Mogelijkheden en beperkingen van de internettap

*J.J. Oerlemans**

In opsporingsonderzoeken wordt in toenemende mate gebruik gemaakt van de internettap. Dat is voorstelbaar aangezien mensen steeds meer gebruik maken van communicatiemiddelen via internet in plaats van de ouderwetse vaste telefoon. Echter, door technologische ontwikkelingen is inhoudelijke communicatie die via internet plaatsvindt steeds minder goed zichtbaar voor opsporingsdiensten. De vraag is daarom of de internettap op den duur nog wel voldoende effectief is en de regeling voor het aftappen moet worden aangepast. In dit artikel wordt hier nader op ingegaan.
Het artikel is als volgt opgebouwd. Eerst wordt beschreven hoe een internettap in zijn werking gaat. Vervolgens wordt de wettelijke regeling van de taplast geanalyseerd. Daarna worden technologische ontwikkelingen beschreven die de internettap minder effectief maken. Ten slotte wordt nagegaan welke alternatieven er zijn voor de internettap en wordt antwoord gegeven op de vraag of de internettap wel een toekomst heeft.

De internettap

Nog niet eens zo heel lang geleden was het tappen van telefoonverkeer van verdachten eenvoudig. Een traditioneel telefoongesprek vindt namelijk plaats over een circuitgeschakeld netwerk.[1] Door een geautomatiseerd proces worden twee telefoons simpelweg met elkaar verbonden. De verbinding via een circuitgeschakeld netwerk is gedurende het gehele gesprek beschikbaar en daarom kan het telefoongesprek via een tap bij de telecommunicatieaanbieder relatief eenvoudig worden afgeluisterd. Op basis van de

* Mr. Jan-Jaap Oerlemans is promovendus bij eLaw@Leiden, Centrum voor Recht in de Informatiemaatschappij van de Universiteit Leiden. Daarnaast is hij juridisch adviseur bij Fox-IT.

1 Het circuitgeschakelde netwerk wordt een 'public switched telephony network' (PSTN) genoemd.

Telecommunicatiewet zijn Nederlandse telefoonaanbieders verplicht hun infrastructuur aan te passen, zodat een tap ten uitvoer kan worden gelegd.
Het aftappen van internetverkeer werkt heel anders dan een traditionele telefoontap. Internetverkeer wordt opgedeeld in pakketjes van gegevens die via verschillende routes een andere computer bereiken. Computers weten naar welk adres de pakketjes moeten worden verstuurd aan de hand van een IP-adres.[2] Na ontvangst worden de gegevens door computers geïnterpreteerd en op die manier kunnen bijvoorbeeld websites op internet worden bekeken, e-mailberichten worden verstuurd en (grote) bestanden worden uitgewisseld. Bij een internettap wordt al het inkomende en uitgaande internetverkeer van een bepaald IP-adres afgetapt. Het afgeluisterde gegevensverkeer kan vervolgens worden verwerkt en voor zover mogelijk voor derden inzichtelijk worden gemaakt. Indien specifiek verkeer er niet uit wordt gefilterd, komt al het internetverkeer mee dat vanuit een bepaald IP-adres wordt gegenereerd. Denk daarbij aan zoektermen die in Google worden ingetypt, chatberichten die met programma's (zoals MSN Messenger) onversleuteld over en weer worden verstuurd, berichten die onversleuteld op onlinewebforums worden geplaatst of via sociale-netwerkdiensten worden verstuurd, maar ook aan bijvoorbeeld YouTube-filmpjes die via internet worden bekeken. Zelfs inloggegevens (inlognaam en wachtwoord) die worden ingevoerd op een website die niet van versleuteling gebruik maakt, zullen zichtbaar over de tap meekomen. Het bovenstaande kan worden afgeleid uit de (technische) werking van een internettap en jurisprudentie. Illustratief is bijvoorbeeld een uitspraak van de Rechtbank Zutphen, waarin onder meer naar aanleiding van een chatgesprek is te lezen: 'Voorts is er een internettap geplaatst op de computer van de verdachte. Uit het internetgedrag van de verdachte is gebleken dat hij MSN-contacten onderhield met slachtoffer 2.'[3]
En in een zaak van de Rechtbank Haarlem wordt bijvoorbeeld het

2 Een IP-adres is een nummer dat uit vier sets van cijfers bestaat. Voor computers binnen de organisatie van de Universiteit Leiden zijn bijvoorbeeld IP-adressen toegewezen van 132.229.0.0 tot en met 132.229.255.255. Op dit moment worden IP-adressen uitgegeven onder Internet Protocol (IP) versie 4, oftewel IPv4. Op termijn moeten we overstappen naar versie 6 van het IP (IPv6). Deze nieuwe standaard zorgt voor nieuwe vraagstukken met betrekking tot het aftappen van internetverkeer. In dit artikel wordt daar verder niet op ingegaan.

3 Rb. Zutphen 7 oktober 2008, LJN BF7037. Zie ook bijvoorbeeld Rb. Breda 20 januari 2007, LJN AZ7281 en Rb. Groningen 20 mei 2010, LJN BM5193.

volgende citaat uit een proces-verbaal genoemd: 'Uit de internettap van verdachte blijkt dat er onder meer 398 websites [zijn] bezocht, waaronder die van Schiphol. [Er] Wordt gekeken naar de aankomende vlucht op 21-04-07 uit Paramaribo en ook die van 20-04 en 21-04.'[4]

Gegevensverkeer van smartphones kan tevens worden afgetapt, waardoor bijvoorbeeld berichten die via het populaire programma 'Whatsapp' standaard onversleuteld worden verstuurd voor opsporingsdiensten zichtbaar worden. Locatiegegevens of andere kenmerken kunnen tevens uit het gegevensverkeer worden gedestilleerd door opsporingsinstanties. Het 'zichtbaar' maken van de gegevens vereist echter specifieke kennis en software die constant actueel moet worden gehouden. De snelle technologische ontwikkelingen en het groeiende volume van het gegevensverkeer vormen uitdagingen voor opsporingsinstanties, maar theoretisch is veel mogelijk.

Door de toenemende afhankelijkheid van mensen van communicatie via internet is het niet vreemd dat opsporingsinstanties deze communicatie onder omstandigheden willen onderscheppen. Het onderschepte internetverkeer kan belangrijk bewijsmateriaal opleveren in opsporingsonderzoeken. Aan de andere kant levert het heimelijk onderscheppen van communicatie een ernstige inbreuk op de persoonlijke levenssfeer van de betrokkenen. Wellicht kan zelfs worden gesteld dat de internettap een grotere inbreuk op de persoonlijke levenssfeer met zich meebrengt dan een traditionele telefoontap waarbij alleen verbale communicatie wordt onderschept. Eventueel zou slechts specifiek verkeer zichtbaar kunnen worden gemaakt door middel van filtersoftware. Aangezien in dit artikel de aftapbaarheid van de internettap centraal staat, wordt op dit aspect verder niet ingegaan.

Cijfers over het gebruik van de internettap door opsporingsdiensten zijn pas sinds korte tijd voorhanden. In 2009 werd bekend dat het aantal internettaps 'explosief' was gestegen. De stichting Nationale Beheersorganisatie Internet Providers (NBIP) constateerde een stijging van 69 internettaps in 2006 naar 335 in 2009.[5] Stichting NBIP faciliteert echter alleen de uitvoering van internettaps voor de

4 Rb. Haarlem 15 februari 2008, LJN BC4535.

5 Zie www.nbip.nl/nieuws/nbip-heeft-tachtig-deelnemers/ (laatst geraadpleegd op 16 maart 2012).

kleine internetserviceproviders (hierna: ISP's). Juist de grote ISP's hebben een goede infrastructuur voorhanden voor het plaatsen van een internettap, maar hier zijn voor de periode 2006-2009 geen tapcijfers over bekend. Wel is in een jaarverslag van het ministerie van Veiligheid en Justitie te lezen dat in 2010 in totaal 1.704 'IP-taps' zijn ingezet.[6] De toenmalige minister van Justitie heeft toegezegd vanaf 1 januari 2010 het aantal internettaps bij te houden en de Kamer hierover te informeren.[7] Op het moment van schrijven (maart 2012) zijn nog geen cijfers over 2011 bekend en is het onduidelijk of wederom een significante stijging voor het gebruik van een internettap heeft plaatsgevonden. Dit is echter wel de verwachting.[8] Samenvattend: een internettap onderschept al het internetverkeer van en naar een bepaald IP-adres. Daarbij komt niet alleen internettelefonieverkeer over de tap mee, maar worden bijvoorbeeld ook onversleutelde zoektermen, chatberichten en privéberichten onderschept. De sterke stijging in het gebruik van de internettap is niet vreemd, gezien de toenemende afhankelijkheid van mensen van internet als middel voor communicatie. Opsporingsinstanties willen als dat nodig is zo veel mogelijk van die communicatie kunnen onderscheppen.

Het aftappen van communicatie brengt een significante inbreuk op de persoonlijke levenssfeer van de betrokkenen met zich mee. Op grond van artikel 8 van het Europees Verdrag van de Rechten van de Mens (EVRM) en het strafvorderlijke legaliteitsbeginsel moet de inbreuk op het recht op privacy daarom bij de wet voorzien zijn. In de volgende paragraaf wordt nader op de wettelijke regeling van Nederland ingegaan.

6 Kamerstukken II 2010/11, 32 710, nr. 1, p. 67 (jaarverslag is aangeboden op 18 mei 2011). Onder een IP-tap wordt een internettap en e-mailtap verstaan. Een reden voor het onderscheid is dat wellicht in de praktijk een aparte taplast voor het tappen van e-mail bij access providers worden afgegeven. Dit blijft echter onduidelijk.

7 Zie Aanhangsel Handelingen II 2009/10, nr. 2010Z04067 (antwoord Kamervragen van de leden Peters en Gerkens over de explosieve toename van internet- en VoIP-taps op 8 april 2010).

8 Zie Aanhangsel Handelingen II 2009/10, nr. 2010Z04067 (antwoord Kamervragen van de leden Peters en Gerkens over de explosieve toename van internet- en VoIP-taps op 8 april 2010): 'Overigens ligt een toename van dit relatief jonge opsporingsinstrument voor de hand nu ook het gebruik van internet een zeer sterke groei heeft doorgemaakt in de afgelopen jaren. Dit zal naar verwachting nog verder toenemen met de groei van het (mobiel) gebruik van internet.'

De taplast

Een 'taplast' is een vordering van een officier van justitie (OvJ) om bepaalde telecommunicatie te onderscheppen voor opsporingsdoeleinden. Een taplast kan op grond van artikel 126m Wetboek van Strafvordering (Sv) worden opgelegd bij een redelijk vermoeden van een misdrijf in de zin van artikel 67 Sv, dat gezien zijn aard of omvang een ernstige inbreuk op de rechtsorde maakt. Een OvJ kan het bevel afgeven indien een machtiging van een rechter-commissaris wordt verkregen en het onderzoek dat dringend vordert.
Op grond van artikel 126m lid 3 Sv kan de taplast worden opgelegd 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 (Tw). De aanbieders moeten hun netwerk of dienst aftapbaar maken op grond van artikel 13 e.v. Tw en dienen hun medewerking te verlenen aan een tapbevel. Een tap zal in de praktijk vaak worden ingezet bij een ISP die de internetverbinding van burgers verzorgt. Deze dienstverleners worden ook wel 'access providers' genoemd en access providers kunnen worden beschouwd als een aanbieder van een openbaar telecommunicatienetwerk of -dienst. Internetverkeer passeert tijdens het transport enkele tussenstations, waaronder die bij access providers, waar het verkeer op een bepaald IP-adres kan worden afgetapt.
Vaste telefonie gaat tegenwoordig ook vaak via internet. Deze vorm van telefonie wordt ook wel 'Voice over IP-telefonie', kortweg VoIP, genoemd. Telecommunicatie aanbieders die deze zogeheten 'managed VoIP-services' via hun infrastructuur aanbieden, zijn verplicht hun netwerk of dienst aftapbaar te maken. Het is wellicht geruststellend voor opsporingsdiensten dat het adviesbureau Stratix in 2009 nog stelde dat managed VoIP-services goed aftapbaar zijn en dat 'verreweg het grootste deel van de communicatie tussen personen plaatsvindt via traditionele spraaktelefonie dan wel via de "managed-VoIP" varianten' (Stratix, 2009, p. 17). Echter, soms gaat communicatie via internet ook via andere 'tussenstations', waardoor het aftappen lastiger wordt. Al in 1996 gaf het toenmalige kabinet aan dat zowel netwerken als diensten aftapbaar zouden

moeten zijn, zodat ook de 'schakelmiddelen' aftapbaar zijn en niet alleen de (kale) netwerken.[9]
Een probleem bij het tappen van internetverkeer bij acces providers is dat internetverkeer door tussenliggende diensten kan worden versleuteld, waardoor de inhoud van de communicatie voor opsporingsdiensten onherkenbaar wordt gemaakt. De wetgever heeft als oplossing voor dit probleem bedacht dat ook deze tussenliggende diensten ('schakelmiddelen') aftapbaar zouden moeten zijn. Met de uitbreiding van de wet moest worden voorkomen dat criminelen gebruik gingen maken van niet-aftapbare moderne telecommunicatiediensten.[10] Over het begrip aanbieder van een openbaar telecommunicatienetwerk of -dienst bestaat echter nog veel onduidelijkheid.
Slechts aanbieders van *openbare* telecommunicatie moeten aftapbaar zijn. De memorie van toelichting van de Telecommunicatiewet stelt dat het hierbij gaat om een dienst die 'openbaar wordt aangeboden en beschikbaar is voor eenieder die van dat aanbod gebruik wil maken tegen de in het openbare aanbod vermelde condities'.[11] Diensten die uitsluitend beschikbaar zijn voor leden van een 'besloten gebruikersgroep' zijn geen openbare telecommunicatiediensten.[12]
Besloten elektronische telecommunicatieaanbieders of elektronische aanbieders van diensten kunnen bij wijze van uitzondering op grond van artikel 13.7 Tw worden afgetapt. Deze bepaling is echter nog (steeds) niet in werking getreden. Over het begrip telecommunicatie-*dienst* bestaat tevens onduidelijkheid. Een telecommunicatiedienst is op grond van artikel 1.1 onder ff Tw een 'dienst die geheel of gedeeltelijk bestaat in de overdracht of routering van signalen via een elektronisch communicatienetwerk verzorgd, voor zover deze niet bestaat uit het verspreiden van programma's'.

9 Kamerstukken II 1995/96, 24 679, nr. 1, p. 8 (brief van de minister over aftappen van telecommunicatie). Zie ook Kamerstukken II 1996/97, 25 544, nr. 3, p. 124 (MvT Telecommunicatiewet).
10 Kamerstukken II 1996/97, 25 544, nr. 3, p. 123 (MvT Telecommunicatiewet).
11 Kamerstukken II 1996/97, 25 533, nr. 3, p. 72 (MvT Telecommunicatiewet).
12 In dit kader is de uitspraak in de Surfnet-zaak van 27 maart 2009 relevant (Rb. Rotterdam 27 maart 2009, LJN BH9324). In een kort geding oordeelde de rechtbank dat Surfnet niet als openbare elektronische communicatiedienst is aan te merken. De kring waaraan Surfnet haar diensten aanbiedt (instellingen van wetenschappelijk en hoger onderwijs), is volgens de rechtbank beperkt te achten en niet toegankelijk voor het algemene publiek.

Het is bijvoorbeeld de vraag of aan de populaire VoIP-dienst 'Skype' een taplast kan worden gegeven. Naar verluidt is de communicatiedienst via internet niet of op zijn minst moeizaam aftapbaar (Europol, 2011, p. 5).[13] In zijn basis levert het bedrijf software die kosteloos via peer-to-peertechnologie een communicatieverbinding tussen twee computers mogelijk maakt.[14] De gegevensuitwisseling tussen computers wordt daarbij versleuteld, waardoor het gegevensverkeer niet bij een ISP geïnterpreteerd kan worden en zichtbaar worden gemaakt. Skype maakt gebruik van een bestaande telecommunicatie-infrastructuur en verzorgt daarbij niet grotendeels de overdracht of routering van signalen. De basisdienst van Skype valt daarom naar mijn mening niet onder het begrip uit de Telecommunicatiewet. Echter, met Skype kan tevens tegen betaling worden gebeld naar houders van vaste en mobiele telefoonnummers. Mijns inziens is het lastiger vol te houden dat Skype met betrekking tot deze dienst geen aanbieder van een openbare telecommunicatiedienst is. Maar zelfs als een dienst van Skype onder Nederlands recht verplicht aftapbaar moet worden gemaakt, is het de vraag of de vordering ten uitvoer kan worden gebracht. Bij peer-to-peertechnologie gaat namelijk niet al het verkeer via een centrale server waar het verkeer kan worden afgeluisterd.

Daarnaast speelt bij Skype een jurisdictieprobleem. Een staat kan van oudsher slechts wetten handhaven op personen en instellingen die zich op het eigen territoir bevinden. Nederland maakt bij het handhaven van zijn wetten buiten Nederlands territoir in principe een inbreuk op de soevereiniteit van de andere staat. Indien het bedrijf niet meewerkt aan een verzoek van Nederlandse autoriteiten is het lastig een bedrijf te dwingen een bevel ten uitvoer te brengen. Slechts met toestemming van de staat waar het bedrijf of de instelling gevestigd is of met een rechtshulpverzoek kan een tap eventueel in het buitenland ten uitvoer worden gelegd. In dat geval zal in de meeste gevallen aan de lokale wetgeving voor het ten uitvoer leggen van een tap moeten worden voldaan. Rechtshulpverzoeken worden niet altijd gehonoreerd en brengen vaak flinke vertraging voor

13 Kamerstukken II 2008/09, 28 684, nr. 232, p. 3. Europol, 2011, p. 5: 'In particular, the perceived anonymity afforded by Communications technologies such as email, instant messaging and Internet telephony (VoIP) has led to them being used increasingly by Organised Crime groups as a countermeasure to law enforcement detection and surveillance.'

14 De dienst van Skype wordt ook wel 'unmanaged VoIP' genoemd.

opsporingsonderzoeken met zich mee. Daarbij moet wel worden opgemerkt dat binnen de Europese Unie wel enige afspraken zijn gemaakt met betrekking tot rechtshulp en aftappen van telecommunicatie als onderdeel daarvan. Mogelijk wordt het handhavingsprobleem minder groot naarmate voor het bedrijf meer commerciële belangen op het spel staan en meer noodzaak bestaat zich fysiek op Nederlands territoir te begeven.
Niet alleen bij Skype bestaat onduidelijkheid of het bedrijf onder het begrip 'aanbieder van een openbaar telecommunicatienetwerk of -dienst' valt. Dezelfde vraag speelt voor hostingproviders of elektronische communicatieaanbieders zoals Gmail. Volgens Knol en Zwenne vallen opslagdiensten echter niet onder het begrip telecommunicatiedienst (Knol en Zwenne, 2009, p. 371). De meeste hostingproviders lijken daardoor niet te hoeven voldoen aan een taplast. De toenmalige minister van Justitie Hirsch Ballin heeft indertijd aangegeven dat *webmail*-diensten zoals Gmail en Hotmail niet als een aanbieder van een openbare telecommunicatiedienst in de zin van de Telecommunicatiewet worden aangemerkt.[15] Deze communicatieaanbieders lijken daarom vooralsnog erop te kunnen vertrouwen dat aan hen geen taplast wordt gegeven. Tevens kan worden afgevraagd of 'proxydienstverleners' of 'VPN-providers' aftapplichtig zijn.[16] Deze diensten leiden het gegevensverkeer naar een bepaalde server om. Hierdoor wordt het IP-adres gewijzigd waaraan een bepaalde computer kan worden herkend. In de context van tappen is belangrijker nog dat in ieder geval bij een VPN-dienst van sterke versleuteling gebruik kan worden gemaakt, waardoor de inhoud van afgetapt gegevensverkeer bij ISP's onherkenbaar wordt gemaakt. De vraag is of een aanbieder van een proxy- of VPN-dienst een openbare dienst aanbiedt die geheel of gedeeltelijk bestaat in de overdracht of routering van signalen via een elektronisch communicatienetwerk. Zelfs indien onder omstandigheden wordt aangenomen dat dit het geval is, speelt ook bij deze dienstverleners vaak het probleem dat ze in het buitenland gevestigd zijn. De medewerking aan een taplast zal daarom in de praktijk moeizaam verlopen. Onduidelijkheid over het begrippenpaar uit de Telecommunicatiewet leidt er in ieder geval toe dat sommige diensten

15 Dit valt af te leiden uit Kamerstukken II 2007/08, 31 145, nr. 9, p. 6 en Kamerstukken I 2008/09, 31 145, F, p. 4.
16 VPN staat voor 'virtual private network'.

niet aftapbaar zijn op het moment dat ze op de markt worden geïntroduceerd (Koops e.a., 2005, p. 30). Voor dit artikel is niet onderzocht of de situatie in 2012 is verbeterd.
Opgemerkt moet worden dat aanbieders van internetcommunicatiediensten op grond van artikel 126m lid 4 Sv wel *vrijwillig* kunnen meewerken aan het ten uitvoer leggen van een taplast. Veel bedrijven vallen namelijk onder het begrip 'aanbieder van een communicatiedienst' in de zin van artikel 126la Sv, waarnaar in artikel 126m lid 4 Sv verwezen wordt. Aanbieders van communicatiediensten hebben hun infrastructuur vaak zo ingericht dat de mogelijkheid bestaat gegevensverkeer af te tappen. Daardoor is het onder omstandigheden tóch mogelijk bij bijvoorbeeld een hostingprovider of (besloten) universiteitsnetwerk internetcommunicatie af te tappen.
Samenvattend kan worden gesteld dat een last tot het aftappen van internetverkeer slechts onder bepaalde voorwaarden door de officier van justitie na machtiging van de rechter-commissaris kan worden opgelegd. Niet duidelijk is echter aan *wie* de aftaplast precies kan worden opgelegd. Deze onduidelijkheid leidt ertoe dat een deel van het internetverkeer niet met een bevel kan worden afgetapt en de inhoud van communicatie die via internet verloopt niet zichtbaar is voor opsporingsdiensten. Daarnaast bestaat er een handhavingsprobleem met betrekking tot buitenlandse telecommunicatiedienstaanbieders.

Naast deze uitvoeringsproblemen van de taplast leiden technologische ontwikkelingen tot een beperking van de effectiviteit van een internettap. Hier wordt in de volgende paragraaf op ingegaan.

Beperkingen internettap

Slechts indien het verkeer van een communicatiedienst *onversleuteld* over de afgetapte internetverbinding bij een ISP gaat, kunnen opsporingsdiensten kennisnemen van de inhoud van de communicatie. In toenemende mate maken communicatiedienstverleners op internet echter standaard gebruik van versleuteling. De techniek van het versleutelen van data wordt cryptografie of 'encryptie' genoemd. Bij versleuteling worden leesbare data ('plaintext') omgevormd in onleesbaar materiaal ('ciphertext') door middel van een

wiskundig algoritme. Met de sleutel (vaak een lange reeks van cijfers en letters) kunnen de data weer leesbaar worden gemaakt. Vaak wordt een wachtwoord gebruikt om ook de sleutel te beveiligen.
Op grond van artikel 126m lid 6 Sv moet de aangebrachte versleuteling door de aanbieder van het openbare telecommunicatienetwerk of -dienst ongedaan worden gemaakt. In de taplast ligt deze plicht tot ontsleuteling besloten, dus daarvoor hoeft geen apart bevel worden afgegeven door de officier van justitie.[17] Ondanks het ontsleutelbevel kan de ISP, waar de tap meestal wordt geplaatst, het verkeer in veel gevallen niet ontsleutelen. Het verkeer wordt immers vaak door tussenliggende diensten versleuteld. De ISP draagt in die situatie geen kennis van de versleuteling. De tussenliggende diensten hoeven vaak niet aan een taplast te voldoen en daarmee ook niet aan de ontsleutelplicht. Bovendien bevinden de diensten zich, zoals eerder aangegeven, dikwijls in het buitenland.
In de afgelopen jaren zijn bijvoorbeeld de populaire communicatiediensten Gmail en Twitter standaard van versleuteling voorzien en andere populaire (communicatie)diensten, zoals Facebook en Hotmail, bieden versleuteling nu (in maart 2012) als optie aan.[18] Bij een internettap bij een ISP is het gegevensverkeer van de computer naar de website 'http://www.website.com' bijvoorbeeld zichtbaar, maar bij 'https://www.website.com' in het geheel niet, voor zover versleuteling over het gehele communicatieproces wordt aangeboden. Het verkeer wordt in het tweede geval namelijk versleuteld met het SSL-protocol.[19]
Burgers kunnen ook zelf van versleuteling gebruik maken teneinde de inhoud van het communicatieverkeer voor opsporingsinstanties onzichtbaar te maken. Daarbij kan bijvoorbeeld worden gedacht aan versleuteling van e-mailverkeer via het populaire programma *Pretty Good Privacy* (PGP). Hierbij is het echter wel van belang dat zowel de verzender als de ontvanger zorgvuldig en consistent met het versleutelsysteem omgaat. Justitie kan de verdachte vooralsnog

17 Kamerstukken II 1998/99, 26 671, nr. 3, p. 24 (MvT Wet computercriminaliteit II).
18 De Nederlandse sociale-netwerkdienst Hyves lijkt overigens geen versleuteling toe te passen. Opgemerkt kan worden dat veel berichten op Twitter openbaar zijn, met uitzondering van zogeheten privéberichten die kunnen worden verstuurd.
19 SSL staat voor 'Secure Socket Layer'. Opgemerkt moet worden dat ook allerlei andere internetprotocollen versleuteld kunnen worden. In dit artikel wordt verder niet op deze technische aspecten ingegaan.

geen bevel geven tot ontsleuteling van communicatieverkeer op grond van artikel 126m lid 7 Sv.[20]
De internettap als opsporingmethode om kennis te nemen van de inhoud van communicatie heeft mede door encryptie sterk aan effectiviteit ingeboet. In de Verenigde Staten is dit probleem door de FBI aangekaart als de 'Going Dark Problem'.[21]

WiFi en Hotspots

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. Een plek waar draadloze internettoegang wordt aangeboden, wordt een 'hotspot' genoemd. Voor het aftappen van internet maakt het geen verschil of de verdachte na ontvangst van de verbinding van de ISP van een draadloos of vast netwerk gebruik maakt. Het probleem zit daar waar de verdachte van andere draadloze internetverbindingen gebruik maakt.
Draadloze verbindingen zijn tegenwoordig wijdverbreid beschikbaar. Gedacht kan worden aan bijvoorbeeld het WiFi-netwerk van de buurvrouw of gratis aangeboden onbeveiligde netwerken in restaurants, treinen of cafés.[22] Indien de internetgebruiker op reis is, kan bijvoorbeeld van verschillende netwerken achter elkaar gebruik worden gemaakt. Slechts bij de aanbieder waar een tapbevel wordt afgegeven, wordt het verkeer afgetapt en daardoor kan niet altijd de gehele internetcommunicatie van een verdachte worden afgeluisterd. Indien opsporingsdiensten al het internetverkeer van een verdachte zouden willen aftappen, moet een tap worden geplaatst op

20 Niet zelden geeft de verdachte echter vrijwillig zijn sleutel af. In dit artikel wordt verder niet ingegaan op het verplicht afgeven van encryptiesleutels.

21 Getuigenis van Valerie Caproni op 17 februari 2011, 'Going dark: Lawful electronic surveillance in the face of new technologies', p. 1: 'In the ever-changing world of modern communications technologies, however, the FBI and other government agencies are facing a potentially widening gap between our legal *authority* to intercept electronic communications pursuant to court order and our practical *ability* to actually intercept those communications.' Beschikbaar via: http://judiciary.house.gov/hearings/pdf/Caproni02172011.pdf (laatst geraadpleegd op 16 maart 2012).

22 Een voorbeeld van een zaak waarbij de verdachte gebruik maakte van de WiFi-verbinding van de buurvrouw, waarna de politie en justitie bij het verkeerde huis een inval deden, is te vinden in de uitspraak van het Hof Den Haag 9 maart 2011, LJN BP7080.

alle netwerk- en dienstaanbieders waarvan een verdachte gebruik maakt. Dat is in de praktijk vaak onmogelijk.
Kortom, een internettap zal niet altijd het door opsporingsdiensten gewenste resultaat opleveren, omdat maar een deel van de communicatie via het afgetapte netwerk of dienst verloopt en omdat verdachten van veel niet-aftapbare (soms standaard) versleutelde communicatiediensten gebruik kunnen maken die zich al dan niet in het buitenland bevinden.

Hoewel de inhoud van het gegevensverkeer vaak niet zichtbaar kan worden gemaakt, komen wel andere relevante gegevens over de tap voorbij. Hier wordt in de volgende paragraaf op ingegaan.

Verkeersgegevens en gegevens bij communicatieaanbieders

Uit de kenmerken van gegevensverkeer kan belangrijke informatie worden afgeleid. Aan de hoeveelheid of het type informatie is bijvoorbeeld te zien of een groot bestand is verstuurd of een gesprek heeft plaatsgevonden. Tevens kan de telecommunicatieaanbieder zien op welke tijdstippen een bepaald apparaat van de internetverbinding gebruik maakt. Locatiegegevens die meekomen over de tap kunnen daarnaast aangeven waar de verdachte zich (grofweg) bevindt. Dergelijke gegevens worden ook wel 'verkeersgegevens' genoemd en kunnen na analyse belangrijk indirect bewijsmateriaal voor opsporingsdiensten opleveren.[23] De informatie kan bijvoorbeeld ondersteunend bewijs opleveren dat een verdachte vanaf een bepaalde computer op een specifiek tijdstip van internet gebruik heeft gemaakt. Bovendien vormen de IP-adressen waarmee de verdachte een verbinding maakt belangrijke aanknopingspunten voor verder onderzoek.
Het IP-adres kan bijvoorbeeld leiden naar een webserver van een bepaalde website of de server van een instelling, bedrijf en/of communicatiedienst zoals Twitter, Gmail, Hotmail, Facebook of Hyves.[24] Opsporingsdiensten kunnen vervolgens de aanbieders van communicatiediensten en zelfs *eenieder* aanspreken met een bevel tot vordering van gegevens teneinde de verdachte te identificeren

23 Zie ook Kamerstukken II 2007/08, 31 145, nr. 9, p. 6.
24 Zie ook Kamerstukken I 2008/09, 31 145, F, p. 4 (nadere MvA).

of de inhoud van de communicatie te achterhalen. Het spoor (in dit geval het IP-adres) kan ook leiden naar een anonimiseringsdienst zoals een proxy- of VPN-dienstverlener. Bij deze dienstaanbieders kan tevens een vordering tot het afgeven van identificerende of opgeslagen gegevens worden gedaan.[25]

Aanbieders van elektronische openbare telecommunicatienetwerken en -diensten zijn per 1 september 2009 verplicht verkeersgegevens met betrekking tot internetverkeer voor zes maanden te bewaren.[26] De gegevens moeten worden bewaard teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.[27] De bewaarplicht geldt niet voor aanbieders van communicatiediensten die niet onder het begrippenpaar uit de Telecommunicatiewet vallen. De gegevens die voorhanden zijn bij aanbieders van communicatiediensten kunnen echter wel met een bevel van een opsporingsambtenaar of OvJ worden gevorderd. De regels voor het vorderen van gegevens door politie en justitie zijn in het Wetboek van Strafvordering geïmplementeerd met de Wet bevoegdheden vorderen gegevens uit 2006.[28] Voor het vorderen van gegevens bij communicatieaanbieders in de zin van artikel 126la Sv geldt een ander regime dan voor het vorderen van gegevens bij overige instellingen, bedrijven of natuurlijk personen.

Bij een aanbieder van een communicatiedienst kunnen op grond van artikel 126n Sv gegevens worden gevorderd over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker. De vordering kan door een OvJ worden afgegeven in het belang van een opsporingsonderzoek bij een misdrijf zoals bedoeld in artikel 67 Sv. Met betrekking tot de opgeslagen gegevens bij de communicatieaanbieder kan worden gedacht aan de

25 Zie bijvoorbeeld Martin, 2011. De verdachte werd gezocht voor het hacken van het 'Sony Playstation Network' in 2011. De verdachte maakte gebruik van de VPN-service met de – in deze context ironische – naam 'Hide My Ass'. De dienst gaf echter de gebruikersgegevens en het IP-adres van de thuiscomputer van de verdachte af op vordering van de FBI.

26 Zie Wet bewaarplicht telecommunicatiegegevens, Stb. 2009, 360. De bewaartermijn voor verkeersgegevens met betrekking tot het internetgebruik is op 16 juli 2011 van twaalf maanden naar zes maanden verlaagd (Stb. 2011, 350). De wet is een implementatie van de Richtlijn dataretentie (2006/24/EG).

27 Kamerstukken II 2006/07, 31 145, nr. 3, p. 2 (MvT Wet bewaarplicht telecommunicatiegegevens).

28 Wet van 16 juli 2005, Stb. 2005, 390.

naam en adresgegevens van de verdachte, rekeninghoudergegevens, het e-mailadres en het IP-adres dat wordt opgeslagen ten tijde van de registratie. In zogenoemde loggegevens van een communicatieaanbieder zijn soms ook IP-adressen te vinden van de computer waarmee de (ook eventueel onbevoegde) gebruiker van een account op een bepaald tijdstip gebruik heeft gemaakt. Deze informatie kan van belang zijn in een opsporingsonderzoek, omdat zij meer informatie verstrekt over een bepaalde verdachte en over de communicatiemiddelen waarvan gebruik is gemaakt.
Hoewel de inhoud van communicatie via een communicatiedienstaanbieder door versleuteling niet altijd bij een tap zichtbaar is, kunnen de opgeslagen inhoudelijke berichten doorgaans wel bij communicatieaanbieders worden gevorderd. Opgeslagen gegevens kunnen op bevel van een OvJ met een schriftelijke voorgaande machtiging van de rechter-commissaris worden gevorderd op grond van artikel 126ng lid 2 Sv, indien het onderzoek dit dringend vordert bij misdrijven die een ernstige inbreuk op de rechtsorde opleveren. Daarbij kan worden gedacht aan verstuurde privéberichten die via sociale-netwerkdiensten, zoals Hyves, Facebook en Twitter, zijn verstuurd of opgeslagen foto's en e-mails bij ISP's en webmailaanbieders. De toenmalige minister van Justitie heeft aangegeven dat er voor het aftappen van e-mailverkeer en het vorderen van opgeslagen e-mailberichten geen verschil in voorwaarden voor de procedure is.[29] De reden daarvoor is dat de inbreuk op de persoonlijke levenssfeer van de betrokkene bij beide opsporingsbevoegdheden vergelijkbaar is.
Belangrijke communicatieaanbieders, zoals Facebook, Google, Microsoft en Twitter, bevinden zich echter in het buitenland. In de Verenigde Staten gelden andere strafvorderlijke regels dan in Nederland. Gegevens bij deze bedrijven kunnen slechts met toestemming van de aangezochte staat of een rechtshulpverzoek worden verkregen. Niet altijd wordt aan de vordering voldaan en het brengt in de regel vertraging met zich mee. Toch is de wetgeving in de Verenigde Staten voor het verkrijgen van de gegevens enigszins vergelijkbaar met die van Nederland, omdat beide landen het Cybercrimeverdrag

29 Kamerstukken II 2004/05, 26 671, nr. 10, p. 10 (NV II).

geratificeerd hebben.[30] Op grond van artikel 32 sub b Cybercrimeverdrag kunnen gegevens zonder rechtshulpverzoek direct worden opgevraagd bij het bedrijf dat over de gegevens handelingsbevoegd is. Die bevoegdheid gegevens af te staan zou kunnen worden afgeleid uit de overeenkomst die is afgesloten met de gebruiker van de communicatiedienst.[31] Het bedrijf moet wel toestemming verlenen tot het verstrekken van die gegevens.[32] Onduidelijk is welke Amerikaanse bedrijven, wellicht onder hun eigen voorwaarden, gegevens vrijwillig afstaan aan buitenlandse opsporingsinstanties en welke bedrijven dat slechts na een officiële rechtshulpprocedure doen. Indien het verzoek tot vorderen van gegevens niet via een officieel rechtshulpverzoek bij een Amerikaanse autoriteit verloopt, valt een zekere mate van controle weg en dat kan nadelig zijn voor de rechtsbescherming van de betrokkene.
Statistieken over de hoeveelheid vorderingen die door opsporingsinstanties bij communicatieaanbieders worden gedaan, zijn schaars.[33] De staatssecretaris van Veiligheid en Justitie geeft in antwoord op Kamervragen aan dat de korpschef van het Korps Landelijke Politie Diensten (KLPD) en de voorzitter van het College van Procureurs-Generaal hebben laten weten dat 'het belang van opsporing en vervolging zich verzet' tegen het aanbieden van statistieken over vorderingen bij sociale-netwerkdiensten.[34] De staatssecretaris heeft deze stellingname verder niet toegelicht.

30 Verdrag inzake de bestrijding van strafbare feiten verboden met elektronische netwerken, Trb. 2002, 18. In art. 16 t/m 18 van het Cybercrimeverdrag zijn bepalingen opgenomen met verplichtingen voor de verdragsstaten over het beschikbaar stellen van gegevens onder bepaalde voorwaarden voor opsporingsdoeleinden.

31 Kamerstukken II 2004/05, 26 671, nr. 10, p. 25 (NV II).

32 Explanatory Report Cybercrimeverdrag, par. 294, beschikbaar op: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (laatst geraadpleegd op 16 maart 2012).

33 Google publiceert daarentegen sinds kort in haar 'transparency report' ook statistieken over opgevraagde gegevens door Nederlandse autoriteiten. In de periode van 1 januari 2011 tot 30 juni 2011 is 64 keer een vordering gedaan voor in totaal 213 gebruikers. In 48% van de gevallen werd door Google aan de vordering voldaan. Beschikbaar via: www.google.com/transparencyreport/governmentrequests/NL/ (laatst geraadpleegd op 16 maart 2012).

34 Zie Aanhangsel Handelingen II 2011/12, nr. 2011Z23302 (antwoord op Kamervragen van het lid El Fassed over onlineprivacy op 8 februari 2012).

Ter overweging

De wetgever zou kunnen overwegen artikel 126m Sv aan te passen om tevens communicatieaanbieders in de zin van artikel 126la Sv aftapplichtig te maken in plaats van slechts aanbieders van openbare telecommunicatiediensten en -netwerken. Enerzijds sluit dit beter aan bij de systematiek van het Wetboek van Strafvordering; er kan dan meer inhoudelijke informatie *realtime* worden vergaard bij bedrijven op Nederlands grondgebied wanneer de verdachte via internet heeft gecommuniceerd. Als bijvoorbeeld 'slechts' netwerkverkeer bij Hyves wordt afgetapt, levert dit wellicht een minder grote inbreuk op privacy op dan wanneer al het internetverkeer bij een ISP wordt afgetapt. Anderzijds roept de maatregel wellicht weerstand op en brengt deze extra kosten voor de communicatieaanbieder met zich mee. Mogelijk wordt innovatie beperkt als een dergelijk brede aftapplicht wordt ingevoerd, omdat nieuwe communicatiediensten en software aftapbaar gemaakt moeten worden. Daarnaast kan worden gewezen op een beveiligingsrisico. Als voorbeeld nemen we Skype. Mogelijk wordt Skype in de toekomst aftapbaar als gevolg van de overname van Skype door Microsoft in mei 2011.[35] Het aftapbaar maken van Skype is denkbaar door via een 'achterdeurtje' in de software toegang te verschaffen tot een verbinding en zo het gesprek voor opsporingsinstanties op te laten nemen. Sommige deskundigen waarschuwen dat op deze wijze software opzettelijk onveilig wordt gemaakt. Deze kwetsbaarheid kan namelijk door kwaadwillenden worden uitgebuit, zodat ook criminelen zich toegang kunnen verschaffen tot de inhoud van communicatie.[36] Voordat een dergelijke verstrekkende wetswijziging wordt doorgevoerd zou meer onderzoek naar de maatregel wenselijk zijn.[37]

35 Zie www.computerworld.com/s/article/9218002/Microsoft_seeks_patent_for_spy_tech_for_Skype (laatst geraadpleegd op 16 maart 2012).

36 Getuigenis van Susan Landau op 17 februari 2011, 'Going dark: Lawful electronic surveillance in the face of new technologies'. Beschikbaar via: http://judiciary.house.gov/hearings/pdf/Landau02172011.pdf (laatst geraadpleegd op 16 maart 2012).

37 Overigens moet er zowel bij de reguliere internettap als bij een tap bij een communicatieaanbieder worden nagedacht over hoe moet worden omgegaan met geheimhoudersgesprekken. In dit artikel wordt op dat aspect verder niet ingegaan.

Tevens kan worden overwogen de bewaarplicht voor internetgegevens naar communicatieaanbieders uit te breiden. Op dit moment geldt de bewaarplicht alleen voor aanbieders van openbare telecommunicatienetwerken en -diensten. Met een bewaarplicht wordt de beschikbaarheid van verkeersgegevens veiliggesteld. Een dergelijke maatregel maakt echter een ernstige inbreuk op de persoonlijke levenssfeer van de betrokkene en brengt aanzienlijke kosten met zich mee (zie ook Prins, 2002, p. 322-323). Het is de vraag of een dergelijke plicht aan communicatieaanbieders moet worden opgelegd en welke uitvoerbaarheidsproblemen daarbij zullen ontstaan.

Een alternatieve manier om tóch inhoudelijke communicatie te verkrijgen is door de vertrouwelijke communicatie te vergaren met een technisch hulpmiddel. Deze bijzondere opsporingsbevoegdheid kan op grond van artikel 126l Sv worden ingezet. In een woning is het plaatsen van een technisch hulpmiddel alleen mogelijk bij verdenking van een misdrijf waar minimaal acht jaar gevangenisstraf op staat. In antwoord op Kamervragen van de leden Gesthuizen en El Fassed op 7 februari 2012 heeft minister Opstelten aangegeven dat het technische hulpmiddel ook een softwareprogramma op de computer van de verdachte zou kunnen zijn.[38] Gegevensverkeer kan theoretisch gezien direct op de computer zelf worden gekopieerd en met de software worden doorgestuurd naar de politie. Het verkeer wordt dan 'afgetapt' voordat versleuteling plaatsvindt en op die manier kan het probleem van versleuteling worden omzeild. De software kan ook een functionaliteit hebben waarbij toetsaanslagen, waaronder wachtwoorden, van de computergebruiker geregistreerd en doorgestuurd worden. Met de wachtwoorden kan encryptie eventueel ongedaan worden gemaakt. In de literatuur wordt wel aangenomen dat het plaatsen van software op de computer voor het opnemen van vertrouwelijke communicatie is toegestaan (Verbeek e.a., 2000, p. 155; Koops, 2007, p. 118). Mijns inziens is het echter niet toegestaan de software op afstand via internet te plaatsen door in te breken op de computer van de verdachte, omdat het een ontoelaatbare inbreuk levert op de persoonlijke levenssfeer van de verdachte, waarvoor geen expliciete grondslag

38 Aanhangsel Handelingen II 2010/11, nr. 2011Z22778. In de antwoorden wordt aangegeven dat van de software sporadisch in een opsporingsonderzoek gebruik wordt gemaakt.

in het Wetboek van Strafvordering voorhanden is (Oerlemans, 2011, p. 901-903).

Conclusie

De internettap wordt op een bepaald IP-adres geplaatst bij een aanbieder van een openbaar telecommunicatienetwerk of -dienst. Daarbij wordt niet slechts (internet)telefonieverkeer afgetapt, maar kan het gehele internetgebruik op tal van verschillende apparaten worden afgetapt. In de praktijk zal een internettap vaak bij een ISP worden geplaatst. Hostingproviders en andere communicatiedienstaanbieders kunnen wel vrijwillig meewerken bij de tenuitvoerlegging van een internettap. Aangezien burgers in toenemende mate afhankelijk worden van internetcommunicatie neemt de internettap een cruciale plaats in bij moderne opsporingsonderzoeken en is de verwachting dat van de bijzondere opsporingsbevoegdheid in toenemende mate gebruik zal worden gemaakt.
Niet duidelijk is aan welke bedrijven en instanties de aftaplast precies kan worden opgelegd. Deze onduidelijkheid leidt ertoe dat een deel van het internetverkeer niet kan worden afgetapt of de inhoud van het gegevensverkeer niet zichtbaar is voor opsporingsdiensten. Zelfs indien de wettelijke regeling met betrekking tot aftappen van telecommunicatie wordt aangepast, zal een deel van het verkeer van een verdachte niet kunnen worden afgetapt, omdat de betrokkene bijvoorbeeld gebruik maakt van veel verschillende (WiFi-) netwerken, al dan niet bewust gebruik maakt van versleuteling, of de communicatieaanbieder waarvan de betrokkene gebruik maakt zich in het buitenland bevindt en deze aanbieder Nederlandse tapvorderingen weigert uit te voeren. Aanpassing van wetgeving is niet vanzelfsprekend, omdat aan een plicht tot aftapbaarheid kosten zijn verbonden en deze wellicht onwenselijke neveneffecten met zich meebrengt met betrekking tot beveiliging en innovatie. Daarnaast moeten wettelijke regelingen worden afgewogen tegen het recht op privacy van de betrokkenen.
Hoewel niet alle inhoudelijke informatie kan worden afgetapt, heeft de internettap naar mijn mening wél een toekomst. Uit de kenmerken van het gegevensverkeer kunnen opsporingsdiensten namelijk relevante informatie afleiden. De zogeheten verkeersgegevens

kunnen als bewijsmateriaal dienen, omdat ze informatie geven over gedragingen van verdachten, en aanknopingspunten bieden voor verder onderzoek. Indien verdachten van anonimiseringsdiensten gebruikmaken om de identiteit of bepaald gegevensverkeer te verbergen, kan dit wellicht uit een internettap worden afgeleid, waarna bij de dienstaanbieder gegevens kunnen worden gevorderd. Opgeslagen inhoudelijke communicatie bij communicatieaanbieders kan bovendien in principe met een vordering worden verkregen. De communicatie kan echter niet altijd *realtime* en onder de Nederlandse normen worden verkregen, zoals dat bij een telefoontap in het verleden meestal wel het geval was. Vergeleken met een internettap brengt het vorderen van gegevens achteraf in veel gevallen vertraging met zich mee. Toch lijken de gegevens van sommige communicatieaanbieders in de Verenigde Staten onder omstandigheden direct opvraagbaar te zijn. Onduidelijk is onder welke voorwaarden de gegevens worden verstrekt. Dit kan de rechtsbescherming van betrokkenen in gevaar brengen.

Kortom, het is niet vanzelfsprekend dat inhoudelijke communicatie via internet kan worden afgetapt. Toch zal een internettap belangrijke informatie en aanknopingspunten verschaffen binnen een opsporingsonderzoek. In combinatie met andere bijzondere opsporingsbevoegdheden kunnen voor opsporingsdiensten goede resultaten worden behaald. Eventueel zouden bestaande regels scherper kunnen worden ingestoken of worden aangepast teneinde meer inhoudelijke communicatie te kunnen onderscheppen. Daarbij moeten geen overhaaste beslissingen worden genomen en is enig onderzoek naar eventuele neveneffecten daarvan noodzakelijk.

Literatuur

Europol
Internet facilitated organised crime
Den Haag, Europol, 2011

Knol, P.C., G.J. Zwenne
Tekst & Commentaar Telecommunicatierecht
Deventer, Kluwer, 2009

Koops, B.J. (red.)
Strafrecht & ICT
Den Haag, Sdu Uitgevers, 2007
Koops, B.J., R. Bekkers e.a.
Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet
Tilburg, TILT & Dialogic, 2005
Martin, A.
LulzSec hacker exposed by the service he thought would hide him
The Atlantic Wire, 23 september 2011 (www.theatlanticwire.com/technology/2011/09/lulzsec-hacker-exposed-service-he-thought-would-hide-him/42895/)
Oerlemans, J.J.
Hacken als opsporingsbevoegdheid?
Delikt en Delinkwent, nr. 8, 2011, p. 888-908
Prins, J.E.J.
Wapenwedloop in cyberspace. Gegevensmunitie ten kosten van privacy?
Ars Aequi, nr. 5, 2002, p. 315-323
Stratix
Grenzen aan de aftapbaarheid?
Hilversum, Stratix Consulting, 2009
Verbeek, J.P.G.M., Th.A. de Roos e.a.
Interceptie van vertrouwelijke communicatie
Den Haag, Sdu Uitgevers, 2000