*Mr. M.E. Koning**

Wetenschappelijk artikel
Van teugelloos 'terughacken' naar 'digitale toegang op afstand'

52

Trefwoorden:
terughacken, digitale toegang op afstand, online-opsporing, digitale opsporing, cybersecurity

Het technisch effect van terughacken op de privacy is de totaalsom van het doorzoeken, aftappen, heimelijk volgen, observeren en infiltreren. Na toegang tot een ICT-systeem maakt de techniek immers alles mogelijk. De inbreuk op het privéleven is potentieel zeer groot. In dit artikel worden twee uiteenlopende inbreuken beschreven. Tevens wordt aangetoond dat het naar de mening van de auteur onmogelijk is om terughacken onder een reeds bestaande strafvorderlijke bevoegdheid te schuiven.

1 Inleiding

Eind december 2011 stuurde de Minister van Justitie en Veiligheid een flink pak papier over cybersecurity naar de Tweede Kamer.[1] Het hete hangijzer bij de herziening van onlineopsporingsbevoegdheden terughacken oftewel online doorzoeken wordt niet geadresseerd.[2] De minister geeft aan dat een dergelijke bevoegdheid nader wordt verkend.[3] Al tweemaal eerder heeft de minister aangegeven dat er in het opsporingsveld behoefte bestaat aan een wettelijke terughackbevoegdheid, maar tot wetgevende stappen is het nog niet gekomen.[4]

Inmiddels kan met zekerheid worden gesteld dat deze opsporingsmethode al wordt gebruikt door het Korps Landelijke Politiediensten (KLPD).[5] Het Openbaar Ministerie (OM) is van mening dat de reeds bestaande bevoegdheden toereikend zijn. In dit artikel wordt de juistheid van die stelling onderzocht. Hierbij zal het terughacken bij de Bredolab-botnet-ontmanteling in relatie tot het privacyrecht juridisch geanalyseerd worden.[6] Vervolgens wordt de vormgeving van een eventuele bevoegdheid nader onder de loep genomen, waarbij een gelaagd bevoegdheidssysteem van digitale toegang op afstand wordt afgewogen tegen meer algemene terughackbepalingen.

2 De feiten

2.1 *Bredolab*

In oktober 2010 werd onder veel mediabelangstelling het criminele computernetwerk Bredolab ontmanteld.[7] Dit zogenoemde botnet bestond uit een netwerk van op afstand bestuurbare computers. De rechtmatige gebruikers van de computers (c.q. slachtoffers) wisten niet dat een ander de controle over het besturingssysteem had genomen middels een computervirus. Het botnet kon via Command & Controlservers door de cybercrimineel worden ingezet voor legio activiteiten, zoals het onderscheppen van creditcardgegevens of het versturen van spam.

---

* **Merel Koning is promovenda bij het Privacy & Identity Lab aan de Radboud Universiteit Nijmegen. Zij studeerde aan het Instituut voor Informatierecht van de UvA en schreef haar masterscriptie over terughacken als opsporingsmethode. Hiervoor onderzocht zij de Bredolab-botnet-ontmanteling. Haar scriptie is beschikbaar op www.bredolab.nl.**

1 *Kamerstukken II* 20011/12, 26 643, nr. 202, incl. bijlage 147059-147061.

2 Terughacken verwijst in deze context naar *het op elektronische wijze heimelijk toegang verschaffen, via een externe verbinding, tot een geautomatiseerd werk of netwerk (ICT-systemen) door opsporingsdiensten.* Terughacken kan bijvoorbeeld door gebruikmaking van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheid, daartoe kan zonder weet van de gebruiker eerst de fysieke controle over het werk verkregen zijn of op afstand worden binnen gedrongen, door bijvoorbeeld tussenkomst van internet. Definitie deels ontleend aan J. Boek, 'Hacken als opsporingsmethode', *NJB* 2000, nr. 11. De inlichtingen- en veiligheidsdiensten komt wel een hackbevoegdheid toe ex artikel 24 Wet op de inlichtingen- en veiligheidsdiensten 2002.

3 *Kamerstukken II* 20011/12, 26 643, nr. 202, p. 9.

4 *Kamerstukken II* 2007/08, 28 684, nr. 232 p. 1. Ook in de MvT bij het *Concept Wetsvoorstel Versterking Bestrijding Computercriminaliteit* van juli 2010, p. 3, wordt vermeld dat de behoefte aan een bevoegdheid voor het online doorzoeken of terughacken nader zal worden onderzocht en om die reden niet in het wetsvoorstel wordt geadresseerd. De opsporingsdiensten zelf geven in de media aan behoefte aan een bevoegdheid te hebben. Zie bijvoorbeeld de *Vrij Nederland* van 28 juni 2011. Online op te vragen via www.vn.nl/Standaard-Media-Pagina/Hackersjacht.htm (laatstelijk geraadpleegd op 5 maart 2012).

5 Zie bijvoorbeeld Rb. Rotterdam 26 maart 2010, *LJN* BM2520 en de antwoorden van de minister op vragen over de toepassing van trojans: *Aanhangsel Handelingen II* 2011/12, nr. 1374.

6 Hiertoe zijn interviews afgelegd met betrokkenen van de ontmanteling: officier van justitie Lodewijk van Zwieten van het Landelijk Parket bij het Openbaar Ministerie, verantwoordelijk voor de vervolging van cybercrime; Alex de Joode, security officer bij hostingprovider LeaseWeb; Ronald Prins, directeur van cybersecuritybedrijf Fox IT. Met Dave Woutersen van GOVCERT.NL heeft een e-mailwisseling plaatsgevonden.

7 Zie bijvoorbeeld http://nieuwsuur.nl/video/193776-de-strijd-tegen-cybercrime.html en www.telegraaf.nl/digitaal/8043747/__Computer virussen_op_bestelling__.html (laatstelijk geraadpleegd op 28 februari 2012).

Het OM startte begin 2010 een publiek-privaat samenwerkingsverband om een bestrijdingsmethode voor botnets te ontwikkelen. Die zomer diende Bredolab zich aan als ideale ontmantelingsproef omdat alle Command & Controlservers in Nederland stonden. Een tussenpersoon huurde al enige tijd 143 servers in het Haarlemse datacenter van de hostingprovider LeaseWeb. Een aantal van deze servers werd verdacht van het besturen van een botnet. LeaseWeb meldde dit in augustus aan het Team High Tech Crime van het KLPD. De botnetbestuurder werd vanaf dat moment verdacht van computervredebreuk in gekwalificeerde vorm, artikel 138ab Wetboek van Strafrecht (Sr) alsmede het opzettelijk en wederrechtelijk toevoegen van gegevens, en het opzettelijk en wederrechtelijk ter beschikking stellen of verspreiden van gegevens die zijn bestemd om schade aan te richten aan een geautomatiseerd werk, artikel 350a lid 1 en 3 Sr.

De ontmanteling bestond uit het aanhouden van de verdachte, het verbreken van het communicatiekanaal tussen de Command & Controlservers en de geïnfecteerde computers alsmede het waarschuwen van de slachtoffers voor de virusinfectie op hun computer.

2.2 *Bredolab-ontmanteling*

In voorbereiding op de ontmanteling werden alle 143 servers van de tussenpersoon voor onderzoek in beslag genomen. Contractueel werd tussen LeaseWeb en het KLPD overeengekomen dat LeaseWeb in beginsel geen actie tegen het botnet of de verdachte tussenpersoon zou ondernemen en de servergebruikers niets van de inbeslagname mochten merken. Het verkeer van en naar vermoedelijke Bredolab Command & Controlservers werd afgetapt. 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 gedurende ongeveer tien weken over de schouder van de verdachte mee gekeken. Zijn identiteit en de kenmerken van Bredolab werden toegevoegd aan het procesdossier.[8]

De ontmanteling vond eind oktober 2010 plaats. Voor het verbreken van het communicatiekanaal tussen de Command & Controlservers en de geïnfecteerde computers zou het afdoende zijn geweest om de servers uit te zetten of de internetverbinding te verbreken.[9] Met het oog op het waarschuwen van de slachtoffers kozen het KLPD en het OM echter voor een andere aanpak. Het KLPD nam alle Command & Controlservers van binnenuit over en kreeg op deze manier de controle over het botnet in handen, waarna LeaseWeb op last van het OM de internetverbinding verbrak van de overige 137 in beslag genomen servers.

De laatste stap van de ontmanteling was het waarschuwen van de slachtoffers. Dit gebeurde vlak na de overname via het botnet zelf. Het KLPD zette een *executable file* klaar op de Command & Controlservers, die de geïnfecteerde computers ophaalden en uitvoerden. Dit bestand leidde, zodra de default browser geopend werd, het slachtoffer naar een waarschuwingspagina. Deze website meldde de virusbesmetting, en gaf een korte uitleg over Bredolab en het publiek-private samenwerkingsverband dat het KLPD voor de ontmanteling had samengesteld.

Daarnaast hebben de opsporingsdiensten informatie betreffende IP-adressen, gestolen credentials en gehackte domeinnamen door GOVCERT.NL wereldwijd laten verspreiden, om ook via de internationaal samenwerkende Computer Emergency Response Teams en internetserviceproviders (isp's) de Bredolab-slachtoffers te waarschuwen.

Analyse van het feitenkader[10] leidt mijns inziens tot de constatering dat bij de Bredolab-ontmanteling op twee momenten sprake is geweest van terughacken. De hacks raakten zowel de verdachte als de slachtoffers.

In de eerste plaats zijn de opsporingsdiensten middels afgevangen toegangs- en decryptiesleutels op de servers van de verdachte binnengedrongen, waardoor ongeveer tien weken heimelijk de handelingen van verdachte zijn gemonitord en onderzocht. Hier hebben zij tevens voldoende informatie vergaard om de Command & Controlservers succesvol van binnenuit over te nemen.

In de tweede plaats zijn de servers daadwerkelijk 'gekaapt' en werd de controle over het gehele botnet overgenomen. Hierdoor verwierven de opsporingsdiensten volledige toegang tot en controle over de computers van de slachtoffers en kon een bestand hieraan worden toegevoegd.

3 Privacyrecht: artikel 8 EVRM

In deze paragraaf worden de twee Bredolab-hacks vanuit het privacyrecht nader bezien.

Het privacyrecht ligt verankerd in meerdere internationale mensenrechtelijke verdragen en de Grondwet. In 1987 legde de Hoge Raad uit dat het privacyrecht in Nederland moet aansluiten bij ontwikkelingen over de grens en dat de inhoud mede moet worden bepaald door artikel 8 Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).[11] In de komende analyse staat dit artikel centraal.

---

8 Uit berichten op de Facebookpagina van verdachte kon het KLPD opmaken dat deze op vrijdag 22 oktober 2010 voor een dancefeest naar Nederland zou komen. De actie (aanhouden, verbreken verbinding en waarschuwen slachtoffers) werd gepland op deze dag. Het was de bedoeling de verdachte bij aankomst op Schiphol aan te houden. Hij kwam echter niet opdagen. Daarop werd de actie uitgesteld naar maandag 25 oktober 2010 en werd een internationaal arrestatiebevel uitgevaardigd door het OM. Verdachte is aangehouden op dinsdag in thuisland Armenië. Het uitleveringsverzoek van Nederland is door Armenië niet ingewilligd en verdachte wordt daar berecht.

9 Zie voor de technische specificaties van Bredolab www.bredolab.nl/technische-specificaties-bredolab/.

10 Het feitenkader is in verkorte vorm weergegeven. Voor een uitgebreide reconstructie zie www.bredolab.nl/feitenreconstructie-ontmanteling/.

11 HR 9 januari 1987, *NJ* 1987, 928.

Het concept privéleven uit artikel 8 EVRM dekt mede de fysieke en psychologische integriteit.[12] In de zaak *Peck/the United Kingdom* benadrukt het Europees Hof voor de Rechten van de Mens (EHRM) dat het recht op persoonlijke ontwikkeling en het aangaan en ontwikkelen van relaties met anderen en de wereld, ook in een publieke of formele context, onder het EVRM kan worden beschermd.[13] In een reeks uitspraken heeft het EHRM geoordeeld dat een individu niet automatisch het recht op bescherming van zijn privéleven verliest als hij zijn persoonlijke eigendommen in een meer publieke omgeving brengt.[14]

Inbreuk op dit recht kan evenwel geoorloofd zijn wanneer aan de cumulatieve voorwaarden van artikel 8 lid 2 EVRM is voldaan. Ten eerste moet sprake zijn van een legitiem doel, welke doelen uitputtend zijn opgenomen in het tweede lid van artikel 8 EVRM.[15] Het tweede criterium behelst de voorzienbaarheid bij wet en is gekoppeld aan drie cumulatieve toetsstenen: (1) de maatregel moet in de nationale wetgeving zijn vastgelegd, (2) ze moet voldoende toegankelijk zijn voor het publiek,[16] en (3) ze moet voldoen aan de voorzienbaarheid.

Daar het gebruik van vage termen onontkoombaar is,[17] bestaat de voorzienbaarheid in het strafrecht uit een voldoende mate van helderheid en niet uit absolute duidelijkheid.[18] Het is belangrijk dat de effecten van de maatregel door de burger kunnen worden ingeschat, zodat het gedrag hierop kan worden aangepast.[19] Het Hof eist echter strenge, heldere en gedetailleerde wettelijke bepalingen ingeval de inbreuk plaatsvindt ter voorkoming van strafbare feiten en gebruik wordt gemaakt van geavanceerde technologie.[20] Tevens wordt een kwalitatief vereiste gesteld: in overeenstemming met de algemene beginselen van de rechtsstaat moet de beperkende maatregel waarborgen bevatten tegen willekeur en misbruik.[21]

Het laatste criterium van artikel 8 lid 2 EVRM is de noodzakelijkheid in een democratische samenleving. Noodzakelijkheid staat niet synoniem voor nodig, wenselijk of nuttig.[22] Het betreft een belangenafweging tussen het effect van de inmenging op recht en rechtsbeleving van de burger en het nagestreefd legitieme doel. De proportionaliteit en subsidiariteit moeten worden meegewogen alsmede maatregelen die zijn genomen ter beperking van de inbreuk.[23] In de belangenafweging komt de Staat een bepaalde *margin of appreciation* toe, een zekere beoordelingsvrijheid om de effectiviteit, proportionaliteit en noodzakelijkheid van de maatregel te beoordelen.

4 Privacy en ICT-systemen

Karin Spaink beschrijft in *Het huis uit, de wereld in: een kleine telefoongeschiedenis* hoe de telefoon in 25 jaar van een formeel communicatiemiddel op een tochtige gang is veranderd in 'ons aller intiemste communicatiemiddel (…) meer dan ooit verweven met onze alledaagse, huiselijke of juist vertrouwelijke activiteiten en gevoelens'.[24] Eenzelfde ontwikkeling heeft plaatsgevonden voor ICT-systemen, zoals smartphones, computers en virtuele diensten. De rol die deze vervullen en het gebruik voor de persoonlijke ontwikkeling maken het goed verdedigbaar dat deze systemen onder de beschermingsomvang van het begrip 'privéleven' uit artikel 8 EVRM vallen.

Het ontbreekt aan jurisprudentie van het EHRM betreffende het online toegang verschaffen of doorzoeken van ICT-systemen.[25] Terughacken is wel in de Duitse rechtspleging besproken in een zaak voor het Constitutioneel Hof.[26] Alhoewel het formeel-rechtelijke kader van deze uitspraak afwijkt van het onderhavige, is het materieelrechtelijke vraagstuk van overeenkomstige aard. Hierdoor kunnen de overwegingen van het Bundesverfassungsgericht richting geven. In de *Online Durchsuchung*-uitspraak stond de vraag centraal of het heimelijk op afstand doorzoeken van een ICT-systeem een geoorloofde opsporingsmethode is. Het antwoord op deze vraag is gebaseerd op het recht op integriteit en vertrouwelijk-

12 EHRM 22 juli 2003, nr. 24209/94 (*YF/Turkey*), r.o. 33.
13 EHRM 28 januari 2003, nr. 44647/98 (*Peck/the United Kingdom*).
14 Bijvoorbeeld EHRM 16 december 1992, nr. 13710/88 (*Niemietz/Germany*) en EHRM 28 januari 2003, nr. 44647/98 *(Peck/the United Kingdom*).
15 Het EHRM pleegt in zijn jurisprudentie weinig aandacht te besteden aan de omlijning en reikwijdte van deze doelen.
16 EHRM 2 augustus 1984, nr. 8691/79 (*Malone/the United Kingdom*).
17 EHRM 24 mei 1988, nr. 10737/84 (*Müller and others/Switzerland*), r.o. 29.
18 EHRM 24 april 1990, nr. 11105/84 (*Huvig/France*), r.o. 26.
19 EHRM 1 juli 2008, nr. 58243/00 (*Liberty and others/the United Kingdom*).
20 EHRM 30 juli 1998, nr. 27671/95 (*Valenzuela/Spain*) en EHRM 24 april 1990, nr. 11801/85 (*Kruslin/France*).
21 EHRM 26 september 1995, nr. 17851/91 (*Vogt/Germany*), r.o. 48. Daarnaast in bijvoorbeeld EHRM 25 maart 1983, nr. 5947/72 (*Silver and others/the United Kingdom*), r.o. 88.
22 EHRM 7 december 1976, nr. 5493/72 (*Handyside/the United Kingdom*).
23 EHRM 25 maart 1983, nr. 5947/72 (*Silver and others/the United Kingdom*), r.o. 97.
24 K. Spaink, 'Het huis uit, de wereld in: een kleine telefoongeschiedenis', in: K. Spaink (red.), *Wie is U?*, Amsterdam: Nijgh & Van Ditmar 2010, p. 16.
25 Een uitvoerige reeks jurisprudentie van het EHRM betreft het aftappen van telefoongesprekken en het doorzoeken van woningen, bijvoorbeeld EHRM 25 maart 1998, nr 44787/98 (*Halford/the United Kingdom*); EHRM 16 februari 2000, nr. 27798/95 (*Amman/Swiss*); EHRM 24 april 1990, nr. 11801/85 (*Kruslin/France*); EHRM 24 april 1990, nr. 11105/84 (*Huvig/France*). Het doorzoeken van harde schijven van verschoningsgerechtigden (meestal na inbeslagname) is wel meermaals onderwerp geweest in een geschil voor het EHRM. EHRM 16 december 1992, nr. 13710/88 (*Niemietz/Germany*) en EHRM 2 september 2008, Decision nr. 15301/04 (*Tamm/Estonia*). Echter, bij het vaststellen van de inbreuk en de aard hiervan (relevant voor de verdere weging van de criteria gegeven in lid twee van artikel 8 EVRM) wordt in dergelijke zaken terecht zwaar getild aan de bijzondere positie van verschoningsgerechtigden. Hierdoor blijft de vraag naar de aard van de inbreuk bij het doorzoeken onbeantwoord.
26 Bundesverfassungsgericht 27 februari 2008, 1 BvR 370/07, 1 BvR 595/07.

heid van ICT-systemen, een afgeleide van het uit artikel 2 van de Duitse grondwet voortvloeiende Algemeen Persoonlijkheidsrecht.[27]

Met betrekking tot het vaststellen van de aanwezigheid en de aard van de inbreuk oordeelt het Bundesverfassungsgericht dat uit het relevante gebruik van informatiesystemen ten behoeve van persoonlijkheidsontplooiing en uit de gevaren voor de persoonlijkheid die verbonden zijn aan dit gebruik, een nood tot grondrechtelijke bescherming volgt.[28] Vervolgens stelt het Bundesverfassungsgericht dat een computer waarschijnlijk meer dan enkel een bulk aan persoonsbetreffende informatie en communicatie bevat. Een derde die zich toegang verschaft tot een ICT-systeem, kan zich potentieel een uiterst groot en veelzeggend databestand verschaffen, zonder op verdere dataverzamelings- en dataverwerkingsmethoden te zijn aangewezen. Dergelijke toegang weegt vele malen zwaarder dan toegang tot afzonderlijke databestanden.[29]

5 Inbreuken op de privacy

5.1 *Inbreuk privacy verdachte*

De Bredolab-verdachte maakte gebruik van gehuurde servers, die exclusief tot zijn beschikking stonden. Het gebruik van *dedicated hostingservers* en *cloud-computing* is een duidelijk zichtbare onlinetrend. Geautomatiseerde werken en persoonlijke gegevens bevinden zich steeds vaker buiten de directe fysieke atmosfeer van de gebruiker in een meer publieke omgeving. Ondanks de afstand is het gebruik van het ICT-systeem hetzelfde. De fysieke afstand tussen gebruiker en ICT-systeem mag niet van doorslaggevende aard zijn, waardoor de servers mijns inziens onder de beschermingsomvang vallen van artikel 8 EVRM.[30] Het heimelijk binnendringen en monitoren van handelingen maakt inbreuk op dit recht.

De vraag is, of een verdachte tijdens de voorbereiding of uitvoering van een strafbaar feit een beroep op het privacyrecht kan doen; de zogenoemde *reasonable expectation of privacy-doctrine*. Door de uitspraak van het EHRM in de zaak *Lüdi/Switzerland* scheen dit beroep slechts beperkt mogelijk, maar het Hof lijkt hier in latere zaken op te zijn teruggekomen.[31] In de zaak *A/France* en *Peck/the United Kingdom* heeft het Hof geoordeeld dat ondanks de strafbare feiten sprake was van schending van het privacyrecht en dat de overheid de bescherming van dit recht had moeten waarborgen.[32]

De reasonable expectation of privacy-doctrine wordt ook door Oerlemans aangehaald in zijn artikel 'Hacken als opsporingsbevoegdheid'.[33] Hij stelt dat: 'Geredeneerd kan worden dat een betrokkene die gebruik maakt van een server – die voornamelijk wordt gebruikt voor illegale activiteiten – geen reasonable expectation of privacy meer heeft', en een beroep op het privacyrecht terughacken zonder expliciete strafvorderlijke bevoegdheid niet in de weg kan zitten. Oerlemans richt zich in het overige gedeelte van zijn artikel op persoonlijke geautomatiseerde werken zonder nadere definiëring van dit begrip. Hij geeft aan dat terughacken van persoonlijke geautomatiseerde werken ontegenzeggelijk inbreuk maakt op het privacyrecht.[34]

Zijn argumentatie bestaat uit een cirkelredenering. Het persoonlijk gebruik van een server is in de meeste gevallen lastig op voorhand vast te stellen net zoals het voornamelijk gebruik voor illegale activiteiten. De justitiële wens voor een terughackbevoegdheid wordt ingegeven door gecombineerde barrières van territorialiteit, anonimiteit en versleuteling. Persoonlijk gebruik en voornamelijk gebruik voor illegale activiteiten zijn pas duidelijk op het moment dat de inhoud van de server bekend is; dus na het terughacken. Door het op voorhand uitsluiten van de toepasbaarheid van het privacyrecht of de legitimiteit van een beroep op dit recht zal de Staat zijn zorgplicht voor grondrechtelijke bescherming verzaken.

5.2 *Inbreuk privacy verdachte geoorloofd?*

Het OM kwalificeert een botnet als een gevaarlijk netwerk, dat de nationale veiligheid kan bedreigen. Daarnaast heeft het OM maatregelen genomen ter voorkoming van strafbare feiten. Dit zijn beide gelegitimeerde doelen onder artikel 8 lid 2 EVRM. Het OM maakte in zijn onderzoek gebruik van de tap- en inbeslagnamebevoegdheid van artikel 126m juncto artikel 96 Wetboek van Strafvordering (Sv). Deze artikelen maken deel uit van het positief recht en zijn middels websites en publicaties in het *Staatsblad* voldoende toegankelijk voor het publiek. Vanwege de technische mogelijkheden bij terughacken en de potentieel grove inbreuk die opsporing op het privacyrecht maakt, worden strenge eisen aan de voorzienbaarheid gesteld.[35] In casu had de toepassing van de artikelen 126m en 96 Sv het effect dat de opsporingsdienst middels afgevangen toegangs- en decryptiesleutels op de servers is binnengedrongen, waar-

27 Zie voor een heldere Engelstalige inleiding tot het Duitse grondwettelijke recht S. Michalowski & L. Woods, *German constitutional law. The protection of civil liberties*, Ashgate: Brookfield 1999. De wenselijkheid van een zusterbepaling binnen het Nederlands recht is door Groothuis en De Jong besproken in de decembereditie van 2010 van dit tijdschrift: M.M. Groothuis & T. de Jong, 'Is een nieuw grondrecht op integriteit en vertrouwelijkheid van ICT-systemen wenselijk? Een verkenning', *P&I* 2010-6, p. 278-283.

28 Bundesverfassungsgericht 27 februari 2008, 1 BvR 370/07, 1 BvR 595/07. Ro. 181.

29 Bundesverfassungsgericht 27 februari 2008, 1 BvR 370/07, 1 BvR 595/07. Ro. 198-207.

30 Analoog aan de uitleg van het begrip '*private life*' in onder andere EHRM 16 december 1992, nr. 13710/88 (*Niemietz/Germany*) en EHRM 28 januari 2003, nr. 44647/98 (*Peck/the United Kingdom*).

31 EHRM 15 juni 1992, nr. 12433/86 (*Lüdi/Switzerland*), r.o. 39.

32 EHRM 23 november 1993, nr. 14838/89 (*A./France*), r.o. 34 en EHRM 28 januari 2003, nr. 44647/98 (*Peck/the United Kingdom*).

33 J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid', *DD* 2011, 62, p. 888-908.

34 J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid', *DD* 2011, 62, p. 897-898.

35 Analoog aan EHRM 26 september 1995, nr. 17851/91 (*Vogt/Germany*), r.o. 48. Daarnaast in bijvoorbeeld EHRM 25 maart 1983, nr. 5947/72 (*Silver and others/the United Kingdom*), r.o. 88.

door gedurende ongeveer tien weken heimelijk de handelingen van de verdachte werden gemonitord en onderzocht.

Het in te schatten effect op de privacy van artikel 126m Sv is dat door aftappen en onderzoek de inhoud van de telecommunicatie, ook al is deze versleuteld, bij opsporingsdiensten bekend wordt en mogelijk als bewijs zal dienen. Het in te schatten effect op de privacy van artikel 96 Sv is dat door inbeslagname beslagene de beschikking over de gegevensdrager verliest en dat de in het verleden opgeslagen gegevens en daarmee het privéleven bij de opsporingsdiensten bekend wordt en mogelijk als bewijs zal dienen.

Het effect van het terughacken van de verdachte komt mijns inziens niet overeen met bovengenoemde effecten. Het binnendringen op een server voor het heimelijk realtime observeren en onderzoeken van handelingen wijkt af van onderzoek aan telecommunicatie en opgeslagen gegevens, waardoor de artikelen 96 en 126m Sv niet voorzien in het effect van een dergelijke inbreuk.[36]

Daarnaast brengt de inbeslagname nog een complicatie met zich mee. Om wille van het onderzoek werd beslag gelegd op de gegevensdragers, waardoor LeaseWeb de juridische beschikkingsmacht over de servers verloor. Het onderzoek richtte zich vervolgens op de aanwezige gegevens en handelingen van de botnetbestuurder, terwijl deze vrije beschikking behield over de servers.[37] LeaseWeb werd over de inbeslagname geïnformeerd; de inbeslagname is bewust niet aan de gebruiker gemeld. Het is uit literatuur, wetsgeschiedenis en jurisprudentie niet duidelijk op te maken hoe de verhoudingen liggen tussen de eigenaar van een gegevensdrager, de eigenaar/gebruiker van de gegevens en de opsporingsdiensten, alsmede welk gewicht in een dergelijk geval aan de notificatieplicht moet worden toegekend.

Bovenstaande leidt mijns inziens tot de conclusie dat de artikelen 96 en 126m Sv in casu geen strenge, heldere en gedetailleerde regels vormen die in de effecten van de inbreuk voorzien. Het is derhalve goed verdedigbaar te stellen dat niet is voldaan aan het vereiste criterium *voorzienbaarheid bij wet* van artikel 8 lid 2 EVRM, waardoor het terughacken naar de verdachte een schending van het privacyrecht oplevert.

5.3 *Inbreuk privacyslachtoffers*

Nadat het KLPD de Command & Controlservers had overgenomen lag de controle over het botnet in hun handen. Hierdoor verwierven de opsporingsdiensten volledige toegang tot en controle over de computers van de slachtoffers en kon het waarschuwingsbestand hieraan worden toegevoegd. Naar analogie van de argumentatie van het Bundesverfassungsgericht kan gesteld worden dat vanwege de belangrijke rol van ICT-systemen in het dagelijks leven en de toegang tot een potentieel uiterst groot en veelzeggend databestand, het terughacken naar de slachtoffers inbreuk maakt op het privacyrecht ex artikel 8 EVRM.

Het OM is van mening dat de inbreuk geoorloofd was en de opsporingsinstanties hiertoe bevoegdheid hadden omdat:[38]

1. De verrichte handelingen zich binnen de grenzen van artikel 2 Politiewet (Polw) bevinden. Officier van justitie (OvJ) van het Landelijk Parket Lodewijk van Zwieten zegt hierover:

'Artikel 2 Politiewet is voldoende. Het is een stukje bescherming van de rechtsorde en bescherming van de openbare orde. Het gevaarlijke systeem bedreigde zowel de rechtsorde als de openbare orde. (…) Het [artikel 2 Polw – MK] is omgrensd wanneer opsporend optreden door de politie een meer dan geringe inbreuk maakt op de privacy van de betrokkenen. Het begrenzend criterium van artikel 2 Politiewet geldt niet als het om de bescherming van de openbare orde gaat. Dit criterium geldt heel nadrukkelijk voor opsporingshandelingen, dus niet voor handhaving.'

2. Het versturen van de executable is een schending van de privacy, maar de minst inbreukmakende die het OM en de KLPD konden verzinnen. OvJ van Zwieten stelt hierover:

'Onthoofden botnet, opsporing en slachtoffer waarschuwen zou zo veel mogelijk in gezamenlijkheid moeten gebeuren, dan kun je effectief een botnet bestrijden. De meest directe infrastructuur naar de slachtoffers was het botnet zelf. (…) Ja, je maakt een inbreuk op de privacy want je stuurt iets naar iemand en een aantal van de geïnfecteerde computers zal zich in huizen bevinden in ruimtes waar mensen onbevangen zichzelf moeten kunnen zijn. En als je mensen daar benadert dan kunnen ze op dat moment niet even onbevangen zichzelf zijn, want ze worden geconfronteerd met de politie en dat is een privacyschending. Maar die privacyschending is niet meer dan gering, want wat er via het botnet gebeurt [doorsturen van wachtwoorden, creditcardgegevens, enz. naar criminelen – MK] is vele malen privacyinbreukmakender dan dat wij met de politie doen.'

3. Artikel 350a lid 4 Sr geeft het OM en het KLPD een strafuitsluitingsgrond. OvJ van Zwieten:

'Meest effectief is dat wij een .exe naar de computers sturen over het botnet. (…). Wat we dus feitelijk hebben gedaan is het toevoegen van gegevens aan een geautomatiseerd werk ex artikel 350a strafrecht. De strafbaarheid

36 In mijn scriptie *Terug-hacken als opsporingsmethode – Een juridische analyse van de terug-hack praktijk van Justitie in relatie tot het privacyrecht naar aanleiding van de Bredolab ontmanteling* zijn de strafvorderlijke artikelen gedetailleerder onderzocht. Zie www.bredolab.nl.

37 LeaseWeb geeft aan volledige medewerking aan opsporingsdiensten te verlenen. Artikel 4.2 *Acceptable Use Policy Leaseweb* (versie geraadpleegd op 1 september 2011). Deze medewerking is privaatrechtelijk vastgelegd tussen huurder en LeaseWeb en geeft geen bevoegdheden voor opsporingsdiensten.

38 Quotes uit het interview met OvJ Van Zwieten ten behoeve van het schrijven van de scriptie *Terug-hacken als opsporingsmethode – Een juridische analyse van de terug-hack praktijk van Justitie in relatie tot het privacyrecht naar aanleiding van de Bredolab ontmanteling.*

vervalt als je dat doet om schade te voorkomen ex artikel 350a lid 4. Dit staat in de wet om überhaupt het desinfecteren van de computer mogelijk te maken. Het is een uitsluiting van de strafbaarheid.'

5.4 *Inbreuk privacyslachtoffers geoorloofd?*

Artikel 2 Politiewet en artikel 350a lid 4 Wetboek van Strafrecht maken deel uit van de Nederlandse wetgeving en zijn middels websites en publicaties in het *Staatsblad* voldoende toegankelijk voor het publiek. De vraag is echter of bij het kennisnemen van deze artikelen de inbreuk voorzienbaar is en als zodanig voor de burger is in te schatten: terughacken via het botnet en daarbij de volledige controle over de computer en toegang tot een potentieel uiterst groot en veelzeggend databestand van het slachtoffer verwerven. Vervolgens deze controle aanwenden om gegevens toe te voegen en het slachtoffer te waarschuwen.

Artikel 2 Polw omschrijft de taakstelling van de politie en verleent beperkte bevoegdheden.[39]

Openbare orde is in de wetsgeschiedenis en praktijk gebonden aan de fysieke openbare ruimte. In beginsel is de burgemeester verantwoordelijk voor handhaving van de openbare orde. De rol van het OM is beperkt tot dadergerichte criminaliteitspreventie, binnen de bestuurlijke driehoek.[40] Politieoptreden tegen een internationaal crimineel computernetwerk op gezag van het OM valt niet onder de openbare orde handhavingstaak en brengt een onwenselijke oprekking van het begrip met zich mee. Laat staan de bijkomstigheid dat 415 burgemeesters de bestrijding van criminele computernetwerken op hun bord krijgen en het effect dat dit zal hebben op het internet. Het is zonder een apocalyptische visie op het effect van cybercriminaliteit op de fysieke openbare ruimte, mijns inziens moeilijk om de aanwezigheid van de Bredolab Command & Controlservers in de Gemeente Haarlem als een concreet voordoende of dreigende verstoring van de openbare orde te zien. Terughacken kan derhalve niet als handeling in de uitvoering van de openbare orde handhavingstaak worden gezien.

Voor de strafvorderlijke taak van de politie is artikel 2 Polw door de tijd heen gebruikt als grondslag voor bepaalde strafvorderlijke bevoegdheden. Zo werden opsporingstechnieken als het observeren van verdachten in de openbare ruimte[41] (inmiddels artikel 126g Sv) en het infiltreren in een crimineel netwerk[42] (inmiddels artikel 126h Sv) in de jaren zeventig en tachtig door de Hoge Raad geacht voldoende rechtsgrond te hebben middels dit artikel.

Echter met het *Zwolsman*-arrest uit 1995 heeft de Hoge Raad een nauw criterium gesteld ter begrenzing van de strafvorderlijke bevoegdheden uit artikel 2 Polw.[43] De voortschrijdende ontwikkeling van het privacyrecht en de toenemende technische verfijning en intensivering van onderzoeksmethoden en -technieken verlangen een meer precieze legitimatie in de wet. Indien bij opsporing slechts een beperkte inbreuk op de persoonlijke levenssfeer wordt gemaakt, biedt de globale taakomschrijving van artikel 2 Polw hiervoor een toereikende wettelijke grondslag, aldus de Hoge Raad. Daarnaast heeft de IRT-affaire geleid tot de invoering van de Wet bijzondere opsporingsbevoegdheden (Wet BOB) in het jaar 2000.[44] De Commissie-Van Traa concludeerde dat voor de verwezenlijking van het rechtsstatelijk gedachtegoed opsporingsmethoden een uitdrukkelijk wettelijke grondslag behoeven.[45] Dit is met de Wet BOB gebeurd. Mijns inziens is er geen aanleiding om in geval van cybercriminaliteit van rechtsstatelijke beginselen af te wijken.

Onlangs legde de Rechtbank 's-Gravenhage uit dat voor het gebruik van openbare onlinebronnen (zoals Google Earth) geen bijzondere opsporingsbevoegdheid is vereist en artikel 2 Politiewet onder de *Zwolsman*-voorwaarden afdoende is. De rechtbank doet een beroep op de wetsgeschiedenis en stelt:

'Zoals de politie, al dan niet in burger, op straat mag surveilleren en rondkijken, zo mag een rechercheur vanachter zijn computer hetzelfde doen op internet. Een uitdrukkelijke wettelijke grondslag is daarvoor niet nodig.'[46]

Het is echter zeer de vraag of de continuatie van de vergelijking tussen fysieke en digitale realiteit wenselijk is. De architectuur en betekenis van ICT-systemen wijkt significant af van de fysieke wereld. Dit verschil was ten tijde van de parlementaire behandeling van Wet computercriminaliteit II minder aanwezig en/of zichtbaar. Met betrekking tot Bredolab heeft deze uitspraak geen invloed op de uitkomst. Toegang tot een pc via een hack valt niet onder openbare bronnen. Daarover zei de Hoge Raad in zijn arrest van 22 februari 2011 in rechtsoverweging 2.4:

'Opmerking verdient daarbij dat onder het doorbreken van enige beveiliging, zoals bedoeld in art. 138a, eerste lid onder a, (oud) Sr, mede dient te worden verstaan het

39 Artikel 2 Politiewet 1993: 'De politie heeft tot taak in ondergeschiktheid aan het bevoegde gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.' Wet van 9 december 1993, tot vaststelling van een nieuwe Politiewet, *Stb.* 1993, 724, laatstelijk gewijzigd op 13 december 2010, *Stb.* 2011, 4.

40 *Kamerstukken II* 1991/92, 22 562, nr. 3; *Kamerstukken II* 1986/87, 19 535, nr. 4 en *Kamerstukken II* 1987/88, 19 403, nr. 15. Bestuurlijke driehoek: burgemeester, korpschef politie en hoofdofficier van justitie.

41 HR 14 oktober 1986, *NJ* 1988, 551.

42 HR 4 december 1979, *NJ* 1980, 356.

43 HR 19 december 1995, *NJ* 1996, 249.

44 Wet van 27 mei 1999, *Stb*. 1999, 245.

45 *Kamerstukken II* 1995/96, 24 072, nr. 10-20, p. 452 (Rapport-Van Traa).

46 Rb. 's-Gravenhage 28 december 2011, *LJN* BU9409, r.o. 10. Zie ook het commentaar op dit vonnis (in het bijzonder reactie 3) van B.J. Koops op de weblog *Recht & Bestuur* van het *NRC Handelsblad*. Beschikbaar op http://weblogs.nrc.nl/rechtenbestuur/2012/02/09/de-uitspraak-mag-de-staat-via-google-earth-bewijs-verzamelen-in-je-achtertuin/ (laatstelijk geraadpleegd op 3 maart 2012).

tegen de wil van de rechthebbende binnendringen in een computer langs een weg die de aanwezige beveiliging niet of onvoldoende afsluit. Daarbij is, anders dan de steller van het middel betoogt, niet van belang of die opening inherent is aan het systeem of is veroorzaakt door andere "aanvallers".'[47]

Het laatste argument van het OM betreft de uitsluiting van schuld. Artikel 350a lid 4 Sr vormt een strafuitsluitingsgrond voor de persoon die opzettelijk en wederrechtelijk gegevens bedoeld om schade aan te richten (malware) in een geautomatiseerd werk verspreidt of beschikbaar stelt, met het oog op de beperking van de schadelijke gevolgen van deze gegevens.[48] Schulduitsluiting ziet toe op gronden die de strafbaarheid van de dader wegnemen. De wederrechtelijkheid van de handeling blijft onverlet.[49] In een rechtsstaat komt het vaststellen van het ontbreken van strafbaarheid toe aan de rechtsprekende macht en niet aan de uitvoerende macht.

Daarnaast is de schulduitsluitingsgrond niet gericht op het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk (computervredebreuk, artikel 138ab Sr) en ook niet op het opzettelijk en wederrechtelijk toevoegen van gegevens (artikel 350a lid 1 Sr). Vraag is of een schulduitsluitingsgrond voor het verspreiden of beschikbaar stellen van malware (artikel 350a lid 3 Sr) terugslaat op de straffeloosheid van de persoon die zich zonder toestemming toegang tot de computer van het slachtoffer verwerft (binnendringen) en gegevens daaraan toevoegt.[50]

De aard van de inbreuk (volledige toegang tot en controle over de computers) bij terughacken staat mijns inziens in de weg aan bevoegdheidsverlening van artikel 2 Polw.[51] Artikel 2 Polw en artikel 350a lid 4 Sr vormen geen strenge, heldere en gedetailleerde wetgeving. Hierdoor kan worden gesteld dat het effect van de inbreuk voor de burger niet is in te schatten. Het is goed verdedigbaar te stellen dat aan het vereiste criterium van artikel 8 lid 2 EVRM *voorzienbaarheid bij wet* niet is voldaan en terughacken derhalve een schending van het privacyrecht oplevert.[52]

6 Digitale toegang op afstand

Zoals gesteld ontberen de opsporingsdiensten momenteel bevoegdheid. De gebezigde term 'terughacken' of 'hacken door de politie' riekt naar onrechtmatigheid en is daarom geschikt zolang een bevoegdheid ontbreekt. Gezien de uitspraken van de minister is het aannemelijk dat op korte termijn een wetsvoorstel wordt gedaan.[53] Bij het formuleren van strafvorderlijke bepalingen is een accuraat en neutraal begrippenapparaat wenselijk. Voor de definiëring van bevoegdheden is het onderscheid tussen online doorzoeken[54] en het plaatsen van een technische voorziening op een geautomatiseerd werk[55] onder anderen door Oerlemans gemaakt.[56] Mijns inziens is deze tweesplitsing niet werkbaar. Het sluit weliswaar aan bij het huidige onderscheid tussen stromende en opgeslagen gegevens in het Wetboek van Strafvordering, maar ontkent de technische realiteit. Zo zal een onlinedoorzoeking in veel gevallen tevens het plaatsen van een technische voorziening behoeven en zal het ICT-systeem in veel gevallen ook worden gemanipuleerd om sporen van de doorzoeking te wissen.

Een gelaagd systeem van digitale toegang op afstand biedt mijns inziens uitkomst. De gelaagde structuur wordt ook bij het geoorloofd binnentreden van een woning gebruikt. Hiertoe wordt een algemene machtiging tot binnentreden afgegeven en is toepassing van ieder afzonderlijk dwangmiddel of bijzondere opsporingsbevoegdheid met eigen waarborgen omkleed. Bij deze gelaagde structuur zijn de effecten van de inbreukmakende opsporingshandelingen bij het wetgevend proces onderzocht en vereisen op moment van toepassing een met waarborgen omklede (rechterlijke) afweging. De architectuur en de betekenis van ICT-systemen vertonen geen overeenkomst met de woning waardoor verdere vergelijking mank gaat. De gelaagde structuur voor digitale toegang op afstand zal op de architectuur en de betekenis van ICT-systemen moeten worden ingericht, met inachtneming van doel, technische betekenis, effect op het privéleven en de juiste beschermingsniveaus.[57]

---

47 *LJN* BN9287.

48 *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 36.

49 C. Cleiren e.a., *Tekst en commentaar Strafrecht*, Deventer: Kluwer 2010, p. 321-340.

50 De Hoge Raad heeft een opmerkelijke uitspraak gedaan waardoor de exacte definiëring van twee artikelen momenteel ter discussie staat. De Raad stelde dat het doen verspreiden of doen installeren van een virus (artikel 350a Sr) computervredebreuk (artikel 138ab Sr) oplevert. HR 22 februari 2011 *LJN* BN9287. Zie voor een analyse van deze uitspraak J.J. Oerlemans & B.J. Koops, 'De Hoge Raad bewijst slechte dienst in high-tech-crimezaak over botnets', *NJB* 2011, 914.

51 Een deel van de slachtoffers bevonden zich niet binnen het Nederlands territorium. De internationale aspecten van het hacken over de grens zijn buiten de reikwijdte van dit artikel gehouden.

52 In mijn scriptie *Terug-hacken als opsporingsmethode – Een juridische analyse van de terug-hack praktijk van Justitie in relatie tot het privacyrecht naar aanleiding van de Bredolab ontmanteling* is ook het derde cumulatieve criterium van artikel 8 EVRM – 'de noodzakelijkheid in een democratische samenleving' – nader onderzocht. Zie www.bredolab.nl.

53 Kamerleden Berndsen en Schouw hebben op 9 maart 2012 kamervragen gesteld over het opstellen van een bevoegdheid, naar aanleiding van de uitreiking van een Big Brother Award aan het KLPD vanwege de hackpraktijk. *Aanhangsel Handelingen II* 2011/12, kv. 2012Z04734.

54 Bijvoorbeeld om gegevens op de computer te bekijken of te kopiëren.

55 Bijvoorbeeld voor het afvangen van toetsaanslagen of nog onversleuteld verkeer.

56 J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid', *DD* 2011, 62, p. 893.

57 De uitspraak van het Bundesverfassungsgericht en de motie-Franken bieden hier handvatten. Bundesverfassungsgericht 27 februari 2008, 1 BvR 370/07, 1 BvR 595/07 en *Kamerstukken I* 2010/11, 31 051, nr. D (Motie-Franken (CDA) c.s.) over criteria in het geval van nieuwe wetsvoorstellen waarbij van een beperking op het grondrecht van de bescherming van de persoonlijke levenssfeer sprake is.