan omzeilen en omdat de opsporingsbevoegdheid botnets kan uitschakelen.

Het binnendringen van een computer door middel van een Trojaans politiepaard leidt onherroepelijk tot een inbreuk op de persoonlijke levenssfeer, tenzij er sprake is van het hacken van een onpersoonlijk geautomatiseerd werk. Nadat de toegang wordt verschaft, is in principe alles op die computer mogelijk. Op die manier kan allerlei privacygevoelige data worden benaderd. Het een en ander heeft tot gevolg dat de opsporingsbevoegdheid in een uitdrukkelijke wettelijke bepaling dient te worden vervat. Hacken kan mijns inziens dus niet onder een van de huidige wettelijke opsporingsbepalingen worden geplaatst. Door het normeren van hacken als bijzondere opsporingsbevoegdheid in ons strafvorderlijk wetboek zal, zowel voor de samenleving als voor opsporingsautoriteiten, inzicht worden verschaft onder welke voorwaarden dergelijke activiteiten in de opsporingsfase mogen worden verricht.

[684] Stol, Leukfeldt & Klap 2012, p. 37.
[685] Interview R. Prins en J.J. Oerlemans op 5 juni 2012 ten burele van Fox-IT te Delft.

Dit zal ten goede komen aan de betrouwbaarheid van de uitoefening van hacken in het opsporingsonderzoek en de risico's tot misbruik minimaliseren. Naast het codificeren van het op afstand binnendringen van geautomatiseerde werken door de politie dient er tevens te worden geïnvesteerd in ICT-expertise bij het rechterlijk apparaat en bij opsporingsautoriteiten.

Hoofdstuk 7 Conclusie en aanbevelingen

7.1 Hoofdlijnen onderzoek

In deze scriptie stond de volgende onderzoeksvraag centraal:

> Bestaat in het Wetboek van Strafvordering een wettelijke basis voor hacken in het opsporingsonderzoek en zo niet, is het wenselijk en noodzakelijk om een dergelijke basis te creëren?

De term hacken in de onderzoeksvraag verwijst naar het heimelijk en op afstand, via internet, binnendringen van een computer(systeem) of netwerk, althans van een geautomatiseerd werk. De strafvorderlijke overheid heeft te kennen gegeven hacken graag te willen toepassen in het opsporingsonderzoek naar computer- en internetgerelateerde criminaliteit. Een uitdrukkelijke basis in de wet ontbreekt echter voor dergelijk optreden. Toch zijn opsporingsautoriteiten er niet voor teruggedeinsd hacken in de opsporingsfase te gebruiken. Bij de Bredolab-ontmanteling, in de Rotterdamse zaak en in het onderzoek naar aanleiding van de Amsterdamse zedenzaak heeft de politie daarmee zijn strafvorderlijke bevoegdheden overschreden.

Vanwege de belangrijke rol van ICT-systemen in het dagelijkse leven en vanwege het heimelijke karakter van het op afstand binnendringen van dergelijke persoonlijke systemen, resulteert hacken in het opsporingsonderzoek in een aanzienlijke inbreuk op het recht op privacy ex artikel 8 EVRM. Het feit dat met de inzet van deze methode de volledige toegang wordt verschaft tot een computersysteem en de daartoe behorende gegevens, versterkt deze stelling temeer. Voor dergelijk ingrijpend overheidsoptreden vereisen het strafvorderlijke legaliteitsbeginsel en artikel 8 lid 2 EVRM een grondslag in de wet. De autoriteiten op opsporingsgebied hebben hacken in de opsporingsfase tot nu toe gelegitimeerd op basis van bestaande opsporingsbevoegdheden. Deze extensieve interpretatie van huidige methoden teneinde het binnendringen van geautomatiseerde werken mogelijk te maken, kan echter niet toelaatbaar worden geacht.

7.2 Mogelijkheden van hacken in het opsporingsonderzoek

Door de voortschrijdende ontwikkelingen op technologisch gebied en de opkomst van het internet is het criminele milieu aan verandering onderhevig. Niet alleen is er een aantal nieuwe (digitale) delicten ontstaan, ook bij de uitvoering van traditionele en conventionele strafbare feiten maken criminelen steeds vaker gebruik van de computer en het internet. De wetgever heeft in het Wetboek van Strafvordering verschillende opsporingsbevoegdheden gecreëerd, waarmee criminele data of correspondentie als zodanig of communicatie over strafbare feiten op geautomatiseerde werken kunnen worden bemachtigd, afgetapt of opgenomen.

Dergelijke informatie kan de politie echter tevens verwerven door het op afstand binnendringen van computers. Nadat men op deze wijze een geautomatiseerde werk is binnengegaan, hebben opsporingsautoriteiten de mogelijkheid om de eigenschappen van deze computer te beoordelen of gegevens op dit systeem te kopiëren (online doorzoeking). Als

ingrijpender alternatief kan de politie een technische voorziening op de harde schijf van het geautomatiseerde werk plaatsen, waarmee toetsaanslagen kunnen worden afgevangen en waarmee communicatie *real time* kan worden gemonitord. De derde optie na het binnendringen van een computer richt zich niet zozeer op de vergaring van opgeslagen of stromende gegevens, maar heeft betrekking op het op afstand besturen van een geautomatiseerd werk. De politie kan de computer op die manier op allerlei manieren beïnvloeden, zodat instellingen kunnen worden aangepast en het geautomatiseerde werk kan worden uitgeschakeld. Hacken vormt in die zin een heel effectief middel in de bestrijding van botnets. Tevens kunnen opsporingsautoriteiten middels het binnendringen van computers de anonimiteit die criminelen op het internet genieten, omzeilen. De invoering van een wettelijke bepaling voor hacken in het opsporingsonderzoek acht ik daarnaast wenselijk met het oog op de aanpak van de problematiek van versleuteling. Criminelen plegen hun gegevens op en gespreksverkeer via computers steeds vaker met ingewikkelde cryptografische technieken onleesbaar en daarmee ontoegankelijk te maken voor opsporingsautoriteiten. Via een hack kan internetverkeer bij de bron worden onderschept, waardoor correspondentie kan worden afgevangen voordat versleuteling plaatsvindt. Door het op afstand plaatsen van software op het geautomatiseerde werk van de verdachte heeft de politie tevens de mogelijkheid om toetsaanslagen te registreren, inclusief de wachtwoorden waarvan de verdachte gebruikmaakt. Met deze bemachtigde wachtwoorden kan de dienstdoende opsporingsambtenaar vervolgens de encryptie ongedaan maken.

7.3 Hacken als aanvulling op het huidige digitale wettelijke kader

Het versleutelprobleem is tevens aan te pakken met de bestaande bevoegdheid tot het opnemen van vertrouwelijke communicatie ex artikel 126l Sv. Deze bevoegdheid geeft opsporingsautoriteiten de ruimte om op de harde schijf van een computer software te plaatsen, waarmee direct afluisteren kan worden gerealiseerd. De opsporingsambtenaar dient hiervoor fysiek aanwezig te zijn op de locatie van de computer die wordt binnengedrongen. Hacken in de opsporingsfase vormt in die zin een te prefereren manier van het vergaren van strafbare communicatie als zodanig of communicatie over strafbare feiten en van het tenietdoen van versleuteling. Het van buitenaf binnendringen van computers kan met hetzelfde doel worden ingezet als het opnemen van vertrouwelijke communicatie, maar voorziet – vanwege het feit dat binnentreden van bijvoorbeeld een woning niet noodzakelijk is – in een lichtere inbreuk op de persoonlijke levenssfeer. Hacken, in het bijzonder de methode van het plaatsen van een technische voorziening op een geautomatiseerd werk, geniet mijns inziens, wanneer deze bevoegdheid met waarborgen wordt omkleed, dan ook de voorkeur.

Indien het opsporingsonderzoek niet zozeer is gericht op de verzameling van stromende communicatie, maar de bedoeling heeft om opgeslagen gegevens of bestanden te verwerven, kan naar mijn mening tevens worden volstaan met hacken door de politie. Op dit moment zou men op grond van de huidige strafvorderlijke wetgeving daarvoor de bevoegdheid tot het doorzoeken ter vastlegging van gegevens ex artikel 125i Sv kunnen inzetten. Voor de uitoefening van deze bevoegdheid is eveneens het betreden van een besloten plaats noodzakelijk. Het op afstand binnendringen van geautomatiseerde werken heeft daarom minder ingrijpende en bezwarende gevolgen voor de privacy van betrokkenen. In specifiek

omlijnde gevallen moet de inzet van hacken in het opsporingsonderzoek dientengevolge voorrang hebben boven de doorzoeking ter vastlegging van gegevens.

7.4 Hacken doorstaat de Straatsburgse toets

Hoewel hacken in vergelijking met de hiervoor behandelde opsporingsbevoegdheden resulteert in een minder grove inbreuk op de persoonlijke levenssfeer, betekent het niet dat er lichtvaardig met deze bevoegdheid mag worden omgesprongen. Het fundamentele recht op privacy blijft immers in het geding. Een inbreuk op het recht op een ongeschonden privéleven ten gevolge van hacken in het opsporingsonderzoek is gepermitteerd, indien aan de cumulatieve vereisten van artikel 8 lid 2 EVRM is voldaan.

Het EVRM eist in dit kader dat met de inzet van hacken door opsporingsautoriteiten een legitiem doel moet worden nagestreefd. Dat doel zal met betrekking tot deze opsporingsbevoegdheid het voorkomen van strafbare feiten zijn. Ten tweede dient hacken als bevoegdheid in de wet te worden vastgelegd. De bepaling dient immers voldoende toegankelijk te zijn voor het publiek. Dat wil zeggen dat de burger op de hoogte moet kunnen zijn van de regels die in het geval van hacken toepasselijk en van belang zijn. Tevens dient er sprake te zijn van strenge, heldere en gedetailleerde wetgeving, zodat de reikwijdte en wijze van uitoefening van de bevoegdheid in voldoende mate voorzienbaar of voorspelbaar is. Dat dient tot uitdrukking te komen bij de formulering van duidelijke eisen in de wettelijke hackbepaling, zoals de aanduiding van categorieën strafbare feiten op grond waarvan de bevoegdheid kan worden uitgeoefend en de wijze waarop de bevoegdheid kan worden uitgeoefend. Met betrekking tot de laatste voorwaarde dient naar mijn mening in de wet onderscheid te worden gemaakt in de drie hiervoor opgesomde hackmethoden: de online doorzoeking, het plaatsen van een technische voorziening op een geautomatiseerd werk en het beïnvloeden van een dergelijk werk. Iedere methode kan met een ander doel worden ingezet, vindt op een andere manier plaats en heeft een ander effect op de privacy. Daarom ben ik van mening dat iedere handeling afzonderlijk in een wettelijke bepaling dient te worden omschreven en met eigen toegespitste waarborgen dient te worden omkleed. De omschrijving moet echter niet te specifiek worden, omdat de wet dan aan soepelheid verliest.

De eis die in dit kader in ieder geval aan een hackbepaling in de wet dient te worden gesteld, is dat de bevoegdheid slechts mag worden uitgeoefend als sprake is van een verdenking van een misdrijf als omschreven in artikel 67 lid 1 Sv, dat bovendien gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. Daarnaast mag het bevel tot hacken door opsporingsautoriteiten slechts worden gegeven, indien het onderzoek dit dringend vordert. De bepaling moet bovendien voorzien in een plicht tot melding achteraf aan de betrokken personen. Voorafgaande aan het zetten van een hack dient door de officier van justitie specifiek te worden aangegeven waar precies naar mag worden gezocht op het geautomatiseerde werk en op welke manier. Daarnaast dient het bevel tevens het misdrijf, de locatie van het geautomatiseerde werk en de geldigheidsduur van het bevel te bevatten. Een verplichte rechterlijke machtiging voorafgaand aan de inzet van de opsporingsbevoegdheid acht ik – vanwege het ingrijpende karakter van het binnendringen van computersystemen –

noodzakelijk. De uitoefening van de bevoegdheid moet daarnaast op strikte wijze worden begeleid, gemonitord en gecontroleerd door de officier van justitie en de rechter-commissaris tezamen. Dergelijk toezicht kan plaatsvinden door de werkplek van de opsporingsambtenaar en de hacker onder de tap te zetten of door op diverse momenten scherm- of video-opnames te maken en vast te leggen.

Aldus moet met de inzet van hacken in het opsporingsonderzoek een legitiem doel worden nagestreefd en dient de inbreuk bij wet te zijn voorzien. Het derde en laatste criterium van het recht op een privéleven ziet op de noodzakelijkheid van de inbreuk in een democratische samenleving. Uit de jurisprudentie omtrent deze voorwaarde vloeit voort dat er voldaan moet zijn aan de eisen van proportionaliteit en subsidiariteit. Het belang dat met het binnendringen van computers kan worden gediend – namelijk de aanpak van versleuteling, anonimiteit en botnets – en de winst die ten opzichte van de bestaande digitale opsporingsmethoden kan worden behaald, rechtvaardigen naar mijn mening de inbreuk die met de inzet van de methode op het recht op privacy wordt gemaakt (proportionaliteit). Tevens kan tegemoet worden gekomen aan de subsidiariteitseis. Hacken in de opsporingsfase resulteert immers in verhouding met het opnemen van vertrouwelijke communicatie en de doorzoeking ter vastlegging van gegevens in een lichtere inbreuk op het recht op een privéleven.

7.5 Opbouw van expertise op digitaal vlak

Het uitsluitend invoeren van een wettelijke bevoegdheid tot hacken acht ik echter onvoldoende. Omdat hacken als zodanig zeer specialistisch is en veel inzicht en vaardigheden vergt, dient te worden geïnvesteerd in digitale expertise bij politie, justitie en het rechterlijk apparaat. Daartoe zullen op justitieel gebied leerprogramma's moeten worden ontwikkeld die de politie in staat zal stellen computer- en internetgerelateerde criminaliteit effectief op te sporen met behulp van de opsporingsbevoegdheid hacken. Vanwege het zeer technische karakter van hacken is het naar mijn mening niet mogelijk om alle opsporingsambtenaren op te leiden tot gedegen hackers, maar dienen zij wel op de hoogte te zijn van de mogelijkheden op dit gebied en de grenzen van een dergelijke bevoegdheid, zodat zij adequaat leiding kunnen geven aan en toezicht kunnen houden op de handelingen van de ervaren hacker. Wellicht dat in dit kader voor politie en justitie (bij)scholingsprojecten kunnen worden gestart, zodat aansluiting kan worden gezocht bij de digitale stand van zaken op het gebied van cybercrime en de opsporing daarvan. Tevens zal het digitale kennisniveau van de rechterlijke macht moeten worden verhoogd. Het internet en andere moderne communicatietechnologieën nemen binnen de samenleving en dientengevolge binnen de rechtspraktijk een steeds nadrukkelijkere plaats in. Het rechterlijk apparaat dient op de hoogte te zijn van wat er op gebied van cybercrime mogelijk is en welke gevolgen dit heeft voor de opsporing en vervolging van deze nieuwe criminaliteitsvorm. De zittende en staande magistratuur, en ook de advocatuur, zullen hier tijdens hun opleiding of met behulp van toegespitste cursussen in voldoende mate mee dienen te worden geconfronteerd. Mijns inziens moeten er dientengevolge specifieke leerprogramma's worden ontwikkeld die zich richten op de in te voeren opsporingsbevoegdheid hacken en nieuwe vormen van criminaliteit op het

internet. Wellicht dat in de toekomst binnen rechtbanken zelfs speciale cybercrimekamers moeten worden ingesteld – te vergelijken met de huidige belastingkamer en de militaire kamer – met cyberrechters die specifiek deskundig zijn op het gebied van de opsporing, vervolging en bestraffing van cybergerelateerde criminaliteit.

7.6 Grensoverschrijdend hacken

Op grond van het verrichte onderzoek kan worden geconstateerd dat voor hacken in het opsporingsonderzoek een wettelijke basis ontbreekt. Het binnendringen van ICT-systemen beschouw ik daarentegen wel als zeer bruikbaar in het opsporingsonderzoek. Ik acht de invoering van een of meerdere artikelen in het Wetboek van Strafvordering daarom zeer gewenst. Hierbij dient wel een kanttekening te worden geplaatst. Strafvorderlijk optreden op het grondgebied van een vreemde staat is vanwege het soevereiniteitsbeginsel niet toegestaan. De politie mag derhalve geen computer binnendringen die zich buiten Nederland bevindt. Door het grensoverschrijdende karakter van het internet worden gegevens overal ter wereld verspreid en opgeslagen. Om deze gegevens toch te kunnen bemachtigen, ziet de politie zich genoodzaakt ook computers te hacken die zich in het buitenland bevinden. Dergelijk handelen van opsporingsautoriteiten is echter niet toegestaan zonder verdragsrechtelijke basis of rechtshulp. De invoering van hacken in de opsporingsfase zal daarom in de praktijk niet altijd van waarde zijn. Het internet kent immers geen grenzen. Gegevens zijn overal ter wereld te vinden en criminelen kunnen gemakkelijk gebruikmaken van computer(systemen) gelegen op het grondgebied van andere staten.

Desalniettemin acht ik de invoering van een wettelijke bevoegdheid tot hacken wel noodzakelijk en gewenst. Zonder een basis in de wet is grensoverschrijdend hacken sowieso niet toelaatbaar. De uitoefening van een opsporingsbevoegdheid, zoals het op afstand binnendringen van een geautomatiseerd werk in een andere staat is met rechtshulp slechts toegestaan, indien dat in ons land ook wettelijk gezien is geoorloofd. Aan het systeem van rechtshulp kleven met betrekking tot het grensoverschrijdend hacken echter enkele bezwaren. Een van die beletselen vloeit voort uit de vluchtigheid van gegevens. Rechtshulpverzoeken vergen over het algemeen veel tijd en inspanning. Voordat de aangezochte staat zijn toestemming voor het binnendringen van geautomatiseerde werken op zijn territorium heeft gegeven, kan van server zijn gewisseld, kan data zijn gewist of kunnen gegevens zijn verspreid over meerdere andere staten. Grensoverschrijdend hacken in de aangezochte staat is dan niet meer nodig. Het systeem van rechtshulp omtrent hacken op andermans grondgebied is tevens om een andere reden niet werkbaar. Voor iedere afzonderlijke grensoverschrijdende opsporingshandeling dient rechtshulp te worden gezocht. De verwachting is dat – doordat landsgrenzen en internetgrenzen niet samenvallen – de politie steeds regelmatiger systemen wenst binnen te dringen die zijn gevestigd op het territorium van een andere staat. Als ons land voor ieder e-mailbericht of voor elke set gegevens rechtshulp moet zoeken, zal dat enorm tijdrovend zijn en een te hoge administratieve werkdruk leggen op de autoriteiten op dat gebied.

Mijns inziens is het daarom beter om te streven naar een verdragsrechtelijke basis voor grensoverschrijdend hacken. Goedkeuring om opsporingsbevoegdheden in het buitenland te kunnen verrichten, kan immers – naast het verzoeken van rechtshulp – ook worden verkregen

bij verdrag. Het sluiten van bilaterale verdragen vormt in dit kader een mogelijkheid, al ontstaat dan het risico dat personen met criminele bedoelingen hun toevlucht zullen zoeken tot staten waarmee ons land geen verdrag heeft gesloten. Criminele gegevens of communicatie over strafbare feiten zijn dan alsnog onbereikbaar voor Nederlandse opsporingsautoriteiten. Mijn aanbeveling strekt daarom tot de ontwikkeling van een groot multilateraal verdrag voor grensoverschrijdend hacken. Daarin moet in ieder geval een notificatieplicht staan vermeld, die de andere staat achteraf op de hoogte stelt van de door bijvoorbeeld Nederland ontplooide opsporingsactiviteiten op zijn grondgebied. Hacken vindt immers heimelijk en vanuit het territorium van Nederland plaats en zal dientengevolge voor de andere staat lastig te ontdekken zijn. Dat is, zoals is betoogd, de kracht van deze opsporingsmethode. Om de andere staat toch in kennis te stellen van het uitoefenen van hacken op zijn grondgebied en om hem de mogelijkheid te bieden zich achteraf te beklagen over de toepassing van deze bevoegdheid acht ik een notificatieplicht van belang.

Ten slotte wil ik nog enkele opmerkingen maken over de reikwijdte van een verdrag omtrent grensoverschrijdend hacken. Het is mogelijk om een dergelijk verdrag te ontwikkelen voor lidstaten van de Europese Unie. Het beginsel van wederzijdse erkenning als ‘hoeksteen van de samenwerking in strafzaken’ zorgt er in dit geval voor dat ingewikkelde rechtshulpkwesties kunnen worden vermeden. Er kan in de lidstaten over en weer worden gehackt door opsporingsautoriteiten, zonder dat de betreffende autoriteiten zich genoodzaakt zien de rechtmatigheid van het optreden van de andere lidstaat te toetsen. Een wereldwijd verdrag tot grensoverschrijdend hacken heeft echter mijn voorkeur. Wederom geldt dat hoe meer staten zich aansluiten bij een dergelijk verdrag, hoe minder ruimte het criminele circuit krijgt om digitaal uit de wijken naar het grondgebied van staten die geen partij zijn bij het verdrag. De politieke haalbaarheid van een verdrag tot grensoverschrijdend hacken valt buiten het bestek van dit onderzoek. Met deze scriptie wil ik slechts signaleren dat er voor politie en justitie problemen bestaan ten gevolge van de grenzeloze verspreiding van gegevens en geautomatiseerde werken. De enige werkbare en juridisch correcte oplossing vormt in mijn ogen de ontwikkeling van een verdrag tot grensoverschrijdend hacken, zodat staten weliswaar hun soevereiniteit enigszins beperken, maar het binnendringen van geautomatiseerde werken op andermans grondgebied wel geoorloofd gebeurd. Daaraan ten grondslag dient een bevoegdheid tot hacken in het Wetboek van Strafvordering te liggen.

7.7 Tot slot

De enige adequate reactie op de bestaande tekortkomingen in het strafvorderlijke wetboek met betrekking tot de opsporing en vervolging van computer- en internetgerelateerde criminaliteit is het initiëren van wetgeving op zowel nationaal als internationaal gebied, zodat hacken door opsporingsautoriteiten in het opsporingsonderzoek toelaatbaar kan plaatsvinden. Die reactie is in elk geval te prefereren boven een strafvorderlijk apparaat dat zijn bevoegdheden structureel overschrijdt.

Literatuurlijst

BOEKEN

Blom 2001
T. Blom, 'Privacy, EVRM en (straf)rechtshandhaving', in: C.H. Brants, P.A.M. Mevis & E. Prakken (red.), *Legitieme strafvordering. Rechten van de mens als inspiratie in de 21ste eeuw*, Antwerpen-Groningen: Intersentia Rechtswetenschappen 2001.

Blom 2011
T. Blom, 'Wetboek van Strafvordering, Boek I, Titel IVa, Afd. 6, Art. 126l', in: C.P.M. Cleiren & M.J.M. Verpalen (red.), *Strafvordering. Tekst en Commentaar*, Deventer: Kluwer 2011.

Burkens e.a. 2006
M.C. Burkens e.a., *Beginselen van de democratische rechtstaat*, Deventer: Kluwer 2006.

Buruma 1998
Y. Buruma, *Internet en Strafrecht, preadvies NJV 1998*, Deventer: Kluwer 1998.

Buruma 2000
Y. Buruma, 'Nederland', in: P.J.P. Tak, *Heimelijke opsporing in de Europese Unie. De normering van bijzondere opsporingsmethoden in de landen van de Europese Unie*, Antwerpen-Groningen: Intersentia Rechtswetenschappen 2000.

Buruma 2001
Y. Buruma, *Buitengewone opsporingsmethoden*, Deventer: W.E.J. Tjeenk Willink 2001.

Cleiren 1992
C.P.M. Cleiren, *De openheid van de wet, de geslotenheid van het recht* (oratie Leiden), Deventer: Kluwer 1992.

Cleiren 2011
C.P.M. Cleiren, 'Wetboek van Strafvordering, Boek I, Titel I, Afd. 1, Art. 1', in: C.P.M. Cleiren & M.J.M. Verpalen (red.), *Strafvordering. Tekst en Commentaar*, Deventer: Kluwer 2011.

Corstens 2011
G.J.M. Corstens, *Het Nederlands strafprocesrecht*, Deventer: Kluwer 2011.

Ekker 2006
A.H. Ekker, *Anoniem communiceren: van drukpers tot weblog* (ITeR-reeks nr. 76), Den Haag: Sdu uitgevers 2006.

Van den Eshof e.a. 2002
G.L.M. van den Eshof e.a., *Opsporing van verborgen informatie* (ITeR-reeks nr. 56), 's-Gravenhage: Sdu Uitgevers 2002.

Hofman 1995
J.A. Hofman, *Vertrouwelijke communicatie. Een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht* (diss. Amsterdam VU), Zwolle: W.E.J. Tjeenk Willink 1995.

Kaspersen 2007
H.W.K. Kaspersen, 'Het Cybercrime-verdrag van de Raad van Europa', in: B.J. Koops, *Strafrecht en ICT*, Den Haag: Sdu Uitgevers 2007.

Klip 2000
A.H. Klip, 'Soevereiniteit in het strafrecht', in: G.J.M. Corstens & M.S. Groenhuijsen (red.), *Rede en Recht: opstellen ter gelegenheid van het afscheid van prof. mr. N. Keijzer van de Katholieke Universiteit Brabant*, Deventer: Gouda Quint 2000.

Koops 2000
B.J. Koops, *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?* (ITeR-reeks nr. 31), Deventer: Kluwer 2000.

Koops 2007
B.J. Koops, ' Cryptografie en strafvordering', in: B.J. Koops, *Strafrecht en ICT*, Den Haag: Sdu Uitgevers 2007.

Koops & Buruma 2007
B.J. Koops & Y. Buruma, 'Formeel strafrecht en ICT', in: B.J. Koops, *Strafrecht en ICT*, Den Haag: Sdu Uitgevers 2007.

Kronenberg & De Wilde 2010
M.J. Kronenberg & B. de Wilde, *Grondtrekken van het Nederlandse strafrecht*, Deventer: Kluwer 2010.

Leukfeldt, Domenie & Stol 2010
E.R. Leukfeldt, M.M.L. Domenie & W.Ph. Stol, *Verkenning cybercrime in Nederland 2009*, Den Haag: Boom Juridische uitgevers 2010.

Meijer 2009
G.H. Meijer, 'Overig. Nr. 77 Nemo tenetur', in: G.H. Meijer, A. Seuters & R. ter Haar, *Leerstukken Strafrecht*, Deventer: Kluwer 2009.

Mevis 2009
P.A.M. Mevis, *Capita Strafrecht*, Nijmegen: Ars Aequi Libri 2009.

Reijntjes, Mos, Sjöcrona 2008
J.M. Reijntjes, M.R.B. Mos & J.M. Sjöcrona, 'Wederzijdse rechtshulp', in: E. van Sliedregt, J.M. Sjöcrona & A.M.M. Orie, *Handboek Internationaal Strafrecht*, Deventer: Kluwer 2008.

Schermer 2003
B.W. Schermer, *Opsporing vs. privacy in peer-to-peer netwerken* (ITeR-reeks nr. 64), 's-Gravenhage: Sdu Uitgevers 2003.

Seuters 2009
A. Seuters, 'Delicten. 25. Huisvredebreuk': in: G.H. Meijer, A. Seuters & R. ter Haar, *Leerstukken Strafrecht*, Deventer: Kluwer 2009

Sjöcrona & Orie 2002
J.M. Sjöcrona & A.M.M. Orie, *Internationaal strafrecht vanuit Nederlands perspectief*, Deventer: Kluwer 2002.

Smits 2006
A. Smits, *Strafvorderlijk onderzoek van telecommunicatie*, Nijmegen: Wolf Legal Publishers 2006.

Vande Lanotte & Haeck 2005
J. Vande Lanotte & Y. Haeck, *Handboek EVRM*, Antwerpen: Intersentia 2005.

Vedder e.a. 2007
A. Vedder e.a., *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, Den Haag: Rathenau Instituut 2007.

Verbeek, De Roos & Van den Herik 2000
J.P.G.M. Verbeek, Th.A. de Roos & J. van den Herik, *Interceptie van vertrouwelijke communicatie* (ITeR-reeks, nr. 35), 's-Gravenhage: Sdu Uitgevers 2000.

Ten Voorde 2010
J.M. ten Voorde, 'Boek 2, Titel V, Art. 138a Wetboek van Strafrecht', in: C.P.M Cleiren & M.J.M. Verpalen, *Strafrecht. Tekst en Commentaar*, Deventer: Kluwer 2010.

Wiemans 2004
F.P.E. Wiemans, *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2004.

ARTIKELEN

Antic 2012
M. Antic, 'De nieuwe cookieregels, onduidelijk, onjuist en ineffectief', *AA* 2012/2.

Boek 2000
J.L.M. Boek, 'Hacken als opsporingsmethode onder de Wet BOB', *NJB* 2000, 11.

Buermeyer 2007
U. Buermeyer, 'Die '"Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme', *HRRS Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht* 2007-4.

Corstens 1995
G.J.M. Corstens, 'Normatieve grenzen van opsporingsmethoden', *DD* 1995, 6.

Crielaard 2011
M. Crielaard, 'Vaak onduidelijk wat Cloud inhoudt', *Computable* 28 juli 2011. (Te vinden via: http://www.computable.nl/artikel/ict_topics/cloud_computing/4061171/2333364/vaak-onduidelijk-wat-cloud-inhoudt.html).

Fox 2007
D. Fox, 'Realisierung, Grenzen und Risiken der "Online-Durchsuchung"', *Datenschutz und Datensicherheit* 2007.

Groothuis & De Jong 2010
M.M. Groothuis & T. de Jong, 'Is een nieuw grondrecht op integriteit en vertrouwelijkheid van ICT-systemen wenselijk? Een verkenning', *P&I* 2010/6.

De Hert, De Vries & Gutwirth 2009
P. de Hert, K. de Vries & S. Gutwirth, 'Duitse rechtspraak over remote searches, datamining en afluisteren op afstand. Het arrest Bundesverfassungsgericht 27 februari 2008 (Online-Durchsuchung) in breder perspectief.', *Computerrecht* 2009, 189.

Van den Hoven van Genderen 2008
R. van den Hoven van Genderen, 'Notice and take down (NTD-) gedragscode, gewenste censuur?', *Computerrecht* 2008, 6.

Koning 2012
M.E. Koning, 'Van teugelloos 'terughacken' naar 'digitale toegang op afstand', *P&I* 2012/2.

Koops 2003
B.J. Koops, 'Het Cybercrime-verdrag, de Nederlandse strafwetgeving en de (computer)criminalisering van de maatschappij', *Computerrecht* 2003, 2.

Koops 2010
B.J. Koops, 'Tijd voor Computercriminaliteit III', *NJB* 2010, 85.

Koops 2012a
B.J. Koops, 'De dynamiek van cybercrimewetgeving in Europa en Nederland', *JV* 2012, 01.

Koops 2012b
B.J. Koops, 'Politieonderzoek in open bronnen op internet. Strafvorderlijke aspecten', *Tijdschrift voor Veiligheid* 2012/02.

Koops & Prinsen 2005
B.J. Koops & M.M. Prinsen, 'Glazen woning, transparant lichaam. Een toekomstblik op huisrecht en lichamelijke integriteit', *NJ* 2005, 12.

Van der Kroft 2011
D. van der Kroft, 'Bredolab: Trojaans paradepaardje van het KLPD?', *Bits of Freedom* 7 november 2011. (Te vinden via: https://www.bof.nl/2011/11/07/bredolab-trojaans-parade-paardje-van-het-klpd/).

Laan 2011
M. Laan, 'KLPD zoekt grenzen op internet op', *BN de Stem* 20 april 2011 (Te vinden via: http://www.bndestem.nl/algemeen/internet/8611463/KLPD-zoekt-grenzen-op-internet-op.ece).

Lake 2011
E. Lake, 'British Firm Offered Spy Software to Egypt', *Washington Times* 25 april 2011. (Te vinden via: http://www.washingtontimes.com/news/2011/apr/25/british-firm-offered-spy software-to-egypt/).

De Lange 2009
A. de Lange, 'Telefooncel criminele vrijplaats', *Het Parool* 25 juli 2009.

Lensing 1994
J.A.W. Lensing, 'De evolutie van de politiebevoegdheden in het raam van de bestrijding van de georganiseerde misdaad.', *DD* 1994, 24.

Van der Linden & Baardman 2011
M. van der Linden & A. Baardman, 'Cybercrime: ontwikkelingen en de invloed daarvan op de strafrechtketen', *Strafblad* 2011/4.

Odinot & De Jong 2012
G. Odinot & D. de Jong, 'Wie belt er nou nog? De veranderende opbrengst van de telefoontap', *JV* 2012, 03.

Oerlemans 2010
J.J. Oerlemans, 'Het conceptwetsvoorstel versterking bestrijding computercriminaliteit nader bezien', *Tijdschrift voor Internetrecht* 2010-5.

Oerlemans 2011a
J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid', *DD* 2011, 62.

Oerlemans 2011b
J.J. Oerlemans, 'Conceptwetsvoorstel Computercriminaliteit III: onzorgvuldige wetgeving?', *Informatie Beveiliging* 2011, nr. 4.

Oerlemans 2012
J.J. Oerlemans, 'Mogelijkheden en beperkingen van de internettap', *JV* 2012, 03.

Oerlemans & Koops 2011
J.J. Oerlemans & B.J. Koops, 'De Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets', *NJ* 2011, 914.

Prins 2012
R. Prins, 'Een veilige cyberwereld vraagt nieuw denken', *JV* 2012, 01.

Proos 2008
M. Proos, 'Justitie enthousiast over hacken computers', *BN de Stem* 17 mei 2008. (Te vinden via: http://www.bndestem.nl/algemeen/binnenland/3134803/Justitie-enthousiast-over-hacken-computers.ece).

Reijntjes 2012
J.M. Reijntjes, 'Opsporing met open grenzen', *Strafblad* 2012/3.

Spierings & Pesselse 2012
C. Spierings & G. Pesselse, 'Reële diefstal van een virtuele amulet: een analyse van het Runescape-arrest vanuit straf- en goederenrechtelijk perspectief', *NTBR* 2012/28.

Stevens & Koops 2009
L. Stevens & E.J. Koops, 'Opzet op de harde schijf: criteria voor opzettelijk bezit van digitale kinderporno', *DD* 2009, 51.

Stol, Leukfeldt & Klap 2012
W.Ph. Stol, E.R. Leukfeldt & H. Klap, 'Cybercrime en politie. Een schets van de Nederlandse situatie anno 2012', *JV* 2012, 01.

Van Tuil 2012
K. van Tuil, 'Wat is VoIP?', *Computerworld* 3 januari 2012. (Te vinden via: http://computerworld.nl/article/13422/wat-is-voip.html).

De Winter 2011
B. de Winter, 'Politie hackt pedosites via Tor', *Webwereld* 31 augustus 2011. (Te vinden via: http://webwereld.nl/nieuws/107777/politie-hackt-pedosites-via-tor.html).

RAPPORTEN

Baaijens-van Geloven 2001
Y.G.M. Baaijens-van Geloven, 'Strafvordering en rechtshulp', in: M.S. Groenhuijsen en G. Knigge (red.), *Het vooronderzoek in strafzaken, tweede interimrapport, onderzoeksproject Strafvordering 2001*, Deventer: Gouda Quint 2001.

Baaijens-van Geloven & Simmelink 2002
Y.G.M. Baaijens-van Geloven & J.B.H.M. Simmelink, 'Normering van de opsporing', in: M.S. Groenhuijsen & G. Knigge (red.), *Dwangmiddelen en rechtsmiddelen. Derde interimrapport onderzoeksproject Strafvordering 2001*, Deventer: Kluwer 2002.

Beijer e.a. 2004
A. Beijer e.a., *De Wet bijzondere opsporingsbevoegdheden – eindevaluatie*, Den Haag: Boom Juridische uitgevers, WODC 2004.

Cuijpers e.a. 2011
C. Cuijpers e.a., *Rapport De wolk in het onderwijs. Privacy aspecten bij cloud computing services*, Tilburg: Tilburg Institute for Law, Technology, and Society 2011. (te vinden via: http://www.surfacademy.nl/media/Seminar%20Privacy/De_wolk_in_het_onderwijs_feb2011[1].pdf).

GOVCERT.NL 2010
GOVCERT.NL, *Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010*, in opdracht van de ministeries van Binnenlandse zaken en Koninkrijksrelaties, Economische Zaken en Justitie 2010.

GOVCERT.NL 2011
GOVCERT.NL, *Cybersecuritybeeld Nederland*. December 2011.

Helmus, Smulders & Van der Zee 2006
S. Helmus, A. Smulders & F. van der Zee, *TNO-rapport. ICT-veiligheidsbeleid in Nederland – Analyse en overwegingen bij herijking*, TNO 2006.

Van der Hulst & Neve 2008
R.C. van der Hulst & R.J.M. Neve, *High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie*, Den Haag: Boom Juridische uitgevers, WODC 2008.

KLPD, Dienst Nationale Recherche 2009
KLPD, Dienst Nationale Recherche, *High tech crime. Criminaliteitsbeeldanalyse 2009*, Driebergen: KLPD 2010.

Knigge & Kwakman 2001
G. Knigge & N.J.M. Kwakman, 'Het opsporingsbegrip en de normering van de opsporingstaak', in: M.S. Groenhuijsen & G. Knigge (red.), *Het vooronderzoek in strafzaken; tweede interimrapport onderzoeksproject Strafvordering 2001*, Deventer: Gouda Quint 2001.

Ministerie van Veiligheid en Justitie 2011
Ministerie van Veiligheid en Justitie, *Juridisch kader Cyber Security*, 's-Gravenhage: Ministerie van Veiligheid en Justitie 2011.

Odinot e.a. 2012
G. Odinot e.a., *Het gebruik van de telefoon- en internettap in de opsporing*, Den Haag: WODC 2012.

VERDRAGEN EN WETGEVING

Trb. 2002, 18.

Stb. 1993, 33.
Stb. 1999, 245.
Stb. 2004, 394.
Stb. 2006, 299.
Stb. 2006, 300.

Aanwijzing opsporingsbevoegdheden 2012 (*Stcrt*. 2012, 10486).

Voorstel voor een kaderbesluit van de Raad betreffende het Europees bewijsverkrijgingsbevel ter verkrijging van voorwerpen, documenten en gegevens voor gebruik in strafprocedures, COM(2003) 688 definitief.

Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006 (GVB1 NW, S. 620).

KAMERSTUKKEN

Kamerstukken II 1967/68, 9 419, nr. 3.

Kamerstukken II 1975/76, 13 872, nr. 3.

Kamerstukken II 1989/90, 21 551, nr. 1-3.

Kamerstukken II 1995/96, 24 072, nr. 10.

Kamerstukken II 1996/97, 25 403, nr. 3.

Kamerstukken II 1997/98, 25 403, nr. 7.

Kamerstukken II 1998/99, 26 671, nr. 3.

Kamerstukken II 2001/02, 28 197, nr. 3.

Kamerstukken II 2001/02, 28 366, nr. 1.

Kamerstukken II 2003/04, 29 441, nr. 3.

Kamerstukken II 2004/05, 26 671, nr. 10.

Kamerstukken II 2007/08, 28 684, nr. 144.

Kamerstukken II 2007/08, 31 145, nr. 9.

Kamerstukken II 2008/09, 28 684, nr. 232.

Conceptwetsvoorstel versterking bestrijding computercriminaliteit 2009/10.

Kamerstukken II 2010/11, 32 710, nr. 1.

Kamerstukken II 2010/11, 25 november 2010, Antwoord op Kamervragen van PvdA Kamerlid Recourt van de minister van Veiligheid en Justitie, kenmerk: 2010Z15331.

Kamerstukken II 2011/12, 7 februari 2012, Antwoord op Kamervragen van de D66 Kamerleden Schouw en Berndsen van de minister van Veiligheid en Justitie, aanhangselnummer 1374.

Kamerstukken II 2011/12, 5 maart 2012, Antwoord op Kamervragen van de PVV Kamerleden Elissen en Van Bemmel, Kooiman van de SP en de D66 leden Berndsen en Schouw van de minister van Justitie, kenmerk: 222096, 2012Z00283 en 2012Z00353.

ELEKTRONISCHE BRONNEN

http://www.eerstekamer.nl/wetsvoorstel/32717_implementatie_kaderbesluit.

http://www.nbip.nl/nieuws/nbip-heeft-tachtig-deelnemers/.

http://nieuwsuur.nl/video/193369-internetbankieren-niet-100-procent-veilig.html.

http://nieuwsuur.nl/video/193776-de-strijd-tegen-cybercrime.html.

http://nos.nl/artikel/378811-robert-m-en-om-in-hoger-beroep.html.

http://oerlemansblog.weblog.leidenuniv.nl/2011/10/.

http://oerlemansblog.weblog.leidenuniv.nl/2011/10/29/hacken-als-opsporingsbevoegdheid.

http://www.om.nl/onderwerpen/verkeer/@156657/kinderporno-anonieme/.
http://www.rijksoverheid.nl/onderwerpen/kinderporno/bestrijding-kinderporno.

OVERIG

Interview R. Prins en J.J. Oerlemans op 5 juni 2012 ten burele van Fox-IT te Delft.

Jurisprudentielijst

EUROPEES HOF VOOR DE RECHTEN VAN DE MENS

EHRM 7 december 1976, nr. 5493/72 (*Handyside/Verenigd Koninkrijk*).
EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland*).
EHRM 26 april 1979, nr. 6538/74 (*The Sunday Times/Verenigd Koninkrijk*).
EHRM 25 maart 1983, nr. 5947/72 (*Silver e.a./Verenigd Koninkrijk*).
EHRM 2 augustus 1984, nr. 8691/79 (*Malone/Verenigd Koninkrijk*).
EHRM 24 mei 1988, nr. 10737/84 (*Müller e.a./Zwitserland*).
EHRM 24 april 1990, nr. 11801/85 (*Kruslin/Frankrijk*).
EHRM 24 april 1990, nr. 11105/84 (*Huvig/Frankrijk*).
EHRM 15 juni 1992, nr. 12433/86 (*Lüdi/Zwitserland*).
EHRM 16 december 1992, nr. 13710/88 (*Niemietz/Duitsland*).
EHRM 23 november 1993, nr. 14838/89 (*A./Frankrijk*).
EHRM 26 september 1995, nr. 17851/91 (*Vogt/Duitsland*).
EHRM 8 februari 1996, nr. 18731/91 (*Murray/Verenigd Koninkrijk*).
EHRM 17 december 1996, nr. 19187/91 (*Saunders/Verenigd Koninkrijk*).
EHRM 25 maart 1998, nr. 44787/98 (*Halford/Verenigd Koninkrijk*).
EHRM 30 juli 1998, nr. 27671/95 (*Valenzuela/Spanje*).
EHRM 12 mei 2000, nr. 35394/97 (*Khan/Verenigd Koninkrijk*).
EHRM 28 januari 2003, nr. 44647/98 (*Peck/Verenigd Koninkrijk*).
EHRM 1 juli 2008, nr. 58243/00 (*Liberty e.a./Verenigd Koninkrijk*).
EHRM 4 december 2008, nr. 30562/04 (*S. en Marper/Verenigd Koninkrijk*).
EHRM 17 december 2009, nr. 5335/06 (*Bouchacourt/Frankrijk*).
EHRM 17 december 2009, nr. 16428/05 (*Gardel/Frankrijk*).
EHRM 17 december 2009, nr. 22115/06 (*M.B./Frankrijk*).

EUROPESE COMMISSIE VOOR DE RECHTEN VAN DE MENS

ECRM 30 maart 1989, nr. 10461/83 (*Chappell/Verenigd Koninkrijk*).
ECRM 9 mei 1989, nr. 12175/86 (*Hope Hewitt en Harman/Verenigd Koninkrijk*).

HOGE RAAD

HR 6 april 1915, *NJ* 1915, 427.
HR 7 februari 1956, *NJ* 1956, 147.
HR 9 januari 1987, *NJ* 1987, 928.
HR 4 maart 1994, *NJ* 1994, 475.
HR 19 december 1995, *NJ* 1996, 249 (*Zwolsman*).
HR 3 december 1996, *NJ* 1997, 574.
HR 18 mei 1999, *NJ* 2000, 104.
HR 18 mei 1999, *NJ* 2000, 107.

HR 22 februari 2011, *LJN* BN9287.
HR 15 april 2011, *NJ* 2012, 345.
HR 20 december 2011, *NJ* 2012, 159.
HR 20 december 2011, *NJ* 2012, 160.
HR 31 januari 2012, *LJN* BQ9251.

GERECHTSHOF

Hof 's-Gravenhage 9 maart 2011, *LJN* BP7080.
Hof 's-Gravenhage 27 april 2011, *LJN* BR6836.

RECHTBANK

Rb. Amsterdam 21 mei 2012, *LJN* BW6148
Rb. Amsterdam 21 mei 2012, *LJN* BW6149
Rb. Rotterdam 27 maart 2009, *LJN* BH9324.
Rb. Rotterdam 26 april 2010, *LJN* BM2520.

OVERIG

BVerfG 27 februari 2008, 'Online-Durchsuchung', m.nt. W.A.M. Steenbruggen, *Mediaforum* 2008, 5.