Binnendringen op afstand: een onderzoek naar de verenigbaarheid van de voorgestelde bevoegdheid met artikel 8 EVRM.

Naam: G.W. Wijnstra

Studentnummer: 850452124

Scriptiebegeleider: Prof. dr. Wouter Ph. Stol

Examinator: Mr. dr. W.H.B. Dreissen

Aantal woorden: 14774

Datum inleveren: 13-09-2017

Inhoudsopgave

Hoofdstuk 1: Inleiding

§ 1.1 Aanleiding

Nieuwe methoden van communicatie hebben onze maatschappij veranderd. E-mail, WhatsApp en Skype zijn inmiddels niet meer weg te denken. Vrijwel iedereen gebruikt dergelijke communicatiediensten. In een rechtsstaat moeten burgers vertrouwelijk kunnen communiceren.[1] Daarom is beveiliging van communicatie van belang. Aanbieders van communicatiediensten zorgen veelal zelf voor beveiliging door versleuteling van hun berichtenverkeer. Opsporingsdiensten hebben de bevoegdheid om in sommige gevallen vertrouwelijke communicatie te onderscheppen, zodat zij hun taak effectief kunnen uitvoeren.[2] Als communicatie tussen A en B echter versleuteld is heeft onderschepping weinig zin, het onderschepte bericht kan niet worden gedecodeerd. Dit levert problemen op voor de opsporingspraktijk.[3] Een mogelijke oplossing is om de communicatie te onderscheppen voordat deze door A gecodeerd wordt of nadat deze door B is gedecodeerd. Om dat voor elkaar te krijgen moeten opsporingsdiensten toegang krijgen tot de gebruikte laptop of smartphone van A of B. In wetsvoorstel Computercriminaliteit III (hierna: CC-III) wordt hiertoe een nieuwe bevoegdheid gegeven: binnendringen op afstand.[4] Met deze uitbreiding wordt beoogd om beter toegang tot de inhoud van (versleutelde) communicatie te kunnen krijgen.[5] Buiten deze mogelijke oplossing voor opsporingsproblemen door encryptie, zijn ook andere oplossingen denkbaar. Deze alternatieven worden in § 5.4 besproken.

Problemen met encryptie zijn er niet alleen in Nederland.[6] Tijdens een EU-vergadering op 8 juli 2016 werd encryptie besproken binnen de context van criminaliteitsbestrijding.[7] Privacy-organisaties zoals Bits of Freedom mengen zich voortdurend in de encryptiediscussie.[8] Het onderwerp is actueel en maatschappelijk relevant. Er bestaat de maatschappelijke wens om criminaliteit tegen te gaan, deze op te sporen en te beschikken over een politie met voldoende

[1] Asscher 2002, p. 11.
[2] Art. 126l & 126la Sv, zie ook § 3.1.
[3] 'Versleuteling berichten WhatsApp probleem voor OM', *AD* 22 augustus 2016, www.ad.nl (zoek op OM &encryptie).
[4] Toekomstig artikel 126nba Sv, zie *Kamerstukken II* 2016/17, 34372, A.
[5] *Kamerstukken II* 2015/16, 34372, 3, p. 9-10 (MvT).
[6] Zie bijv.: 'Frankrijk en Duitsland willen versleuteld chatten inperken', *NOS* 23 augustus 2016, www.nos.nl (zoek op Frankrijk, Duitsland & encryptie).
[7] Voor resultaten van een enquête onder lidstaten zie: <https://www.asktheeu.org/en/request/input_provided_by_ms_on_question#incoming-11727>, laatst geraadpleegd op 01-07-2017.
[8] Zie bijv.: 'Bits of Freedom biedt Bertholee cursus grondrechten aan', *Bits of Freedom* 18 september 2016, www.bof.nl (zoek op grondrechten Bertholee).

bevoegdheden. Aan de andere kant bestaat er een behoefte aan vrijheid en privacy. Deze twee behoeften staan in dit geval op gespannen voet met elkaar.

De discussie over encryptie bestaat al sinds de jaren 90. Koops concludeerde destijds dat nietsdoen aan het encryptieprobleem de voorkeur verdient.[9] Sindsdien is er echter veel veranderd. De benodigde software om te versleutelen is gemakkelijk en vaak gratis te verkrijgen. Zonder veel moeite is online te vinden hoe dit versleutelingsproces werkt.[10] Bekende aanbieders als WhatsApp, Skype, Google en Apple versleutelen data automatisch, zonder dat de gebruiker daar iets voor hoeft te doen. Ook de wens om criminaliteit te bestrijden is sinds de jaren 90 veranderd. Na de aanslagen op de Twin Towers in New York is het wereldbeeld omgeslagen. Terreur maakt deel uit van onze samenleving en het lijkt erop dat we in Europa voorlopig nog niet verlost zijn van terroristische aanslagen. Veiligheid is mede door deze ontwikkeling een belangrijk maatschappelijk thema geworden en daarmee ook de opsporingsbevoegdheden. Dit rechtvaardigt nieuw juridisch onderzoek naar encryptie.

Deze inleiding bestaat verder uit de afbakening van het onderzoek (§ 1.2), een begrippenlijst (§ 1.3) en de centrale vraag, opbouw en gebruikte methode (§ 1.4).

§ 1.2 Afbakening

Het doel van dit onderzoek is om een juridische kennisbijdrage te leveren aan opsporingsproblemen die ontstaan door encryptie. Technische vraagstukken worden slechts voor zover juridisch van belang behandeld.

Door gebruik van encryptie kunnen zowel bestanden als communicatie versleuteld worden.[11] Dit onderzoek richt zich uitsluitend op de communicatie.

In het wetsvoorstel CC-III krijgen opsporingsdiensten de bevoegdheid om op afstand een geautomatiseerd werk binnen te dringen, om daar vervolgens opsporingshandelingen te verrichten.[12] Het aftappen en opnemen van communicatie is een onderzoeksdoel.[13] De inlichtingsbevoegdheden die de AIVD heeft op grond van de Wet op de inlichtingen- en

[9] Koops 1999, p. 289-295.
[10] Schneier, Seidel & Viajayakumar 2016, p. 6.
[11] Voorbeelden: kinderpornofoto's op een harde schijf (bestand), apps, e-mails, chats (communicatie).
[12] Toekomstig artikel 126nba Sv, zie *Kamerstukken II* 2016/17, 34372, A.
[13] *Kamerstukken II* 2016/17, 34372, 26, p. 8-9.

veiligheidsdiensten vallen buiten het bereik van mijn onderzoek. De toegestane omvang van dit onderzoek en het besloten karakter van de AIVD zijn daarvoor de redenen.

Gezien de beperkte omvang van dit onderzoek wordt het recht op vertrouwelijke communicatie uitsluitend afgeleid uit artikel 8 EVRM. Artikel 17 IVBPR, artikel 7 Handvest EU en artikelen 10 en 13 Grondwet bevatten vergelijkbare bepalingen, maar analyse van deze bepalingen wordt achterwege gelaten. Voor artikel 13 Gw is niet eens zeker of moderne communicatiemiddelen binnen de reikwijdte vallen.[14] Voor wat betreft EU-recht geldt dat de toets of een inbreuk op het recht van vertrouwelijke communicatie gerechtvaardigd kan worden, gelijk is aan die van het EHRM.[15] Het EVRM kent een sterke verbinding met democratische idealen en door uitspraken van het EHRM kunnen bepalingen verbindend geïnterpreteerd worden.[16] Dat zijn hoofdredenen voor de keuze voor het EVRM.

§ 1.3 Begrippen

Alvorens de centrale vraagstelling te formuleren, zal ik eerst enkele relevante begrippen daaruit definiëren:

Op afstand binnendringen:	De bevoegdheid voor opsporingsdiensten om op afstand geautomatiseerde werken binnen te dringen en om daar onderzoek te doen ten behoeve van de opsporing van strafbare feiten.[17] Dit wordt ook wel terughacken genoemd, maar deze term dekt de lading onvoldoende. Bij een onderschept bericht is vaak geen sprake van een hack, dus kan er ook niet “terug” gehackt worden.
Versleutelde communicatie:	Alle communicatie die met een elektronische sleutel beveiligd is.
Recht op vertrouwelijke communicatie:	Het recht om in het geheim te communiceren met een bepaald publiek, te plaatsen binnen het bredere recht op privacy.[18]

[14] Zie bijv.: Prins 2013.
[15] Zie Lensen 2012, p. 28.
[16] Nieuwenhuis & Hins 2011, p. 33-34.
[17] Toekomstig art.126nbaSv in voorgestelde wet computercriminaliteit III, *Kamerstukken II* 2016/17, 34372, A.
[18] Asscher 2002, p. 11-13.

Het recht wordt erkend in artikel 10 Gw, artikel 7 Handvest EU, artikel 17 IVBPR en artikel 8 EVRM.

§ 1.4 Centrale vraag, opbouw & methode

De centrale vraag luidt:

Is het onderscheppen van vertrouwelijke communicatie, wanneer gebruik gemaakt wordt van de bevoegdheid tot binnendringen op afstand uit de toekomstige Wet Computercriminaliteit III, verenigbaar met het recht op vertrouwelijke communicatie, zoals dit af te leiden valt uit artikel 8 EVRM?

Om deze vraag te beantwoorden wordt in hoofdstuk twee het recht op vertrouwelijke communicatie uiteengezet. In hoofdstuk drie wordt beschreven waarom de huidige opsporingsbevoegdheden mogelijk niet meer voldoen. In hoofdstuk vier komt encryptie aan bod. Hoofdstuk vijf beschrijft een voorgestelde opsporingsbevoegdheid als oplossing voor opsporingsproblemen met encryptie: het binnendringen op afstand. In hoofdstuk zes wordt getoetst of en hoe binnendringen op afstand verenigbaar kan zijn met het recht op vertrouwelijke communicatie. De uiteindelijke conclusie volgt in hoofdstuk zeven.

De gebruikte methoden voor dit onderzoek zijn een literatuurstudie en jurisprudentieonderzoek. De rechtsspraak van het EHRM betreffende artikel 8 EVRM met betrekking tot '*respect for correspondence'* is onderzocht. Relevante literatuur is gevonden door te zoeken op relevante trefwoorden in: zoekmachines van de bibliotheek van Tilburg University, Kluwer Navigator en Google scholar. Door verwijzingen in de gevonden artikelen, arresten of boeken, is er weer andere literatuur bijgekomen (sneeuwbalmethode). De zoektocht naar literatuur is dus via een gemengde methode tot stand gekomen. Tenslotte zijn relevante wetten, verdragen en parlementaire stukken geraadpleegd.

Hoofdstuk 2: Het recht op vertrouwelijke communicatie

§ 2.1 Inleiding

Het recht op vertrouwelijke communicatie is ontstaan als reactie op overheidsbemoeienis. De burger dient beschermd te worden tegen de machtige staat en moet vertrouwelijk kunnen communiceren met een bepaald publiek.[19] Deze zogenaamde 'staatsvrije sfeer' is de eerste grondslag van het recht. De tweede grondslag is het dienen van het openbare debat. Vrije deelname aan het publieke debat is alleen mogelijk als iedereen zelf de keuze heeft wie er van hun communicatie kennisneemt.[20]

Het recht op vertrouwelijke communicatie is te beschouwen als onderdeel van het ruimere recht op eerbiediging van de persoonlijke levenssfeer. Communicatie via internet en mobiele telefoons krijgt een steeds belangrijkere rol. Daarom is bescherming van deze communicatie volgens Koops van belang.[21] Het recht wordt in artikel 8 EVRM erkend en daarnaast in artikel 10 Gw, artikel 7 Handvest EU en artikel 17 IVBPR. Artikel 8 EVRM is een ieder verbindende bepaling en heeft in Nederland verbindende kracht op basis van artikel 93 Gw.[22] Artikel 94 Gw bepaalt dat nationaal recht opzij gezet dient te worden als er strijd is met een dergelijke bepaling uit een gesloten verdrag. In de praktijk zal de Nederlandse rechter het Nederlandse recht zoveel mogelijk verdragsconform uitleggen.[23] De voorrang die EVRM-bepalingen zo krijgen op nationaal recht, heeft voor een betere bescherming gezorgd.[24] De reikwijdte, beperkingsgronden en mogelijke positieve verplichtingen van artikel 8 EVRM worden in §2.2 besproken. In §2.3 volgt tenslotte een tussenconclusie.

§ 2.2 Artikel 8 EVRM

kader 1

Artikel 8. Recht op eerbiediging van privé-, familie- en gezinsleven

[19] Asscher 2002, p. 11.
[20] Asscher 2002, p. 18.
[21] E.J. Koops, Commentaar op artikel 13 van de Grondwet, in: E.M.H. Hirsch Ballin en G. Leenknegt (red.), Artikelsgewijs commentaar op de Grondwet, webeditie 2016 (www.Nederlandrechtsstaat.nl).
[22] Nieuwenhuis & Hins 2011, p. 61-62.
[23] Nieuwenhuis & Hins 2011, p. 61 & HR 16 november 1990, ECLI:NL:HR:1990:ZC0044.
[24] Steenbruggen 2009, p. 80.

1 Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2 Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

§ 2.2.1 Achtergrond

De doelstelling van artikel 8 EVRM (zie kader 1) is om de burger te beschermen tegen onrechtmatige en willekeurige inmenging van de overheid.[25] Er worden vier grondrechten beschermd, die onderling een sterke samenhang kennen. Ieders privéleven, familie- en gezinsleven, woning en correspondentie moeten gerespecteerd worden. Deze rechten worden in de uitspraken van het EHRM nader uitgewerkt. Het Hof schaart communicatie onder zowel de bescherming van het privéleven als bescherming van correspondentie.[26]

In lid twee van deze bepaling wordt aangegeven onder welke voorwaarden een beperking op dit recht is toegestaan en met welke waarborgen dit omgeven moet zijn. Het EHRM behandelt mogelijke inbreuken op dit artikel door een overheid in twee stappen. Eerst moet vastgesteld worden of de mogelijke inbreuk binnen de reikwijdte van art. 8 EVRM valt. Daarna is de vraag of deze inbreuk te rechtvaardigen is, waarbij aan alle criteria van lid twee voldaan moet zijn.

§ 2.2.2 Reikwijdte

Voor dit onderzoek is van belang om vast te stellen of moderne communicatietechnieken onder de bescherming van artikel 8 EVRM vallen. Vooral gaat het dan om technieken, waarbij vaak sprake is van versleuteling zoals e-mail en WhatsApp. Het recht op bescherming van de vertrouwelijkheid van communicatie wordt gekenmerkt door elementen als ‘respect’, ‘correspondentie’ en ‘privéleven’. Het woord ‘respect’ duidt op een plicht voor de staat om af te

[25] EHRM 16 december 1992, 13710/88 (*Niemietz/Duitsland*), § 31.
[26] EHRM 6 september 1978, 5029/71 (*Klass/Duitsland*), § 41.

zien van acties die inbreuk maken op de vertrouwelijke correspondentie van de burger.[27] Het bereik van de term correspondentie is steeds aan de moderne tijd aangepast en omvat allerlei soorten communicatie.[28] Zo vallen surfgedrag, e-mails en telefoongesprekken vanaf werk onder de bescherming van artikel 8 EVRM.[29] Deze vallen zowel onder de noemer privéleven als correspondentie.[30]

Daar waar ten tijde van de sluiting van het verdrag, de brief een veel voorkomende vorm van correspondentie was, is dat nu natuurlijk anders. De bepalingen uit het EVRM dienen naar de huidige tijd te worden geïnterpreteerd: "*The Court must also recall that the Convention is a living instrument which, as the Commission rightly stressed, must be interpreted in the light of present-day conditions*."[31] Moderne communicatiemiddelen zullen daarom onder de bescherming van artikel 8 EVRM vallen.[32]

Deze stelling vindt steun in de zaak *Klass*.[33] Uit de tekst van artikel 8 EVRM blijkt niet eenduidig of telefoongesprekken onder de reikwijdte vallen. Het Hof oordeelt in *Klass* dat telefoongesprekken onder de bescherming van het privéleven en correspondentie vallen.[34]

In de zaak *Copland* stelt het Hof dat de bescherming van e-mails en persoonlijk internetverkeer logisch volgt uit eerdere uitspraken.[35] Het Hof maakt geen onderscheid tussen email en ander persoonlijk internetverkeer. Het lijkt voor het Hof niet relevant welke internetapplicatie daarbij gebruikt wordt.[36] Versleutelde berichten via internetapplicaties zoals WhatsApp zullen dan ook binnen de reikwijdte van artikel 8 EVRM vallen. Een tekstbericht via een app is immers niet wezenlijk anders dan een bericht van een pieper, alleen het middel verschilt. Datzelfde geldt voor een Skypegesprek en een regulier telefoongesprek. Het Hof kiest ervoor om de verbinding met het privéleven te maken, wanneer er sprake is van nieuwere communicatiemiddelen. Ik zie geen reden waarom van deze lijn zal worden afgeweken.

Eenmaal vastgesteld dat een communicatie binnen de reikwijdte valt, moet nog vastgesteld worden of er een schending heeft plaatsgevonden. Wil het EHRM een klacht hierover in behandeling nemen, dan is hiervoor een direct getroffen klager nodig. Echter, het Hof

[27] Asscher 2002, p. 126.
[28] Asscher 2002, p. 129.
[29] EHRM 3 april 2007, 62617/00 (*Copland/Verenigd Koninkrijk*), § 41.
[30] EHRM 3 april 2007, 62617/00 (*Copland/Verenigd Koninkrijk*), § 41.
[31] EHRM 25 april 1978, 5856/72 (*Tyrer/Verenigd Koninkrijk*), § 31.
[32] Zie ook: Asscher 2002, p. 136-137.
[33] EHRM 6 september 1978, 5029/71 (*Klass/Duitsland*).
[34] EHRM 6 september 1978, 5029/71 (*Klass/Duitsland*), § 41.
[35] EHRM 3 april 2007, 62617/00 (*Copland/Verenigd Koninkrijk*), § 41.
[36] Steenbruggen 2009, p. 85.

heeft al eens een algemene klacht tegen geheime opsporingsmethoden in behandeling genomen.[37] In *Zakharov* accepteerde het Hof diens klacht betreffende het bestaan van maatregelen ter onderschepping van vertrouwelijke communicatie.[38] Bewijs dat hijzelf slachtoffer was geworden van deze maatregel was niet nodig.

§ 2.2.3 Beperkingsgronden

In een democratische samenleving kan het wenselijk zijn dat opsporingsdiensten een inbreuk plegen op het recht op vertrouwelijke communicatie. Onderschepping van communicatie tussen criminelen of terroristen kan van levensbelang zijn. Artikel 8 EVRM lid 2 stelt drie voorwaarden onder welke een dergelijke inbreuk te rechtvaardigen is:

1) de inbreuk moet bij wet voorzien zijn,

2) een legitiem doel dienen en

3) noodzakelijk zijn in een democratische samenleving.

Als aan één van deze drie voorwaarden niet wordt voldaan, is er sprake van een schending.[39]

Bij wet voorzien betekent niet alleen wet in formele zin, ook wetgeving in materiële zin en zelfs ongeschreven recht of een bevel van de burgemeester kunnen deze voorwaarde vervullen.[40] De beperking zal voor de burger toegankelijk en voorzienbaar moeten zijn.[41] De toegankelijkheid heeft vaak met publicatie van wetgeving te maken. Om aan de eis van voorzienbaarheid te voldoen, moet de burger redelijkerwijs kunnen voorspellen, wanneer zijn grondrecht eventueel beperkt gaat worden.[42] Alleen een formele basis in het nationale recht is niet voldoende. In de zaak *Malone* klaagde Malone over zijn afgeluisterde telefoongesprekken door de politie.[43] Het Hof stelde dat de wet ook aan kwaliteitseisen moet voldoen. Nationale wetgeving moet voldoende waarborgen bevatten om willekeur te voorkomen.[44] Dit geldt zeker wanneer een bevoegdheid heimelijk wordt ingezet.[45] Hierdoor kan een burger immers niet voor

[37] Zie bijv.: EHRM 6 september 1978, 5029/71 (*Klass/Duitsland*) en EHRM 18 mei 2010, 26839/0 (*Kennedy/Verenigd Koninkrijk*).
[38] EHRM 4 december 2015, 47143/06 (*Zakharov/Rusland*).
[39] Nieuwenhuis & Hins 2011, p. 122.
[40] Nieuwenhuis & Hins 2011, p. 123, EHRM 26 april 1979 13166/87 (*Sunday Times/Verenigd Koninkrijk*), EHRM 2 juni 2002, 33129/96 (*Olivieira/Nederland*).
[41] EHRM 26 april 1979 13166/87 (*Sunday Times/Verenigd Koninkrijk*).
[42] Nieuwenhuis & Hins 2011, p. 123.
[43] EHRM 2 augustus 1984, 8691/79 (*Malone/Verenigd Koninkrijk*), § 59-61.
[44] EHRM 2 augustus 1984, 8691/79 (*Malone/Verenigd Koninkrijk*), § 67.
[45] EHRM 2 augustus 1984, 8691/79 (*Malone/Verenigd Koninkrijk*), § 67.

zijn recht opkomen, omdat hij er geen weet van heeft. Het minimumniveau van bescherming ontbrak in Engeland volgens het Hof en daarom werd besloten dat de inbreuk in dit geval niet bij wet voorzien was.[46]

In de zaak *Zakharov* zet het Hof de voorwaarden voor een rechtmatige inbreuk op vertrouwelijke communicatie op een rijtje.[47] Dit zijn de minimumvoorwaarden om misbruik van bevoegdheden door de autoriteiten tegen te gaan in geval van onderschepping van communicatie:

a) De nationale wet dient voldoende toegankelijk te zijn en duidelijk. Burgers moeten kunnen inschatten onder welke omstandigheden de overheid hun communicatie mag onderscheppen.

b) Duidelijk moet zijn welke categorieën personen onderwerp kunnen worden van deze opsporingsbevoegdheid. De categorie misdrijven op basis waarvan de bevoegdheid mag worden ingezet moet duidelijk zijn, evenals de duur van de maatregel.

c) De procedures voor het opslaan, onderzoeken, gebruiken en vernietigen van onderschepte data, dienen duidelijk te zijn.

d) De afgeluisterde persoon weet daar zelf meestal niet van, daarom moeten de procedures voor toestemming en beoordeling achteraf zorgen voor voldoende waarborgen.

e) Het proces waarin de toestemming tot stand komt, dient ervoor om te zorgen dat de bevoegdheid alleen wordt ingezet wanneer deze noodzakelijk is in een democratische samenleving. De autoriteit die toestemming verleent, dient onafhankelijk te zijn. Voor toestemming moet er sprake zijn van een redelijke verdenking jegens de betreffende persoon. De maatregel dient proportioneel te zijn ten aanzien van het nagestreefde doel.

f) De toezichthoudende organen moeten transparant en onafhankelijk zijn. Zij dienen voldoende middelen te hebben om effectieve en voortdurende controle uit te oefenen.

g) Zodra dit mogelijk is en het doel van de maatregel niet in gevaar komt, dienen de betrokkenen op de hoogte te worden gesteld van de jegens hen ingezette opsporingsbevoegdheden.

[46] EHRM 2 augustus 1984, 8691/79 (*Malone/Verenigd Koninkrijk*), § 79-80.
[47] EHRM 4 december 2015, 47143/06 (*Zakharov/Rusland)*, zie bijv. ook EHRM 4 december 2012, 41452/07 (Lenev/Bulgarije), EHRM 26 juni 2006, 54934/00 (*Weber en Saravia /Duitsland).*

h) Er moeten mogelijkheden bestaan op nationaal niveau voor individuen om de rechtmatigheid van hun onderschepte communicatie aan te vechten.[48]

Deze recente samenvatting van eerdere uitspraken betreffende de heimelijke onderschepping van communicatie door het Hof is voor mij doorslaggevend in de toets of de waarborgen van de voorgestelde bevoegdheid tot binnendringen voldoende zijn.[49]

Ten tweede moet de beperking *een legitiem doel dienen*. De genoemde doelen in artikel 8 lid 2 EVRM geven de staten veel speelruimte. Openbare veiligheid en het voorkomen van strafbare feiten worden onder andere als legitiem doel genoemd. Daarnaast neemt het EHRM snel genoegen met het gestelde doel. De genoemde doeleinden worden betrekkelijk ruim uitgelegd.[50] Zo begrijpt het Hof dat de politie soms vertrouwelijke communicatie zal moeten onderscheppen ter preventie of opsporing van misdrijven.[51] De mogelijke maatregelen om beter met versleuteling om te kunnen gaan, dienen hetzelfde doel. Ten aanzien van dit vereiste is daarom geen probleem te verwachten.

Ten derde moet de beperking *noodzakelijk* zijn in een *democratische samenleving*. Noodzakelijk ziet het Hof niet zo zwaar als onmisbaar, maar ook niet zo licht als toelaatbaar. Het Hof toetst of de beperking proportioneel is ten opzichte van het belang dat ermee gediend wordt. Er moet volgens het EHRM sprake zijn van een '*pressing social need*': een dwingende maatschappelijke behoefte.[52] Oerlemans stelt dat daar waar het opsporingsbevoegdheden betreft het Hof beoordeelt of er een eerlijke balans bestaat tussen de zwaarte van de inbreuk op iemands levenssfeer aan de ene kant en de noodzakelijkheid om deze opsporingsbevoegdheid in te zetten aan de andere kant.[53] Deze ernst of zwaarte van de inbreuk moet in verhouding staan tot het gediende belang.[54] Criminaliteitsbestrijding en veiligheid kunnen de inzet van een opsporingsbevoegdheid waarbij communicatie wordt onderschept rechtvaardigen. Of de inzet in de praktijk te rechtvaardigen valt, wordt in concreto door het Hof getoetst: de omstandigheden van het geval wegen daarin mee.[55] De duur van de maatregel, de impact van de inmenging in

[48] EHRM 4 december 2015, 47143/06 (*Zakharov/Rusland).*
[49] Voor een algemeen toetsingskader betreffende digitale opsporingsbevoegdheden zie Oerlemans 2017, p. 69-83.
[50] Nieuwenhuis & Hins 2011, p. 125-126.
[51] EHRM 2 augustus 1984, 8691/79 (*Malone/Verenigd Koninkrijk*), § 81.
[52] EHRM 26 april 1979 13166/87 (*Sunday Times/Verenigd Koninkrijk*), EHRM 7 december 1976, 5493/72 (*Handyside/Verenigd Koninkrijk*).
[53] Oerlemans 2017, p. 76.
[54] Nieuwenhuis & Hins 2011, p. 127.
[55] Oerlemans 2017, p. 76 & Nieuwenhuis 2011, p. 129.

de levenssfeer, het feit waar iemand van verdacht wordt en het succes van eerdere pogingen tot het verkrijgen van de benodigde informatie zijn meewegende factoren.[56]

Deze billijke afweging van belangen is niet het enige onderdeel van de noodzakelijkheidstoets. De opsporingsbevoegdheid zal daarnaast ook geschikt moeten zijn om het gestelde doel te bereiken.[57] Een minder ingrijpend alternatief mag hiervoor niet aanwezig zijn (subsidiariteitstoets).[58]

Het Hof geeft verdragsstaten een zekere beoordelingsruimte om vast te stellen of een inbreuk op artikel 8 EVRM noodzakelijk is in een democratische samenleving. Deze beoordelingsruimte is vrij ruim als het doel het beschermen van de nationale veiligheid is.[59] Geheime opsporingsbevoegdheden worden door het Hof echter ook juist als een potentieel gevaar voor diezelfde democratische samenleving gezien.[60] Ook bij de noodzakelijkheidstoets spelen daarom de aanwezige adequate en effectieve waarborgen tegen misbruik een rol.[61] Deze moeten ervoor zorgen dat de inbreuk beperkt wordt tot die gevallen waarin deze noodzakelijk is in een democratische samenleving.[62] Indien deze waarborgen ontbreken, is de betreffende bevoegdheid niet noodzakelijk en wordt artikel 8 EVRM geschonden.

§ 2.2.4 Positieve verplichtingen

Naast de negatieve verplichting voor de overheid om af te zien van inbreuken op het grondrecht van artikel 8 EVRM, kan er mogelijk ook een positieve verplichting ontstaan om juist iets te doen.[63] Het recht op vertrouwelijke communicatie heeft weinig betekenis als burgers niet vertrouwelijk kunnen communiceren.[64] Artikel 8 EVRM kan leiden tot een plicht om individuen te beschermen tegen inbreuken door andere individuen.[65]

De toets van het Hof als het gaat om het vaststellen van een inbreuk is vrij duidelijk. Eerst wordt vastgesteld of er een inbreuk heeft plaatsgevonden en dan wordt gekeken of deze is te rechtvaardigen. Om te bepalen of er uit een verdragsbepaling een positieve verplichting voor de Staat voortvloeit, hanteert het Hof de '*fair balance' test*. Het belang van de samenleving bij

[56] EHRM 2 september 2010, 35623/05 (*Uzun/Duitsland*), § 80.
[57] Nieuwenhuis 2011, p. 129-130.
[58] Oerlemans 2017, p. 77 & Nieuwenhuis 2011, p. 130.
[59] EHRM 26 juni 2006, 54934/00 (*Weber en Saravia /Duitsland),* § 104-106.
[60] EHRM 26 juni 2006, 54934/00 (*Weber en Saravia /Duitsland),* § 104-106.
[61] EHRM 4 december 2015, 47143/06 (*Zakharov/Rusland),* § 232.
[62] EHRM 4 december 2015, 47143/06 (*Zakharov/Rusland),* § 232.
[63] Oerlemans 2017, p. 71.
[64] Gerards 2014, p. 230.
[65] Oerlemans 2017, p. 72.

een actief overheidsoptreden staat hierbij tegenover het belang van de overheid om juist niet te hoeven optreden. De positieve verplichting moet dan leiden tot een redelijk evenwicht tussen deze twee belangen.[66]

Mogelijkheden om vertrouwelijk te communiceren zijn er voldoende; hiervoor hoeft de overheid niets te doen. Toch kunnen er andere positieve verplichtingen ontstaan. In ieder geval heeft de overheid een zorgvuldigheidsplicht. Deze is af te leiden uit de zaak *Craxi II*. Hier was sprake van getapte telefoongesprekken in een corruptieonderzoek. De inhoud van deze gesprekken kwam in handen van de pers en door de publicatie van deze gesprekken werd het recht van oud-premier Craxi geschonden. Ondanks dat de schending (het openbaar maken) door een private partij gebeurde, werd Italië als verdragsstaat verantwoordelijk gehouden. De staat had moeten zorgen dat deze gesprekken niet in de handen van derden zouden komen.[67]

In de zaak *K.U.* heeft het Hof ook een positieve verplichting aangenomen.[68] De lidstaat moet burgers beschermen tegen inbreuken van andere burgers. Goede regelgeving en effectieve opsporing van dit soort inbreuken zijn daarom belangrijk.[69] Mogelijk betekent dit ook dat de overheid haar burgers dient te informeren, wanneer de politie bij uitoefening van haar taak, stuit op kwetsbaarheid van een bepaald communicatiemiddel.[70] Het recht op vertrouwelijke communicatie werkt alleen als de burger erop kan vertrouwen dat zijn communicatie veilig getransporteerd wordt. De overheid dient maatregelen te nemen om te zorgen dat de betreffende dienstverleners geen onrechtmatige inbreuk maken. Daarnaast zal zij waar mogelijk moeten voorkomen dat kwaadwillenden een inbreuk kunnen maken via deze dienstverleners.[71]

§ 2.3 Tussenconclusie

Artikel 8 EVRM beschermt de burger tegen inbreuk op zijn vertrouwelijke communicatie door de overheid. Moderne communicatiemiddelen vallen binnen de reikwijdte van dit artikel. De toekomstige bevoegdheid tot binnendringen op afstand zal aan de vereisten van artikel 8 lid 2 EVRM moeten voldoen. Als er sprake is van een inbreuk op het recht van vertrouwelijke communicatie zal deze inbreuk (1) moeten zijn voorzien bij wet, (2) een legitiem doel moeten dienen en (3) noodzakelijk dienen te zijn in een democratische samenleving. Onderschepping

[66] Gerards 2014, p. 233, voorbeeld van *fair balance test*: EHRM 8 juli 2003 36022/97 (Hatton e.a./Verenigd Koninkrijk), § 118-130.
[67] EHRM 17 oktober 2003, 25337/94 (*Craxi II/Italië*), § 68-76.
[68] EHRM 2 december 2008, 2872/02 (*K.U./Finland*).
[69] Oerlemans 2017, p. 71-72.
[70] Steenbruggen 2009, p. 138.
[71] Steenbruggen 2009, p. 141.

van communicatie gebeurt in het geheim, daarom zijn er strenge vereisten om arbitraire inmenging door de overheid te voorkomen. In de zaak *Zakharov* zijn acht voorwaarden te vinden, deze voorwaarden worden gebruikt om de voorgestelde opsporingsbevoegdheid later aan artikel 8 EVRM te toetsen.[72] Op basis van het EVRM kunnen ook positieve verplichtingen ontstaan voor de lidstaat. Deze bestaan uit een bepaalde plicht om het recht op vertrouwelijke communicatie te beschermen jegens andere burgers en de zorgvuldigheidsplicht als een opsporingsdienst inbreuk op dit recht maakt jegens een van haar burgers.

[72] EHRM 4 december 2015, 47143/06 (*Zakharov/Rusland*), § 227-301.

Hoofdstuk 3: Huidige onderscheppingsbevoegdheden in relatie tot versleutelde communicatie

§ 3.1 Inleiding

De wetgever acht uitbreiding van opsporingsbevoegdheden nodig. Toenemend gebruik van encryptie is daarvan de belangrijkste oorzaak.[73] In dit hoofdstuk wordt besproken waarom het huidige stelsel bevoegdheden niet meer lijkt te voldoen. In § 3.2 worden de algemene opsporingsbevoegdheden en de problemen daarmee besproken. In § 3.3 worden de specifieke bevoegdheden en de problemen daarmee uiteengezet. In § 3.4 volgt tenslotte een tussenconclusie.

§ 3.2 Algemene opsporingsbevoegdheden

De artikelen 141,142 Sv en artikel 3 Politiewet (2012) geven de politie een taakopdracht waaruit bevoegdheden kunnen worden afgeleid. Deze bevoegdheden mogen alleen ingezet worden op een wijze die een beperkte inbreuk maakt op grondrechten van burgers.[74] Onderschepping van communicatie is te kwalificeren als een zware inbreuk.[75] De algemene taakopdracht kan daarom geen grondslag zijn voor onderschepping van vertrouwelijke communicatie.

Minder algemeen en mogelijk van toepassing zijn de bevoegdheden van artikelen 94 en 95 Sv. Het betreft hier de bevoegdheid tot inbeslagname van voorwerpen ten behoeve van waarheidsvinding of het afnemen van wederrechtelijk verkregen voordeel. Een agent kan bij een aanhouding een mobiele telefoon in beslag nemen en zo mogelijk vertrouwelijke communicatie onderscheppen. Gegevens zijn echter geen voorwerpen die in beslag kunnen worden genomen.[76] Ook bij inzet van de bevoegdheid van artikel 94 en 95 Sv ontbreekt een rechterlijke toets en een specifieke gerichtheid. De Hoge Raad is het hier mee eens en vindt waarheidsvinding wel een heel breed criterium en stelt dat deze bevoegdheid zeker niet kan strekken tot een uitgebreid onderzoek aan een mobiele telefoon.[77] Algemene bevoegdheden zijn vanwege het ontbreken van waarborgen ongeschikt voor onderschepping van communicatie.[78]

[73] WODC 2012, p. 32-33.
[74] HR 1 juli 2014, ECLI:NL:HR:2014:1563, § 2.4.
[75] Oerlemans 2017, p. 79-80.
[76] *Kamerstukken II* 1989/90, 21551, 3.
[77] HR 25 oktober 2016, ECLI:NL:PHR:2016:1049, § 78-82 & HR 25 oktober 2016, ECLI:NL:PHR:2016:1048.
[78] Zie ook: *Kamerstukken II* 2015/16, 29 279, 278, p. 63-64 & Koops 2017.

§ 3.3 De specifieke bevoegdheden

Voor onderschepping van communicatie heeft de politie twee specifieke bevoegdheden: de bevoegdheid om vertrouwelijke communicatie op te nemen (art. 126l Sv) en de bevoegdheid om te tappen (art. 126m Sv). De tap via een communicatiedienst is de meest specifieke en eerst zal gekeken moeten worden of via deze weg het opsporingsdoel behaald kan worden.[79] Personen waarvan redelijkerwijs verwacht kan worden, dat zij over kennis beschikken om opgenomen gegevens te ontsleutelen, kunnen worden verplicht aan ontsleuteling mee te werken.[80] Deze plicht geldt niet voor de verdachte en betreft uitsluitend zelf aangebrachte versleuteling.[81] Er ontstaat geen verplichting om technische mogelijkheden te creëren om te kunnen ontsleutelen. Wanneer iemand niet feitelijk in staat is om mee te werken aan ontsleuteling, is hij ontslagen van deze verplichting.[82] WhatsApp bijvoorbeeld kan op basis van deze artikelen niet worden gedwongen tot medewerking. Bij end-to-end encryptie, zoals WhatsApp gebruikt, heeft de aanbieder zelf geen toegang tot de onversleutelde inhoud van gesprekken.[83] Dit is een probleem voor opsporingsdiensten omdat zo de inhoud van communicatie niet meer te onderscheppen is. De tapbevoegdheid is daarom in de praktijk steeds minder effectief. Een andere ontwikkeling die de effectiviteit in de weg staat zijn de verschillende wifispots die worden gebruikt. Een tap met behulp van de internetserviceprovider wordt ook moeilijker.[84] De reguliere tap zal in de toekomst door deze ontwikkelingen verder in effectiviteit afnemen.

Het tweede en zwaardere middel dat opsporingsdiensten kunnen inzetten is de bevoegdheid tot het opnemen van communicatie met een technisch hulpmiddel.[85] Dit kan bijvoorbeeld een geplaatste bug zijn, die toetsaanslagen registreert op een laptop.[86] Deze bevoegdheid maakt het in sommige gevallen wel mogelijk om de encryptie te omzeilen. Een e-mail kan uitgelezen worden, voordat deze versleuteld wordt verstuurd. Doordat er een apparaatje geplaatst moet worden, is deze bevoegdheid risicovoller dan de reguliere tapbevoegheid.[87] Het risico bestaat dat de bug ontdekt wordt of de opsporingsambtenaar betrapt wordt bij het plaatsen ervan. Wanneer het computercriminaliteit zoals hacken betreft, is het heel moeilijk om te bepalen op welke locatie een bug geplaatst zou moeten worden. Er worden vaak

[79] T & C Sv, Blom, artikel 126m Sv, actueel tot 1 juli 2015.
[80] Artikel 126m Sv lid 6.
[81] Artikel 126m Sv lid 7.
[82] T & C Sv, Blom, artikel 126m, § 15, actueel tot 1 juli 2015.
[83] Zie kader 4 en hoofdstuk 4.
[84] WODC 2012, p. 18.
[85] Artikel 126l Sv.
[86] *Kamerstukken II* 1996/97, 25403, 3, p. 36 (MvT), artikel 126s geeft dezelfde bevoegdheid m.b.t. de georganiseerde misdaad en artikel 126zf Sv regelt deze bevoegdheid wanneer er sprake is van aanwijzingen voor een terroristisch misdrijf.
[87] *Kamerstukken II* 1996/97, 25403, 3, p. 36 (MvT).

verschillende toegangspunten tot het internet gebruikt, waardoor het moeilijker wordt om een IP-adres te traceren naar een specifieke locatie.[88] Ook zijn er verschillende manieren om anoniem te acteren op internet, zoals proxyservers, VPN-netwerken en het Tor-netwerk.[89] Deze anonimiteit is een probleem voor de inzet van de bevoegdheid van artikel 126l Sv.

Voor deze twee bevoegdheden gelden wel de nodige waarborgen. De bevoegdheid is toegekend aan de officier van justitie. Voorafgaande machtiging van de rechter-commissaris is vereist.[90] Er moet sprake zijn van een misdrijf waarvoor voorlopige hechtenis mogelijk is en het begane misdrijf dient een ernstige inbreuk op de rechtsorde te zijn.[91] Er dient sprake te zijn van een geconcretiseerde verdenking en de waarheidsvinding staat voorop.[92] Er is een maximumtermijn van vier weken, welke telkens met maximaal vier weken kan worden verlengd.[93] De inhoud van opgenomen communicatie is verifieerbaar, doordat deze opgenomen moet worden.[94]

§ 3.4 Tussenconclusie

Algemene taakopdrachten en opsporingsbevoegdheden kunnen niet worden ingezet om versleutelde communicatie te onderscheppen. Hiervoor ontbreken de juiste waarborgen en dit zou strijd met het EVRM opleveren. Deze waarborgen zijn er wel bij de specifieke bevoegdheden uit artikel 126l Sv (opnemen van communicatie met een technisch hulpmiddel) en 126m Sv (tappen). De reguliere tap echter is steeds minder effectief door encryptie. Het plaatsen van een technisch hulpmiddel om de communicatie op te nemen kan dit probleem mogelijk oplossen. Deze kent echter het risico van betrapping of ontdekking. Daarnaast is er het probleem om identiteit en locatie van de verdachte te kunnen achterhalen om überhaupt een technisch hulpmiddel te kunnen plaatsen. Onderzoek naar uitbreiding van opsporingsbevoegdheden lijkt gezien deze omstandigheden gerechtvaardigd.

[88] Oerlemans 2017, p. 37-38 & *Kamerstukken II* 2015/16 34372, 3, p. 11 (MvT).
[89] Voor een uitgebreide beschrijving zie Oerlemans 2017, p. 38-42.
[90] Artikel 126l Sv lid 4, voor beoordeling van een dergelijke machtiging, zie HR 11 oktober 2005, ECLI:NL:HR:2005:AT4351, overweging 3.5.2.
[91] Artikel 67 Sv lid 1.
[92] *Kamerstukken II 1996/97, 25403, 3, p. 38 (MvT).*
[93] Artikel 126l Sv lid 5.
[94] Zie bijv. Hof Amsterdam 23 december 2009, ECLI:NL:GHAMS:2009:BK7941, waarin niet opgenomen communicatie leidde tot bewijsuitsluiting.

Hoofdstuk 4: Encryptie

§ 4.1 Inleiding

Encryptie betreft het proces waarbij tekst of spraak wordt omgezet naar onleesbare of onverstaanbare varianten met behulp van een wiskundig algoritme.[95] Leesbare tekst verandert zo in een reeks onsamenhangende tekens. Deze samenhang is alleen te ontdekken met de sleutel van de betreffende encryptie. Onderschepping van communicatie zonder bezit van deze sleutel is niet effectief. De daadwerkelijke inhoud is dan niet meer vast te stellen voor opsporingsdiensten.[96]

Encryptie is in toenemende mate te verkrijgen en wordt steeds vaker onderdeel van het normale dataverkeer.[97] In veel producten zoals WhatsApp (zie kader 4) is deze encryptietechnologie standaard geïntegreerd. De dienstverlener heeft zelf geen toegang tot de inhoud van de communicatie.[98] Een tapverzoek is daarom niet effectief.[99] De politie ervaart dit als nadeel van sterke encryptie. De digitale veiligheid de samenleving in zijn geheel is een reden om juist sterke encryptie te bevorderen. In § 4.2 bespreek ik het kabinetsstandpunt waarin deze voor- en nadelen van sterke encryptie besproken worden. Het hoofdstuk wordt afgesloten met een tussenconclusie (§ 4.3).

kader 4

Voorbeeld end-to-end werking van WhatsApp

Stel, Alice wil een WhatsApp naar Bob sturen. De app wordt dan eerst versleuteld op de telefoon van Alice middels de publieke sleutel van Bob. Dit versleutelde bericht wordt vervolgens verstuurd naar de centrale server van WhatsApp en van daaruit doorgestuurd naar Bob zijn telefoon. Daar wordt de app uiteindelijk weer ontsleuteld, met de geheime sleutel die alleen Bob (WhatsApp dus niet!) heeft. De server van WhatsApp bevat dan ook geen leesbare berichten,

[95] Voor het doel van dit onderzoek is de exacte beschrijving en werking van encryptie niet noodzakelijk en wordt daarom niet tot in detail beschreven. Voor een technische beschrijving zie Schneier 2007.
[96] Oerlemans 2017, p. 44-45.
[97] *Kamerstukken II* 2015/16, 26643, p. 1.
[98] Zie: Ellen Nakashima, 'WhatsApp, the messaging service, announces full encryption on all platforms', *Washington Post* 5 april 2016, washingtonpost.com (zoek op: WhatsApp, full encryption).
[99] Voor technische gedetailleerde omschrijvingen, zie Schneier 2007.

deze zijn versleuteld. Bij end-to-end-encryptie is een app vanaf het moment van verzenden vanaf Alice haar telefoon tot de ontvangst op Bob zijn telefoon versleuteld.

§ 4.2 Kabinetsstandpunt over encryptie

Op 4 januari 2016 stelde het kabinet een standpunt op aangaande encryptie.[100] Encryptie is belangrijk voor het vertrouwen van de burger in de moderne Nederlandse economie. Encryptie geeft echter ook kwaadwillenden de mogelijkheid om heimelijk met elkaar te communiceren, zonder dat opsporingsdiensten deze communicatie leesbaar kunnen onderscheppen.[101] De aanslagen in Parijs, waarbij de daders mogelijkerwijs gebruik maakten van encryptie waren aanleiding voor het schrijven van het kabinetsstandpunt.[102]

Encryptie is essentieel voor de beveiliging van het digitale domein. Zonder encryptie is het nagenoeg onmogelijk om wachtwoorden, back-ups en andere gegevens veilig te houden in geval van een hack of diefstal. De overheid wil in de toekomst meer digitaal kunnen regelen met haar burgers. Afscherming van deze vertrouwelijke gegevens is zonder gebruik van encryptie vrijwel onmogelijk. Ook voor communicatie binnen de overheid, zoals bij diplomatieke aangelegenheden is deze bescherming belangrijk. Voor bedrijven geldt dat bedrijfsgegevens en communicatie vertrouwelijk moeten kunnen blijven. Ook burgers moeten vertrouwelijk kunnen communiceren.[103] Een journalist moet zijn bron kunnen beschermen. Veel stakeholders zijn gebaat bij een goede encryptie.[104]

Tegelijkertijd onderkent de regering de problemen voor opsporingsdiensten. In belang van de nationale veiligheid en het opsporen van strafbare feiten is het soms nodig dat zij toegang hebben tot communicatie. Kwaadwillenden gebruiken daarom vaak encryptie. Hiervoor is weinig technische kennis nodig en encryptie is vaak al geïntegreerd in de gebruikte apps. Dat maakt het moeilijker om op tijd inzicht te verkrijgen in de communicatie van criminelen. Ook de bewijsvoering die nodig is voor een veroordeling kan daarmee moeilijker worden.[105]

[100] *Kamerstukken II* 2015/16, 26643.
[101] *Kamerstukken II* 2015/16, 26643, p. 1.
[102] Waarschijnlijk gebruikte deze terroristencel juist helemaal geen encryptie, zie: B. Schneier, 'Paris terrorists used Double ROT-13 Encryption', *blog* 15 november 2015, raadplegen via: <https://www.schneier.com/blog/archives/2015/11/paris_terrorist.html>.
[103] Asscher 2002, p. 11.
[104] *Kamerstukken II* 2015/16, 26643, p. 2.
[105] *Kamerstukken II* 2015/16, 26643, p. 3.

Een rechtmatige onderschepping van communicatie maakt inbreuk op het grondrecht van vertrouwelijke communicatie. Deze onderschepping moet daarom een legitiem doel dienen, bij wet voorzien zijn en noodzakelijk zijn in een democratische samenleving. Binnen dit kader zullen de belangen voor wat betreft encryptie moeten worden afgewogen.[106]

De versleuteling blijkt vaak niet te kraken en het vorderen van de sleutel bij de betreffende dienstverlener is nauwelijks effectief, omdat deze de sleutel vaak niet heeft.[107] Het belang van de nationale veiligheid en opsporing van strafbare feiten nopen tot de zoektocht naar oplossingen. Echter er is geen oplossing mogelijk (op dit moment), zonder dat daarmee afbreuk wordt gedaan aan de algemene veiligheid van digitale systemen. Oplossingen waarbij encryptie verzwakt wordt of waarbij een achterdeurtje wordt ingebouwd, maakt systemen kwetsbaar voor kwaadwillenden. Dit acht de regering onwenselijk. In de huidige proportionaliteitsafweging wordt voorrang gegeven aan de digitale veiligheid van iedereen. Sterke encryptie is immers van belang voor een veilig internet, voor het recht op vertrouwelijke communicatie en voor de Nederlandse economie. Daarom zijn er op dit moment geen wettelijke maatregelen wenselijk, die tornen aan de ontwikkeling van, het gebruik van en de beschikbaarheid van sterke encryptie in Nederland.[108]

§ 4.3 Tussenconclusie

Sterke encryptie is nodig in onze democratische samenleving. Het verbieden van encryptie zou het internet onveiliger maken voor burgers, bedrijven en overheid. Dit maatschappelijk belang wordt groter geacht dan het belang voor de opsporingsdiensten. Dit zorgt ervoor dat het voor opsporingsdiensten moeilijk is om communicatie te onderscheppen. De voorgestelde bevoegdheid tot binnendringen op afstand beoogt dit nadeel voor opsporingsdiensten te verkleinen, daarover meer in hoofdstuk vijf.

[106] *Kamerstukken II* 2015/16, 26643, p. 3-4, zie voor een uitgebreide beschrijving van artikel 8 EVRM hoofdstuk 2 van dit onderzoek.
[107] Zie voorbeeld kader 4.
[108] *Kamerstukken II* 2015/16, 26643, p. 4-5.

Hoofdstuk 5: Binnendringen op afstand

§ 5.1 Inleiding

Onderschepping van communicatie in het kader van een strafrechtelijk onderzoek levert problemen op omdat deze communicatie vaak versleuteld is. Onderschepte communicatie wordt daardoor niet meer lees- of verstaanbaar. De samenleving hecht waarde aan opsporing van criminaliteit. Om die taak te kunnen uitvoeren is het wenselijk dat opsporingsdiensten toegang tot de inhoud van de communicatie tussen criminelen kunnen krijgen. Een oplossing voor deze problemen met encryptie is gewenst. Het wetsvoorstel CC-III voorziet in een opsporingsbevoegdheid die mogelijkerwijs soelaas biedt. Het betreft de bevoegdheid om op afstand een geautomatiseerd werk binnen te dringen.[109]

Met deze bevoegdheid wordt het mogelijk om bijvoorbeeld de mobiele telefoon van een verdachte binnen te dringen. Communicatie kan vervolgens worden uitgelezen in onversleutelde vorm. Bij de zender kan dit voordat versleuteling heeft plaatsgevonden. Bij de ontvanger kan men het bericht lezen als het ontsleutelingsproces is voltooid. Het verschil met de bestaande bevoegdheid is dat er eerst binnengedrongen moet worden in een geautomatiseerd werk, daarvoor is een bevel van de rechter nodig.[110] Vervolgens wordt er onderzoek verricht in dat geautomatiseerde werk. Wanneer dat het heimelijk aftappen of opnemen van communicatie betreft, dan is hiervoor nog een tweede rechterlijk bevel nodig op grond van artikelen 126l, 126m, 126s, 126t of 126zg Sv voor de onderschepping van deze communicatie.[111] In dit geval wordt het binnengedrongen geautomatiseerde werk gebruikt om de bevoegdheid van het aftappen van de communicatie te faciliteren. Een tweede manier van onderschepping van communicatie is het vastleggen van gegevens. Wanneer de communicatie op het geautomatiseerde werk is opgeslagen, denk bijvoorbeeld aan e-mails, dan kan deze worden gekopieerd of overgenomen.[112]

Het wetsvoorstel waarvan deze toekomstige opsporingsbevoegdheid deel uitmaakt, ligt nu ter goedkeuring bij de Eerste Kamer.[113] In § 5.2 wordt de toekomstige wet beschreven en in § 5.3 vat ik de voornaamste discussies samen. In § 5.4 bespreek ik enkele alternatieven. In § 5.5 wordt afgesloten met een tussenconclusie.

[109] Toekomstig artikel 126nba Sv, zie *Kamerstukken II* 2016-17 34372, A.
[110] Zie: artikelen 126nba, 126uba en 126zba van het wetsvoorstel CC-III.
[111] *Kamerstukken II* 2015/16, 34372, 3, p. 23 (MvT).
[112] *Kamerstukken II* 2015/16, 34372, 3, p. 23 (MvT).
[113] *Kamerstukken I* 2016/17, 34372, A.

§ 5.2 Binnendringen op afstand (de toekomstige bepaling)

Teneinde (cyber)criminaliteit en terrorisme effectief te kunnen bestrijden is uitbreiding van de strafvorderlijke bevoegdheden nodig, zo wordt gesteld door de wetgever.[114] Deze bevoegdheden zullen moeten aansluiten bij de snelle ontwikkelingen in de technologie. Het wetsvoorstel CC-III is reeds plenair behandeld en aangenomen in de Tweede Kamer.[115] Op het moment van schrijven van dit onderzoek is het voorstel in behandeling bij de Eerste Kamer.[116] Onderdeel van dit wetsvoorstel is de bevoegdheid tot binnendringen op afstand (artikel 126nba Sv, zie kader 5). Wanneer het georganiseerde misdaad betreft is toekomstig artikel 126uba Sv van toepassing en bij terroristische misdrijven toekomstig artikel 126zpa Sv.

kader 5

Voorgesteld artikel 126nba lid 1 Sv

1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat bij de verdachte in gebruik is en, al dan niet met een technisch hulpmiddel, onderzoek doet met het oog op:

a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;

b. de uitvoering van een bevel als bedoeld in de artikelen 126l of 126m;

c. de uitvoering van een bevel als bedoeld in artikel 126g, waarbij de officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel op een persoon wordt bevestigd; en, ingeval van een misdrijf, waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen;

[114] *Kamerstukken II* 2015/16, 34372, 3, p. 6-7 (MvT).
[115] *Kamerstukken I* 2016/17, 34472, p. 4-5.
[116] Voorlopig verslag: *Kamerstukken I* 2016/17, 34472, B. Laatst gezocht naar officiële stukken op 14 mei 2017.

d. de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen, of die eerst na het tijdstip van afgifte van het bevel worden opgeslagen, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;

e. de ontoegankelijkmaking van gegevens, bedoeld in artikel 126cc, vijfde lid. Artikel 11.7a van de Telecommunicatiewet is niet van toepassing op handelingen ter uitvoering van een bevel als bedoeld in de eerste volzin.

Ter verduidelijking van dit voorgenomen artikel wil ik een aantal termen nader toelichten:

- Voor de term *binnendringen* is aansluiting gezocht bij artikel 138ab Sr. Er dient een beveiliging van een geautomatiseerd systeem te zijn doorbroken.[117]
- Een *geautomatiseerd werk* is een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen.
- Onder een *technisch hulpmiddel* wordt verstaan: 'een softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel.'[118]
- Wanneer er sprake is van een *ernstige inbreuk in de rechtsorde* hangt af van de ernst van de feiten en de omstandigheden van het geval, dus niet alleen van de delictsomschrijving. Moord, handel in drugs, terrorisme zijn vrij duidelijke voorbeelden, maar ook kunnen veel minder zware delicten hieronder vallen, zoals bijvoorbeeld omkoping van een ambtenaar.[119]

Het binnendringen op afstand zelf is slechts een voorbereidende handeling. Hiermee kunnen mogelijk versleutelde gegevens alsnog toegankelijk worden voor opsporingsdiensten. Eenmaal binnen in het geautomatiseerde werk, volgt de onderzoeksfase. Opsporingshandelingen zullen worden verricht met het oog op bepaalde onderzoeksdoelen. Aftappen en opnemen van communicatie wordt specifiek genoemd als onderzoeksdoel.[120]

[117] Kamerstukken *II* 1989/90, 21551, 3, p. 15-16.
[118] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', art. 1 lid g, raad te plegen via: <www.rijksoverheid.nl/documenten/rapporten/2017/05/10/tk-bijlage-besluit-onderzoek-in-een-geautomatiseerd-werk>, verschenen op 10 mei 2017.
[119] Hoge Raad 30 september 2014, ECLI:NL:PHR:2014:2162, r.o. 7-10.
[120] *Kamerstukken II* 2016/17, 34372, 26, p. 8-9.

In het wetsvoorstel CC-III staan een aantal grondslagen om krachtens algemene maatregel van bestuur nadere regels te stellen. Op moment van schrijven is er een consultatieversie van deze AMvB beschikbaar. Deze kan mogelijk nog worden aangepast.[121] Toch heb ik gemeend om bij gebrek aan een definitieve AMvB deze consultatieversie te gebruiken voor verduidelijking.

In dit conceptbesluit wordt de categorie misdrijven uitgebreid op basis waarvan de bevoegdheid mag worden ingezet, wanneer er sprake is van vastlegging van gegevens. Verdenking van misdrijven behorend bij computercriminaliteit in enge zin (misdrijven die niet zonder gebruik of tussenkomst van een computer of netwerk kunnen worden gepleegd) worden toegevoegd. Voorbeelden hiervan zijn: computervredebreuk (artikel 138ab Sr) en ernstige 'spam', waardoor de toegang tot een geautomatiseerd werk geblokkeerd wordt (artikel 138b Sr). Ook andere ernstige misdrijven gepleegd met behulp van een geautomatiseerd werk (gedigitaliseerde criminaliteit) worden toegevoegd.[122] Voorbeelden hiervan zijn: witwassen (artikel 420bis Sr) en mensensmokkel (artikel 197a Sr).[123] Als reden voor deze uitbreiding wordt aangegeven dat er vaak geen ander aanknopingspunt is dan het betreffende geautomatiseerde werk. Tevens wordt er een duidelijk maatschappelijk belang gediend met de opsporing, vervolging en bestraffing van deze strafbare feiten. Hiermee kan er flexibel worden ingespeeld op toekomstige technologische ontwikkelingen in de cybercriminaliteit.[124]

Daarnaast worden er regels gesteld om de deskundigheid van opsporingsambtenaren te waarborgen. Het onderzoek is voorbehouden aan opsporingsambtenaren die beschikken over specifieke kennis en vaardigheden op terrein van ICT.[125]

In het conceptbesluit wordt uitgelegd hoe de inzet van deze bevoegdheid in de toekomst in zijn werk zal gaan en welke waarborgen er zijn. Er wordt onderscheid gemaakt tussen een tactisch team en een technisch team. Het tactische team dat bezig is met een onderzoek stelt een projectvoorstel op.[126] De verdachte wordt hierin beschreven, evenals de verdenking, de noodzaak van inzetten van de specifieke bevoegdheid en de verwachting van wat dit onderzoek gaat opleveren. De betreffende officier van justitie wint vervolgens advies in bij het technisch team over de haalbaarheid van dit specifieke onderzoek. Dit advies is van groot belang voor de

[121] *Kamerstukken II* 2016/17, 34372, 26.
[122] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', p. 16-17.
[123] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', p. 16-17.
[124] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', p. 16-17.
[125] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', p. 8-9.
[126] Het tactische team verzamelt informatie over strafbare feiten en verdachte personen. Bron: www.politie.nl/themas/recherche.html.

inschatting, beheersing en beperking van de risico's. De gedachte hierachter is dat door de scheiding van het tactische en technische team de kans dat het technische team wordt beïnvloed bij de afwegingen over haalbaarheid en risico's kleiner wordt. Het technisch team stelt vervolgens een adviesrapport op, waarbij wordt aangegeven welk technisch hulpmiddel gebruikt gaat worden. De officier van justitie gebruikt dit rapport om toestemming te verkrijgen voor het inzetten van de bevoegdheid bij de rechter-commissaris. Zodra het bevel volgt van de officier van justitie kan er begonnen worden met het binnendringen op afstand.[127]

Nadat een plan van aanpak is opgesteld en een proefopstelling is getest, begint het technische team met het daadwerkelijke onderzoek. De tijdens dit onderzoek vastgelegde gegevens worden vastgelegd op een technische infrastructuur van het technische team. Deze infrastructuur moet goed beveiligd zijn tegen wijziging van gegevens en toegang door onbevoegden. In theorie hebben de tactische opsporingsambtenaren geen toegang tot deze gegevens. Alleen de resultaten van het onderzoek voor zover deze vallen binnen het bevel van de officier, horen bij het tactische team terecht te komen. Bij het opnemen van vertrouwelijke communicatie, is de kans aanwezig dat gegevens worden verkregen over andere personen dan de verdachte. Deze gegevens zijn niet van belang voor het opsporingsonderzoek. In een dergelijk geval wordt alleen de communicatie waarvan email-adressen en/of telefoonnummers op de voorafgaande lijst staan aan het tactische team doorgegeven.[128]

Van groot belang is het dat er een gedegen verslaglegging plaatsvindt van de verrichte handelingen tijdens het onderzoek. Dit wordt logging genoemd. Zo kan worden vastgesteld of een bepaalde handeling of bewerking die heeft plaatsgevonden van invloed is geweest op de betrouwbaarheid en integriteit van het onderzoek. Deze logging is vooral bedoeld voor interne controle, bij onregelmatigheden wordt de officier middels een proces-verbaal op de hoogte gebracht en kan hij samen met de rechter oordelen over de bewijskracht van de vastgelegde gegevens.[129]

§ 5.3 Discussie

In de fase voorafgaand aan de goedkeuring in de Tweede Kamer zijn er een enkele stakeholders geraadpleegd. Zo onderkent de Raad van State de noodzaak om bevoegdheden

[127] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', p. 9.
[128] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', p. 10.
[129] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', p. 10.

uit te breiden in moderne technologische tijden.[130] De Raad stelt dat de bevoegdheid voor verschillende doeleinden kan worden aangewend, maar dat er tegelijkertijd niet gedifferentieerd wordt naar de mate van inbreuk op de persoonlijke levenssfeer. Het binnendringen met als doel een identiteit vast te stellen is een kleinere inbreuk, dan wanneer het doel is om via een webcam mee te kijken.[131]

De Nederlandse Orde van Advocaten (NOvA), privacy organisatie Bits of Freedom (BOF) en de Autoriteit persoonsgegevens (AP) hebben zich kritisch uitgelaten over de mogelijk nieuwe bevoegdheid.[132] De NOvA keurt de bevoegdheid af, omdat deze een te grote inbreuk op grondrechten van burgers maakt en de noodzaak ervan in haar ogen onvoldoende is aangetoond.[133] BOF is nog veel kritischer. Zij stelt dat het een grenzeloze bevoegdheid betreft, dat deze in strijd is met fundamentele grondrechten en met internationaal recht. Ook zullen extra cyberrisico's ontstaan omdat er gebruik gemaakt gaat worden van zwakheden.[134] Deze zwakheden kunnen ook door kwaadwillenden worden uitgebuit. Het lijkt erop dat de politie een belang kan krijgen bij zwakheden in onze nationale cyberveiligheid, dit acht BOF zeer onwenselijk. Daarnaast wijst BOF nog op problemen die in Duitsland zijn ontstaan, waarbij de software die de Duitse overheid gebruikte om binnen te dringen vrij gemakkelijk te hacken bleek, waardoor informatie in verkeerde handen kon vallen.[135] De AP stelt vragen bij de eisen van proportionaliteit en subsidiariteit. Grote groepen burgers (die vaak niet eens verdachte zijn) kunnen door de inzet van deze bevoegdheid worden geraakt, daarom acht de AP een betere onderbouwing noodzakelijk.[136]

Voor deze onderbouwing en noodzaak wijst de minister op verschillende rapporten waarin de omvang van cybercrime wordt geschetst.[137] Drie knelpunten hinderen de effectiviteit van de opsporing en maken de nieuwe bevoegdheid noodzakelijk: versleuteling, het gebruik van verschillende toegangspunten voor het internet en de opslag van informatie in de cloud.[138] De problemen met versleuteling zijn reeds in hoofdstuk vier besproken. Doordat draadloze verbindingen overal beschikbaar zijn en burgers gebruik maken van veel verschillende Wi-Fi-netwerken en/of hotspots ontstaat er een probleem met een eventuele tap. Deze zou geplaatst

[130] *Kamerstukken II* 2015/16, 34372, 4.
[131] Aink 2016, p. 44.
[132] De Autoriteit persoonsgegevens stond voor 1-1-2016 bekend als het College bescherming persoonsgegevens.
[133] *Kamerstukken II* 2015/16, 34372, 3, bijlage Advies NOvA.
[134] *Kamerstukken II* 2015/16, 34372, 3, bijlage Advies Bits of Freedom.
[135] *Kamerstukken II* 2015/16, 34372, 3, bijlage Advies Bits of Freedom.
[136] *Kamerstukken II* 2015/16, 34372, 3, bijlage Advies CBP.
[137] *Kamerstukken I* 2016/17, 34372, D, p. 1.
[138] *Kamerstukken I* 2016/17, 34372, D, p. 3-4.

moeten worden op alle netwerk- en dienstenaanbieders waarvan gebruik wordt gemaakt. Dit blijkt in de praktijk onmogelijk.[139]Het probleem van opslag in de cloud is dat de gegevens zich niet op een vaste plaats bevinden, waardoor de netwerkzoeking (artikel 125j lid 1 Sv) niet meer effectief is. Cloudcomputingdiensten als Hotmail, Dropbox slaan de gegevens op verschillende servers op, zonder dat de gebruiker van de dienst daar invloed op heeft. Hierdoor bevinden de gegevens zich vaak in meerdere landen tegelijk, waardoor er ook jurisdictieproblemen ontstaan.[140] De nieuwe bevoegdheid moet de situatie rond deze knelpunten verbeteren. De regering acht verder de waarborgen ruimschoots voldoende om aan de vereisten uit het EVRM te voldoen.[141]

Op 11 februari 2016 zijn er rondetafelgesprekken geweest over de nieuwe bevoegdheid, waarbij verschillende partijen hun standpunten konden toelichten. Zo acht de politie deze nieuwe bevoegdheid nodig om de effectiviteit en slagkracht op peil te houden in moderne technologische tijden. Ook vindt de politie dat de bevoegdheid met voldoende waarborgen is omkleed en wordt gesteld dat burgers geen angst hoeven te hebben voor grootschalige inzet van de bevoegdheid.[142]

De Raad voor de rechtspraak geeft in haar positiebepaling twee bezwaren. Als eerste meent zij dat er betere toetsing achteraf moet komen, dus nadat de bevoegdheid is ingezet. De regering stelt dat de bestaande regeling voor inzet van bijzondere opsporingsbevoegdheden, aangevuld met de extra waarborgen uit CC-III voldoet om een rechtmatige toepassing te waarborgen.[143] Het tweede bezwaar betreft het binnendringen van een geautomatiseerd werk gelokaliseerd buiten de Nederlandse grenzen.[144] Hier bestaat nog geen internationaalrechtelijke basis voor.[145] De Nederlandse wet staat opsporen buiten Nederland toe op grond van artikel 539a Sv, zo stelt de regering.[146] Tegelijkertijd wordt wel onderkend dat er behoefte bestaat aan internationale afspraken over het verzamelen van bewijs.[147]

Fox-It, een bedrijf dat zich bezighoudt met netwerk- en computerbeveiliging, toont zich een groot voorstander van de nieuwe bevoegdheid tijdens deze gesprekken. Het moet wel als een laatste redmiddel moet worden gebruikt, maar het ‘terughacken’ is het ideale middel om

[139] *Kamerstukken II* 2015/16, 34372, 3, p. 10-11 (MvT).
[140] *Kamerstukken II* 2015/16, 34372, 3, p. 11-12 (MvT).
[141] *Kamerstukken I* 2016/17, 34372, D, p. 5-6.
[142] Rondetafelgesprek Wetsvoorstel computercriminaliteit III, positie politie.
[143] *Kamerstukken I* 2016/17, 34372, D, p. 30-31.
[144] Rondetafelgesprek Wetsvoorstel computercriminaliteit III, positie Raad voor de rechtspraak.
[145] Zie Koops & Goodwin 2014 en voor hetzelfde vraagstuk in de V.S.: Ghappour 2017.
[146] *Kamerstukken I* 2016/17, 34372, D, p. 33.
[147] *Kamerstukken I 2016/17*, 34372, D, p. 38-40.

criminele infrastructuren bloot te leggen en zo echte locaties en identiteit te achterhalen zo wordt gesteld. Hackers en buitenlandse veiligheidsdiensten schenden onze privacy al dagelijks, juist door de nieuwe bevoegdheid zal het internet veiliger worden.[148] De kanttekening die ik hierbij plaats, is die van de mogelijke effectiviteit. Het is niet ondenkbaar dat criminelen zich gaan aanpassen aan het bestaan van deze nieuwe bevoegdheid en een effectieve contrastrategie bedenken.

Tijdens de plenaire behandeling van het wetsvoorstel werd flink gediscussieerd over onbekende kwetsbaarheden. Dit is een lek in software ontdekt door anderen dan de maker ervan, waarvoor nog geen patch voorhanden is: de zogenaamde zero-day. Door gebruik te maken van een dergelijk lek kan de politie zich toegang verschaffen tot een geautomatiseerd systeem. Zo kan de politie baat hebben bij het in stand houden van lekken. Dit kan de loyaliteit naar de digitale veiligheid van iedereen in gevaar brengen. Als de zero-day blijft bestaan, kunnen kwaadwillenden daar immers ook gebruik van maken en grote schade mee aanrichten. Dit spanningsveld heeft geleid tot een amendement. Daarin wordt verplicht om een kwetsbaarheid te melden.[149] Na machtiging van de rechter-commissaris zou in uitzonderlijke gevallen een melding uitgesteld kunnen worden.[150] Het bestaan van de mogelijkheid tot uitstel is voer voor discussie. Het lijkt mij onwenselijk dat de samenleving enorme schade oploopt door exploitatie van een bewust nog niet gemeld lek, terwijl deze schade bij een tijdige melding had kunnen worden voorkomen. Een dergelijke samenloop van omstandigheden vond plaats bij de uitbraak van het WannaCry virus.[151] De meldingsprocedure zal daarom kritisch moeten worden bekeken.

Buiten de kwetsbaarheden werd nog gediscussieerd over de vraag wat dan precies een geautomatiseerd werk is in het kader van deze wet. Zo werd de zorg geuit dat er op basis van de nieuwe bevoegdheid wordt binnengedrongen in een auto.[152] De regering stelt dat het uitsluiten van bepaalde geautomatiseerde werken, juist mogelijkheden geeft aan criminelen om opsporing te ontlopen en dat er voldoende waarborgen bestaan om oneigenlijk gebruik tegen te gaan.[153]

[148] Position Paper Fox-IT t.b.v. hoorzitting/rondetafelgesprek Computercriminaliteit III d.d. 11 februari 2016.
[149] *Kamerstukken II 2016/17, 34372, 14.*
[150] *Kamerstukken II 2016/17, 34372, 26, p. 1-9*.
[151] 'Wannacry werd mede mogelijk gemaakt door lek bij NSA', *NRC 14 mei 2017*, nrc.nl (zoek op WannaCry & NSA).
[152] *Kamerstukken II 2016/17, 34372, 26, p. 10-11*.
[153] *Kamerstukken I* 2016/17, 34372, D, p.14.

§ 5.4 Alternatieven

Binnendringen op afstand is niet het enige mogelijkheid om problemen met encryptie voor opsporingsdiensten te verminderen. In deze paragraaf bespreek ik kort drie alternatieven. Door de dynamiek en het continu veranderende digitale landschap is het best mogelijk dat ten tijde van het lezen van dit onderzoek er weer andere oplossingen bedacht zijn. Daarom is dit niet als een uitputtende lijst van alternatieven bedoeld, maar als een korte samenvatting van veel genoemde alternatieven en de redenen waarom deze (nog) geen nieuwe wetgeving hebben opgeleverd.

Een eerste alternatief is het decryptiebevel. Een verdachte zou kunnen worden verplicht om zijn wachtwoorden prijs te geven, zodat bestanden of communicatie toegankelijk gemaakt kunnen worden voor opsporingsdiensten. Een weigering van de verdachte om hieraan mee te werken, zou dan strafbaar gesteld worden. Na advies van de Raad van State heeft de regering in december 2015 uiteindelijk toch besloten om het decryptiebevel te schrappen uit het wetsvoorstel CC-III. Het adviesorgaan was niet overtuigd van de noodzaak en effectiviteit van een dergelijke bevoegdheid. Criminelen kunnen ook rekenen: als er op weigering een straf van twee jaar staat en zij weten dat als ze alles prijsgeven die straf veel hoger uitpakt, dan zullen ze deze straf accepteren om veroordeling voor een zwaarder delict te voorkomen. Ook kan het voorkomen dat een verdachte zijn wachtwoord vergeet. Dat zal iedere strafpleiter als argument gaan aanvoeren natuurlijk, maar het zou toch bizar zijn om vergeetachtigheid te straffen. Tenslotte voorziet de Raad ook problemen met het nemo teneturbeginsel uit artikel 6 EVRM, een verdachte hoeft immers niet mee te werken aan zijn eigen veroordeling.[154] Er dient een balans te zijn tussen de dwang om het wachtwoord prijs te geven en het publieke belang dat ermee gediend wordt. De aanzienlijke mate van dwang zou in het licht van eerdere uitspraken van het EHRM te hoog zijn om door het publieke belang gecompenseerd te kunnen worden.[155] Deze argumenten hebben tot de schrapping van het decryptiebevel uit het wetsvoorstel geleid, ondanks een hernieuwd voorstel van het CDA om het bevel last minute alsnog opnieuw in het wetsvoorstel op te nemen.[156]

Een tweede mogelijk alternatief kan het zogenaamde achterdeurtje zijn. Dit is een bewust ingevoerde mogelijkheid in een programma of app, waarmee de versleuteling ongedaan gemaakt kan worden. Dit zou dan via de betreffende dienstverlener gaan. Diensten als WhatsApp en Telegram zullen dan moeten zorgen, dat zij bij een rechtmatig verzoek de

[154] *Kamerstukken II 2015/16*, 34372, 4, p. 25-34.
[155] *Kamerstukken II 2015/16*, 34372, 4, p. 25-34.
[156] *Kamerstukken II 2016/17,* 34372, 26, p. 12-15.

communicatie in onversleutelde vorm aan de opsporingsdiensten kunnen overdragen. Bij monde van persofficier Egberts heeft het OM ook zijn interesse in een dergelijke bevoegdheid aangegeven.[157] Getuige het regeringsstandpunt met betrekking tot encryptie zal van een dergelijke bevoegdheid voorlopig in ieder geval nog geen sprake zal zijn. Door deze technische mogelijkheid te creëren, worden versleutelde bestanden van goedwillenden ook kwetsbaar voor criminelen, terroristen en buitenlandse veiligheidsdiensten.[158] Dit is onwenselijk voor de betrouwbaarheid van onze ICT-systemen en de samenleving als geheel. Ook kun je vragen stelen bij de effectiviteit van een dergelijke bevoegdheid. De moderne crimineel is digitaal zeer op zijn hoede en zodra bekend is dat bijvoorbeeld WhatsApp berichten doorgeeft aan opsporingsdiensten, zullen zij doorschakelen naar andere apps om versleutelde berichten te versturen. Is daar eenmaal toegang toe verkregen, dan gaan ze weer door naar de volgende of laten ze zelf een app ontwikkelen ergens. Zo loop je als politie steeds achter de feiten aan. CEO's Tim Cook van Apple en Jan Koum van WhatsApp waarschuwen dat het onmogelijk is om een achterdeurtje te creëren dat niet ook door kwaadwillenden geëxploiteerd kan worden. Voor miljoenen normale mensen zal de veiligheid online dan afnemen. We vertrouwen allemaal op sterke encryptie om online veilig te communiceren, winkelen en bankzaken te regelen.[159]

Het derde alternatief is het gebruik maken van een Trusted Third Party. Dit lijkt op het zojuist besproken achterdeurtje met als verschil dat de sleutel om de versleuteling ongedaan te maken in bezit komt van een derde partij. Na een gevoerde juridische procedure zou deze derde partij de sleutel tijdelijk aan opsporingsdiensten kunnen geven, zodat zij toegang krijgen tot de onversleutelde berichten of bestanden. Deze oplossing is geen nieuwe en is eerder besproken. In 1997 werd in de Verenigde Staten het Clipper-Chip voorstel gelanceerd. Elke telefoon zou worden uitgerust met een door de NSA ontworpen chip. Hiermee wordt iedere telefoon uitgerust met een speciale cryptografische code. Deze code zou door de overheid bewaard worden en na rechterlijke toestemming worden overgedragen. Zo konden opsporingsdiensten onversleutelde toegang tot een specifieke telefoon krijgen. Dit programma heeft het uiteindelijk niet gered. Wetenschappers gaven aan dat het technisch vrijwel onmogelijk was om op deze schaal een waterdicht systeem te ontwerpen, dat niet de veiligheid van iedereen compromitteert.[160] Hierdoor ontstaat er een veiligheidsrisico voor goedwillenden. De enorme kosten en jurisdictieproblemen

[157] 'Versleuteling berichten WhatsApp probleem voor OM', *AD* 22 augustus 2016, www.ad.nl (zoek op OM &encryptie).
[158] *Kamerstukken II* 2015/2016, 26643, 383, p. 4.
[159] 'Whatsapp row explained: backdoors and bad guys', *Financial Times* 27 maart 2017, www.ft.com (zoek op Whatsapp & backdoor).
[160] Zie: Abelson e.a. 1997.

waren de andere punten waarop dit voorstel uiteindelijk strandde. [161] Wellicht wordt het door toekomstige technologische ontwikkelingen wel mogelijk om een dergelijk systeem te ontwerpen, daarom is het goed om deze ontwikkelingen te blijven monitoren.

§ 5.5 Tussenconclusie

Als de wet CC-III in werking treedt, krijgt de politie de bevoegdheid om in bepaalde gevallen binnen te dringen in een geautomatiseerd werk. Dit zou een oplossing kunnen betekenen voor versleutelingsproblemen van opsporingsdiensten. De drie bekendste alternatieven om versleuteling van communicatie ongedaan te krijgen voldoen om uiteenlopende redenen niet. Toch is een oplossing gewenst, zodat opsporingsdiensten in staat zijn om hun taken uit te voeren. De wetgever meent in de bevoegdheid tot binnendringen op afstand het juiste alternatief te hebben gevonden. Deze bevoegdheid is niet onomstreden. Voorstanders vinden de nieuwe bevoegdheid noodzakelijk en menen dat er voldoende waarborgen ingebouwd zijn om willekeurige inzet te voorkomen. Critici hebben twijfels bij de onafhankelijke controle op uitoefening van de bevoegdheid en bij het niet melden van zero-days. Los van deze bezwaren lijkt de bevoegdheid in theorie geschikt om versleutelde communicatie leesbaar te onderscheppen. Of het ook een wenselijke uitbreiding van opsporingsbevoegdheden is, beantwoord ik aan de hand van de vraag of de bevoegdheid verenigbaar is met artikel 8 EVRM in hoofdstuk 6.

[161] Zie: Abelson e.a. 2015, p. 70.

Hoofdstuk 6: De toets aan artikel 8 EVRM

§ 6.1 Inleiding

De vraag of de mogelijk nieuwe bevoegdheid tot binnendringen op afstand, indien deze wordt ingezet voor onderschepping van vertrouwelijke communicatie, verenigbaar is met artikel 8 EVRM, wordt in dit hoofdstuk beantwoord. Daartoe moet het wettelijk stelsel aangaande deze bevoegdheid een legitiem doel dienen (§ 6.2), bij wet voorzien zijn (§ 6.3) en tenslotte noodzakelijk zijn in een democratische samenleving (§ 6.4). In § 6.5 worden mogelijke positieve verplichtingen behandeld. In § 6.6 trek ik mijn conclusie en doe ik enkele aanbevelingen.

§ 6.2 Legitiem doel

Het doel van de nieuwe bevoegdheid is om (cyber)criminaliteit en terrorisme effectief te kunnen bestrijden.[162] In lid 2 van artikel 8 EVRM staat de veiligheid van de staat genoemd als legitiem doel. Als criminaliteit en terrorisme beter bestreden kunnen worden, wordt het veiliger in Nederland. Op deze vereiste zal de wet dan ook niet stranden.[163]

§ 6.3 Bij wet voorzien

De volgende vraag is of de nieuwe bevoegdheid bij wet is voorzien. Is de bepaling voor de burger toegankelijk en voorzienbaar?[164] Aangenomen mag worden dat de toekomstige wet in het Staatsblad wordt gepubliceerd, de toegankelijkheid zal ik dan ook niet toetsen. De voorzienbaarheid ziet vooral op de voorspelbaarheid voor de burger. Binnendringen op afstand is een opsporingsbevoegdheid die plaatsvindt, zonder dat degene die voorwerp van het onderzoek is daarvan af weet. Bij een dergelijke bevoegdheid dient de nationale wet aan strenge eisen te voldoen en voorzien te zijn van voldoende waarborgen.[165]

In de zaak *Zakharov* heeft het EHRM buiten de eis van toegankelijkheid een aantal aanvullende voorwaarden voor de kwaliteit van de nationale wet op een rijtje gezet als samenvatting van eerdere uitspraken (zie kader 6).[166] Deze zaak betrof het afluisteren van

[162] *Kamerstukken II* 2015/16, 34372, 3, p. 6-7 (MvT).
[163] Vgl. ook Oerlemans 2017, p. 74.
[164] EHRM 26 april 1979 13166/87 (*Sunday Times/Verenigd Koninkrijk*).
[165] EHRM 2 augustus 1984, 8691/79 (*Malone/Verenigd Koninkrijk*), § 67.
[166] EHRM 4 december 2015, 47143/06 (*Zakharov/Rusland),* § 229-231*.*

telefoongesprekken in Rusland. Toekomstig artikel 126nba Sv biedt zelfs ruimere mogelijkheden om communicatie en gegevens te onderscheppen, zoals bijvoorbeeld e-mails en apps. De inbreuk op iemands levenssfeer kan groter zijn dan in de zaak *Zakharov* het geval was. Hoe groter de inbreuk is, hoe sterker de waarborgen moeten zijn. De bevoegdheid tot binnendringen op afstand in een geautomatiseerd werk zal daarom tenminste aan alle criteria uit *Zakharov* moeten voldoen.

Als eerste criterium dient duidelijk te zijn tegen welke personen de opsporingsbevoegdheid kan worden ingezet en voor hoelang. De bevoegdheid tot binnendringen kan worden ingezet tegen personen die verdacht worden van een misdrijf waarvoor voorlopige hechtenis mogelijk is (artikel 126nba lid 1 Sv), die verdacht worden van georganiseerde misdaad (artikel 126uba lid 1 Sv) en wanneer er aanwijzingen zijn voor een terroristisch misdrijf (artikel 126zba lid 1 Sv). Is eenmaal binnengedrongen dan kan vertrouwelijke communicatie in twee situaties worden onderschept. Welke gebruikt wordt is afhankelijk van het stadium waarin de uitwisseling van de communicatie zich bevindt.[167] Als het communicatie betreft die reeds heeft plaatsgevonden en die is opgeslagen op het geautomatiseerde werk, dan is er sprake van het vastleggen van gegevens.[168] Op grond van artikel 126nba lid 1 sub c-d Sv, 126uba lid 1 sub c-d Sv, 126zba lid 1 sub c-d Sv, mag dit alleen als er sprake is van verdenking van een misdrijf waarop naar wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld of bij een misdrijf dat per AMvB is aangewezen. Als de communicatie niet is opgeslagen, maar deze afgetapt of opgenomen wordt, dan gelden de reguliere bepalingen 126l, 126m, 126s, 126t en 126zg Sv.[169] Naast een bevel voor het binnendringen is daarmee ook een afzonderlijk bevel voor het tappen of opnemen nodig. Toepassing van de vereisten voor inzet van de bevoegdheid uit deze artikelen leidt niet tot een verandering in de categorie personen uit artikel 126nba, 126uba en 126zba Sv. De bevoegdheid mag hooguit vier weken worden toegepast en daarna voor een periode van vier weken worden verlengd.[170]

Zo op het eerste gezicht lijkt dat hiermee duidelijk wordt jegens welke categorie personen de opsporingsbevoegdheid kan worden ingezet. Het criterium van voorlopige hechtenis heeft niet eerder tot problemen met het EVRM geleid wanneer er sprake was heimelijk aftappen of

[167] *Kamerstukken II* 2015/16, 34372, 3, p. *20-21 & p. 23-25 (MvT).*
[168] *Kamerstukken II* 2015/16, 34372, 3, p. *20-21 & p. 23-25 (MvT).*
[169] Zie lid 1 sub b van de artikelen 126nba, 126uba en 126zba Sv & *Kamerstukken II* 2015/16, 34372, 3, p. *20-21 & p. 23-25 (MvT).*
[170] *Kamerstukken II* 2015/16, 34372, 3, p. *54 (MvT).*

opnemen van communicatie. De mogelijkheid om per AMvB de categorieën misdrijven welke de inzet van de bevoegdheid rechtvaardigen uit te breiden (in geval van het vastleggen van gegevens) is echter wel punt van discussie. De minister is voornemens om een aantal computermisdrijven toe te voegen.[171] Deze specifieke uitbreiding is in mijn ogen niet direct een probleem. De toets of er sprake is van een ernstige inbreuk blijft immers altijd overeind. Toch vind ik het bestaan van de mogelijkheid tot uitbreiding per AMvB merkwaardig. De mogelijk nieuwe bevoegdheid dient gecompenseerd te worden met sterke waarborgen en die lijken ook aanwezig. Maar dan wordt toch deze opening gelaten, die afbreuk doet aan deze waarborgen. Een AMvB biedt minder waarborgen dan een formele wet en kan relatief eenvoudig worden opgesteld. Goedkeuring van de Staten-Generaal is niet nodig. Theoretisch kan de minister de categorie misdrijven bijna onbeperkt uitbreiden. Dit is niet goed voor de voorzienbaarheid voor de burger, hij kan immers straks niet meer overzien wanneer de bevoegdheid tegen hem kan worden ingezet. Aan de andere kant gaan technologische ontwikkelingen razendsnel en kan ik me voorstellen dat flexibiliteit gewenst is. Stel dat er een ineens een nieuw soort criminaliteit ontstaat, die niet binnen de vereisten van acht jaar of meer gevangenisstraf past, maar wel veel schade aanricht in onze samenleving. Dan zou het wenselijk kunnen zijn om snel te kunnen schakelen. Hiervoor is een AMvB dan geschikter dan een formele wet. Daarom zou onderzocht mogen worden over of deze uitbreiding per AMvB niet middels een voorhangprocedure met extra waarborgen omkleed kan worden.

Het tweede criterium houdt in dat er duidelijke procedures betreffende de opslag en vernietiging van de verkregen gegevens moeten zijn. Van belang is hier de scheiding van tactische en technische teams om integriteit van de gegevens te waarborgen. Het technische team is het team dat het binnendringen gaat uitvoeren en het tactische team is belast met het gehele opsporingsonderzoek. Het tactische team krijgt van het technische team alleen gegevens die van belang zijn voor het betreffende opsporingsonderzoek.[172] Het technische team zorgt vervolgens voor een opslag van de verkregen gegevens op een veilige infrastructuur.[173] Door de regels voor vastlegging is ook duidelijk wat er tijdens het onderzoek met de gegevens gebeurt.[174] Wanneer een onderzoek eindigt, wordt het technisch hulpmiddel verwijderd en het transport van gegevens gestopt. [175]Twee maanden na beëindiging van de zaak en nadat de

[171] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', p. 7-8.
[172] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', p. 10-11.
[173] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', p. 21.
[174] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', p. 21.
[175] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', p. 25.

potentiele verdachte op de hoogte is gesteld, worden de gegevens vernietigd.[176] De verwerking, vernietiging en opslag van gegevens zijn daarmee in theorie in alle fases met voldoende waarborgen omkleed. Hoe dit in de praktijk gaat werken zal moeten worden geëvalueerd.

Als derde dienen er duidelijke en goede procedures te zijn voor het verkrijgen van toestemming om de opsporingsbevoegdheid in te zetten. Wanneer een officier van plan is om de bevoegdheid tot binnentreden op afstand te gaan gebruiken, legt hij dit eerst voor aan de Centrale Toetsingscommissie (CTC).[177] De CTC adviseert vervolgens het College van procureurs-generaal. Het College kan daaropvolgend goedkeuring verlenen aan de officier van justitie. Als laatste vraagt de officier een machtiging voor inzet van de bevoegdheid bij de rechter-commissaris. De rechter-commissaris toetst of het bevel tot inzet aan alle eisen voldoet. De machtiging die hij verleent, strekt tot alle onderdelen van dit bevel.[178] De rechter-commissaris oordeelt ook over de proportionaliteit en subsidiariteit in de specifieke omstandigheden van het geval.[179] Er is eerst een uitgebreide interne toetsing en daarna is er nog een onafhankelijke rechter, die ook naar de specifieke omstandigheden van het geval kijkt. De waarborgen betreffende toestemming zijn volgens mij in orde.

Het vierde criterium betreft een onafhankelijk, transparant toezicht op uitoefening van de bevoegdheid. De toepassing van de bevoegdheid is afhankelijk van voorafgaande rechterlijke toestemming. Als er strafvervolging wordt ingesteld, dan toetst de rechter of de opsporingsambtenaar en officier van justitie rechtmatig hebben gehandeld, wanneer hij ter terechtzitting oordeelt over de tenlastelegging.[180] Buiten deze twee momenten ligt tijdens de uitoefening van de bevoegdheid het algemeen toezicht bij de Inspectie Veiligheid en Justitie.[181] De inspectie houdt toezicht op de kwaliteit van de taakuitvoering van de politie.[182] Hiertoe worden de inspecteurs van deze dienst in staat gesteld om relevante informatie te verzamelen. In 2016 zijn verschillende onderzoeken gedaan bij de politie, waaronder een onderzoek naar de maatregelen betreffende integriteit bij de politie.[183] De inspectie rapporteert rechtstreeks aan de minister.[184] De rapporten van de inspectie zijn openbaar en hiermee transparant.[185] Een zekere onafhankelijkheid blijkt uit de missie van de inspectie. De inspectie wil namelijk bijdragen aan

[176] Concept AMvB 'Besluit onderzoek in een geautomatiseerd werk', p. 14-15.
[177] *Kamerstukken II* 2015/16, 34372, 3, p. 37-38 (MvT).
[178] *Kamerstukken II* 2015/16, 34372, 3, p. 29-30 (MvT).
[179] *Kamerstukken II* 2015/16, 34372, 3, p. 29-30 (MvT).
[180] *Kamerstukken I* 2016/17, 34372, D, p. 30-31.
[181] Toekomstig artikel 126nba Sv, lid 7 & art. 65 Politiewet 2012.
[182] Geldend protocol werkwijze inspectie V & J 2014, p. 4.
[183] Jaarbericht 2016, Inspectie Veiligheid en Justitie, p. 15-19, zie bijvoorbeeld *Kamerstukken II* 2016/17, 28844, 104.
[184] Artikel 66 Politiewet 2012.
[185] Geldend protocol werkwijze inspectie V & J 2014, p. 8-9.

een rechtvaardige samenleving en heeft een waakhondfunctie.[186] De inspectie kan op eigen initiatief naar aanleiding van een incident een onderzoek starten en is in die zin ook onafhankelijk.[187] Toch zijn hier enige kanttekeningen bij te plaatsen. Zo worden het hoofd en de andere ambtenaren van de inspectie door de minister aangewezen.[188] Er bestaan geen specifieke vereisten wie er in de inspectie plaatsnemen. Bij een onevenwichtige samenstelling zou de onafhankelijkheid van het orgaan in het geding kunnen komen. Stel bijvoorbeeld dat er voornamelijk oud-politie mensen in de inspectie terecht komen, dan zouden die onbewust meer waarde aan het opsporingsbelang kunnen toekennen dan wanneer er een aantal strafpleiters in de inspectie zitten. Daarnaast is de inspectie ook belast met toezicht op algemene terreinen als sanctietoepassing, asiel, migratie en nationale veiligheid.[189] De vraag is dan ook of er voldoende specifieke expertise en capaciteit in huis is om voor een goed toezicht op de bevoegdheid uit artikel 126nba Sv te zorgen. Verbetering van het voorgestelde toezicht is daarom in mijn ogen wenselijk.

Als vijfde moet de persoon tegen wie de bevoegdheid wordt ingezet, daarvan op de hoogte gesteld worden. In geval van inzet van een bijzondere opsporingsbevoegdheid geldt in Nederland de notificatieplicht (art. 126bb Sv). De betrokkene moet in kennis te worden gesteld van het feit dat op afstand heimelijk is binnengedrongen in een geautomatiseerd werk van hem. Deze melding kan alleen in belang van het onderzoek uitgesteld worden.[190] Deze waarborg is wettelijk goed geregeld.

De laatste en zesde vereiste is een goede klachtregeling voor de burger. Er is in het wetsvoorstel CC-III niet voorzien in een specifieke klachtregeling. Als een burger een klacht heeft met betrekking tot de inzet van een opsporingsbevoegdheid kan hij een klacht indienen bij de politie of later als onafhankelijk orgaan bij de Nationale ombudsman. Eventuele incidenten kunnen worden opgepakt door de inspectie V en J.[191] De burger kan voor zijn rechten opkomen bij een onafhankelijke instantie en heeft daarmee de mogelijkheid tot indienen van een klacht, zodat aan deze vereiste wordt voldaan.

kader 6

[186] Geldend protocol werkwijze inspectie V & J 2014, p. 8-9.

[187] Geldend protocol werkwijze inspectie V & J 2014, p. 5-6.
[188] Art. 57 lid 2 Wet veiligheidsregio's 2017.
[189] Geldend protocol werkwijze inspectie V & J 2014, p. 4.
[190] *Kamerstukken II* 2015/16, 34372, 3, p. 39-40 (MvT).
[191] Geldend protocol werkwijze inspectie V & J 2014, p. 5-6.

toets *Zakharov* criteria:	
1) Categorieën personen/duur	+/-
2) Duidelijke procedures m.b.t. verkregen data	+
3) Procedure toestemming	+
4) Onafhankelijk, transparant toezicht	+/-
5) Notificatie wanneer mogelijk	+
6) Klachtregeling	+
Verbetering van de waarborgen 1 & 4 is wenselijk, zie daarvoor mijn aanbevelingen in § 6.7.	

§ 6.4 Noodzakelijk in een democratische samenleving

De derde vereiste is dat een inbreuk noodzakelijk moet zijn in een democratische samenleving. De vraag is of de bevoegdheid proportioneel is ten opzichte van het belang dat ermee gediend wordt. Tevens dient er een dwingende maatschappelijke behoefte aanwezig te zijn.[192] Het opsporen van zware criminaliteit en terrorisme is hier het gediende belang. Dit is een zwaarwegend belang in een democratische samenleving en kan het inzetten van geheime opsporingsbevoegdheden rechtvaardigen.[193] Maatschappelijk gezien bestaat er behoefte aan een effectieve opsporing.

Ook wordt getoetst of de ingezette bevoegdheid geschikt is om het gestelde doel te bereiken. Het doel zal in dit geval zijn het onderscheppen van vertrouwelijke communicatie tussen criminelen teneinde bewijs te vergaren of ernstige strafbare feiten te voorkomen. Door op afstand een geautomatiseerd werk binnen te dringen kan de veelal versleutelde communicatiestroom tussen criminelen beter onderschept worden.[194] De effectiviteit van de voorgenomen bevoegdheid zal in de praktijk moeten blijken, maar op voorhand lijkt de bevoegdheid geschikt voor het gestelde doel.

[192] EHRM 26 april 1979 13166/87 (*Sunday Times/Verenigd Koninkrijk*), EHRM 7 december 1976, 5493/72 (*Handyside/Verenigd Koninkrijk*).
[193] EHRM 26 juni 2006, 54934/00 (*Weber en Saravia /Duitsland),* § 104-106.
[194] *Kamerstukken II* 2015/16, 34372, 3, p. 3 (MvT).

Minder ingrijpende alternatieven om hetzelfde doel te bereiken mogen niet voor handen zijn. Verkregen gegevens onder de huidige tapbevoegdheid zijn vaak versleuteld.[195] Om toch bij deze versleutelde gegevens te komen lijkt uitbreiding van de bevoegdheden nodig.[196] Andere oplossingen voor dit probleem voldoen om uiteenlopende redenen niet en verzwakking van encryptie is ook geen optie.[197] De bevoegdheid lijkt de subsidiariteitstoets hiermee te doorstaan.

Het bestaan van de bevoegdheid zal geen strijd met het noodzakelijkheidsprincipe opleveren. Wel is het zo dat het Hof een schending in concreto zal toetsen. De omstandigheden van het geval zullen dan tot een nieuwe afweging leiden. Bij een geheime opsporingsbevoegdheid, zoals het binnendringen op afstand is, moeten er voldoende waarborgen zijn. Als deze er in de praktijk niet blijken te zijn geweest, acht het Hof de bevoegdheid niet noodzakelijk.[198] Bij die waarborgen zijn nog vraagtekens te plaatsen (zie § 6.3). De vraag is dan ook nog of de voorgenomen bevoegdheid uiteindelijk de noodzakelijkheidstoets van het EHRM doorstaat. In § 6.6 doe ik drie aanbevelingen om deze twijfels weg te nemen.

§ 6.5 Positieve verplichtingen

Om te beoordelen of er ook positieve verplichtingen voor de staat bestaan aangaande de bevoegdheid tot binnendringen op afstand, hanteert het Hof de '*fair balance'* test. Deze mogelijke verplichtingen moeten dan zorgen voor evenwicht tussen het recht op vertrouwelijke communicatie voor de burger en het algemeen belang dat door de overheid wordt gediend.[199] Binnen dit vraagstuk past de vraag over hoe omgegaan moet worden met de ontdekking van onbekende kwetsbaarheden (zero-days). Om de bevoegdheid uit te oefenen kunnen opsporingsdiensten kwetsbaarheden gebruiken. Vaak zullen dit bekende kwetsbaarheden zijn die nog niet door de betreffende (software) fabrikant zijn gedicht, maar de mogelijkheid bestaat ook dat tijdens de uitoefening van de bevoegdheid gebruik wordt gemaakt van een onbekende kwetsbaarheid in het systeem. Het laten voortbestaan van deze bij de fabrikant nog onbekende kwetsbaarheid kan zorgen voor schade bij andere burgers en/of bedrijven.

[195] *Kamerstukken II* 2015/16, 34372, 3, p. 7-8 (MvT).
[196] *Kamerstukken II* 2015/16, 34372, 3, p. 7-8 (MvT).
[197] Zie § 5.4 & § 4.2.
[198] Zie 2.2.3. & EHRM 26 juni 2006, 54934/00 (*Weber en Saravia /Duitsland),* § 104-106.
[199] Gerards 2014, p. 233, voorbeeld van *fair balance test*: EHRM 8 juli 2003 36022/97 (Hatton e.a./Verenigd Koninkrijk), § 118-130.

Een voorbeeld is de aanval met het WannaCry virus, waarbij waarschijnlijk gebruik gemaakt werd van een lek bij de NSA. Bedrijven over de hele wereld kregen te maken met computersystemen die ineens versleuteld waren middels zogenaamde ransomware. Dit is software waarbij pas na betaling van losgeld weer toegang tot de computer verkregen kan worden. De gevolgen waren niet alleen financieel, maar ook konden bijvoorbeeld operaties in ziekenhuizen niet uitgevoerd worden. De NSA had naar verluid de aanval grotendeels kunnen voorkomen door op tijd het lek aan Microsoft te melden.[200] De mogelijke gevolgen van het in stand houden van een onbekende kwetsbaarheid kunnen enorm zijn. Een situatie waarbij de politie bewust geen melding maakt van een lek en er later door dat lek een enorme cyberaanval plaatsvindt, waarbij grote schade voor de samenleving ontstaat, is hoogst onwenselijk.

Te beargumenteren valt dat de onbekende kwetsbaarheid zonder de uitoefening van de bevoegdheid door bijvoorbeeld de politie ook had bestaan, dus dat de veiligheid voor burgers en bedrijven niet minder zal worden door gebruik te maken van onbekende kwetsbaarheden, ze bestaan immers al. Echter is het scenario ook niet ondenkbaar dat de politie zelf slachtoffer wordt van een hack en dat de zero-day die de politie gebruikt door kwaadwillenden op deze manier wordt ontdekt. In dat geval, heeft uitoefening van de bevoegdheid er wel voor gezorgd dat geautomatiseerde systemen van burgers en bedrijven onveiliger worden, dan dat ze voorafgaand aan de inzet van de bevoegdheid waren.

Per brief geeft de staatssecretaris aan dat kwetsbaarheden in beginsel direct of zo snel mogelijk worden gemeld aan de betreffende fabrikant.[201] Alleen in uitzonderlijke gevallen kunnen omstandigheden ontstaan waardoor er een groot belang bij is om de kwetsbaarheid (tijdelijk) niet te melden.[202] Er vindt dus een afweging plaats tussen het achterhouden van de kwetsbaarheid uit opsporingsbelang en het belang van de samenleving om het lek te dichten. Dit overstijgt het belang van een specifiek onderzoek en daarom worden deze beslissingen landelijk genomen.[203] Stel bijvoorbeeld dat criminelen een eigen app ontwikkelen om onderling te communiceren. De specifieke app kent slechts een aantal (criminele) gebruikers. Het belang voor de samenleving om een kwetsbaarheid in die specifieke app te melden is in een dergelijk geval erg klein. Betreft het echter een kwetsbaarheid in veel gebruikte systemen als Windows of iOS, dan wordt dit belang erg groot. Hier zou dan wel een zeer acuut en belangrijk

[200] 'Wannacry werd mede mogelijk gemaakt door lek bij NSA', *NRC 14 mei 2017*, nrc.nl (zoek op WannaCry & NSA).
[201] *Kamerstukken II* 2016/17, 26643, 428, p. 4.
[202] *Kamerstukken II* 2016/17, 26643, 428, p. 4.
[203] *Kamerstukken II* 2016/17, 26643, 428, p. 4.

opsporingsbelang tegenover moeten staan. Ik zou me voor kunnen stellen dat dit bijvoorbeeld zou moeten kunnen als er sterke aanwijzingen zijn voor een terroristische aanslag op zeer korte termijn.

Melding van onbekende kwetsbaarheden wordt geregeld in voorgesteld artikel 126ffa Sv.[204] De basisregel is dat een onbekende kwetsbaarheid gemeld wordt. Op grond van een zwaarwegend opsporingsbelang kan de officier echter een bevel geven om een kwetsbaarheid niet te melden. Dit bevel kan niet anders gegeven worden dan na machtiging van de rechter-commissaris. Deze onafhankelijke toets is een waarborg, echter vraag ik me af of deze voldoende is. Heeft de rechter-commissaris in een concreet geval technisch voldoende kennis of toegang tot deze kennis om een snelle risicoanalyse te maken? Immers hoe langer het duurt om te melden, hoe groter de gevaren voor de digitale veiligheid van de samenleving. In de praktijk lijkt het me moeilijk om het risico dat de samenleving loopt door niet te melden op korte termijn vast te stellen.

Het belang dat tegenover het risico voor de samenleving moet staan in de afweging is een zwaarwegend opsporingsbelang. Een acute bedreigende situatie voor de samenleving lijkt een dergelijk belang te kunnen zijn. In een dergelijke situatie kun je ook nog de vraag stellen of je niet toch melding moet maken. Het lek is immers niet direct gedicht. Daarvoor zal de softwarefabrikant een patch uit moeten brengen en deze zal vervolgens ook nog door de gebruikers moeten worden geïnstalleerd. Tot dit proces voltooid is, hebben opsporingsdiensten nog steeds toegang via het lek en kunnen zij mogelijke updates wellicht zelfs blokkeren. Dit proces kan normaal gesproken niet binnen enkele uren worden voltooid. Ik acht de kans dan ook uiterst klein dat directe melding negatieve gevolgen zal hebben in een situatie van acute dreiging. Met onder andere het WannaCry virus hebben we gezien wat de enorme gevolgen en schade voor de samenleving kunnen zijn. Als dit voorkomen kan worden, dan moet politie daar in mijn ogen alles aan doen. Bescherming van de burgers is immers een taak van de politie.[205] In geval van een onbekende kwetsbaarheid betekent dit gewoon melden. Het lek is niet direct gedicht, waardoor acute opsporingsactiviteiten gewoon door kunnen gaan. Hoe sneller gemeld wordt, hoe sneller de digitale veiligheid voor de samenleving toeneemt. Daarom pleit ik voor een meldplicht zonder uitzonderingen, in plaats van het voorgestelde stelsel, waarbij de beoordeling bij de rechter-commissaris terechtkomt. Met melden voorkom je problemen in de toekomst,

[204] *Kamerstukken II* 2016/17, 34372, 14, toekomstig artikel 126ffa Sv.
[205] Art. 3 Politiewet (2012).

bescherm je het belang van de digitale veiligheid van de samenleving en behoud je nog steeds de mogelijkheid tot toegang in een geval van acute dreiging.

§ 6.6 Conclusie & aanbevelingen

De voorgestelde bevoegdheid tot binnendringen op afstand dient een legitiem doel, namelijk de veiligheid van de staat. Om vast te stellen of de voorgestelde bevoegdheid ook bij wet voorzien is en of deze noodzakelijk is in een democratische samenleving is de bevoegdheid getoetst aan de criteria uit *Zakharov*. Twijfel is mogelijk over de mogelijkheid om per AMvB de categorieën misdrijven uit te breiden en over het onafhankelijke toezicht. De kans bestaat dat het EHRM strengere dan de *Zakharov* criteria hanteert voor de inzet van de toekomstige bevoegdheid. Binnendringen op afstand kan immers een grotere inbreuk op de levenssfeer opleveren dan de telefoontap. De waarborgen zouden daarom boven iedere twijfel verheven moeten zijn. Om de belangrijkste twijfels weg te nemen, doe ik drie aanbevelingen.

De eerste aanbeveling is om een extra waarborg in te bouwen omtrent de uitbreiding van categorieën per AMvB. Ruggenspraak en toetsing voor een nieuwe AMvB is zeer wenselijk. Zo is dit bijvoorbeeld ook geregeld in artikel 16 lid 9 Elektriciteitswet (zie kader 7).[206] Om tijdsverlies te voorkomen, zou dit middels een zogenaamde voorhangprocedure kunnen gebeuren. Een bepaling vergelijkbaar met dit artikel zou dan de voorzienbaarheid voor de burger aanzienlijk vergroten. Omstreden onderdelen van een voorgestelde AMvB zullen tot discussies leiden, waarbij ook tegenstanders de kans krijgen om hun argumenten naar voren te brengen. Hierdoor zal een uitbreiding per AMvB zeer goed gemotiveerd moeten worden. De burger wordt hiermee in de toekomst beter beschermd tegen een te willekeurige uitbreiding van de reikwijdte van artikel 126nba Sv per AMvB.

kader 7

Artikel 16 lid 9 Elektriciteitswet 1998

De voordracht voor een krachtens dit artikel vast te stellen algemene maatregel van bestuur wordt niet gedaan dan nadat het ontwerp in de Staatscourant is bekendgemaakt en aan een ieder de gelegenheid is geboden om binnen vier weken na de dag waarop de bekendmaking is

[206] Zie*: Kamerstukken II* 2011/12, 33350, 3.

geschied, wensen en bedenkingen ter kennis van Onze Minister te brengen. Gelijktijdig met de bekendmaking wordt het ontwerp aan de beide kamers der Staten-Generaal overgelegd.

De tweede aanbeveling betreft een nieuw op te richten afdeling binnen de Inspectie V & J die regelmatig controleert op de inzet van de bevoegdheden gebaseerd op de wet CC-III. Dit komt zowel de kwaliteit als de onafhankelijkheid van het toezicht ten goede. Het binnendringen op afstand betreft een nieuwe bevoegdheid voor opsporingsdiensten en specifieke (ICT) kennis is nodig om een goede controle op deze bevoegdheid uit te oefenen. Een specialistische afdeling zal hierin mijns inziens beter kunnen voorzien dan een orgaan belast met algemeen toezicht op de politie. Buiten de kwaliteit, hecht het EHRM ook waarde aan de onafhankelijkheid van dat toezicht. Om deze onafhankelijkheid optimaal te waarborgen, zou voor benoeming van deze afdeling een procedure gelijk aan de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) kunnen worden gevolgd. Zowel de uitvoerende macht, de wetgevende macht als de rechtsprekende macht zijn daar bij de benoemingsprocedure betrokken en de dienst heeft volledige onderzoeksvrijheid.[207]

Bijkomend voordeel is dat het nieuw op te richten orgaan of afdeling tevens klachten van burgers in behandeling kan nemen, zodat ook in de klachtprocedure de kwaliteit verbetert. Met deze twee uitbreidingen meen ik dat de waarborgen voldoen aan de *Zakharov* criteria.

Tenslotte adviseer ik nog het mogelijke uitstel van melding van een zero-day uit artikel 126ffa Sv te schrappen. De digitale veiligheid van de samenleving is gebaat bij directe melding. Situaties waarin het acute opsporingsbelang belangrijker is dan deze veiligheid zijn nauwelijks denkbaar. Tussen melding en daadwerkelijk dichten van een lek zit immers ook nog tijd en blokkeren van een update zou mogelijk moeten zijn. Een meldplicht zou daarom beter zijn voor iedereen en ervoor zorgen dat Nederland voldoet aan de positieve verplichtingen, die ontstaan uit artikel 8 EVRM. Met deze aanpassing en de twee eerdergenoemde aanbevelingen meen ik dat de voorgestelde bevoegdheid verenigbaar is met het recht op vertrouwelijke communicatie uit artikel 8 EVRM, zonder deze aanbevelingen vind ik dat nog uiterst twijfelachtig.

[207] Zie art. 64 & 65 Wiv.

Hoofdstuk 7: Conclusie

De hoofdvraag die aan dit onderzoek ten grondslag ligt luidt: '*Is het onderscheppen van vertrouwelijke communicatie, wanneer gebruik gemaakt wordt van de bevoegdheid tot binnendringen op afstand uit de toekomstige Wet Computercriminaliteit III, verenigbaar met het recht op vertrouwelijke communicatie, zoals dit af te leiden valt uit artikel 8 EVRM?'.* Middels de deelvraagstukken, die behandeld zijn in hoofdstukken 2 tot en met 6 kom ik tot de volgende conclusie en beantwoording van de hoofdvraag.

De voorgenomen bevoegdheid tot binnendringen op afstand valt binnen de reikwijdte van het recht op vertrouwelijke communicatie van artikel 8 EVRM. Tegenover heimelijke opsporingsmethoden zoals de voorgenomen bevoegdheid moeten strikte waarborgen staan. Waar deze waarborgen aan moeten voldoen is samengevat in de zaak *Zakharov*.

Bestaande bevoegdheden om communicatie te onderscheppen worden minder effectief of zijn risicovol. Encryptie speelt daarbij een belangrijke rol. Deze encryptie is belangrijk voor de digitale veiligheid van de samenleving en kan daarom niet afgeschaft worden. Dit leidt tot een probleem voor opsporingsdiensten.

Als antwoord op dit probleem wil de wetgever in wetsvoorstel CC-III een bevoegdheid tot binnendringen in een geautomatiseerd werk creëren. In theorie is het mogelijk om met deze bevoegdheid de versleuteling van communicatie te omzeilen. Twijfels zijn er met betrekking tot het toezicht en onbekende kwetsbaarheden.

Of aan alle criteria uit de zaak *Zakharov* wordt voldaan is daarom maar zeer de vraag. De onafhankelijke controle, de mogelijke uitbreiding per AMvB en het beleid betreffende onbekende kwetsbaarheden zijn pijnpunten. *Zakharov* ging over het afluisteren van telefoons. De voorgenomen bevoegdheid tot binnendringen kan nog meer inbreuk op iemands levenssfeer veroorzaken. Daarom zou de voorgenomen bevoegdheid tenminste zonder enige twijfel de toets aan de criteria uit *Zakharov* moeten doorstaan. Dit is niet het geval. Daarnaast zorgt het beleid met betrekking tot onbekende kwetsbaarheden mogelijk nog voor problemen met de positieve verplichtingen die ontstaan uit artikel 8 EVRM. Dit gesteld hebbende meen ik dat de onderschepping van communicatie, wanneer gebruikt wordt gemaakt van de bevoegdheid tot binnendringen op afstand uit de toekomstige wet CC-III in haar huidige vorm niet zonder twijfel verenigbaar is met het recht op vertrouwelijke communicatie van artikel 8 EVRM.

Om deze twijfels weg te nemen heb ik drie aanbevelingen gedaan. Als eerste zou uitbreiding per AMvB niet zonder inspraak tot stand mogen komen. Als tweede zou er een onafhankelijke gespecialiseerde afdeling bij de Inspectie V & J moeten komen. Tenslotte pleit ik voor directe melding van onbekende kwetsbaarheden.

Literatuurlijst

Abelson e.a. 1997

H. Abelson e.a., *The risks of key recovery, key escrow, and trusted third-party encryption* (Columbia University Academic Commons)*, 1997.*

Abelson e.a. 2015

H. Abelson e.a.*, '*Keys under doormats: mandating insecurity by requiring government access tof all data and communicatiefs.', *Journal of Cybersecurity* 2015, afl. 1, p. 69-79.

Aink 2016

J.R.J. Aink, 'Het wetsvoorstel Computercriminaliteit III: Een High Tech inhaalslag?', *Praktijkwijzer Strafrecht*, afl. 16, p. 42-46.

Asscher 2002

L. Asscher, *Communicatiegrondrechten*, Amsterdam: Otto Cramwinckel Uitgever 2002.

Gerards 2014

J.H. Gerards, *EVRM-algemene beginselen*, Den Haag: SDU-uitgevers 2014.

Ghappour 2017

A. Ghappour, 'Searching places unknown: law enforcement jurisdiction on the dark web'*,* *Stanford Law Review* 2017, afl. 69, p. 1075-1135.

Koops 1999

E.J. Koops, *The crypto controversy, a key conflict in the information society*, Den Haag: Kluwer 1999.

Koops 2012

E.J. Koops, *Het decryptiebevel en het nemo-teneturbeginsel, nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten,* Tilburg 2012*.*

Koops 2017

E.J. Koops, 'Digitaal huisrecht', *NJB* 2017/147, afl. 3, p. 183-187.

Koops & Goodwin 2014

E.J. Koops & M. Goodwin, *Cyberspace, the cloud, and cross-border criminal investigation,* Tilburg: Tilburg Institute for Law, Technology and Society 2014.

Koops, Leenes & De Hert, NJB 2008/914

E.J. Koops, R.E. Leenes, P. de Hert, 'Grondrechten en nieuwe technologieën, een rechtsvergelijkend overzicht', *NJB* 2008/914, afl. 19, p. 1157-1164.

Leenes, Koops & De Hert 2008

R.E. Leenes, E.J. Koops & P. de Hert, *Constitutional rights and new technologies, a comparative study*, Den Haag: Asser 2008.

Lensing 2012

J.A.W. Lensing, 'Grondrechten van de EU in de Nederlandse straf(proces)rechtelijke praktijk', *Strafblad* 2012, afl.1, p. 19-31.

Nieuwenhuis & Hins 2011

A.J. Nieuwenhuis & A.W. Hins, *Hoofdstukken grondrechten*, Nijmegen: Ars Aequi Libri 2011.

Oerlemans 2017

J.J. Oerlemans, *Investigating cybercrime*, Amsterdam: SIKS 2007.

Prins 2013

C. Prins, 'Art. 13 Grondwet: herkansing voor modernisering', *NJB* 2013/56, afl. 2, p 71.

Schneier 2007

B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*, Indianapolis: John Wiley & Sons 2007.

Schneier, Seidel & Viajayakumar 2016

B. Schneier, K. Seidel & S. Viajayakumar*, A worldwide survey of encryption products*, Cambridge: Berkman Center Harvard 2016.

Steenbruggen 2009

W.A.M. Steenbruggen, *Publieke dimensies van privé-communicatie*, Amsterdam: Otto Cramwinckel Uitgever 2009.

WODC 2012

Rapport WODC, *Het gebruik van de telefoon- en internettap in de opsporing,* Den Haag: Boom Lemma 2012.

Jurisprudentielijst

EHRM:

EHRM 7 december 1976, 5493/72 (*Handyside/Verenigd Koninkrijk*)

EHRM 25 april 1978, 5856/72 (*Tyrer/Verenigd Koninkrijk*)

EHRM 6 september 1978, 5029/71 (*Klass/Duitsland*)

EHRM 26 april 1979 13166/87 (*Sunday Times/Verenigd Koninkrijk*)

EHRM 2 augustus 1984, 8691/79 (*Malone/Verenigd Koninkrijk*)

EHRM 16 december 1992, 13710/88 (*Niemietz/Duitsland*)

EHRM 2 juni 2002, 33129/96 (*Olivieira/Nederland*)

EHRM 8 juli 2003 36022/97 (Hatton e.a./Verenigd Koninkrijk)

EHRM 17 oktober 2003, 25337/94 (*Craxi II/Italië*)

EHRM 26 juni 2006, 54934/00 (*Weber en Saravia /Duitsland)*

EHRM 3 april 2007, 62617/00 (*Copland/Verenigd Koninkrijk*)

EHRM 2 december 2008, 2872/02 (*K.U./Finland*)

EHRM 18 mei 2010, 26839/0 (*Kennedy/Verenigd Koninkrijk*)

EHRM 2 september 2010, 35623/05 (*Uzun/Duitsland*)

EHRM 4 december 2012, 41452/07 (Lenev/Bulgarije)

EHRM 4 december 2015, 47143/06 (*Zakharov/Rusland*)

Nederlandse jurisprudentie:

HR 8 april 2003, ECLI:NL:PHR:2003:AE8771

HR 11 oktober 2005, ECLI:NL:HR:2005:AT4351

HR 1 juli 2014, ECLI:NL:HR:2014:1563

HR 25 oktober 2016, ECLI:NL:PHR:2016:1048

HR 25 oktober 2016, ECLI:NL:PHR:2016:1049

Hof Amsterdam 23 december 2009, ECLI:NL:GHAMS:2009:BK7941

Rb Rotterdam 26 april 2010, ECLI:NL:RBROT:BM2520