Cadet-Vaandrig D.R. Pols

Extraterritoriaal inlichtingen verzamelen in het cyberdomein binnen de grenzen van het internationaal recht

Een onderzoek naar de mogelijkheden van de MIVD
voor het extraterritoriaal verzamelen van inlichtingen in het cyberdomein
binnen de grenzen van het internationaal recht

Extraterritoriaal inlichtingen verzamelen in het cyberdomein binnen de grenzen van het internationaal recht

Welke mogelijkheden heeft de Militaire Inlichtingen- en Veiligheidsdienst voor het extraterritoriaal verzamelen van inlichtingen in het cyberdomein, binnen de grenzen van het internationaal recht?

Cadet-Vaandrig D.R. Pols
Krijgswetenschappen

Nederlandse Defensie Academie (NLDA)
Breda, 12 maart 2014

Begeleiders:
Kolonel Mr. dr. P.A.L. Ducheine (NLDA)
Luitenant-Kolonel Mr. dr. G.L.C. Van den Bosch (NLDA)

Versie 3

Summary

In general, the cyber domain is becoming more and more important in the temporary world. The armed forces also recognize that some activities, like communications and intelligence gathering, are conducted through the cyber domain. Besides, the cyber domain creates new opportunities to gather intelligence. This was published by Edward Snowden, who leaked documents containing information of the National Security Agency and their (illegal) activities. After the news of the NSA, a discussion about intelligence gathering started. The discussion also reached The Netherlands.

One of the Dutch services which are able to gather intelligence is called the Military Intelligence- and Security Service. The gathering of intelligence can be performed both domestically and abroad. The aim of this research is find out which possibilities the Dutch Military Security- and Intelligence Service has to gather intelligence in the cyber domain, within the boundaries of international law.

First a choice was made for two principles of international law: the non-intervention principle and the principle of sovereignty. A broad selection of articles and books on the subject served as material for a literature study. For both principles a workable definition was formulated. Secondly, it was examined if the Law on Intelligence- and Security Services (2002) is applicable abroad. In order to decide whether the law contained an extraterritorial function, the law itself, the legislative history, the reports of the supervisory committee and the report of the evaluation committee were studied. In third place the abilities of the Military Intelligence- and Security Service to gather intelligence were investigated. Also in the chapter according to the abilities of the Military Intelligence- and Security Service, both the law itself and the legislative history were studied. Besides, the reports of the supervisory committee and the evaluation committee were examined.

The research showed no extraterritorial function for the Law on Intelligence- and Security Services. Nevertheless, the law will be applied by analogy abroad. So the abilities of the Military Intelligence- and Security Service can be conducted outside Dutch territory. A close look at the law and the legislative history showed that just a few abilities to gather intelligence were aimed at the cyber domain. By conducting an own analyses it became clear that, because of some technological innovations, some other abilities can also serve as intelligence gathering abilities in the cyber domain.

In the end a list was made containing seven special abilities and two additional abilities which the Military Intelligence- and Security Service can perform in order to gather intelligence abroad in the cyber domain. These abilities can be applied without infringing a state's sovereignty and without performing a prohibited intervention. So both the non-intervention principle and the principle of sovereignty will not be violated by applying the nine mentioned abilities of the Military Intelligence- and Security Service to gather intelligence abroad in the cyber domain. Unfortunately no answer could be found on the question whether the use of malware, by accessing an computer network for instance, could be regarded as a violation of the principle of sovereignty. Therefore further research is needed on this subject.

Samenvatting

Tegenwoordig wordt het cyberdomein steeds belangrijker. Ook de strijdkrachten merken dat bepaalde activiteiten, zoals communicatie en het verzamelen van inlichtingen, steeds vaker via het cyberdomein plaatsvindt. Dat het cyberdomein nieuwe mogelijkheden creëert voor het verzamelen van inlichtingen werd duidelijk toen klokkenluider Edward Snowden zich uitte over de *National Security Agency (NSA)* en de (illegale) activiteiten die de *NSA* ontplooit. Vanwege het nieuws over de *NSA*, startte een discussie omtrent het verzamelen van inlichtingen. Deze discussie bereikte ook Nederland.

Eén van de Nederlandse inlichtingendiensten is de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Het verzamelen van inlichtingen kan zowel in het binnenland als in het buitenland plaatsvinden. Dit onderzoek richt zich op de mogelijkheden die de MIVD heeft voor het extraterritoriaal verzamelen van inlichtingen in het cyberdomein, binnen de grenzen van het internationaal recht.

In eerste instantie is de keuze gemaakt om louter twee internationaalrechtelijke beginselen te behandelen, te weten het non-interventiebeginsel en het soevereiniteitsbeginsel. Om een goede omschrijving van beiden beginselen te formuleren is een literatuurstudie gedaan waarbij veel boeken en artikelen zijn gelezen. Ten tweede is in dit onderzoek onderzocht of de Wet op Inlichtingen- en Veiligheidsdiensten (WIV) 2002 ook in het buitenland geldig is. Om dit te bepalen zijn de wetstekst, de wetsgeschiedenis, rapporten van de Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (CTIVD) en het rapport van de evaluatiecommissie onderzocht. Tevens werd in het hoofdstuk over de bevoegdheden van de MIVD in het cyberdomein, die de MIVD op basis van de WIV heeft, gebruik gemaakt van de wetstekst, de wetsgeschiedenis, rapporten van de CTIVD en het rapport van de evaluatiecommissie.

Het onderzoek wees uit dat de WIV geen extraterritoriale werking heeft. Desalniettemin wordt de wet naar analogie in het buitenland toegepast. De bevoegdheden die de MIVD op basis van deze wet heeft kunnen dus in het buitenland worden uitgeoefend. Bij het bestuderen van de wetstekst en de wetsgeschiedenis kwam naar voren dat slechts een aantal bevoegdheden van de MIVD kunnen worden gebruikt om inlichtingen te verzamelen in het cyberdomein. Daarnaast werd door een eigen analyse van de wetstekst en de wetsgeschiedenis duidelijk dat een aantal andere bevoegdheden van de MIVD, vanwege technologische innovaties, ook relevant zijn om inlichtingen te verzamelen in het cyberdomein.

Uiteindelijk is een opsomming gemaakt van zeven bijzondere bevoegdheden en twee additionele mogelijkheden van de MIVD die kunnen worden toegepast om extraterritoriaal inlichtingen te verzamelen in het cyberdomein. Deze negen bevoegdheden van de MIVD kunnen worden uitgeoefend zonder de soevereiniteit van een staat te schenden dan wel een verboden interventie te plegen. Dus zowel het non-interventiebeginsel als het soevereiniteitsbeginsel worden niet geschonden als deze negen bevoegdheden worden uitgeoefend om extraterritoriaal inlichtingen te verzamelen in het cyberdomein. Helaas kon geen antwoord worden gevonden op de vraag of het gebruik van *malware*, bijvoorbeeld bij het binnendringen van een computer, kan worden beschouwd als een schending van het non-interventiebeginsel dan wel het soevereiniteitsbeginsel. Om een antwoord op deze vraag te krijgen dient meer onderzoek te worden verricht.

Lijst van afkortingen

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
CTIVD	Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten
ICISS	International Commission on Intervention and State Sovereignty
IGH	Internationaal Gerechtshof
IOV	Individueel Onderzoeksvoorstel
NNV	Nota naar aanleiding van het nader verslag
NSA	National Security Agency
PCIJ	Permanent Court of International Justice
PDA	Personal Digital Assistant
VN	Verenigde Naties
WIV	Wet op Inlichtingen- en Veiligheidsdiensten

Inhoudsopgave

1. Inleiding

Vandaag de dag speelt het cyberdomein een grote rol in het leven van de mens. Daar waar men vroeger veelal gebruik maakte van pen en papier, is het tegenwoordig heel gewoon om brieven te sturen via een digitaal post systeem (lees: e-mail) of om aantekeningen te maken op een computer, laptop of *tablet*. Daar waar men vroeger fysiek bij iemand langs moest gaan om contact met anderen te zoeken, is het nu heel makkelijk om bijvoorbeeld met een mobiele telefoon of door het gebruik van *social media* (via internet) contact te leggen met personen over de hele wereld. Er zit echter ook een keerzijde aan alle positieve mogelijkheden die zijn ontstaan in het cyberdomein: de mogelijkheden binnen het cyberdomein met negatieve consequenties. Een goed voorbeeld hiervan zijn cyberaanvallen.

1.1 Aanleiding

Op 28 oktober 2013 werd in het Algemeen Dagblad een tweetal artikelen gepubliceerd met betrekking tot het cyberdomein. In het eerste artikel werd vermeld dat er een *"Explosieve stijging van cyberaanvallen"* had plaatsgevonden. In 2012 waren, volgens dit krantenartikel, maar liefst zes keer zoveel cyberaanvallen uitgevoerd op computersystemen van bedrijven en overheden in Nederland dan in 2006. Ook wordt in het artikel vermeld dat de veiligheid van de staat tussen 2010 en mei 2013 tien keer in het geding is geweest.[1] De koptekst van het tweede artikel luidt: *"Cyberaanval zorgt voor grote rampen"*. Ook in dit artikel wordt duidelijk dat Nederland te maken heeft met honderden cyberaanvallen per jaar. In dit artikel wordt tevens IT-manager Ludolf Luehmann aangehaald van Shell die zegt dat cyberaanvallen onder andere mensenlevens zal (gaan) kosten.[2]

Het is krijgsmachten niet ontgaan dat de wereld in een snel tempo verandert en dat het cyberdomein een steeds grotere rol gaat spelen in het leven van de mens. Krijgsmachten zijn zich bewust van het feit dat steeds meer activiteiten zich (gaan) afspelen in het cyberdomein. Een (groot) deel van de communicatie verloopt via dit domein en vele inlichtingen worden niet meer verzameld door mensen (*Human Intelligence*), maar door systemen die gebruik maken van het cyberdomein, zoals het onderscheppen van e-mail en telefoongesprekken. Tijdens de *Concept Development and Experimentation Conference (CD&E Conference)* van het *Allied Command Transformation (ACT)* in Den Haag, werd een goed voorbeeld gegeven over mogelijke negatieve consequenties van het cyberdomein. Zo

[1] Nieuwenhuis (2013a).

[2] Nieuwenhuis (2013b).

kan bijvoorbeeld de lokale bevolking in een missiegebied al op de hoogte zijn van een aanstaande patrouille richting hun dorp, nog voordat deze patrouille fysiek ter plaatse is, omdat zij dit via bijvoorbeeld *social media* vernemen.[3] Vanwege *operational security* kan het wenselijk zijn dat de bevolking juist niet weet wanneer er een patrouille zal langskomen. Ook voor krijgsmachten zijn er dus mogelijke negatieve consequenties aan het cyberdomein te verbinden. Bovenstaand voorbeeld was slechts één van deze negatieve consequenties.

Daar in de twee bovenstaande artikelen uit het Algemeen Dagblad vaak sprake is van *hackers* of *non-state actors* die bijvoorbeeld cyberaanvallen uitvoeren, spelen staten ook een rol in het cyberdomein. Zojuist is al aangehaald dat krijgsmachten (als uitvoeringsorgaan van de staat) steeds meer gebruik maken van het cyberdomein voor communicatiedoeleinden of inlichtingendoeleinden. Dat het cyberdomein gebruikt wordt voor het vergaren van inlichtingen werd al te meer duidelijk toen klokkenluider Edward Snowden in juni 2013 een boekje open deed over de activiteiten van de *National Security Agency (NSA)*.

Zo meldt Gellman op 16 augustus 2013 in een artikel in de *Washington Post* dat de *NSA* duizenden keren de regels omtrent privacy heeft geschonden en geregeld buiten haar bevoegdheden heeft geopereerd.[4] Ook werd bekend dat de inlichtingen- en veiligheidsdiensten uit zowel de Verenigde Staten (VS) als Groot-Brittannië over de hele wereld glasvezelkabels 'afluisteren', computersystemen *hacken* en spionageactiviteiten ontplooien. Een voorbeeld hiervan is de berichtgeving omtrent het aftappen van de telefoon van de Duitse bondskanselier Angela Merkel.[5]

[3] Voorbeeld aangehaald tijdens CD&E Conferentie van ACT NATO in Den Haag 2013.

[4] Gellman (2013).

[5] De kranten *Der Spiegel* en *The Guardian* kwamen als één van de eerste naar buiten met berichten over het 'afluisteren' van glasvezelkabels, het *hacken* van computersystemen en andere spionageactiviteiten van de NSA. Deze berichten brachten zij naar buiten op basis van de documenten die zij in handen kregen via klokkenluider Edward Snowden. Op de website van *Der Spiegel* is een chronologisch overzicht te vinden met alle berichtgeving over de *NSA*: http://www.spiegel.de/international/topic/nsa_spying_scandal/. Daarnaast is op de website van *The Guardian* een pagina opgenomen met wat de uitkomsten van de hele NSA affaire betekenen voor de burger (bijvoorbeeld: het is mogelijk dat u wordt afgeluisterd door de NSA of dat uw computer is *gehackt* door de *NSA*): http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

Al met al heeft bovenstaande berichtgeving omtrent cyberaanvallen en de activiteiten van de *NSA* mijn aandacht getrokken. Door bovenstaande berichtgeving te combineren raakte ik steeds meer geïnteresseerd in wat veiligheidsdiensten en/of inlichtingendiensten allemaal mogen in het cyberdomein. Zeker de berichtgeving omtrent de *NSA* heeft bijgedragen aan de vorming van mijn onderzoeksvraag. De schending van privacyregels, welke Gellman in zijn artikel in de *Washington Post* vermeldde, duidt op een schending van nationale wetgeving. Er kwamen echter ook activiteiten aan het licht die zich in een internationaal speelveld afspeelden (bijvoorbeeld het afluisteren van Angela Merkel of het *hacken* van buitenlandse computersystemen). In dit internationale speelveld gelden internationale regels. Daar waar op nationaal niveau vaak wel duidelijk is welke activiteiten ondernomen mogen worden door een veiligheidsdienst en/of inlichtingendienst, is dit op internationaal niveau minder duidelijk. Dat is dan ook het gebied waarop dit onderzoek betrekking heeft: het internationaal recht.

1.2 Relevantie

Het verzamelen van inlichtingen (in het cyberdomein) is, na de berichtgeving over de *NSA* door klokkenluider Snowden, erg actueel. Niet alleen in de Verenigde Staten, maar ook in andere (Europese) landen is de discussie over de (inlichtingen)activiteiten van veiligheidsdiensten opgelaaid. Ook Nederland behoort tot deze landen.

1.2.1 Maatschappelijke relevantie

Hoewel Snowden zich uitliet over de *NSA* uit de Verenigde Staten, raakt het verzamelen van inlichtingen ook andere landen, waaronder Nederland. Bijna ieder persoon uit de (Nederlandse) samenleving kan doelwit zijn van inlichtingen- en veiligheidsdiensten. Daarbij kan bijvoorbeeld de vrijheid van burgers worden aangetast of kan inbreuk worden gemaakt op de privacy van de burger. Een dergelijke inbreuk kan bijvoorbeeld plaatsvinden bij het aftappen van telefoongesprekken, het monitoren van internetverkeer en vele andere (inlichtingen)activiteiten. Hoewel elke burger recht heeft op vrijheid en privacy, zijn er redenen te bedenken om hier toch inbreuk op te maken. Derhalve is het voor eenieder van belang kennis te kunnen nemen van de mogelijkheden (en bevoegdheden) van Nederlandse inlichtingen- en veiligheidsdiensten. Zo weten zij wat (in het geval van dit onderzoek) de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) mag en wanneer bijvoorbeeld het internetgedrag van een individu in de gaten mag worden gehouden (in het buitenland).

1.2.2 Wetenschappelijke relevantie

Zoals reeds vermeld is het verzamelen van inlichtingen (in het cyberdomein) erg actueel sinds klokkenluider Snowden zich uitte over de *NSA*. Het verzamelen van inlichtingen binnen de grenzen van de eigen staat is gebonden aan nationale wetten. Als inlichtingen- en veiligheidsdiensten echter inlichtingen willen verzamelen in het buitenland, krijgen zij te maken met het internationaal recht. Met dit onderzoek wil ik een bijdrage leveren aan de discussie omtrent de bevoegdheden van de MIVD. Specifiek beoog ik een bijdrage te leveren aan de discussie omtrent het extraterritoriaal uitvoeren van bevoegdheden in het cyberdomein door de MIVD in relatie tot het internationaal rechtelijke verbod op het gebruik van geweld, het non-interventiebeginsel en het soevereiniteitsbeginsel.

1.2.3 Militaire relevantie

De uitkomsten van dit onderzoek zijn op twee (militaire) niveaus relevant. Ten eerste het politiek-strategische niveau. Vanwege de actualiteit zullen velen zich afvragen wat Nederland en de Nederlandse inlichtingen- en veiligheidsdiensten allemaal voor (extraterritoriale) inlichtingenactiviteiten ontplooien. Door inzicht te geven in de mogelijkheden en bevoegdheden van de MIVD kan het politiek-strategisch niveau zich verantwoorden tegenover bijvoorbeeld de samenleving. Ten tweede zijn de uitkomsten relevant voor het niveau dat de bevoegdheden daadwerkelijk uitvoert: de medewerkers van de MIVD. Zij dienen uiteindelijk binnen de wettelijke kaders de bevoegdheden te ontplooien en inlichtingen te verzamelen.

1.3 Probleemanalyse en doelstelling

Het verzamelen van inlichtingen door inlichtingendiensten of veiligheidsdiensten kan zowel in het binnenland als in het buitenland plaatsvinden. In Nederland is de Wet op Inlichtingen- en Veiligheidsdiensten (WIV) uit 2002 het wettelijk kader waarin bevoegdheden zijn opgenomen voor het verzamelen van inlichtingen door de MIVD. Of de MIVD zich bij het verzamelen van inlichtingen in het cyberdomein houdt aan de regels, is tweeledig op te vatten. Enerzijds kan men kijken of de MIVD zich bij daadwerkelijke inlichtingenactiviteiten in het cyberdomein houdt aan de bevoegdheden die in de WIV zijn vastgelegd. Anderzijds kan men kijken of de (volgens de WIV) wettelijk toegestane (extraterritoriale) inlichtingenactiviteiten in het cyberdomein stroken met een aantal internationaal rechtelijke beginselen. Dit onderzoek richt zich op de tweede interpretatie van de gestelde vraag, waarbij de beginselen van non-interventie en soevereiniteit centraal staan.

De doelstelling van dit onderzoek is om vast te stellen waar het verzamelen van inlichtingen in het cyberdomein wordt begrensd door het internationaal recht, door de volgens de WIV 2002 toegestane bevoegdheden van de MIVD in het cyberdomein te onderwerpen aan de internationaalrechtelijke beginselen van non-interventie en soevereiniteit. De centrale vraag die ik wil beantwoorden in dit onderzoek is welke mogelijkheden de MIVD heeft, op basis van de bevoegdheden die in de WIV 2002 zijn vastgelegd, voor het extraterritoriaal verzamelen van inlichtingen in het cyberdomein, binnen de grenzen van het internationaal recht.

1.4 Aannames, beperkingen en definities

Alvorens de aannames en beperkingen te behandelen verdient de zinsnede '*voor het extraterritoriaal verzamelen van inlichtingen in het cyberdomein'* enige uitleg. De uitgangssituatie in dit onderzoek betreft twee soevereine staten (staat X en staat Y), welke beide lid zijn van de Verenigde Naties (VN). Deze twee staten bevinden zich niet in een onderling (militair) conflict: er heerst vrede tussen hen. Toch wil staat X bepaalde informatie hebben die in staat Y aanwezig is. Over dergelijke activiteiten hebben beiden staten geen onderlinge overeenkomst (bijvoorbeeld in de vorm van een bilateraal verdrag, *Memorandum of Understanding*, of *Status Of Forces Agreement*) afgesloten. Staat X wil de informatie bemachtigen door gebruik te maken van het cyberdomein (dus zonder het fysiek ontplooien van troepen over de grens). Deze vorm van het verzamelen van informatie (gegevens) wordt in dit onderzoek 'het digitaal verzamelen van inlichtingen in het buitenland' of het 'extraterritoriaal verzamelen van inlichtingen in het cyberdomein' genoemd.

In relatie tot de zojuist geciteerde zinsnede, speelt ook een definitiekwestie. Tot dusver is gesproken over het (extraterritoriaal) verzamelen van inlichtingen (in het cyberdomein). Inlichtingen worden echter niet verzameld. Er worden gegevens (of informatie) verzameld, zoals ook blijkt uit de terminologie van artikel 17 van de WIV.[6] Na het verzamelen volgt een analyseslag van de gegevens (of informatie) door deskundigen. Na deze analyse kan gesproken worden over inlichtingen. Gemakshalve worden de termen in dit onderzoek door elkaar gebruikt. Met alle drie wordt overigens hetzelfde bedoeld: het verzamelen van gegevens (dan wel informatie) waarover nog geen analyseslag heeft plaatsgevonden.

[6] Artikel 17 van de wet van 7 februari 2002, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2002), *Stb.* 2002, 148.

Dan volgen nu de aannames en beperkingen. In de doelstelling en centrale vraag komen reeds een aantal aannames en beperkingen naar voren. Ten eerste gaat het, gezien het korte tijdsbestek waarin dit onderzoek afgerond dient te worden, te ver om te kijken naar veiligheidsdiensten en/of inlichtingendiensten van andere landen. Ook gaat het te ver om andere Nederlandse veiligheidsdiensten en/of inlichtingendiensten te onderzoeken (lees: de Algemene Inlichtingen- en Veiligheidsdienst –AIVD–). Daarom beperkt dit onderzoek zich slechts tot de Nederlandse Militaire Inlichtingen- en Veiligheidsdienst. Tevens zal niet het gehele internationale recht worden onderzocht: daar is het veel te omvangrijk voor. Aangezien het onderzoek gaat over extraterritoriale inlichtingenactiviteiten in het cyberdomein, richt ik mij in dit onderzoek op een aantal beginselen binnen het internationaal recht die mogelijk een conflict opleveren met deze extraterritoriale inlichtingenactiviteiten.

Deze internationaalrechtelijke beginselen zijn beperkt tot een tweetal beginselen die (direct of indirect) zijn af te leiden uit het Handvest van de Verenigde Naties (VN Handvest), te weten het non-interventiebeginsel en het soevereiniteitsbeginsel. Tevens hebben deze twee beginselen een gewoonterechtelijke status, wat inhoudt dat ook staten die het VN Handvest niet aanvaarden (en dus geen lid zijn van de VN), tóch gebonden zijn aan deze regels. Dit geldt eveneens voor het geweldsverbod, dat is vastgelegd in artikel 2, lid 4 van het Handvest van de Verenigde Naties: *“All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”*.[7] Het internationaalrechtelijke geweldsverbod zal, onder andere omwille van de omvang van dit onderzoek, worden uitgesloten van het onderzoek. De tweede reden om het geweldsverbod uit te sluiten van dit onderzoek is dat het louter (extraterritoriaal) verzamelen van inlichtingen (in het cyberdomein) doorgaans geen fysiek geweld zal opleveren.

Naast bovenstaande, zelf geïnitieerde, aannames en beperkingen is er nog een laatste beperking die voortkomt uit externe factoren. Helaas werd geen toegang verleend tot daadwerkelijke operaties van de MIVD omdat dit de *modus operandi* dan wel het (huidige) kennisniveau van de MIVD zou (kunnen) prijsgeven. Derhalve komen de mogelijkheden die in dit onderzoek worden besproken (met betrekking tot de nieuwe (cyber)middelen die kunnen worden gebruikt bij de uitoefening van de bijzondere bevoegdheden) voort uit een eigen analyse.

[7] Article 2 of the Charter of the United Nations.

1.5 Rapportage

Gezien de doelstelling van dit onderzoek, kunnen de uitkomsten van dit onderzoek van belang zijn voor zowel de MIVD als de politiek. Ten eerste zullen de uitkomsten van dit onderzoek een beeld scheppen over de extraterritoriale inlichtingenactiviteiten in het cyberdomein in relatie tot de twee genoemde beginselen. Daarnaast worden de bevoegdheden van de MIVD, zoals deze zijn vastgelegd in de WIV, bezien in het kader van het cyberdomein. Wellicht dat de uitkomsten van dit onderzoek bij kunnen dragen aan een antwoord op de vraag of de WIV 2002 nog voldoet aan de huidige eisen die gesteld worden aan het inlichtingenapparaat van de krijgsmacht. Misschien kan hier voordeel uit behaald worden door de MIVD en/of de politiek bij het eventueel herzien en/of herformuleren van de WIV. Daarnaast kan de politiek de uitkomsten van dit onderzoek gebruiken om zich over de inlichtingenactiviteiten van de MIVD te verantwoorden tegenover bijvoorbeeld de samenleving.

1.6 Deelvragen en opbouw

Om uiteindelijk een antwoord te kunnen formuleren op de gestelde centrale vraag, is een drietal deelvragen opgesteld. Elk van de deelvragen zal een deel van de onderzoeksvraag beantwoorden. Na de inleiding, hoofdstuk één, wordt in hoofdstuk twee de eerste deelvraag behandeld. De eerste deelvraag luidt: “Hoe begrenst het internationaal recht het verzamelen van inlichtingen in het cyberdomein?”. Om deze deelvraag te beantwoorden wordt gekeken naar het Handvest van de VN. Uit dit Handvest zijn (direct of indirect) een drietal beginselen af te leiden waarmee het verzamelen van inlichtingen in conflict kan komen: het geweldsverbod, het non-interventiebeginsel en het soevereiniteitsbeginsel. Zoals reeds vermeld bij de aannames en beperkingen, zal in dit onderzoek slechts worden stilgestaan bij het non-interventiebeginsel en het soevereiniteitsbeginsel.

Vervolgens zal in hoofdstuk drie de tweede deelvraag van dit onderzoek worden beantwoord. De tweede deelvraag in dit onderzoek luidt als volgt: “In hoeverre is de Wet op Inlichtingen- en Veiligheidsdiensten 2002 geldig in het buitenland?”. Hiermee wordt nader onderzocht of de MIVD de in de WIV toegestane inlichtingenactiviteiten in het cyberdomein ook mag uitvoeren in het buitenland. Bij de beantwoording van deze vraag zal niet alleen worden gekeken naar de WIV zelf, maar ook naar de wetsgeschiedenis (waaronder de memorie van toelichting) bij deze wet. Daarnaast zal worden gekeken naar hoe experts of autoriteiten op dit gebied naar de WIV kijken en deze interpreteren met betrekking tot toegestane (extraterritoriale) inlichtingenactiviteiten in het cyberdomein.

In hoofdstuk vier komt de derde deelvraag aan bod: “Welke bevoegdheden heeft de Militaire Inlichtingen- en Veiligheidsdienst, op basis van de Wet op Inlichtingen- en Veiligheidsdiensten (WIV) 2002, voor het verzamelen van inlichtingen in het cyberdomein?”. Net als bij de tweede deelvraag, zal bij de derde deelvraag, naast de wetstekst zelf, ook worden stilgestaan bij de wetsgeschiedenis en de zienswijzen van experts en autoriteiten op dit gebied.

Per hoofdstuk zal een subconclusie volgen met een antwoord op de gestelde deelvraag in dat hoofdstuk. Alle antwoorden op de deelvragen vormen tezamen een antwoord op de onderzoeksvraag. De onderzoeksvraag over welke mogelijkheden de MIVD heeft, op basis van de bevoegdheden die in de WIV 2002 zijn vastgelegd, voor het extraterritoriaal verzamelen van inlichtingen in het cyberdomein, binnen de grenzen van het internationaal recht, zal in het laatste hoofdstuk, de conclusie, beantwoord worden door alle antwoorden op de deelvragen te combineren.

2. Begrenzing internationaal recht

Het recht is een erg breed domein en binnen het recht zijn vele (twee)delingen te maken. Eén van deze tweedelingen is de scheiding tussen nationaal recht en internationaal recht, welke beiden weer onderverdeeld kunnen worden. Dit hoofdstuk richt zich op het internationaal recht. De deelvraag die in dit hoofdstuk zal worden beantwoord luidt: “Hoe begrenst het internationaal recht het verzamelen van inlichtingen in het cyberdomein?”.

Om deze deelvraag te beantwoorden zal eerst kort worden stilgestaan bij de verschillende rechtsbronnen (zoals het verdragenrecht en het gewoonterecht) en bij de primaire subjecten binnen de internationale rechtsorde. Daarna zal achtereenvolgens worden ingegaan op het non-interventiebeginsel en het soevereiniteitsbeginsel. Voor beide beginselen wordt de reikwijdte van het beginsel behandeld. Ook wordt voor beide beginselen een omschrijving gegeven en wordt uiteengezet wanneer een schending van de beginselen optreedt. Voor het non-interventiebeginsel zullen tevens de uitzonderingen worden besproken.

2.1 Inleiding

Binnen het internationaal recht is er een verscheidenheid aan rechtsbronnen. De primaire bronnen binnen het internationaal recht zijn gewoonterecht en verdragen.[8] Voor verdragen worden verschillende synoniemen gebruikt die juridisch niet van elkaar verschillen. Zo wordt ook gesproken over conventies, handvesten, statuten en protocollen. Naast verdragen en het gewoonterecht zijn er nog een aantal andere rechtsbronnen. De belangrijksten van deze secundaire rechtsbronnen zijn de algemene rechtsbeginselen en de rechtspraak (door bijvoorbeeld een tribunaal).[9]

Staten zijn de primaire subjecten binnen de internationale rechtsorde. Verdragen worden bijvoorbeeld uitsluitend door staten ondertekend en geratificeerd. Een staat kan dan ook niet gebonden worden aan een regel binnen het internationaal recht zonder daar zelf, als staat, mee in te stemmen.[10] Is een staat het niet eens met een bepaald verdrag? Dan tekent en/of ratificeert die staat het verdrag niet en kan daarmee (zoals zojuist aangegeven) niet gebonden worden aan de regels die in dat verdrag staan.

[8] Article 29 of the Statute of the International Court of Justice.

[9] Cogen (2003), p. 1-2.

[10] Nollkaemper (2011), p. 51, p. 178.

Voor wat betreft gewoonterecht ligt het iets gecompliceerder, aangezien gewoonterecht niet zwart op wit is vastgelegd. Is een staat het niet eens met gewoonterecht dat gevormd wordt, dan zal de betreffende staat dat moeten laten blijken tijdens de periode waarin het gewoonterecht gevormd wordt. Dat kan de staat doen door dusdanig te handelen, dat uit de handelingen duidelijk blijkt dat de staat het niet eens is met de regel die gewoonterechtelijk gevormd wordt. De staat treedt dan op als *persistent objector*: een staat die het niet eens is met het gewoonterecht dat gevormd wordt. Doet een staat dit niet? Dan geldt het gevormde gewoonterecht ook voor die staat.[11] Belangrijk om te vermelden is dat bepaalde regels die in verdragen worden vastgelegd, tevens gelden als internationaal gewoonterecht. Staten die het verdrag niet hebben getekend, worden dan nog steeds geacht zich aan de regel te houden (mits zij geen *persistent objector* zijn).[12]

Het verdrag waar de meeste staten mee akkoord zijn gegaan is het VN Handvest. Thans zijn 193 staten lid van VN.[13] In het Handvest van de VN staan een aantal regels, beginselen, die een uitkomst kunnen bieden op de vraag hoe het internationaal recht het verzamelen van inlichtingen in het cyberdomein begrenst. Een tweetal beginselen zal worden besproken: het non-interventiebeginsel en het soevereiniteitsbeginsel. Er is gekozen om deze twee beginselen te behandelen, omdat het extraterritoriaal verzamelen van inlichtingen (in het cyberdomein) mogelijk conflicten oplevert met deze twee beginselen.

2.2 Non-interventiebeginsel

Hoewel niet nader wordt ingegaan op het geweldsverbod, staat het geweldsverbod wel in relatie tot het non-interventiebeginsel.[14] Zoals uit de bewoording van artikel 2, lid 4 uit het VN Handvest is af te leiden, is het verboden met geweld de territoriale integriteit en de politieke onafhankelijkheid van een staat te schenden. Het hebben van een territoir is één van de drie eigenschappen waarover een entiteit moet beschikken om zichzelf een staat te kunnen noemen. Het territoir van een staat wordt afgebakend door grenzen (*borders*). Alles binnen

[11] Nollkaemper (2011), p. 188-189.

[12] Article 38 of the Vienna Convention of the law of treaties.

[13] Verenigde Naties (2014), via http://www.un.org/en/members/index.shtml#text.

[14] Jamnejad & Wood (2009), p. 380.

die grenzen is dus territoir van een bepaalde staat.[15] Het schenden van deze grenzen levert dan ook een schending van de territoriale integriteit van die staat op en is in strijd met het non-interventiebeginsel, want: *"A condition of any one state's sovereignty is a corresponding obligation to respect every other state's sovereignty: the norm of non-intervention is enshrined in Article 2.7 of the UN Charter. A sovereign state is empowered in international law to exercise exclusive and total jurisdiction within its territorial borders. Other states have the corresponding duty not to intervene in the internal affairs of a sovereign state.".*[16]

2.2.1 Omschrijving

Uit bovenstaand citaat is af te leiden dat ook in het Handvest van de VN een bepaling is opgenomen met betrekking tot het niet mogen interveniëren in nationale (interne) aangelegenheden van andere staten. Deze bepaling is vastgelegd in artikel 2, lid 7 van het Handvest. In dit artikel staat vermeld dat: *"Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII.".*[17]

Daarnaast zijn er nog een aantal andere bronnen waaruit een omschrijving van het non-interventiebeginsel volgt. Eén van deze bronnen is het *Permanent Court of International Justice (PCIJ)*, dat in 1927 tijdens de *Lotuse case* stelt dat: *"the territorial principle, accordance to which each nation has dominion over its territory and – on the other hand - has no authority to interfere in any way in matters taking place on the territories of other nations.*".[18] Ook het Internationaal Gerechtshof (IGH) doet meerdere malen uitspraken over interventies. De twee meest bekende *cases* zijn de zogeheten *Corfu Channel case* en de *Nicaragua case*.

[15] Holsti (2004), p. 95.

[16] International Commission on Intervention and State Sovereignty (2001), p. 12.

[17] Article 2 of the Charter of the United Nations.

[18] Judgment Lotus case (1927), para. 212.

In de *Corfu Channel case* van 1949 stelt het IGH dat: *"The Court can only regard the alleged right of intervention* [to secure possession of evidence in the territory of another State, in order to submit it to an international tribunal and thus facilitate its task] *as the manifestation of a policy of force, such .as has, in the past, given rise to most serious abuses and such as cannot, whatever be the present defects in international organization, find a place in international law."*.[19]

Daarnaast stelt het IGH in 1986, tijdens de *Nicaragua case*, dat: *"The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference…Expressions of an opinio juris of States regarding the existence of this principle are numerous".*[20] Het Internationaal Gerechtshof vervolgt met: *"In this respect it notes that, in view of generally accepted formulations, the principle forbids all States or groups of States to intervene directly or indirectly in the internal or external affairs of other States.*".[21]

Tevens zijn er een aantal schrijvers die een definitie of omschrijving geven van het non-interventiebeginsel. Bijvoorbeeld Holsti die zegt dat: *"no outside party has the right to interfere in its domestic affairs.".*[22] Of Krasner die beweert dat: *"No state has the right to intervene in the internal affairs of another.".*[23] Jamnejad en Wood stellen in hun artikel *Current Legal Developments* meerdere malen dat er sprake is van een interventie als dit gebeurt onder dwang (*coercion*) en als er met de inmenging een beleidsverandering in de andere staat wordt beoogd.[24] Daarbij benadrukken zij dat het dwangelement aanwezig moet zijn om het non-interventiebeginsel te schenden, omdat anders *"any act which had an effect on another state could fall within the prohibition.".*[25]

---

[19] Judgment Corfu Channel case (1949), p. 45-35.

[20] Judgment Nicaragua case (1986), p. 106-107 (para. 202).

[21] Judgment Nicaragua case (1986), p. 108 (para. 205).

[22] Holsti (2004), p. 152.

[23] Krasner (2001), p. 21.

[24] Jamnejad & Wood (2009), p. 347-348, p. 371.

[25] Jamnejad & Wood (2009), p. 382.

Ook het IGH geeft duidelijk aan wanneer er sprake is van een verboden interventie: *"Intervention is wrongful when it uses methods of coercion regard such choices* [vrije keuze voor een politiek, economisch, sociaal en cultureel systeem]*, which must remains free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention".*[26] Ook het Internationaal Gerechtshof haalt zowel het dwangelement als de beoogde beleidsverandering aan.

In relatie tot het cyberdomein stelt Gill dat: *"'cyber intervention' will be defined as coercive cyber activity… falling below the threshold of a use of force amounting to an armed attack, which is intended to (or has the effect of) violate a State's sovereignty by preventing it from carrying out State functions, and/or preventing it from exercising activities or making choices which it is entitled to engage in or make under international law."*.[27]

2.2.2 Schending

Nu is duidelijk wat er onder het non-interventiebeginsel wordt verstaan en wanneer er sprake is van een verboden interventie. Hoe staat dat echter met activiteiten in het cyberdomein? Levert het extraterritoriaal verzamelen van inlichtingen in het cyberdomein een mogelijke schending van het non-interventiebeginsel op? Volgens Gill niet, mits geen specifieke regels binnen het internationaal recht worden geschonden. Want, zo stelt hij: *"in the absence of such acts, the obtaining of information in itself falls short of coercive or dictatorial interference, and would not constitute 'intervention' in the legal sense.".*[28] Later in dezelfde bijdrage herhaalt Gill nog eens zijn standpunt dat het verzamelen van informatie uit digitale bronnen, in de meeste gevallen, geen interventie oplevert: *"acts constituting illegal interference which lack the element of coerciveness necessary to constitute 'intervention', such as engaging in espionage consisting wholly of (illegally) obtaining and monitoring information from digital sources from foreign governments, corporations or private individuals, would not, in most cases, constitute 'intervention'.".*[29]

[26] Judgment Nicaragua case (1986), p. 108 (para. 205).

[27] Gill (2013), p. 218.

[28] Gill (2013), p. 224.

[29] Gill (2013), p. 232.

Ook Ziolkowski vindt dat het verzamelen van informatie in het cyberdomein geen interventie oplevert. Zij stelt namelijk dat *"A forbidden intervention in domestic affairs requires the element of coercion of the other State. Scholars assert that illegal coercion implies massive influence, inducing the affected State to adopt a decision with regard to its policy or practice which it would not entertain as a free and sovereign State. It is clear that clandestine information gathering as such will not fulfill this requirements."*.[30] Tot slot stelt de *International Group of Experts*, welke in 2013 de zogeheten *Tallinn Manual* schreef, dat het binnendringen van een systeem van een andere staat het non-interventiebeginsel niet schendt: *"It follows that cyber espionage and cyber exploitation operations lacking a coercive element do not per se violate the non-intervention norm principle. Mere intrusions into another State's systems does not violate the non-intervention principle. In the view of the International Group of Experts, this holds true even where such intrusions requires the breaching of protective virtual barriers (e.g., the breaching of firewalls or the cracking of passwords)."*.[31]

2.2.3 Uitzonderingen

De bepaling uit artikel 2, lid 7 van het VN Handvest geeft staten echter geen vrijbrief om te doen en laten wat staten willen. Er zijn namelijk drie mogelijkheden waarop toch geïntervenieerd kan worden. Uit artikel 2, lid 7 blijkt dit al: er wordt geen afbreuk gedaan aan de dwangmaatregelen uit hoofdstuk 7 van het VN Handvest.[32] Hoofdstuk 7 betreft de artikelen 39 tot en met 51, waarin verschillende dwangmaatregelen worden genoemd die de VN kan treffen. Deze dwangmaatregelen variëren van diplomatieke-, tot economische sancties tot het gebruik van geweld. Over het algemeen worden de uitzonderingen in tweeën verdeeld: de ene uitzondering betreft een interventie met toestemming van de Veiligheidsraad van de VN. De Veiligheidsraad van de VN dient in een dergelijk geval een resolutie aan te nemen waarin expliciet is opgenomen dat er bepaalde handelingen ondernomen mogen worden door andere lidstaten om (één van) de doelstellingen van de VN na te leven.

[30] Ziolkowski (2013b), p. 433.

[31] Tallinn Manual (2013), p. 44.

[32] Burci (1996), p. 245.

De tweede uitzondering wordt genoemd in artikel 51 en betreft het inherente recht op individuele of collectieve zelfverdediging: *"Nothing in the present Charter shall impair the inherent right of individual or collective selfdefense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of selfdefense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."*.[33] Bij het uitoefenen van de zelfverdediging is het staten tevens toegestaan geweld te gebruiken. Indien mogelijk, niet alleen bij zelfverdediging, maar bij elk conflict tussen staten, hebben geweldloze oplossingen de voorkeur.

Alvorens een staat een beroep kan doen op zelfverdediging moet aan een aantal voorwaarden worden voldaan. Als niet aan deze voorwaarden wordt voldaan, is het gebruik van geweld niet aan te merken als zelfverdediging en dus in strijd met het VN Handvest. Eén van de voorwaarden waaraan zelfverdediging moet voldoen is dat er sprake moet zijn van een gewapende aanval: *"Self-defense under the Charter is a justifiable act of force undertaken by a state that is the victim of an armed attack or by the allies of an attacked state acting in its defense."*.[34] De reikwijdte van het recht op zelfverdediging is onderwerp van discussie. Inmiddels wordt het (preëmptieve) recht op zelfverdediging ook geaccepteerd als er aan de zogenaamde *Caroline*-criteria wordt voldaan: *"instant, overwhelming, and leaving no choice of means, and no moment for deliberation."*.[35] Het gaat te ver voor dit onderzoek om deze uitzondering nog uitgebreider te behandelen.

Naast de twee uitzonderingen die in het VN Handvest worden genoemd, is er nog een derde mogelijkheid waarop een staat in een andere staat kan interveniëren. De betreffende staat dient dan zelf hulp te vragen aan een andere staat (of aan meerdere andere staten). Vaak wordt dit een interventie met toestemming van de gaststaat genoemd, men spreekt ook wel van *consent*. Aangezien de staat waar het conflict zich afspeelt het eens is met de buitenlandse troepenmacht, kan niet worden gesproken van een schending van het non-interventiebeginsel.

[33] Article 51 of the Charter of the United Nations.

[34] Barkham (2001), p.74.

[35] Brief van Mr Webster naar Lord Ashburton, geciteerd in Lubell (2010), p. 44.

2.2.4 Reikwijdte

Er bestaan verschillende meningen over de reikwijdte van het non-interventiebeginsel. Een aantal voorbeelden van (typen) interventies die door sommige staten als legitiem worden gezien zijn interventies voor het verspreiden van de democratie, interventies om zelfbeschikking te bewerkstelligen voor een bepaalde groep mensen[36] en interventies om mensenrechten te beschermen (humanitaire interventies).[37] Vooral deze laatste vorm van interveniëren is de laatste decennia, na het einde van de Koude Oorlog, in opspraak geraakt.[38] Volgens voorstanders zijn humanitaire interventies toegestaan omdat deze niet indruisen tegen de doelen van de VN. Tegenstanders stellen daarentegen dat het non-interventiebeginsel absoluut is en er louter geïntervenieerd mag worden op één van de drie bovenstaande manieren.[39] Een toename in voorstanders zorgt ervoor dat de Veiligheidsraad zijn invloed, met betrekking tot het uitvoeren van interventies, aan het verliezen is.[40]

Desalniettemin bestaat het beginsel nog steeds binnen het international recht.[41] De *International Commission on Intervention and State Sovereignty (ICISS)* stelt: *"But all that said, the many examples of intervention in actual state practice throughout the 20th century did not lead to an abandonment of the norm of non-intervention."*.[42] Tevens wil een schending van de norm, de schending van een bepaald beginsel, niet meteen zeggen dat die norm, of dat beginsel, niet meer geldt of overbodig is. Tot slot kan worden gesteld dat er (nog) geen verandering van de norm van non-interventie heeft plaatsgevonden, aangezien nog geen enkele regering beweert dat er een recht op interventie bestaat. Ook volgens Kohen is er in de afgelopen vijfentwintig jaar, die verstreken zijn na de uitspraak van het IGH met betrekking tot de *Nicaragua case*, geen verandering opgetreden in het non-interventiebeginsel: "*What has happened over the course of the last 25 years has not altered the conclusions reached by the court with regard to the principle of non-intervention."*.[43]

---

[36] Hensel (2004), p. 39-40.

[37] Holsti (2004), p. 142; McCorquodale (1996), p. 21.

[38] Canefe (1996), p. 91.

[39] Jamnejad & Wood (2009), p. 360.

[40] Wolfrum (2002), p. 110; Kohen (2012), p. 157, 162-164.

[41] Jamnejad & Wood (2009), p. 380.

[42] International Commission on Intervention and State Sovereignty (2001), p. 12.

[43] Kohen (2012), p. 164.

Dus zelfs in 2011, vijfentwintig jaar na de uitspraak van het IGH in de Nicaragua casus, staat het non-interventiebeginsel nog steeds en is er volgens Kohen nog steeds geen ruimte voor humanitaire interventies. Wel dient vermeld te worden, dat er toch humanitaire interventies plaats kunnen vinden. Situaties waarin bijvoorbeeld mensenrechten worden geschonden, kunnen namelijk door de Veiligheidsraad van de VN worden aangemerkt als een bedreiging of schending van de vrede, zoals vastgelegd in artikel 39 van het VN Handvest.[44] Dit stelt de Veiligheidsraad van de VN in staat om een resolutie aan te nemen om deze bedreiging of schending van de vrede te herstellen. De reeds in dit onderzoek aangehaalde bevoegdheden die zijn vastgelegd in de artikelen uit hoofdstuk 7 van het Handvest mogen daarvoor gebruikt worden, inclusief het (met geweld) interveniëren in een andere staat.

2.3 Soevereiniteitsbeginsel

Naast de relatie tussen het geweldsverbod en het non-interventiebeginsel, bestaat er ook een relatie tussen het soevereiniteitsbeginsel en het non-interventiebeginsel: *"… for any inroads made on state sovereignty indicate that to a greater or lesser degree, the non-intervention norm has been violated."*.[45] Ook Vincent haalt de verbondenheid tussen beiden beginselen aan: *"The principle of non-intervention identifies the right of states to sovereignty as a standard in international society and makes explicit the respect required for it in abstention from intervention."*.[46] Deze twee beginselen kunnen dan ook moeilijk los van elkaar worden gezien. Dat vindt ook Cronin: *"As such, sovereignty carries within it the fundamental rights of territorial integrity, non-intervention and autonomy in making political decisions."*.[47]

[44] Holsti (2004), p. 141-142, p. 159-163; Philpott (2001), p. 42.

[45] Thomas (1985), p. 11.

[46] Geciteerd in: Thomas (1985), p. 16.

[47] Cronin (2002), p. 149.

Daar waar het non-interventiebeginsel direct is af te leiden uit het VN Handvest, is het soevereiniteitsbeginsel niet letterlijk terug te vinden in het VN Handvest. Desalniettemin bevat artikel 2, lid 1, volgens Thomas, twee ideeën: *"that of state sovereignty, and that of sovereign equality."*.[48] Elke staat is in juridisch opzicht gelijk, ongeacht de grootte van het territoir, het economisch vermogen, het aantal inwoners, de welvaart in de staat of welke andere eigenschap van een staat dan ook. Toch is het niet altijd even duidelijk wat soevereiniteit nu precies is en is het begrip soevereiniteit onderhevig geweest aan veranderingen: *"The understanding of sovereignty has undergone changes since its formal establishment in the Peace of Westphalia in 1648."*.[49] Daarnaast wordt het begrip op verschillende manieren gebruikt.[50] Zo onderscheidt Krasner maarliefst vier manieren waarin soevereiniteit wordt gebruikt: "*international legal sovereignty, Westphalian sovereignty, domestic sovereignty, and interdependence sovereignty."*.[51]

2.3.1 Omschrijving

Het meest gangbare onderscheid dat wordt gemaakt binnen soevereiniteit is het verschil tussen interne- en externe soevereiniteit. Mostov onderzoekt bijvoorbeeld *"the distinction between external and internal sovereignty."*.[52] Ook Dinstein spreekt (indirect) over interne- en externe soevereinitiet: *"As far as the internal structure of the state is concerned, the theory of sovereignty –in the sense of supreme power (summa potestas)- ..."* Een aantal zinnen later vervolgt hij: *"In the context of international law, sovereignty is understood to be an attribute of the state as a member of the international community."*.[53]

[48] Thomas (1985), p. 47.

[49] Ziolkowski (2013a), p. 156.

[50] Dinstein (2005b), p. 111.

[51] Krasner (1999), p. 3, p. 9.

[52] Mostov (2008), p. 19.

[53] Dinstein (2005b), p. 111.

De *ICISS* verstaat onder interne soevereiniteit het volgende: *"Internally, sovereignty signifies the capacity to make authoritative decisions with regard to the people and resources within the territory of the state".*[54] Krasner verwoordt interne soevereiniteit als de *"exclusive control within a given territory".*[55] Ook Philpott geeft een dergelijke omschrijving: hij omschrijft interne soevereiniteit als de *"supreme authority within a territory".*[56] Dit licht hij nader toe, door alle delen van deze brede definitie, *supreme, authority* en *territoriality*, nader te omschrijven. Fleck spreekt over nationale soevereiniteit en omschrijft interne soevereiniteit ongeveer hetzelfde: *"National sovereignty is characterized by an exclusive power of a state on its territory.".*[57] Keren en Sylvan kennen eenzelfde soort definitie toe aan het begrip interne soevereiniteit: *" a nation's right to exercise its own law and practice over its territory".*[58] Het komt er in alle omschrijvingen en definities op neer dat de staat het oppergezag (*control, authority, power*) heeft binnen de grenzen van de staat (*territory*).

Naast interne-, is er ook externe- of staatssoevereiniteit. De *International Group of Experts,* die de *Tallinn Manual* schreef, stelt dat: *"The accepted definition of 'sovereignty' was set forth in the Island of Palmas Arbitral Award of 1928. It provides that 'Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion any other State, the functions of a State.'".*[59] Krasner omschrijft staatssoevereiniteit als: *"In the contemporary world, sovereignty primarily has been linked with the idea that states are autonomous and independent from each other… More recently, sovereignty has come to be associated with the idea of control over transborder movements… Finally, sovereignty has meant that political authorities can enter into international agreements. They are free to endorse any contract they find attractive. Any treaty among states is legitimate provided that it has not been coerced.".*[60]

---

[54] International Commission on Intervention and State Sovereignty (2001), p. 13.

[55] Krasner (2001), p. 26.

[56] Philpott (2001), p. 16.

[57] Fleck (2005), p. 53.

[58] Keren & Sylvan (2002), p. ix.

[59] Tallinn Manual (2013), p. 16.

[60] Krasner (2001), p. 21.

Vooral de laatste zin van bovenstaand citaat wordt door andere schrijvers vaak benadrukt. Elke staat is vrij in de keuzes die de staat maakt. Daarnaast kan een staat pas gebonden worden aan een bepaalde afspraak als de staat daarover een overeenkomst (bijvoorbeeld in de vorm van een verdrag) heeft afgesloten.[61] Het IGH haalt tevens aan dat *"matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy."*.[62]

In dit onderzoek zal voornamelijk worden stilgestaan bij de externe soevereiniteit, aangezien er wordt gekeken naar extraterritoriale inlichtingenactiviteiten. Het betreft, bij het uitvoeren van deze activiteiten, een relatie tussen staten, niet de relatie(s) binnen een staat. Uit alle omschrijvingen en definities van externe soevereiniteit die in deze paragraaf zijn behandeld is een nieuwe omschrijving gevormd: de staat is autonoom en (politiek) onafhankelijk van andere staten en de staat is vrij, zonder inmenging van andere staten, in het maken van zijn eigen keuzes, inclusief het vormen van buitenlands beleid. In het vervolg van dit onderzoek zal bovenstaande omschrijving voor externe- dan wel staatssoevereiniteit worden gehanteerd.

Naast alle genoemde definities en omschrijvingen van onder andere het begrip externe soevereiniteit, stelt Simpson dat: *"While the interpretation of nonintervention, sovereignty, or domestic jurisdiction may differ, the core principle remains the same – the sanctity of the state."*.[63] Simpson raakt hier de kern van het soevereiniteitsprobleem als men spreekt over het extraterritoriaal verzamelen van inlichtingen: de onschendbaarheid (*sanctity*) van de staat enerzijds en de mogelijkheid tot het verzamelen van inlichtingen in het buitenland anderzijds. Wanneer is nu sprake van een schending van de soevereiniteit?

[61] Nollkaemper (2011), p. 178.

[62] Judgment Nicaragua case (1986), p. 108 (para. 205).

[63] Simpson (1996), p. 36.

2.3.2 Schending

Ziolkowski stelt dat: *"Territorial sovereignty is violated by any acts causing physical effects on another State's territory.".* Daarnaast stelt zij dat de *"disruption of networks and systems"* zonder fysieke schade ook een schending van de soevereiniteit kunnen opleveren.[64] Verder zijn staten volgens Ziolkowski, op specifieke uitzonderingen na, vrij om in vredestijd, met welke middelen dan ook, extraterritoriaal gegevens te verzamelen (via het cyberdomein): *"In consequence, States are – in general, and apart from a few specific limitations – free to conduct peacetime espionage activities, by whatever means they choose".*[65]

Zelf gaat Ziolkoswki niet verder in op de specifieke beperkingen. Gill zegt daar wel iets over. Gill stelt namelijk dat het onderscheppen dan wel opslaan van overheidscommunicatie, of andere gegevens die onder het internationaal recht worden beschermd, een schending van het non-interventiebeginsel én het soevereiniteitsbeginsel oplevert.[66]

Naast Gill, beweert ook Pirker iets over het verzamelen van informatie. Pirker gaat in op het verzamelen van informatie door het binnendringen van computersystemen: *"Intrusions into the computer systems of another State could be undertaken to gain valuable information or to manipulate data. International law generally does not regulate and thus does not prohibit espionage.".*[67] Een aantal pagina's later herhaalt hij dit standpunt nogmaals en voegt hij daaraan toe dat het ook is toegestaan om bepaalde beschermingsmaatregelen te omzeilen: *"intrusions into foreign computer systems are thus not per se prohibited, espionage being also a very common practice among States. This finding remains unchanged even where protective barriers such as passwords or firewalls have to be overcome for the purpose of espionage.".*[68]

---

[64] Ziolkowski (2013a), p. 163.

[65] Ziolkowski (2013b), p. 462.

[66] Gill stelt dat: "*This* [conducting espionage on foreign States and their citizens] *may well violate the domestic law of the States concerned and, in some cases, constitute not only an arguably unfriendly act, but one which violates the targeted State's sovereignty, in so far as it involves intercepting governmental communications, or those which are otherwise protected under international law… However, such data retrieval and surveillance does not, in itself, constitute 'intervention' in the sense of coercive interference, except possibly in the situation that governmental offices or diplomatic premises are violated or diplomatically protected communications are intercepted and stored."* Zie Gill (2013), p. 225.

[67] Pirker (2013), p. 191.

[68] Pirker (2013), p. 202.

In een ander hoofdstuk uit *Peacetime Regime for State Activities in Cyberspace* gaat Ziolkowski wel in op een mogelijke specifieke beperking ten aanzien van het in vredestijd verzamelen van informatie op computers van een andere staat: *"With regard to 'cyber intrusions' into IT-systems or computer networks physically located on another State's territory or area under its exclusive jurisdiction, a violation of the territorial sovereignty of the target State is thinkable in terms of an 'exercise of jurisdiction' by a representative of a foreign state (but not the mere 'virtual trespass')."*.[69] Een schending van de soevereiniteit kan volgens Ziolkowski dus optreden als er, bij het binnendringen van IT-systemen, handhavende rechtsmacht wordt uitgeoefend. Indien louter toegang wordt verschaft tot het IT-systeem wordt geen handhavende rechtsmacht uitgevoerd en wordt de soevereiniteit niet dus niet geschonden.

Nu duidelijk is wat er (in dit onderzoek) onder het non-interventiebeginsel en het soevereiniteitsbeginsel wordt verstaan, duidelijk is wanneer deze beginselen worden geschonden en duidelijk is wat de reikwijdte van beide beginselen is (voor het extraterritoriaal verzamelen van inlichtingen in het cyberdomein), zal in de subconclusie antwoord worden gegeven op de in dit hoofdstuk gestelde deelvraag.

2.4 Subconclusie

De vraag die centraal stond in dit hoofdstuk was hoe het internationaal recht het verzamelen van inlichtingen in het cyberdomein begrenst. In voorgaande paragrafen zijn twee internationaalrechtelijke beginselen behandeld die het verzamelen van inlichtingen in het cyberdomein begrenzen. Beiden beginselen zijn, impliciet of expliciet, vastgelegd in het VN Handvest. Tevens gelden de in dit hoofdstuk genoemde beginselen als gewoonterecht.

Het eerste beginsel, verweven met zowel het geweldsverbod als met soevereiniteits-beginsel, dat het extraterritoriaal verzamelen van inlichtingen in het cyberdomein begrenst is het non-interventiebeginsel. Volgens dit beginsel is het niet toegestaan om te interveniëren in (interne aangelegenheden van) andere staten. Om van een verboden interventie te spreken moet sprake zijn van een dwangelement (*coercion*). Daarnaast dient met de handeling (de inmenging) een beleidsverandering in de doelstaat beoogd te worden of plaats te vinden.

[69] Ziolkowski (2013b), p. 463.

Als aan deze twee voorwaarden wordt voldaan zal sprake zijn van een verboden interventie en zal het non-interventiebeginsel worden geschonden. Toch zijn er drie mogelijkheden om in een andere staat te interveniëren: interventie met autorisatie van de VN Veilgheidsraad, het inherente recht op individuele dan wel collectieve zelfverdediging en interventie met instemming van de staat waar de interventie plaatsvindt (*consent*).

Voor het extraterritoriaal verzamelen van inlichtingen kunnen deze drie mogelijkheden van belang zijn (bijvoorbeeld voor het extraterritoriaal verzamelen van inlichtingen ter zelfverdediging). Als echter de WIV 2002 als uitgangspunt wordt genomen voor het extraterritoriaal verzamelen van inlichtingen, dan speelt bovenstaande niet.

Ten tweede wordt het verzamelen van inlichtingen begrensd door het soevereiniteitsbeginsel. In dit onderzoek zal voornamelijk worden gericht op de externe soevereiniteit van staten, ook wel staatssoevereiniteit genoemd. In dit onderzoek wordt de volgende omschrijving van soevereiniteit gehanteerd: de staat is autonoom en (politiek) onafhankelijk van andere staten en de staat is vrij, zonder inmenging van andere staten, in het maken van zijn eigen keuzes, inclusief het vormen van buitenlands beleid. Het soevereiniteitsbeginsel wordt geschonden als een staat fysiek aanwezig is op het territoir van de andere staat, als er bij het uitvoeren van activiteiten fysieke effecten optreden op het territoir van de andere staat en/of als er handhavende rechtsmacht wordt uitgeoefend op het territoir van de andere staat.

Met bovenstaande omschrijvingen van het non-interventiebeginsel en het soevereiniteitsbeginsel en de vaststelling wanneer sprake is van een schending van (één van) beide beginselen, zal in het volgende hoofdstuk worden bezien of de WIV 2002 (een nationale wet) ook in het buitenland geldig is.

3. Geldigheid WIV in het buitenland

Hoofdstuk twee, het theoretisch kader, begon met een inleiding over het domein recht. De tweedeling tussen nationaal recht en internationaal recht werd aangehaald. Deze tweedeling is er niet voor niets. Nationaal recht is geldig in de eigen staat, maar in het beginsel niet in andere staten. Desalniettemin zijn er nagenoeg altijd uitzonderingen op de hoofdregel, zo ook op deze. Zo draagt de militair bijvoorbeeld altijd het Wetboek van Militair Strafrecht met zich mee, ook als de militair zich in het buitenland bevindt. Dat betekent dat de staat jurisdictie heeft over personen die een strafbaar feit hebben gepleegd, ook als zij dit strafbare feit in een ander land plegen. De Nederlandse strafwet is dan ook toepasselijk *"op iedere militair, die zich buiten Nederland aan enig strafbaar feit schuldig maakt".*[70] Geldt een dergelijke extraterritoriale werking ook voor de WIV? De deelvraag die in dit hoofdstuk wordt beantwoord is in hoeverre de Wet op Inlichtingen- en Veiligheidsdiensten van 2002 geldig is in het buitenland. Om deze deelvraag te beantwoorden zullen eerst de taken van de MIVD, zoals deze zijn weggelegd in de WIV, uiteen worden gezet. Vervolgens zal worden gekeken naar een mogelijke extraterritoriale werking van de WIV. In de derde paragraaf wordt de extraterritoriale toepassing van de WIV behandeld. Er zal worden afgesloten met een subconclusie waarin een antwoord wordt gegeven op de zojuist gestelde deelvraag.

3.1 Taken MIVD

De WIV is opgebouwd uit verschillende hoofdstukken. Zoals gebruikelijk bij wetten worden in het eerste hoofdstuk de algemene bepalingen vermeld. In het tweede hoofdstuk worden de verschillende inlichtingen- en veiligheidsdiensten aangehaald: de AIVD en de MIVD. Tevens staan in dit hoofdstuk de taken van beide diensten. De taken van de MIVD zijn vastgelegd in artikel 7 van de WIV. Het betreft een zestal taken, de zogeheten a-taak, b-taak, c-taak, d-taak, e-taak en f-taak.

De a-taak is onderverdeeld in twee delen. De MIVD dient onderzoek te verrichten naar het potentieel en de strijdkrachten van andere mogendheden om zo een juiste opbouw en een doeltreffend gebruik van de krijgsmacht te bewerkstelligen. Daarnaast dient de MIVD onderzoek te verrichten naar factoren die van invloed kunnen zijn op de internationale rechtsorde (voor zover de krijgsmacht daarbij betrokken is of naar verwachting betrokken zal worden). De b-taak van de MIVD houdt in: het verrichten van veiligheidsonderzoeken, zoals bedoeld in de Wet Veiligheidsonderzoeken (WVO).

[70] Artikel 4 van het Wetboek van Militair Strafrecht (1903).

Net als de a-taak, is ook de c-taak onderverdeeld in verschillende deeltaken. Het betreft het verrichten van onderzoek dat nodig is voor het treffen van maatregelen ter voorkoming van activiteiten, met als doel de veiligheid of de paraatheid van de krijgsmacht te schaden. Daarnaast valt onder de c-taak het verrichten van onderzoek dat nodig is voor het treffen van maatregelen om de mobilisatie en de concentratie van de strijdkrachten juist te laten verlopen. De derde en laatste deeltaak betreft het verrichten van onderzoek dat nodig is voor het treffen van maatregelen om een ongestoorde voorbereiding en inzet van de krijgsmacht te bewerkstelligen. Samenhangend met de c-taak wordt van de MIVD verwacht, zoals uiteengezet in de d-taak, dat zij maatregelen bevorderen om de onder de c-taak genoemde belangen te beschermen. Denk bijvoorbeeld aan de bescherming van gegevens die geheim moeten blijven. Deze gegevens kunnen fysiek, maar ook met behulp van bijvoorbeeld een wachtwoord worden beschermd.

De vijfde taak, de e-taak, betreft het verrichten van onderzoek betreffende andere landen. Aangezien het een taak van de MIVD betreft, wordt met deze taak bedoeld dat onderzoek wordt verricht naar andere landen, mits het onderwerp van onderzoek een militaire relevantie heeft. Tot slot de zesde en laatste taak van de MIVD, de f-taak, omvat het opstellen van dreigingsanalyses. Deze dreigingsanalyses worden opgesteld om bepaalde personen (zoals vastgesteld in de artikelen 4, derde lid onder b en 41, eerste lid onder c van de Politiewet 2012) te beveiligen, alsmede het bewaken en beveiligen van objecten en diensten die op grond van artikel 16 van de Politiewet 2012 zijn aangewezen. Wederom de kanttekening dat het hier personen, objecten en diensten met een militaire relevantie betreft.[71]

In tabel 3.1 zijn de taken nog eens kort en overzichtelijk opgesomd.

[71] In artikel 7a van de Wet op Inlichtingen- en Veiligheidsdiensten 2002 is een nadere toelichting gegeven op de f-taak. In dit artikel wordt vermeld dat de MIVD een dreigingsanalyse zal opstellen als gegevens worden verkregen van bepaalde personen dan wel organen. Dit is tot dusver een limitatieve lijst van een zestal partijen, waaronder bijvoorbeeld de politie en het openbaar ministerie. Tevens is het, ingevolge van lid 2 van artikel 7a, toegestaan om gegevens te verzamelen ten behoeve van het opstellen van de dreigingsanalyses (indien de gegevens die op grond van lid 1 zijn verstrekt dat noodzakelijk maken).

Taak	Omschrijving
A-taak	Onderzoek verrichten naar het potentieel en de strijdkrachten van andere mogendheden
	Onderzoek verrichten naar factoren die van invloed (kunnen) zijn op de handhaving en bevordering van de internationale rechtsorde
B-taak	Veiligheidsonderzoeken verrichten
C-taak	Onderzoek verrichten dat nodig is voor het treffen van maatregelen ter voorkoming van activiteiten die als doel hebben de veiligheid of paraatheid van de krijgsmacht te schaden
	Onderzoek verrichten dat nodig is voor het treffen van maatregelen ter bevordering van een juist verloop van mobilisatie en concentratie der strijdkrachten
	Onderzoek verrichten dat nodig is voor het treffen van maatregelen ten behoeve van een ongestoorde voorbereiding en inzet van de krijgsmacht
D-taak	Bevorderen van maatregelen ter bescherming van de onder de c-taak genoemde belangen
E-taak	Onderzoek verrichten betreffende andere landen
F-taak	Opstellen van dreigingsanalyses

Tabel 3.1 Taken MIVD

3.2 Extraterritoriale werking WIV

In eerste opzicht lijkt een antwoord op de deelvraag van dit hoofdstuk snel gevonden. Uit bovenstaand takenpakket van de MIVD blijkt dat een buitenlandtaak is weggelegd voor de MIVD. Niet alleen voor de MIVD is er een buitenlandtaak weggelegd, vastgelegd in artikel 7, lid 2 onder e, maar ook voor de AIVD is deze buitenlandtaak aanwezig in de WIV (vastgelegd in artikel 6, lid 2 onder d). Het verschil in beiden buitenlandtaken schuilt in de toepassing van de taken. De MIVD zal de buitenlandtaak alleen uitvoeren met betrekking tot zaken die een militaire relevantie hebben. Men zou dus geneigd zijn te concluderen dat de in dit hoofdstuk gestelde deelvraag kan worden beantwoord. Op basis van de in de wet vastgelegde buitenlandtaak is het namelijk verleidelijk te concluderen dat de WIV een extraterritoriale werking heeft.

Helaas ligt het niet zo simpel als het in eerste instantie lijkt. De WIV 2002 is namelijk een nationale wet en behoort niet tot het internationaal recht. Een nationale wet is in het beginsel niet geldig in het buitenland. Dat stelde ook het *PCIJ* in 1927 bij de behandeling van de *Lotus case*: *"The fundamental consequence of their independence and sovereignty is that no municipal law… can apply or have binding effect outside the national territory."*.[72]

Zoals in de inleiding van dit hoofdstuk reeds is aangehaald, zijn er altijd uitzonderingen op de regel.[73] Dit gaat niet op voor de WIV: de WIV heeft geen extraterritoriale werking. Dat stelt ook de Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (CTIVD) in 2007 tijdens een studiemiddag betreffende inlichtingenactiviteiten in het buitenland: *"De Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002 (WIV 2002) geldt niet buiten het Nederlands territoir. Het is een nationale wet, waarin geen expliciet extraterritorialiteitsbeginsel is opgenomen.".* Daarnaast wordt in hetzelfde verslag vermeld dat er in de WIV een taak is weggelegd voor zowel de AIVD als de MIVD om onderzoek te verrichten *naar* andere landen. Er staat niet expliciet vermeld dat er onderzoek dient te worden verricht *in* andere landen.[74]

[72] Judgment Lotus case (1927), para. 105.

[73] In dit geval betreft het de regel dat een nationale wet niet geldig is in het buitenland.

[74] Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2007), p. 1.

In 2011 herhaalt de CTIVD haar standpunt in een rapport inzake de uitvoering van de inlichtingentaak buitenland door de AIVD. Het internationaalrechtelijke beginsel van soevereiniteit wordt tevens benadrukt door de CTIVD: *"In het internationaal recht worden staten aangemerkt als soeverein. Dit betekent dat zij op het eigen grondgebied, behoudens internationale afspraken en verdragen, volledig en bij uitsluiting bevoegd zijn om wetgevende, rechtsprekende en administratieve handelingen uit te oefenen. Het wereldwijd erkende soevereiniteitsbeginsel is gecodificeerd in artikel 2 lid 1 van het Handvest van de Verenigde Naties. Indien inlichtingen- en veiligheidsdiensten in het buitenland heimelijk inlichtingen verzamelen dan zal dit, indien het betrokken land hiervan op de hoogte geraakt, als een inbreuk op de soevereiniteit van dat land worden gezien. Het gaat immers om handelingen van de Nederlandse uitvoerende macht op het territoir van een andere staat. Inlichtingendiensten en hun medewerkers of agenten die in het buitenland opereren dienen zich te realiseren dat de staat binnen wiens grenzen zij hun activiteiten ontplooien mogelijk hiertegen zal optreden. Zij vallen op dat moment onder de territoriale rechtsmacht van de desbetreffende buitenlandse staat."*.[75]

Hoewel het hier gaat over een rapport omtrent de buitenlandtaak en inzet van bijzondere bevoegdheden van de AIVD, beschikt de MIVD ook over een buitenlandtaak en beschikt de MIVD ook over de mogelijkheid tot het inzetten van bijzondere bevoegdheden. De beweringen die in bovenstaand rapport worden gedaan gelden dus eveneens voor de MIVD.

Naast bovenstaande bewering van de CTIVD, stelt de CTIVD ook dat: *"De vraag naar de rechtmatigheid van de inzet van bijzondere bevoegdheden in het buitenland lijkt inderdaad moeilijk eenduidig te beantwoorden. Wel is duidelijk dat de inzet van bijzondere bevoegdheden in het buitenland op gespannen voet staat met het beginsel van soevereiniteit. Zoals hierboven toegelicht acht Nederland het zelf onaanvaardbaar als buitenlandse inlichtingendiensten heimelijke activiteiten op Nederlands grondgebied ontplooien. Daarnaast ontbreekt een formele legitimatie voor deze activiteiten aangezien een nationale wet zoals de Wiv 2002 niet eenzijdig activiteiten kan legitimeren op het grondgebied van een andere staat."*.[76]

[75] Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2011a), p. 8.

[76] Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2011a), p. 9.

Ook de commissie die de WIV 2002 evalueert (evaluatiecommissie) stelt in het evaluatierapport dat de WIV een nationale wet is en er in deze wet geen extraterritorialiteitsbeginsel is opgenomen: *"In de Wiv zijn geen bepalingen te vinden die duiden op extraterritoriale werking van deze wet."*.[77] In diezelfde evaluatie wordt ook aangehaald dat: *"In het internationaal recht worden staten aangemerkt als soeverein, wat inhoudt dat ze in beginsel zelf de hoogste macht bezitten tot regeling en bestuur op hun eigen territorium zonder inmenging van andere staten of organisaties. Die soevereiniteit is onder andere vastgelegd in artikel 2 lid 1 van het Handvest van de Verenigde Naties. Het daar uitgedrukte soevereiniteitsbeginsel omvat mede het beginsel van non-interventie. Staten zijn niet bevoegd om zonder toestemming van een ander land in dat land activiteiten te ontplooien, op een manier die inbreuk maakt op de soevereiniteit van dat land."*.[78]

3.3 WIV naar analogie toepassen in het buitenland

Daar waar het in eerste opzicht makkelijk leek om de deelvraag, in hoeverre de WIV in het buitenland geldig is, te beantwoorden, blijkt uit de vorige paragraaf dat het toch gecompliceerder is dan het lijkt. In principe bevat de WIV geen extraterritorialiteitsbeginsel en is dus niet in het buitenland geldig.

Toch merkt De Vries, destijds Minister van Binnenlandse Zaken en Koninkrijksrelaties, in een brief van 2001 het volgende op over het uitoefenen van de bijzondere bevoegdheden (uit de WIV) voor het verzamelen van inlichtingen in het buitenland: *"De diensten moeten bij het uitoefenen van bijzondere bevoegdheden in het buitenland in de eerste plaats de grenzen in acht nemen die voor de uitoefening van die bevoegdheden in ons eigen land gelden. Het kan uiteraard niet zo zijn dat de diensten in het buitenland meer zouden mogen dan hen binnen de eigen landgrenzen is toegestaan. Tegelijkertijd is het natuurlijk niet zo dat de diensten in het buitenland alles mogen doen wat hen binnenlands is toegestaan. Nederland bezit slechts rechtsmacht op het eigen territoir en ons land kan niet eenzijdig bevoegdheden in andere landen creëren. De grenzen aan de mogelijkheden van de diensten om hun bijzondere bevoegdheden in het buitenland uit te oefenen worden dan ook in beginsel bepaald door de ter plaatse geldende wetgeving."*.[79]

[77] Evaluatiecommissie (2013), p. 41.

[78] Evaluatiecommissie (2013), p. 41.

De MIVD dient zich bij de inzet van de bijzondere bevoegdheden in het buitenland dus te houden aan de WIV 2002: de MIVD mag in het buitenland niet meer dan in Nederland. Tevens moet de MIVD zich bij de uitoefening van de bijzondere bevoegdheden in het buitenland houden aan de daar geldende regelgeving. Het lijkt er dus op dat de MIVD extraterritoriaal inlichtingen mag verzamelen als zij zich houden aan de ter plaatse geldende wetgeving.

Ook de CTIVD zegt iets over inlichtingenactiviteiten in het buitenland. Zoals in de vorige paragraaf aangehaald, onderkent de CTIVD in 2007 tijdens een studiemiddag omtrent inlichtingenactiviteiten in het buitenland dat de WIV niet van toepassing is op inlichtingenactiviteiten in het buitenland. Desalniettemin stelt de CTIVD dat een aantal vereisten uit de wet (naar analogie) relevant zijn voor inlichtingenactiviteiten in het buitenland: *"Hoewel de WIV 2002 formeel niet van toepassing is op inlichtingenactiviteiten in het buitenland, wordt door eenieder onderschreven dat een aantal uit de WIV 2002 voortvloeiende vereisten (naar analogie) voor deze activiteiten relevant zijn."*.[80]

In het toezichtrapport inzake de uitvoering van de inlichtingentaak buitenland door de AIVD, is de CTIVD minder voorzichtig in haar uitspraak met betrekking tot de toepassing van de WIV in het buitenland: *"Dat een formeel juridische rechtsbasis voor dit onderzoek ontbreekt, kan naar het oordeel van de Commissie evenwel alleen gebillijkt worden indien bij ieder optreden van de AIVD in het buitenland de Wiv 2002 naar analogie wordt toegepast. De in de Wiv 2002 voorgeschreven procedures voor de inzet van bijzondere bevoegdheden dienen naar het oordeel van de Commissie ook in het buitenland nageleefd te worden."*.[81]

Dat deze bepaling niet louter geldt voor de AIVD, maar ook voor de MIVD blijkt een aantal pagina's verder in het rapport: *"Ook de taakomschrijving van de MIVD bevat een inlichtingentaak buitenland. Artikel 7 lid 2 sub e Wiv 2002 beschrijft op dezelfde wijze als voor de AIVD het onderzoek betreffende andere landen, zij het dat het onderzoek betreft ten aanzien van onderwerpen met een militaire relevantie."*.[82]

---

[79] Brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties De Vries (2001), p. 10.

[80] Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2007), p. 3.

[81] Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2011a), p. 16.

[82] Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2011a), p. 16.

Naast de Minister van Binnenlandse Zaken en Koninkrijksrelaties in 2001 en de CTIVD in 2007 respectievelijk 2011, stelt de evaluatiecommissie in 2013, hoewel er geen extraterritorialiteitsbeginsel is opgenomen in de WIV, dat: *"de Nederlandse wetgever in het belang van de nationale veiligheid aan de I&V-diensten als taak opgedragen om inlichtingen te vergaren over andere landen. Dit betekent dat de diensten ook buiten de eigen landsgrenzen moeten kunnen opereren en daarbij bijzondere bevoegdheden kunnen aanwenden, zoals het inzetten van agenten."*.[83] Een aantal pagina's verder in het evaluatierapport concludeert de evaluatiecommissie dat: *"de buitenlandtaak van de I&V-diensten in de Wiv, in combinatie met het Aanwijzingsbesluit Buitenland, voldoende legitimatie vormt voor Nederlandse inlichtingenactiviteiten in het buitenland. Analoge toepassing van de Wiv in het buitenland is volgens de evaluatiecommissie nog steeds opportuun. Daarmee worden volgens de evaluatiecommissie voldoende garanties geboden voor een legitieme en doelmatige taakuitoefening door de diensten in het buitenland."*.[84]

Kortom, zowel de CTIVD als de evaluatiecommissie concluderen dat de WIV in principe niet in het buitenland geldt, aangezien er in de nationale wet geen extraterritorialiteitsbeginsel is opgenomen. Desalniettemin concluderen beiden dat de WIV naar analogie wordt toegepast bij het ontplooien van inlichtingenactiviteiten in het buitenland en dat dit voldoende rechtsbasis biedt. Ook de Minister van Binnenlandse Zaken en Koninkrijksrelaties De Vries stelt in 2001 dat de bijzondere bevoegdheden in het buitenland mogen worden ingezet.

3.4 Subconclusie

In dit hoofdstuk stond de vraag centraal in hoeverre de Wet op Inlichtingen- en Veiligheidsdiensten van 2002 geldig is in het buitenland. Daar het in de eerste paragraaf duidelijk leek wat het antwoord op bovenstaande deelvraag was, namelijk dat de wet extraterritoriaal geldig is omdat er voor de MIVD expliciet een buitenlandtaak is opgenomen in de WIV, bleek in de tweede paragraaf dat het beantwoorden van de vraag veel gecompliceerder was. Een nationale wet is namelijk in het beginsel niet geldig in het buitenland. Op een basisregel zijn echter nagenoeg altijd uitzonderingen, zo ook op deze regel. Helaas is de WIV geen uitzondering op de regel. In de WIV is niet expliciet een extraterritorialiteitsbeginsel opgenomen en is daarom niet geldig in het buitenland.

[83] Evaluatiecommissie (2013), p. 41.

[84] Evaluatiecommissie (2013), p. 44.

Desalniettemin stellen zowel de CTIVD als de evaluatiecommissie dat bij het uitvoeren van inlichtingenactiviteiten in het buitenland, de WIV naar analogie toegepast dient te worden. Ook de Minister van Binnenlandse Zaken en Koninkrijksrelaties De Vries stelt in 2001 dat de bijzondere bevoegdheden in het buitenland mogen worden ingezet. Daarbij wordt vermeld dat de MIVD niet meer mag in het buitenland dan dat de MIVD in Nederland mag. De MIVD moet zich dus aan alle voorwaarden houden om de in de wet toegestane taken (met bijbehorende bevoegdheden) uit te voeren.

Het komt er in het kort op neer dat de WIV niet geldig is in het buitenland, maar wel als zodanig (naar analogie) wordt toegepast in het buitenland om de taken die in de WIV staan uit te kunnen voeren. Omdat de WIV naar analogie wordt toegepast bij het uitvoeren van inlichtingenactiviteiten in het buitenland, zal in het volgende hoofdstuk worden stilgestaan bij de bevoegdheden die de MIVD, op basis van de WIV, kan gebruiken voor de taakuitvoering.

4. Bevoegdheden MIVD

In hoofdstuk twee zijn de internationaalrechtelijke beginselen van non-interventie en soevereiniteit uiteengezet. Er is gekozen om, voor het vervolg van dit onderzoek, een omschrijving aan te houden waaraan de toegestane inlichtingenactiviteiten van de MIVD in het cyberdomein zullen worden getoetst. Alvorens dat te doen, dient helder te worden welke bevoegdheden de MIVD heeft voor het extraterritoriaal verzamelen van inlichtingen in het cyberdomein. Deze bevoegdheden zijn vastgelegd in de WIV uit 2002. De bevoegdheden van de MIVD worden ingezet ten einde de taken van de MIVD, zoals beschreven in het vorige hoofdstuk, uit te voeren.

In dit hoofdstuk zal eerst een paragraaf volgen waarin de algemene bevoegdheid van de MIVD tot het verzamelen van gegevens uiteen wordt gezet. In de daaropvolgende paragraaf zal worden stilgestaan bij de bijzondere bevoegdheden die de MIVD mag inzetten om hun taken uit te voeren. Tevens wordt per bijzondere bevoegdheid bezien wat dit betekent voor het cyberdomein. Vervolgens zal een paragraaf volgen waarin een aantal aanvullende bevoegdheden dan wel mogelijkheden uiteen worden gezet die de MIVD kan gebruiken om aan de gewenste gegevens te komen zonder de bijzondere bevoegdheden in te (hoeven) zetten. Tot slot zal een subconclusie volgen waarin de deelvraag van dit hoofdstuk wordt beantwoord: “Welke bevoegdheden heeft de Militaire Inlichtingen- en Veiligheidsdienst, op basis van de Wet op Inlichtingen- en Veiligheidsdiensten 2002, voor het verzamelen van inlichtingen in het cyberdomein?”

4.1 Algemene bevoegdheden MIVD

In het vorige hoofdstuk van dit onderzoek zijn de taken van de MIVD, zoals vastgelegd in het tweede hoofdstuk van de WIV, uiteengezet. In hoofdstuk drie van de WIV volgen de bevoegdheden van de AIVD en de MIVD. Beiden diensten hebben in het beginsel dezelfde bevoegdheden, zij het dat de MIVD zich richt op zaken met een militaire relevantie. De bevoegdheden kunnen worden gebruikt voor een goede taakuitvoering dan wel ter ondersteuning van een goede taakuitvoering. Deze bevoegdheden worden in dit hoofdstuk besproken. De eerste bevoegdheid die is weggelegd in de WIV is te vinden in artikel 12. Het betreft de algemene bevoegdheid tot het verwerken van gegevens.[85] In de memorie van toelichting is te lezen dat onder gegevensverwerking het volgende wordt verstaan:

[85] Artikel 12 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

"Gegevensverwerking of verwerking van gegevens is elke bewerking of geheel van bewerkingen met betrekking tot gegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.".[86] Het verzamelen van gegevens, waarop dit onderzoek is gericht, is dus eveneens toegestaan in gevolge van artikel 12. In lid 2 van artikel 12 staat dat de verwerking (dus inclusief de verzameling) van gegevens slechts mag plaatsvinden voor een bepaald doel dan wel voor een goede taakuitvoering. In de artikelen volgend op artikel 12 wordt voornamelijk gesproken over een aantal voorwaarden waaraan de verwerking van gegevens moet voldoen. Vervolgens wordt in artikel 17 nog eens vermeld dat de diensten bevoegd zijn tot het verzamelen van gegevens en dat zij zich daarbij mogen richten tot bepaalde personen en organen.

4.2 Bijzondere bevoegdheden MIVD

De algemene bevoegdheid van de MIVD tot het verzamelen van gegevens wordt nader gespecificeerd in de artikelen 20 tot en met 29 van de WIV. Deze artikelen omvatten verscheidene bijzondere bevoegdheden waarvan de MIVD gebruik mag maken bij het uitvoeren van haar taken. In artikel 18 van de WIV staat vermeld dat de MIVD bevoegd is om alle bijzondere bevoegdheden in te zetten ten behoeve van de a-taak, c-taak en e-taak. Zie tabel 4.1 op de volgende pagina voor een schematische weergave van de bevoegdheden die per taak van de MIVD mogen worden uitgeoefend.

[86] Kamerstukken II 1997/98, 25 877, nr. 3, p. 17.

Taak	**Algemene bevoegdheid**	**Bijzondere bevoegdheden**
A-taak Onderzoek verrichten naar: - Potentieel en strijdkrachten andere mogendheden - Factoren van invloed op handhaving en bevordering internationale rechtsorde	Ja	Ja
B-taak Veiligheidsonderzoeken verrichten	Ja	Nee
C-taak Onderzoek verrichten dat nodig is voor het treffen van maatregelen: - Ter voorkoming van activiteiten met als doel de veiligheid of paraatheid van de krijgsmacht schaden - Ter bevordering van een juist verloop van de mobilisatie - Ten behoeve van een ongestoorde voorbereiding en inzet van de krijgsmacht	Ja	Ja
D-taak Bevorderen van maatregelen ter bescherming van de onder de c-taak genoemde belangen	Ja	Nee
E-taak Onderzoek verrichten betreffende andere landen	Ja	Ja
F-taak Opstellen van dreigingsanalyses	Ja	Nee

Tabel 4.1 Bevoegdheden per taak

Het uitvoeren van de bijzondere bevoegdheden is echter wel aan een aantal voorwaarden verbonden. Zo is de inzet van bijzondere bevoegdheden pas toegestaan als de gewenste gegevens niet openbaar of via partner(inlichtingen)diensten kunnen worden verkregen.[87] Tevens dient, over het algemeen, toestemming te worden gevraagd aan de minister (of het daartoe gemandateerde hoofd van de MIVD) om de bijzondere bevoegdheid te mogen uitvoeren, tenzij anders is vermeld in het betreffende artikel. Daarnaast wordt in artikel 31 een aantal aanvullende voorwaarden aangehaald ten behoeve van het uitvoeren van de bijzondere bevoegdheden. Het betreft de beginselen van proportionaliteit en het subsidiariteit.

Met betrekking tot het proportionaliteitsbeginsel dient de uitoefening van bijzondere bevoegdheden achterwege te blijven als dit een onevenredig nadeel oplevert voor de betrokkene. Volgens het subsidiariteitsbeginsel dient de MIVD die bijzondere bevoegdheid te gebruiken die het minste nadeel oplevert voor de betrokkene.[88] Artikel 32 vult hierop aan dat meteen gestaakt dient te worden met de uitoefening van de bijzondere bevoegdheden indien het gewenste doel is bereikt of als inmiddels een andere bijzondere bevoegdheid tot het zelfde resultaat zal leiden (lees: de gewenste gegevens kunnen worden verzameld door het toepassen van een andere bijzondere bevoegdheid die minder nadeel voor de betrokkene oplevert).[89] Tevens dient per bijzondere bevoegdheid aan een aantal aanvullende eisen te worden voldaan. Daar waar nodig, zullen deze aanvullende eisen worden vermeld.

4.2.1 Reikwijdte bijzondere bevoegdheden

In de memorie van toelichting is het volgende te lezen: *"Bij de regeling van de bijzondere bevoegdheden is ervoor gekozen deze zodanig te formuleren, dat enerzijds voldoende duidelijk is wat de reikwijdte en strekking van elk van de te onderscheiden bevoegdheden is en anderzijds dat wordt bewerkstelligd dat de ter uitvoering van die bevoegdheden in te zetten inlichtingenmiddelen in de verschillende – al dan niet technische – toepassingsvarianten door de gekozen formulering adequaat worden afgedekt. Dit laatste is gerealiseerd door in de desbetreffende artikelen te kiezen voor een categoriale aanduiding*

[87] Evaluatiecommissie (2013), p. 35-36.

[88] Artikel 31 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

[89] Artikel 32 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

van een aantal specifieke toepassingsvarianten die evenwel naar hun aard op hetzelfde zijn gericht (zoals bijvoorbeeld volgen of observeren), in plaats van de omschrijving van een specifieke toepassingsvariant sec. Deze zo techniekloos mogelijke formuleringen hebben een aantal voordelen. Ten eerste, dat reeds op voorhand wordt ingespeeld op mogelijke technologische ontwikkelingen op het terrein van de betreffende middelen die daarmee tevens op voorhand onder de reikwijdte van de betreffende regeling vallen. Ten tweede wordt daarmee ook voorkomen dat er te veel zicht ontstaat op de specifieke (technische) mogelijkheden die de diensten ter beschikking staan.".[90]

Op basis van het bovenstaande met betrekking tot het zo techniekloos mogelijk formuleren van de bijzondere bevoegdheden kunnen de artikelen, waarin de bijzondere bevoegdheden zijn weggelegd, breed worden geïnterpreteerd qua toepassingsmiddelen. Daarom heeft een aantal bevoegdheden van de MIVD raakvlakken met het cyberdomein.

Hoewel de wetgever de bijzondere bevoegdheden zo techniekloos mogelijk heeft geformuleerd, dient er toch een kanttekening geplaatst te worden bij de bijzondere bevoegdheden. Het is namelijk gebleken dat de bevoegdheden onvoldoende geschikt zijn voor de technologische innovaties van het afgelopen decennium. Dat stelt de evaluatiecommissie: *"Het is de evaluatiecommissie gebleken dat er met name knel- en aandachtspunten bestaan die een gevolg zijn van een discrepantie tussen de huidige wettelijke regeling en de voortschrijdende technologie."*.[91]

Ook de CTIVD merkte in 2011, ten aanzien van een aantal bijzondere bevoegdheden, op dat: *"Het onderscheid tussen kabelgebonden en niet-kabelgebonden communicatie doet naar het oordeel van de Commissie wat gedateerd aan. Het gebruik van kabels bij het internationale telecommunicatieverkeer is vanwege de grote capaciteit van de moderne glasvezeltechnologie toegenomen. Voor telecommunicatieverkeer tussen verschillende continenten wordt vaak gebruik gemaakt van kabels die op de zeebodem zijn gelegd. Op deze wijze wordt een groot deel van het trans-Atlantische telefoonverkeer afgehandeld."*. Mede daarom vindt de MIVD dat er een nieuwe wettelijke (bijzondere) bevoegdheid moet komen om ook kabelgebonden telecommunicatie (ongericht) te kunnen intercepteren.[92]

---

[90] Kamerstukken II 1997/98, 25 877, nr. 3, p. 29.

[91] Evaluatiecommissie (2013), p. 69.

[92] Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2011b), p. 38.

Desalniettemin kan een aantal bijzondere bevoegdheden worden bezien in relatie tot het cyberdomein. Vanwege technologische ontwikkelingen die zich sinds het opstellen van de WIV hebben voorgedaan, zijn nieuwe (cyber)middelen ontwikkeld die kunnen worden gebruikt voor het uitvoeren van de bijzondere bevoegdheden. Helaas werd geen toegang verleend tot daadwerkelijke operaties van de MIVD omdat dit de *modus operandi* dan wel het (huidige) kennisniveau van de MIVD zou (kunnen) prijsgeven. Derhalve komen de mogelijkheden die in dit onderzoek worden besproken (met betrekking tot de nieuwe (cyber)middelen die kunnen worden gebruikt bij de uitoefening van de bijzondere bevoegdheden) voort uit een eigen analyse. In de volgende tien paragrafen zullen alle bijzondere bevoegdheden uiteen worden gezet. Daarnaast zal per bijzondere bevoegdheid worden bezien of deze relevant is in het cyberdomein. Daar waar de bijzondere bevoegdheden relevant zijn voor het cyberdomein zal, op basis van een eigen analyse, per bijzondere bevoegdheid, stil worden gestaan bij de mogelijkheden in het cyberdomein.

4.2.2 Observeren en volgen

In artikel 20 is de eerste bijzondere bevoegdheid opgenomen. De MIVD is bevoegd om natuurlijke personen en zaken te observeren en te volgen. Tevens valt binnen deze bevoegdheid het vastleggen van gegevens die worden verzameld tijdens de observatie of tijdens het volgen.[93] Het moge duidelijk zijn dat het fysiek observeren en volgen onder deze bevoegdheid valt. Daarvoor kunnen volgmiddelen, plaatsbepalingsapparatuur en registratiemiddelen worden gebruikt. Met betrekking tot het observeren en volgen via het cyberdomein is de wetstekst minder duidelijk.

In de memorie van toelichting wordt daarentegen gesproken over foto- en videoapparatuur waarmee gegevens kunnen worden vastgelegd. Tegenwoordig is het mogelijk om, nadat toegang is verschaft tot een geautomatiseerd werk zoals een computer (zie paragraaf 4.2.6), de (al dan niet ingebouwde) *webcam* of de (al dan niet ingebouwde) microfoon van die computer te gebruiken en controleren. Zo is het bijvoorbeeld mogelijk om een *webcam* van een computer te gebruiken als beveiligingscamera. Men kan dan bijvoorbeeld met behulp van een *App* (applicatie op een *smartphone*) zien wat de *webcam* van de computer ziet.[94]

---

[93] Artikel 20 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

[94] Tal van voorbeelden zijn op Internet te vinden (onder andere van bedrijven) over hoe men de camera van een computer of laptop (*webcam*) kan gebruiken als beveiligingscamera. Vaak is het mogelijk om hetgeen de

Tevens is het mogelijk om, zonder medeweten van een ander, toegang te verschaffen tot diens *webcam* en deze te besturen. Dit gebeurd bijvoorbeeld door gebruik te maken van *malware (malicious software)* of een Trojaans paard, maar kan op nog veel andere manieren.[95]

Daarnaast zijn er meer mogelijkheden om personen en/of zaken via het cyberdomein te volgen. Denk bijvoorbeeld aan een ruime interpretatie van het begrip plaatsbepalingapparatuur. Een navigatiesysteem bepaalt ook de plaats (van bijvoorbeeld een auto waarin het navigatiesysteem wordt gebruikt) waar een persoon en/of zaak zich plaatsvindt. Door digitaal toegang te verschaffen tot dergelijke navigatiesystemen kunnen dus ook personen dan wel zaken worden gevolgd.

Ook geautomatiseerde werken als *smartphones* en *tablets* kunnen plaatsbepalingen doen. Door gebruik te maken van de zojuist aangehaalde *malware* en andere manieren om toegang te verschaffen tot een geautomatiseerd werk, kan bijvoorbeeld plaatsbepalingsoftware worden geïnstalleerd op dat geautomatiseerde werk (bijvoorbeeld op een *smartphone* of op een *tablet*), waardoor personen gevolgd kunnen worden.

De bevoegdheid tot het binnendringen van dergelijke systemen (of zoals in de bewoording van de WIV: geautomatiseerde werken) is niet opgenomen in dit artikel. Deze bevoegdheid, welke wordt behandeld in paragraaf 4.2.6, bestaat wel in gevolge van artikel 24 van de WIV, waarin het de MIVD is toegestaan een geautomatiseerd werk binnen te treden.

Al met al schept bovenstaande nieuwe mogelijkheden voor de MIVD. Nu hoeft de MIVD niet fysiek een plaats te betreden om bijvoorbeeld bepaalde middelen of apparatuur aan te brengen, zij kunnen nu op afstand personen en/of zaken volgen en observeren. Er zijn echter wel beperkingen. Zo staat een *webcam* op een vaste plaats, namelijk geïntegreerd in of gepositioneerd naast een computer of laptop. Als de persoon of zaak niet aanwezig is bij de *webcam* kan louter worden geconstateerd (geobserveerd) dat de persoon of zaak niet aanwezig is. Het is dan niet mogelijk om personen of zaken te volgen.

---

webcam ziet, door gebruik te maken van een *App,* ook te zien op de mobiele telefoon of *tablet*. Vanwege de enorme hoeveelheid aan voorbeelden wordt hier volstaan met de vermelding dat op het Internet bij zoekmachines (zoals Google) zoektermen in de richting van '*remote access to webcam*' kunnen worden ingetypt voor de talloze voorbeelden.

[95] Hannon (2010), via: http://www.google.com/patents/US20120151606

Daarnaast is het op afstand moeilijker te bepalen of de te volgen persoon (of zaak) aanwezig is bij het navigatiesysteem of bij de *smartphone* of *tablet*. Ook kan de gebruiker van een geautomatiseerd werk besluiten zijn *webcam* af te plakken of kan een gebruiker zijn navigatiesysteem, *smartphone* of *tablet* niet gebruiken, uitschakelen of door een ander laten gebruiken. Tevens is het mogelijk dat een te volgen persoon of zaak niet over dergelijke middelen beschikt (zoals een *webcam*, navigatiesysteem, *smartphone* of *tablet*). Wil de MIVD iemand overal volgen, zal terug moeten worden gegrepen op het daadwerkelijk plaatsen van middelen dan wel apparatuur, al kunnen een aantal van bovenstaande beperkingen ook optreden bij het fysiek plaatsen van middelen of apparatuur (bijvoorbeeld dat de gebruiker besluit zijn auto of *smartphone* door een ander te laten gebruiken).

4.2.3 Inzet agenten en oprichting rechtspersonen

De MIVD is volgens artikel 21 bevoegd tot de inzet van natuurlijke personen, onder verantwoordelijkheid en instructie van de MIVD, om gegevens te verzamelen over personen en organisaties die van belang (kunnen) zijn voor de taakuitvoering van de MIVD. Ook is de MIVD bevoegd tot het bevorderen dan wel treffen van maatregelen om de te behartigen belangen van de MIVD te beschermen.[96] De personen die deze bevoegdheid uitvoeren worden ook wel agenten genoemd.[97] Deze agenten worden doelbewust door de dienst ingezet met als hoofdtaak het verwerven van een informatiepositie. Deze informatiepositie moet de agenten in staat stellen om de gewenste gegevens te verzamelen. Opgemerkt dient te worden dat bij het verkrijgen dan wel behouden van deze informatiepositie het (op voorwaarden) is toegestaan strafbare feiten te plegen dan wel mee te werken aan het uitvoeren van strafbare feiten. Deze bevoegdheid mag worden toegepast onder een dekmantel door het aannemen van een bepaalde identiteit (bijvoorbeeld een andere naam) of hoedanigheid (bijvoorbeeld een bepaalde functie in een beroepsgroep).[98]

[96] Artikel 21 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

[97] Het betreft hier geen informanten. Het gebruik van informanten wordt namelijk ontleend aan artikel 17 van de WIV, waarin staat dat de dienst zich mag richten tot 'de natuurlijke persoon die door de positie waarin hij verkeert dan wel de hoedanigheid die hij heeft over gegevens beschikt of kan beschikken die voor een goede taakuitvoering van de dienst van belang kunnen zijn'. Een informant kan louter om gegevens worden gevraagd. Agenten, daarentegen, worden door de dienst ingezet en aangestuurd. Zie ook Kamerstukken II 1997/98, 25 877, nr. 3, p. 31.

[98] Kamerstukken II 1997/98, 25 877, nr. 3, p. 31-35.

Naast de inzet van natuurlijke personen is het de MIVD, ter ondersteuning van operationele activiteiten, ook toegestaan rechtspersonen op te richten en in te zetten. Dit is bijvoorbeeld van belang om een aangenomen dekmantel geloofwaardig(er) te maken of om de aangenomen identiteit af te schermen.[99]

In relatie tot het cyberdomein is deze bevoegdheid van betekenis in het aannemen van bijvoorbeeld een andere cyberhoedanigheid. Zo kan bijvoorbeeld de (cyber)hoedanigheid worden aangenomen van een computermedewerker die op afstand hulp biedt voor een bepaald computerprobleem. Men kan deze hoedanigheid meteen gebruiken om gegevens van die computer te verzamelen. Deze informatie kan echter ook worden verkregen door het, op basis van artikel 24, binnentreden van een geautomatiseerd werk (zoals een computer) Daarnaast kan men zich, bijvoorbeeld op internetfora, voordoen als lotgenoot dan wel infiltreren in een bepaalde beweging om meer informatie over die persoon te verzamelen. Ook is het, bij een brede interpretatie van het wetsartikel, mogelijk om bijvoorbeeld een *Internet Service Provider* op te richten als zijnde rechtspersoon. Op die manier kan het internetverkeer van een bepaald persoon in de gaten worden gehouden. Al is het in de gaten houden van het internetgedrag van iemand ook mogelijk in gevolge van artikel 25.

4.2.4 Doorzoeken besloten plaatsen en gesloten voorwerpen en vaststellen identiteit

In gevolge van artikel 22 van de WIV is de MIVD bevoegd, al dan niet met behulp van een technisch hulpmiddel, besloten plaatsen en gesloten voorwerpen te doorzoeken. Ook is het toegestaan, ten behoeve van het vaststellen van de identiteit van een bepaald persoon, onderzoek te verrichten aan voorwerpen.[100] Onder besloten plaatsen worden bijvoorbeeld loodsen, bedrijfsgebouwen en woningen verstaan. Met gesloten voorwerpen worden bijvoorbeeld koffers en containers bedoeld. Denk bij het vaststellen van de identiteit van een bepaald persoon bijvoorbeeld aan het onderzoeken van vingerafdrukken. Bovenstaande is uiteraard ook te combineren: als een besloten plaats wordt onderzocht en/of doorzocht, mogen de daar aanwezige gesloten voorwerpen ook worden onderzocht en/of doorzocht. Tevens is het toegestaan om niet gesloten voorwerpen als kasten en laden te doorzoeken.[101]

[99] Kamerstukken II 1997/98, 25 877, nr. 3, p. 31-35.

[100] Artikel 22 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

[101] Kamerstukken II 1997/98, 25 877, nr. 3, p. 35-36.

De bevoegdheid zoals deze is weggelegd in artikel 22 van de WIV is lastig te bezien in het cyberdomein. Uit de bewoording van de nota naar aanleiding van het nader verslag van 19 maart 2001 is op te maken dat het gaat om het betreden (lees: binnentreden) van besloten plaatsen.[102] Dit duidt op het fysiek binnentreden van bijvoorbeeld een woning of loods. Indien men de woning via het cyberdomein wil 'binnentreden', kan worden gedacht aan het toegang verschaffen tot een geautomatiseerd werk (en de daarop aangesloten apparaten zoals een *webcam*) in die woning. Deze bevoegdheid valt echter niet onder de bevoegdheid van artikel 22, maar onder de bevoegdheid van artikel 24 welke in paragraaf 4.2.6 zal worden behandeld.

Het derde deel van de bevoegdheid, met betrekking tot het vaststellen van de identiteit van een bepaald persoon, heeft wel mogelijkheden in het cyberdomein. Zo kan de identiteit van iemand worden vastgesteld door bijvoorbeeld gezichtsherkenning of op basis van een stemvergelijking.[103] Deze gegevens over het gezicht of de stem van een persoon kunnen worden verkregen door gebruik te maken van bijvoorbeeld de (al dan niet ingebouwde) *webcam* en/of (al dan niet ingebouwde) microfoon van een geautomatiseerd werk (zoals een computer, *smartphone* of *tablet*). Hierbij dient echter wel opgemerkt te worden dat voor het gebruik van de *webcam* of microfoon van een geautomatiseerd werk, eerst toegang dient te worden verschaft tot dat geautomatiseerde werk. Zoals zojuist ook al is aangehaald, is de bevoegdheid tot het binnentreden van een geautomatiseerd werk weggelegd in artikel 24 van de WIV en valt derhalve niet onder de bevoegdheid van artikel 22.

4.2.5 Openen brieven en andere geadresseerde zendingen

De vierde bevoegdheid van de MIVD, vastgelegd in artikel 23, betreft het openen van brieven en andere geadresseerde zendingen, zonder dat de zender en/of ontvanger daar weet van heeft of goedkeuring voor heeft gegeven.[104] Met andere geadresseerde zendingen worden bijvoorbeeld drukwerken, pakjes en postpakketten bedoeld. Zoals in de memorie van toelichting is te lezen, is de bevoegdheid uit artikel 23 expliciet toegevoegd aan de WIV 2002, omdat de bevoegdheid in de oude WIV nog niet was vastgelegd.

---

[102] Kamerstukken II 2000/01, 25 877, nr. 14, p. 73.

[103] Zie bijvoorbeeld Hes, Hooghiemstra & Borking, p. 22-25 of TNO Rapport 35264, p. 53-66.

[104] Artikel 23 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

Voorafgaand aan dergelijke activiteiten dient de MIVD daar echter eerst toestemming voor te krijgen van de rechtbank in Den Haag. Een rechter moet de lastgeving, ingediend door de MIVD, bezien en daar een oordeel over geven om vervolgens een last wel of niet af te geven (wel of geen toestemming te verlenen om de post van bepaalde personen te openen). Daarnaast is in lid 8 van het artikel te lezen dat de ambtenaar die deze bevoegdheid uitvoert, zich moet legitimeren, met het legitimatiebewijs dat door het hoofd van de MIVD aan de persoon is verstrekt, aan de post- dan wel vervoersinstelling.[105]

De relatie met het cyberdomein is met betrekking tot het openen van brieven en andere geadresseerde zendingen uiteraard snel te leggen. Reeds in de inleiding van dit onderzoek werd aangehaald dat het cyberdomein een steeds belangrijkere rol gaat spelen in het leven van de mens. Eén van de gevolgen daarvan is dat brieven steeds vaker digitaal worden verzonden in de vorm van bijvoorbeeld e-mails. Daarnaast worden zendingen tegenwoordig ook op andere manieren geadresseerd (bijvoorbeeld in de vorm van SMS-berichten of berichten die via *social media* naar elkaar worden gestuurd).

Een dergelijke brede interpretatie (‘digitale’ brieven zoals e-mails en andere geadresseerde zendingen zoals SMS-berichten en berichten via *social media*) gaat niet op. In de memorie van toelichting bij de WIV is te lezen dat wordt aangesloten bij de formulering uit de Postwet als het gaat om de zinsnede ‘andere geadresseerde zendingen’. Het gaat bijvoorbeeld drukwerken, pakjes en postpakketten.[106] Dit zijn allen voorbeelden van fysieke (dus geen digitale) ‘andere geadresseerde zendingen’. Derhalve kan onder een ‘brief’ ook worden aangesloten bij wat daarmee wordt bedoeld in de Postwet. In de Postwet wordt onder een brief verstaan: *“de op een fysieke drager aangebrachte geadresseerde schriftelijke mededelingen”*.[107] Het moge duidelijk zijn dat ‘digitale brieven’ hier niet onder vallen, eveneens als SMS-berichten en berichten via *social media* niet vallen onder ‘andere geadresseerde zendingen’. Deze bijzondere bevoegdheid is dan ook niet relevant voor het verzamelen van inlichtingen in het cyberdomein.

[105] Kamerstukken II 1997/98, 25 877, nr. 3, p. 36-39.

[106] Kamerstukken II 1997/98, 25 877, nr. 3, p. 37.

[107] Artikel 2 van de wet van 25 maart 2009, houdende regels inzake de volledige liberalisering van de postmarkt en de garantie van de universele postdienstverlening (Postwet 2009), *Stb*. 2009, 155.

4.2.6 Binnendringen in een geautomatiseerd werk

In de vijfde bevoegdheid van de MIVD, vastgelegd in artikel 24 van de WIV, staat dat de MIVD een geautomatiseerd netwerk mag binnendringen.[108] Bij het binnendringen mag gebruik gemaakt worden van technische hulpmiddelen, valse signalen, valse sleutels en valse hoedanigheden. Om het geautomatiseerde werk binnen te treden is het de MIVD toegestaan enige beveiliging te doorbreken alsmede technische voorzieningen aan te brengen (in bijvoorbeeld de betreffende computer). Dit alles met als doel om de versleuteling van gegevens die in het geautomatiseerde werk worden verwerkt en/of opgeslagen tegen te gaan dan wel om de gegevens (die in het geautomatiseerde werk worden verwerkt en/of opgeslagen) over te nemen.[109]

In de memorie van toelichting van de WIV is te lezen dat het binnendringen van een geautomatiseerd werk in de praktijk in het bijzonder (dus niet uitsluitend) zal gaan om het binnendringen in (*stand-alone*) pc's.[110] Daarnaast wordt vermeld dat het begrip 'geautomatiseerd werk' moet worden uitgelegd zoals dit begrip in het Wetboek van Strafrecht is uitgelegd. Het gaat dan voornamelijk om de definitie die in artikel 80sexies van het Wetboek van Strafrecht is opgenomen.[111] Artikel 80sexies van het Wetboek van Strafrecht definieert een geautomatiseerd werk als: *"een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen."*.[112] Volgens de memorie van toelichting bij deze wet spreekt de definitie van: *"opslag, verwerking èn overdracht van gegevens. Het gaat hier om cumulatieve voorwaarden."*.[113]

Derhalve kan onder geautomatiseerd werk, naast een (*stand-alone*) pc, elke andere inrichting voor opslag, verwerking én overdracht van gegevens worden verstaan. Vandaag de dag kan men dan bijvoorbeeld denken aan laptops, *tablets*, maar ook aan de nieuwste mobiele telefoons (*smartphones*) en *PDA's* (*Personal Digital Assistant*). Al deze apparaten (inrichtingen) hebben de mogelijkheid om gegevens op te slaan, te verwerken én over te dragen en vallen derhalve onder de definitie van 'geautomatiseerd werk'.

---

[108] Artikel 24 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

[109] Kamerstukken II 1997/98, 25 877, nr. 3, p. 39-40.

[110] Kamerstukken II 1997/98, 25 877, nr. 3, p. 39.

[111] Kamerstukken II 1997/98, 25 877, nr. 3, p. 39.

[112] Artikel 80sexies van het Wetboek van Strafrecht (1881).

[113] Kamerstukken II 1998/99, 26 671, nr. 3, p. 44.

Naast de zojuist genoemde fysieke inrichtingen (zoals *tablets*), kan ook worden gedacht aan niet-fysieke (digitale) inrichtingen die de mogelijkheid hebben om gegevens op te slaan, te verwerken én over te dragen. Denk aan websites op het internet (bijvoorbeeld in de vorm van webfora)[114], die ook een inrichting zijn die gegevens op slaan (bijvoorbeeld in de vorm van berichten die op een forum worden geplaatst), gegevens verwerken (bijvoorbeeld in de vorm van een stemming of *poll*) en gegevens overdragen (bijvoorbeeld aan andere internetgebruikers of aan 'derden').

Het moge duidelijk zijn dat bovenstaande direct betrekking heeft op het cyberdomein. Desalniettemin zijn er twee denkrichtingen mogelijk met betrekking tot deze bevoegdheid. Enerzijds kan toegang worden verschaft tot een geautomatiseerd werk door fysiek aanwezig te zijn bij het geautomatiseerd werk dat men binnen wil treden. Men zal dan fysiek de betreffende computer (of ander geautomatiseerd werk) moeten binnentreden en de gewenste informatie moeten kopiëren door bijvoorbeeld gebruikmaking van een USB-stick of door het maken van foto's van (het beeldscherm met) de gewenste informatie.

Anderzijds kan ook zonder fysiek aanwezig te zijn, namelijk *remotely* (op afstand), toegang worden verschaft tot het geautomatiseerde werk. De gewenste gegevens worden dan ook op afstand gekopieerd. Dit is een belangrijke mogelijkheid voor de MIVD om, zonder fysiek aanwezig te zijn op het territoir van een andere staat, gegevens te verzamelen van geautomatiseerde werken die zich bevinden op het territoir van die andere staat.

Als eenmaal toegang is verschaft tot een geautomatiseerd werk kan het verzamelen van gegevens beginnen. Soms zal daarvoor echter het gebruik van *malware* nodig zijn. Deze *malware* kan nodig zijn om bijvoorbeeld de *webcam* of microfoon van een computer te gebruiken of om er zorg voor te dragen dat enige tijd toegang tot het geautomatiseerde werk gegarandeerd is omdat het enige tijd duurt om de gewenste gegevens te kopiëren. De *malware* is dan bijvoorbeeld bedoeld om de gebruiker van het geautomatiseerde werk niet te laten vermoeden dat er gegevens van zijn of haar geautomatiseerd werk gekopieerd wordt.

Als de *malware* voor bovenstaande doelen worden gebruikt, kan het gebruik van de *malware* worden aangemerkt als 'het aanbrengen van technische voorzieningen' ten einde de versleuteling van gegevens die in het geautomatiseerde werk worden verwerkt en/of opgeslagen tegen te gaan dan wel om de gegevens die in het geautomatiseerde werk worden verwerkt en/of opgeslagen over te nemen.

[114] Briefing (18 december 2013) AIVD en MIVD aan de Tweede Kamer omtrent interceptie, dia 14-15.

4.2.7 Aftappen, opnemen en afluisteren

De zesde bevoegdheid van de MIVD is vastgelegd in artikel 25. De MIVD mag volgens dit artikel, ongeacht waar een en ander plaatsvindt, gericht elke vorm van gesprek, telecommunicatie en gegevensoverdracht door middel van een geautomatiseerd werk aftappen, opnemen en afluisteren. Indien daarbij gebruik moet worden gemaakt van technische hulpmiddelen, is dit eveneens toegestaan.[115] Met het gericht aftappen, opnemen en afluisteren van gesprekken wordt bijvoorbeeld bedoelt dat met richtmicrofoons gesprekken worden afgeluisterd en/of opgenomen. Bij afluisteren en/of opnemen van telecommunicatie moet worden gedacht aan een telefoontap op een bepaald telefoonnummer of telefoontoestel.

Deze bevoegdheid (in zijn geheel) mag pas worden uitgeoefend als aan een aantal voorwaarden is voldaan. Er dient een verzoek met een aantal zaken (telefoonnummer of IP-adres, identiteit van de persoon of organisatie en de reden tot uitoefenen van de bevoegdheid) ingediend te worden, welke moet worden goedgekeurd door de minister. Daarmee geeft de minister toestemming aan het hoofd van de MIVD om de bevoegdheid uit te (mogen) voeren.[116]

Ook is het de MIVD onder deze bevoegdheid, wederom in relatie tot het cyberdomein, toegestaan om gegevensoverdracht binnen een geautomatiseerd ‘af te tappen’ en ‘op te nemen’. Dat klinkt misschien ingewikkeld, maar hiermee wordt bedoeld dat de MIVD het dataverkeer, de dataoverdracht (gegevensoverdracht), tussen bijvoorbeeld verschillende computers mag aftappen en opnemen.[117] Daarnaast stelt de CTIVD dat: *“Op grond van dit artikel kan de AIVD* [maar ook de MIVD, want beiden beschikken over dezelfde (bijzondere) bevoegdheden] *bijvoorbeeld gesprekken opnemen met behulp van een microfoon, telefoongesprekken aftappen, e-mailberichten lezen en het internetgedrag van een persoon in de gaten houden.”*.[118]

[115] Artikel 25 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

[116] Kamerstukken II 1997/98, 25 877, nr. 3, p. 40-43.

[117] Kamerstukken II 1997/98, 25 877, nr. 3, p. 40-43.

[118] Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2009), p. 5.

Het afluisteren en/of opnemen van telecommunicatie heeft dus niet alleen betrekking op telefoongesprekken[119], zoals ook in de memorie van toelichting wordt aangehaald[120], maar kan ook betrekking hebben op internetverkeer. Met behulp van een zogeheten internettap (te vergelijken met een telefoontap) kan dan het internetgedrag van een bepaald IP-adres (gekoppeld aan een bepaald persoon) in de gaten worden gehouden.[121]

Tevens kan bij een brede interpretatie van artikel 25 worden gedacht aan het afluisteren en opnemen van gesprekken door gebruik te maken van de (al dan niet ingebouwde) microfoon of *webcam* met spreekfunctie van een computer, laptop, *tablet* of zelfs mobiele telefoon. Ook kan worden gedacht aan de inhoud van e-mails, SMS-berichten of berichten (waaronder afbeeldingen en films) die via *social media* (bijvoorbeeld via Whats App, Facebook Messenger of Snap Chat) aan elkaar worden verzonden.[122]

4.2.8 Ontvangen en opnemen niet-kabelgebonden telecommunicatie

Verbonden met de zesde bijzondere bevoegdheid, is de zevende bijzondere bevoegdheid van de MIVD, welke is vastgelegd in artikel 26. Artikel 26 stelt dat de MIVD bevoegd is om ter verkenning niet-kabelgebonden telecommunicatie, vanuit of naar het buitenland, te ontvangen en op te nemen. Als daarbij versleuteling van de communicatie ongedaan moet worden gemaakt, is de MIVD daar eveneens toe bevoegd volgens dit artikel.[123]

---

[119] Volgens de AIVD en MIVD gaat het naast telefoonnummers ook over IP-adressen, de route van de communicatie, de omvang van het bericht, de lengte van het gesprek enzovoorts. Daarnaast gaat het bij de inhoud niet alleen om telefoongesprekken, maar om gesproken woorden in het algemeen, films, afbeeldingen, body van e-mails, SMS-berichten enzovoorts. Zie: Briefing (18 december 2013) AIVD en MIVD aan de Tweede Kamer omtrent interceptie, dia 8.

[120] Kamerstukken II 1997/98, 25 877, nr. 3, p. 41.

[121] Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2009), p. 6-7.

[122] Briefing (18 december 2013) AIVD en MIVD aan de Tweede Kamer omtrent interceptie, dia 8.

[123] Artikel 26 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

Deze bijzondere bevoegdheid staat ook wel bekend als *searchen*. In de Nota van Wijziging van 29 september 1999 wordt het begrip *searchen* nader uitgelegd: *"Bij het zogeheten «searchen» tracht men door het verkennen van de telecommunicatie, te achterhalen wat de aard van de telecommunicatie is die over bepaalde frequenties (technische kenmerken) loopt en welke persoon of organisatie van de desbetreffende telecommunicatie de afzender is (de «identiteit»). Voorts – in combinatie met de eerdergenoemde gegevens – is het «searchen» erop gericht om vast te stellen of het hier gaat om telecommunicatie waarvan kennisneming voor een goede taakuitvoering van de diensten noodzakelijk is."*.[124]

Er wordt dus gekeken of de inhoud van de ontvangen en opgenomen niet-kabelgebonden telecommunicatie mogelijk van belang is voor een goede taakuitvoering. Indien de MIVD van mening is dat bovenstaande het geval is, zal conform artikel 25 toestemming moeten worden gevraagd voor de zogeheten gerichte interceptie.

Tevens dient, in relatie tot deze bijzondere bevoegdheid, opgemerkt te worden dat het niet-kabelgebonden telecommunicatie betreft met zijn oorsprong of bestemming in andere landen. Volgens de zojuist aangehaalde Nota van Wijziging betekent dit dat niet-kabelgebonden telecommunicatie die zich volledig binnen Nederland afspeelt, onder de bevoegdheid van artikel 25 valt en niet onder deze bevoegdheid (artikel 26).[125] Zoals ook in de Nota naar aanleiding van een nader verslag (NNV) van 19 maart 2001 wordt gesteld: *"«Searchen» op binnenlandse telecommunicatie is niet toegestaan."*.[126]

In relatie tot het cyberdomein betekent dit dat allerlei niet-kabelgebonden telecommunicatie kan worden opgevangen en opgenomen. Ook SMS-berichten en berichten via *social media*, zoals Whats App, Facebook Messenger en Snap Chat zijn niet-kabelgebonden en kunnen derhalve, bij een brede interpretatie van deze bijzondere bevoegdheid, worden ontvangen en opgenomen. Uiteraard geldt ook voor deze niet-kabelgebonden telecommunicatie dezelfde criteria, namelijk dat het ontvangen en opnemen slechts ter verkenning is (doelbewust kennisnemen van de inhoud kan op basis van artikel 25) en dat binnenlandse telecommunicatie niet onder deze bevoegdheid valt.

[124] Nota van Wijziging (1999), p. 21.

[125] Nota van Wijziging (1999), p. 23-24.

[126] Nota naar aanleiding van het nader verslag (2001), p. 36.

4.2.9 Ongericht ontvangen en opnemen niet-kabelgebonden telecommunicatie

Artikel 27, waarin de achtste bijzondere bevoegdheid van de MIVD is weggelegd, lijkt op artikel 26. Toch zijn er verschillen. De frase 'die zijn oorsprong of bestemming in andere landen heeft' ontbreekt. Ook wordt (in lid 3) gesproken over een nadere selectie van de middels deze bevoegdheid verzamelde gegevens.[127] Bij deze bevoegdheid is het toegestaan om etherverkeer (in de ruimste zin van het woord) op te vangen en op te nemen. Hierbij moet bijvoorbeeld gedacht worden aan telecommunicatieverkeer dat via een satellietkanaal plaatsvindt of op een bepaalde frequentie wordt uitgezonden. Het betreft hier dus geen interceptie van berichten afkomstig van een specifiek persoon of een specifieke organisatie waarop men zich richt. De nadere selectie kan, op basis van een andere bevoegdheid, wel plaatsvinden aan de hand van een technisch kenmerk, een persoon of een organisatie.[128]

Aangezien deze bevoegdheid zich niet specifiek tegen een persoon of organisatie richt dan wel gerelateerd is aan een technisch kenmerk, hoeft geen toestemming van de minister te worden verkregen om deze bevoegdheid uit te voeren. Indien de MIVD gericht wenst te zoeken binnen de ongericht opgevangen communicatie, dan dient wel toestemming aan de minister, of het daartoe gemandateerde hoofd van de MIVD, worden gevraagd. Deze bevoegdheid is vastgelegd in artikel 25, waar gericht naar personen of organisaties wordt afgeluisterd. Wordt louter naar een bepaald woord of een combinatie van woorden gezocht in de ongericht opgevangen communicatie, wordt deze toestemming voor één jaar verleend.

Dit in tegenstelling tot alle andere gevallen (waarin selectie plaatsvindt), waarin de toestemming slechts voor drie maanden wordt verleend. Reden voor dit verschil is dat bij het gericht zoeken naar bepaalde woorden in ongericht verzamelde communicatie, niet direct inbreuk wordt gemaakt op persoonlijke levenssfeer.[129] Bij het selecteren, bijvoorbeeld op basis van identiteit, nummer (waaronder IP-adres)[130] of een nader omschreven onderwerp, wordt namelijk wel (of in meerdere mate) inbreuk gemaakt op de persoonlijke levenssfeer. In relatie tot het cyberdomein kan worden aangesloten bij wat er in de vorige paragraaf is gesteld met betrekking tot SMS-berichten en berichten via *social media*. Om kennis te nemen van de inhoud van dergelijke berichten dient conform artikel 25 van de WIV te worden gehandeld.

---

[127] Artikel 27 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

[128] Kamerstukken II 1997/98, 25 877, nr. 3, p. 44.

[129] Kamerstukken II 1997/98, 25 877, nr. 3, p. 44-46.

[130] Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2009), p. 6-7.

4.2.10 Opvragen verkeersgegevens

In artikel 28 wordt de negende bevoegdheid van de MIVD vermeld.[131] De memorie van toelichting verduidelijkt de wat lastige wetstekst. Het is de MIVD toegestaan om zogeheten verkeersgegevens op te vragen van natuurlijke- dan wel rechtspersonen die een overeenkomst zijn aangegaan met een aanbieder tot het gebruik van een openbaar telecommunicatienetwerk of tot de levering van een openbare telecommunicatiedienst. Naast de personen die een overeenkomst zijn aangegaan is de MIVD ook bevoegd de verkeersgegevens op te vragen van natuurlijke- dan wel rechtspersonen die daadwerkelijk gebruik maken van het openbare telecommunicatienetwerk en/of de openbare telecommunicatiedienst.

De verkeersgegevens waarover wordt gesproken betreft al het verkeer dat over telecommunicatie-infrastructuur of telecommunicatie-inrichtingen plaatsvindt. Tevens betreft het gegevens die gekoppeld zijn aan een bepaald (telefoon)nummer. Ook is het mogelijk de verkeersgegevens op te vragen van specifieke personen of organisaties. De gegevens die opgevraagd kunnen worden, kunnen bestaan uit zowel uitgaande als binnenkomende oproepen of verbindingen die worden gelegd met het betreffende (telefoon)nummer, de betreffende persoon of de betreffende organisatie. Bij gegevens kan men in deze situatie denken aan aanvangstijd, duur en eindtijd van oproepen en/of verbindingen. Ook kan worden gedacht aan gegevens met betrekking tot bepaalde (telefoon)nummers, personen of organisaties waarmee verbindingen worden gelegd door het betreffende telefoonnummer, de betreffende persoon of de betreffende organisatie. Tevens betreft het mogelijke gegevens over de identiteit van personen en/of organisaties aan wie het te volgen (telefoon)nummer is gekoppeld. De persoon of instantie die over de gewenste gegevens beschikt is, volgens deze wet, verplicht de gegevens te verstrekken aan de MIVD. Het betreft zowel gegevens die reeds voor het verzoek van de MIVD zijn verwerkt, als gegevens die na het verzoek nog binnenkomen en nog (moeten) worden verwerkt.[132]

[131] Artikel 28 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

[132] Kamerstukken II 1997/98, 25 877, nr. 3, p. 46-47.

Wat echter volgens de CTIVD niet onder deze bepaling valt zijn SMS-berichten. Bij het versturen van de gegevens met betrekking tot SMS-berichten wordt meteen de inhoud van die SMS-berichten meegestuurd. Deze inhoud wordt echter beschermd door het telefoongeheim, dat is vastgelegd in artikel 13 van de Grondwet. Ook internetverkeer dat wordt opgevraagd waarvan de bezochte websites worden meegestuurd (lees: waarvan de inhoud wordt meegestuurd), valt niet onder de bepaling van artikel 28. Uit voorgaande kan tevens worden afgeleid dat enige andere vorm van telecommunicatie waarvan de inhoud wordt meegezonden (denk bijvoorbeeld aan Whats App berichten) niet onder deze bepaling valt. Desalniettemin kunnen betreffende gegevens van SMS-berichten (op basis van een telefoonnummer), internetverkeer (op basis van een IP-adres) en andere vormen van telecommunicatie waarvan de inhoud wordt meegestuurd wel worden opgevraagd, zij het dat dit dient te gebeuren onder de noemer van artikel 25.[133]

4.2.11 Opvragen abonneegegevens

Aansluitend op de bijzondere bevoegdheid uit artikel 28, is het volgens de tiende bevoegdheid van de MIVD, vastgelegd in artikel 29, toegestaan om zogeheten abonneegegevens op te vragen. Het betreft hier bijvoorbeeld gegevens met betrekking tot de naam, het adres, de postcode, het nummer en de soort dienst waarvan de gebruiker gebruik maakt.[134] Eveneens als bij artikel 28 gaat het hier om gegevens van natuurlijke- dan wel rechtspersonen die een overeenkomst zijn aangegaan dan wel daadwerkelijk gebruik maken van diensten zoals deze zijn genoemd in het tweede lid van zowel artikel 28 als 29.

Daarnaast wordt aangesloten bij wat in de vorige paragraaf, betreffende de bijzondere bevoegdheid van artikel 28, is vermeld, namelijk dat naast het telefoonnummer ook een IP-adres op grond van deze bevoegdheid achterhaald kan worden. Is het achterhalen van het (telefoon)nummer of IP-adres echter bedoeld om vervolgens een tap (telefoontap dan wel internettap) te plaatsen, dan dient het nummer of IP-adres verkregen te worden op basis van artikel 25 WIV.[135]

[133] Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2009), p. 9-10.

[134] Artikel 29 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

[135] Kamerstukken II 1997/98, 25 877, nr. 3, p. 48.

4.3 Overige bevoegdheden ten behoeve van de taakuitvoering

Naast de tien bovenstaande bijzondere bevoegdheden van de MIVD, beschikt de MIVD over aanvullende mogelijkheden ten behoeve van haar taakuitvoering. Bij het uitvoeren van de bijzondere bevoegdheden kan toegang tot een bepaalde plaats noodzakelijk zijn. Artikel 30 van de WIV voorziet in deze behoefte. Volgens dit artikel heeft de MIVD toegang tot elke plaats, mits dit redelijkerwijs nodig is om een aantal bijzondere bevoegdheden uit te voeren. Het betreft hier de bevoegdheden zoals vastgelegd in artikel 20, lid 1 onder a (het aanbrengen van observatie- en registratiemiddelen), artikel 20, lid 1 onder b (het aanbrengen van volgmiddelen, plaatsbepalingsapparatuur, registratiemiddelen), artikel 22, lid 1 onder a, artikel 24 en artikel 25.[136]

Eerder in dit onderzoek is vermeld dat MIVD de bijzondere bevoegdheden ook mag inzetten ten behoeve van de buitenlandtaak. De zojuist genoemde bepaling met betrekking tot de toegang tot elke plaats is dus ook van toepassing op de buitenlandtaak van de MIVD. Deze bepaling is van belang voor de MIVD indien de MIVD toegang wil tot een plaats binnen Nederland om gegevens te verzamelen met betrekking tot een ander land. Het moge echter duidelijk zijn dat soevereiniteit van een andere staat worden geschonden als de MIVD deze bevoegdheid buiten de grenzen van Nederland zal uitvoeren. Men is dan namelijk fysiek aanwezig op het territorium van een andere staat. Indien hiertoe geen toestemming is verkregen door de staat waar de MIVD verblijft, dan is de aanwezigheid een inbreuk op de soevereiniteit van de betreffende staat.

In relatie tot het cyberdomein is deze aanvullende bevoegdheid minder relevant. Zojuist is al gesteld dat deze bevoegdheid kan worden gebruikt om toegang te verkrijgen tot elke plaats waar men fysiek aanwezig dient te zijn. Men kan dan denken aan het plaatsen van microfoons of videoapparatuur op de betreffende plaats of men kan denken aan het verzamelen van gegevens door binnen te dringen in een geautomatiseerd werk. Wordt één van deze bevoegdheden op afstand toegepast (het virtueel ‘plaatsen’ van microfoons, dus het gebruik maken van *webcams* of microfoons van bijvoorbeeld laptops of het op afstand binnendringen van een geautomatiseerd werk), dan wordt niet fysiek de plaats betreden en zal deze aanvullende bevoegdheid niet nodig zijn.[137]

[136] Artikel 30 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

[137] Kamerstukken II 1997/98, 25 877, nr. 3, p. 48.

4.4 Overige mogelijkheden MIVD

Naast alle (bijzondere) bevoegdheden van de MIVD, die in de WIV zijn vastgelegd, om gegevens te verzamelen, heeft de MIVD nog een aantal andere opties voor het verzamelen van gegevens. Deze opties zijn niet allemaal direct opgenomen in de WIV, maar wel uit de WIV af te leiden. Een tweetal aanvullende mogelijkheden zal worden besproken.

4.4.1 Open bronnen

Ten eerste beschikt de MIVD over de mogelijkheid tot het raadplegen van bronnen die voor eenieder toegankelijk zijn. Dit zijn de zogenaamde *open sources* (open bronnen). Hiervoor kan de MIVD bijvoorbeeld gebruik maken van het internet (maar ook van meer klassieke open bronnen als kranten). Hoewel het internet niet altijd even betrouwbaar is, aangezien eenieder op internet kan plaatsen wat hij of zij wil, kunnen gegevens op het wereldwijde web wel een indicatie geven over de gewenste gegevens.

Wil men bijvoorbeeld weten over welke wapens een bepaalde staat beschikt of wil men weten wat voor vaste tactieken, technieken en procedures een bepaalde staat heeft met betrekking tot het uitvoeren van bepaalde operaties, dan kan daarvoor voor een ieder toegankelijke bronnen worden gebruikt (denk naast internet bijvoorbeeld ook aan openbaar beschikbare handleidingen of leidraden van andere krijgsmachten).

In principe is bovenstaande mogelijkheid van de MIVD ook in de WIV vastgesteld. Artikel 31 van de WIV stelt namelijk dat de (bijzondere) bevoegdheden van de MIVD pas mogen worden toegepast indien de gewenste informatie niet uit open bronnen dan wel uit bronnen waar de MIVD reeds toegang tot heeft, kan worden verkregen.[138] Indien dit alles niet mogelijk is, is het de MIVD toegestaan om (op bepaalde voorwaarden) de bijzondere bevoegdheden te gebruiken om alsnog aan de gewenste gegevens te komen.[139]

[138] Artikel 31 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

[139] Kamerstukken II 1997/98, 25 877, nr. 3, p. 52.

4.4.2 Partnerdiensten

Naast bovenstaande mogelijkheid tot het raadplegen van openbare bronnen, heeft de MIVD nog een andere optie om gegevens te verzamelen. Deze mogelijkheid is af te leiden uit artikel 36. In het eerste lid van artikel 36 is vermeld dat de MIVD, in het kader van een goede taakuitvoering bevoegd is om omtrent door, of ten behoeve van, de dienst verwerkte gegevens mededeling te doen aan een aantal partijen. In het eerste lid onder d valt te lezen dat deze bevoegdheid geldt voor het meedelen aan de daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen, alsmede andere daarvoor in aanmerking komende internationale beveiliging- verbindingsinlichtingen- en inlichtingenorganen.[140]

Dit houdt in dat de door de MIVD verzamelde gegeven mogen worden verstrekt aan bijvoorbeeld (buitenlandse) partnerinlichtingendiensten. Andersom moet dit dan ook mogelijk zijn. De MIVD moet dan ook in staat zijn om gegevens te verkrijgen van (buitenlandse) partnerinlichtingendiensten. De CTIVD is eveneens van mening dat: *"Buitenlandse inlichtingendiensten zijn een belangrijke bron van informatie voor de onderzoeken in het kader van de inlichtingentaak."*.[141] Hoewel het hier een rapport omtrent de activiteiten van de AIVD betreft, kan eenzelfde redenering worden gevolgd voor de MIVD, aangezien beide diensten een inlichtingentaak buitenland in hun takenpakket hebben.

Dit schept een extra mogelijkheid voor de MIVD om aan gegevens te komen. Mocht de MIVD bijvoorbeeld geen toestemming krijgen om een bepaalde bijzondere bevoegdheid uit te voeren of heeft de MIVD een vermoeden dat een partner(inlichtingen)dienst wel over de gewenste gegevens beschikt, kan de MIVD zich tot betreffende partner richten om de gegevens te verzamelen, zonder daarvoor gebruik te maken van de in de WIV toegestane bijzondere bevoegdheden. Deze mogelijkheid is tweeledig. Enerzijds kan de MIVD namelijk contact zoeken met de partnerdienst in de staat waarover de MIVD gegevens wil hebben. Anderzijds kan de MIVD zich richten tot partnerdiensten in 'derde' staten die mogelijk reeds over de gegevens gewenste gegevens van een andere staat beschikken.

[140] Artikel 36 van de Wet op Inlichtingen- en Veiligheidsdiensten (2002).

[141] Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2011a), p. 17.

4.5 Subconclusie

In dit hoofdstuk stond de vraag centraal welke bevoegdheden de MIVD heeft, op basis van de WIV 2002, voor het verzamelen van inlichtingen in het cyberdomein. In artikel 18 van de WIV is vastgelegd dat alle bijzondere bevoegdheden mogen worden ingezet ten behoeve van de a-taak, de c-taak en de e-taak van de MIVD. De bijzondere bevoegdheden zijn door de wetgever zo techniekloos mogelijk geformuleerd. Enerzijds om middelen die, door technologische innovaties, in de toekomst worden ontwikkeld onder de reikwijdte van de bijzondere bevoegdheden te laten vallen. Anderzijds om zo min mogelijk inzicht te geven in de middelen en mogelijkheden die de MIVD heeft om de bevoegdheden uit te voeren.

Hoewel de wetgever de bijzondere bevoegdheden zo techniekloos mogelijk heeft geformuleerd, stelt zowel de CTIVD (in 2011) als de evaluatiecommissie (in 2013) dat de WIV 2002 niet voldoet aan de technologische ontwikkelingen van het afgelopen decennium. Toch zijn aantal bijzondere bevoegdheden te bezien in het kader van het cyberdomein.

Op basis van de artikelen 12 en 17 uit de WIV heeft de MIVD de bevoegdheid tot het verzamelen van gegevens. Daarnaast heeft de MIVD de beschikking over een tiental bijzondere bevoegdheden om deze gegevens te verzamelen. In het cyberdomein zijn een aantal van deze bijzondere bevoegdheden relevant. Van een ander aantal zijn slechts delen van de bijzondere bevoegdheden relevant in het cyberdomein. Zie tabel 4.2.

Artikel	**(Deel van de) bijzondere bevoegdheid relevant in het cyberdomein**
Artikel 20	Observeren en volgen
Artikel 21	Alleen de oprichting van rechtspersonen
Artikel 22	Alleen het vaststellen van identiteit
Artikel 24	Binnendringen in een geautomatiseerd werk
Artikel 25	Aftappen, opnemen en afluisteren
Artikel 26	Ontvangen en opnemen niet-kabelgebonden telecommunicatie
Artikel 27	Ongericht ontvangen en opnemen niet-kabelgebonden telecommunicatie
Artikel 28	Opvragen verkeersgegevens
Artikel 29	Opvragen abonneegegevens

Tabel 4.2 Bijzondere bevoegdheden MIVD

In dit hoofdstuk is een aantal cybermogelijkheden besproken in relatie tot de bijzondere bevoegdheden van de MIVD. Zo is het tegenwoordig mogelijk om op basis van de bijzondere bevoegdheid uit artikel 20, na toegang te hebben verschaft tot een geautomatiseerd werk, middels de (al dan niet ingebouwde) *webcam* personen of zaken te volgen en te observeren. Ook kunnen, indien via het cyberdomein toegang wordt verschaft, personen of zaken worden gevolgd met behulp van informatie uit een navigatiesysteem. Daarnaast kan bij het, op basis van artikel 22, vaststellen van de identiteit van een persoon, gebruik worden gemaakt van de (al dan niet ingebouwde) *webcam* of microfoon van bijvoorbeeld een computer.

Ook kan, op basis van artikel 24 van de WIV, een geautomatiseerd werk worden binnengedrongen. Onder een geautomatiseerd werk wordt (naast computers) verstaan: elke inrichting ten behoeve van opslag, verwerking en overdracht van gegevens. Denk daarbij bijvoorbeeld aan de mogelijkheid tot het binnendringen van fysieke inrichtingen als laptops, *tablets*, mobiele telefoons en *PDA's*, maar denk ook aan het binnendringen van niet-fysieke (digitale) inrichtingen zoals webfora. Bij het verschaffen van toegang tot deze geautomatiseerde werken mag enige vorm van beveiliging (bijvoorbeeld wachtwoorden of *firewalls*) worden doorbroken. Daarnaast mogen technische voorzieningen (in bijvoorbeeld de computer) worden aangebracht om de gewenste gegevens te kopiëren. Denk hierbij bijvoorbeeld aan het gebruik van *malware*.

Tevens kan op basis van artikel 25 elke vorm van gesprek, telecommunicatie en gegevensoverdracht binnen een geautomatiseerd werk worden afgetapt, worden opgenomen en worden afgeluisterd. Dat betekent dat gegevens die worden verstuurd tussen inrichtingen ten behoeve van opslag, verwerking en overdracht van gegevens (zie voorbeelden hierboven) kunnen worden afgetapt en opgenomen. Hieronder valt ook het lezen van e-mails en het in de gaten houden van het internetgedrag van bepaalde personen. Daarnaast kunnen ook gesprekken worden opgenomen die worden gevoerd (of kunnen worden ontvangen) via de microfoon van een geautomatiseerd werk.

Volgens de bijzondere bevoegdheid uit artikel 26 kan niet-kabelgebonden telecommunicatie worden opgevangen en opgenomen. Hieronder vallen ook SMS-berichten dan wel berichten die via *social media* (zoals Whats App, Facebook Messenger en Snap Chat) worden verzonden. Opgemerkt dient te worden dat dit louter ter verkenning is en dat voor kennisneming van de inhoud van de betreffende berichten conform artikel 25 WIV dient te worden gehandeld.

Tot slot kunnen, op basis van artikel 28 en 29, zogeheten verkeers- en abonneegegevens worden opgevraagd. Dit gaat op basis van een nummer. Onder nummer kan men, naast een telefoonnummer, ook het IP-adres van bijvoorbeeld een computer (of ander geautomatiseerd werk dat is aangesloten op het internet) verstaan. Bij de gegevens die op grond van deze bijzondere bevoegdheden kunnen worden opgevraagd kan men denken aan de aanvangstijd, duur en eindtijd van een gesprek of gelegde verbinding. Wil men echter kennisnemen van de inhoud van de gesprekken, het internetgedrag of de berichten, dan dient gehandeld te worden conform artikel 25 van de WIV.

Naast de bijzondere bevoegdheden heeft de MIVD nog een tweetal aanvullende mogelijkheden om gegevens te verzamelen (in het cyberdomein). Ten eerste kunnen zij gebruik maken van open bronnen. De wet schrijft dit in principe ook voor: er mag pas gebruik worden gemaakt van bijzondere bevoegdheden als de gewenste informatie niet uit open bronnen kan worden verkregen. Ten tweede kan de MIVD, bijvoorbeeld als geen toestemming wordt verleend tot het uitoefenen van bijzondere bevoegdheden, zich richten tot partner(inlichtingen)diensten die mogelijk over de gewenste gegevens beschikken.

Het is nu duidelijk welke bevoegdheden de MIVD heeft, op basis van de WIV, voor het verzamelen van gegevens in het cyberdomein. Daarnaast is aangetoond dat de WIV, hoewel de wet geen extraterritorialiteitsbeginsel bevat, naar analogie wordt toegepast in het buitenland. Ook zijn de beginselen van non-interventie en soevereiniteit uiteengezet in het theoretisch kader. Deze drie hoofdstukken zullen in de conclusie worden gecombineerd om antwoord te geven op de onderzoeksvraag welke mogelijkheden de MIVD heeft, op basis van de bevoegdheden uit de WIV, om binnen de grenzen van het internationaal recht extraterritoriaal inlichtingen te verzamelen in het cyberdomein.

5. Conclusie

Het cyberdomein speelt een steeds grotere rol in het leven van de mens. Ook voor krijgsmachten wordt het cyberdomein steeds belangrijker. Het verzamelen van inlichtingen gebeurt bijvoorbeeld steeds vaker door gebruik te maken van dit domein. In dit onderzoek stond de vraag centraal welke mogelijkheden de MIVD heeft voor tot het extraterritoriaal verzamelen van inlichtingen in het cyberdomein, binnen de grenzen van het internationaal recht.

Om deze vraag te beantwoorden zijn een drietal deelvragen opgesteld, welke allen zijn uitgewerkt in een apart hoofdstuk. Na de inleiding volgde een theoretisch kader met een tweetal internationaalrechtelijke beginselen waarmee extraterritoriale inlichtingenactiviteiten in het cyberdomein mogelijk in conflict kunnen komen. Vervolgens is een hoofdstuk besteed aan de WIV 2002 en de mogelijke extraterritoriale werking van die wet. Zowel de AIVD als de MIVD opereren op basis van deze wet. Daarna volgde een hoofdstuk met de (bijzondere) bevoegdheden van de MIVD, welke in de WIV 2002 zijn weggelegd. Al deze bevoegdheden van de MIVD zijn tevens bezien in het licht van het cyberdomein.

In deze conclusie zullen alle bevindingen uit dit onderzoek nog eens kort de revue passeren. Daartoe zullen de subconclusies van de verschillende hoofdstukken kort worden behandeld. Vervolgens zullen de drie subconclusies worden samengevoegd om antwoord te geven op de hoofdvraag welke mogelijkheden de MIVD heeft, op basis van de bevoegdheden die in de WIV 2002 zijn vastgelegd, voor het extraterritoriaal verzamelen van inlichtingen in het cyberdomein, binnen de grenzen van het internationaal recht.

5.1 Begrenzing internationaal recht

Een tweetal internationaalrechtelijke beginselen wordt impliciet of expliciet genoemd in het VN Handvest. Tevens gelden deze twee beginselen als internationaal gewoonterecht. Het betreft de beginselen van non-interventie en soevereiniteit. In de inleiding werd ook nog gesproken over het geweldsverbod. In diezelfde inleiding werd echter reeds duidelijk dat het extraterritoriaal verzamelen van inlichtingen (in het cyberdomein) doorgaans geen fysiek geweld, *use of (armed) force*, oplevert. Indien een activiteit geen fysiek geweld oplevert, wordt het geweldsverbod niet geschonden. Daarom is het geweldsverbod verder uitgesloten van het onderzoek en werd de focus in dit onderzoek gelegd op het non-interventiebeginsel en het soevereiniteitsbeginsel.

5.1.1 Non-interventiebeginsel

In het theoretisch kader, hoofdstuk twee, is nadrukkelijk aandacht besteed aan een tweetal beginselen. Allereerst werd het non-interventiebeginsel uiteengezet. Er is sprake van een verboden interventie als de ene staat met een actie (lees: het extraterritoriaal verzamelen van inlichtingen) een verandering in beleid beoogd in de andere staat, dan wel dat er met de actie daadwerkelijk een verandering in het beleid van de andere staat plaatsvindt. Daarnaast moet deze verandering niet vrijwillig, maar door dwang (*coercion*) plaatsvinden. Als aan deze twee voorwaarden wordt voldaan spreekt men van een verboden interventie en wordt het non-interventiebeginsel geschonden. Deze lijn wordt doorgetrokken naar het cyberdomein. Men spreekt dan over een zogeheten cyberinterventie. Een verboden cyberinterventie dient aan exact dezelfde voorwaarden te voldoen als een 'normale' interventie (het dwangelement en het beogen of teweegbrengen van een verandering in beleid moeten aanwezig zijn).

5.1.2 Soevereiniteitsbeginsel

Naast het non-interventiebeginsel is aandacht besteed aan het soevereiniteitsbeginsel. Uit de vele omschrijvingen en definities van soevereiniteit is een omschrijving gekozen om in dit onderzoek te hanteren: de staat is autonoom en (politiek) onafhankelijk van andere staten en de staat is vrij, zonder inmenging van andere staten, in het maken van zijn eigen keuzes, inclusief het vormen van buitenlands beleid.

Evenals voor het non-interventiebeginsel is voor het soevereiniteitsbeginsel uiteengezet wanneer dit beginsel doorgaans zal worden geschonden. Het fysiek aanwezig zijn in de andere staat, om daar inlichtingen te verzamelen, zal doorgaans een schending van de soevereiniteit van die staat opleveren, tenzij toestemming is verleend voor het ontplooien van dergelijke activiteiten op het territoir van die staat. Ook vindt er een schending van het soevereiniteitsbeginsel plaats indien er, zonder fysiek aanwezig te zijn op het territoir van die staat, fysieke effecten worden veroorzaakt op het territoir van de andere staat. Daarnaast levert het uitoefenen van handhavende rechtsmacht (jurisdictie) op het territoir van een andere staat doorgaans een schending van het soevereiniteitsbeginsel op, tenzij hierover andere afspraken zijn gemaakt met de betrokken staat.

Verschillende auteurs hebben deze lijn doorgetrokken naar het cyberdomein, aangezien het tegenwoordig mogelijk is om middels het cyberdomein inlichtingen te verzamelen. Wordt dus middels cyberactiviteiten (bijvoorbeeld het extraterritoriaal verzamelen van inlichtingen via het cyberdomein) handhavende rechtsmacht uitgeoefend of worden er fysieke effecten veroorzaakt op het territoir van die staat, dan spreekt men van een soevereiniteitsschending.

5.2 Extraterritoriale werking WIV

Na een hoofdstuk met betrekking tot het internationaal recht, volgde hoofdstuk drie. Hoofdstuk drie had betrekking op zowel het internationaal- als het nationaal recht. In dit hoofdstuk stond de vraag centraal in hoeverre de WIV van 2002 extraterritoriaal geldig is. Gezien het takenpakket van de MIVD, leek een antwoord op de vraag snel gevonden. De zogeheten e-taak van de MIVD betreft de inlichtingentaak buitenland: er dient onderzoek verricht te worden naar andere staten.

Toch ligt het gecompliceerder dan hierboven wordt geschetst. De WIV is namelijk een nationale wet. Nationale wetten zijn in het beginsel niet internationaal geldig. De WIV vormt geen uitzondering op deze regel. In de WIV is geen extraterritorialiteitsbeginsel opgenomen en derhalve niet geldig in het buitenland volgens de CTIVD en de evaluatiecommissie. Desalniettemin stellen zowel de CTIVD als de evaluatiecommissie dat de WIV naar analogie moet worden toegepast in het buitenland. Daarnaast impliceert ook de Minister van Binnenlandse Zaken en Koninkrijksrelaties De Vries in 2001 dat de (bijzondere) bevoegdheden van de MIVD in het buitenland kunnen worden uitgeoefend.

5.3 Bevoegdheden MIVD

Hoewel de WIV geen extraterritorialiteitsbeginsel bevat, wordt de WIV wel naar analogie in het buitenland toegepast. Derhalve kunnen ook de (bijzondere) bevoegdheden van de MIVD in het buitenland worden uitgeoefend. In eerste instantie is de algemene bevoegdheid tot het vergaren van gegevens weggelegd in de artikelen 12 en 17 van de WIV. Het verzamelen van gegevens is gebonden aan verschillende voorwaarden zoals proportionaliteit en subsidiariteit (artikel 31). Daarnaast staan in artikel 20 tot en met 29 de bijzondere bevoegdheden van de MIVD. Volgens artikel 18 van de WIV kunnen deze bijzondere bevoegdheden worden ingezet ten behoeve van de a-taak, de c-taak en de e-taak.

De wetgever heeft de bijzondere bevoegdheden om twee redenen zo techniekloos mogelijk geformuleerd. Ten eerste wilde de wetgever het hiermee mogelijk maken om middelen die door technologische innovatie worden ontwikkeld (en kunnen worden gebruikt bij het uitvoeren van de bijzondere bevoegdheden) onder de reikwijdte van de bijzondere bevoegdheden te vallen. Daarnaast beoogde de wetgever zo min mogelijk inzicht te geven in de middelen en mogelijkheden die de MIVD heeft ten aanzien van het uitvoeren van de bijzondere bevoegdheden. Toch stellen zowel de CTIVD (in 2011) als de evaluatiecommissie (in 2013) dat de WIV 2002 niet voldoet aan de technologische ontwikkelingen van het afgelopen decennium.

Met betrekking tot het cyberdomein zijn verschillende bijzondere bevoegdheden interessant. Zo is het op basis van artikel 20 bijvoorbeeld mogelijk om gebruik te maken van (al dan niet ingebouwde) *webcams* en navigatiesystemen om personen te volgen en observeren. Om deze bevoegdheid uit te voeren dient echter eerst toegang te worden verschaft tot een geautomatiseerd werk, wat is toegestaan volgens de bijzondere bevoegdheid van artikel 24.

In gevolge van artikel 26 is het mogelijk om niet-kabelgebonden telecommunicatie op te vangen en op te nemen. In relatie tot het cyberdomein kan dan ook worden gedacht aan e-mails, SMS-berichten en berichten (waaronder afbeeldingen en films) die via *social media* worden verzonden. Ook kunnen, op basis van artikel 28 en 29, zogeheten verkeers- dan wel abonneegegevens worden opgevraagd. Denk bijvoorbeeld aan de aanvangstijd, duur en eindtijd van een gesprek (via een telefoonnummer) of gelegde verbinding (via een IP-adres).

Om kennis te nemen van de inhoud dient echter te worden gehandeld conform artikel 25 van de WIV. Op basis van de bijzondere bevoegdheid uit artikel 25 kan namelijk elke vorm van gesprek, telecommunicatie en gegevensoverdracht binnen een geautomatiseerd werk worden afgetapt, opgenomen en/of afgeluisterd. Met geautomatiseerd werk wordt overigens bedoeld elke inrichting ten behoeve van opslag, verwerking en overdracht van gegevens. Onder deze omschrijving vallen, naast computers, bijvoorbeeld ook fysieke inrichtingen als laptops, *tablets*, mobiele telefoons (*smartphones*) en *PDA's* en niet-fysieke (digitale) inrichtingen als webfora.

Naast de bijzondere bevoegdheden heeft de MIVD nog een tweetal aanvullende mogelijkheden om gegevens te verzamelen: het raadplegen van open bronnen en het raadplegen van partner(inlichtingen)diensten.

5.4 Mogelijkheden extraterritoriaal verzamelen van inlichtingen MIVD

Aangezien de WIV naar analogie in het buitenland wordt toegepast, de MIVD alle bijzondere bevoegdheden kan inzetten ten behoeve van de buitenlandtaak en omdat een aantal bijzondere bevoegdheden mogelijkheden biedt in het cyberdomein, kan de MIVD extraterritoriaal inlichtingen verzamelen in het cyberdomein. In hoeverre kunnen deze activiteiten worden ontplooid zonder daarmee het non-interventiebeginsel dan wel het soevereiniteitsbeginsel te schenden? Dat is de vraag die centraal stond in dit onderzoek.

Volgens zowel Gill als Ziolkowski bevat het verzamelen van informatie via het cyberdomein doorgaans geen dwangelement. Er kan daartoe niet gesproken worden van een verboden interventie. Het non-interventiebeginsel wordt doorgaans dan ook niet geschonden bij het extraterritoriaal verzamelen van inlichtingen in het cyberdomein. Volgens bijvoorbeeld de *International Group of Experts*, die de *Tallinn Manual* schreven, kan er zelfs doorgaans niet worden gesproken van een verboden interventie als bij de digitale inlichtingenactiviteit *virtual barriers* (zoals *firewalls* en wachtwoorden) moeten worden doorbroken.

Daarnaast zetten een aantal auteurs verschillende extraterritoriale inlichtingenactiviteiten in het cyberdomein uiteen om vervolgens te concluderen dat deze doorgaans geen schending van het soevereiniteitsbeginsel zullen opleveren. Het verschaffen van toegang tot bijvoorbeeld een computer of computernetwerk (of in de bewoording van de WIV: geautomatiseerd werk), dat zich bevindt op het territoir van een andere staat, levert doorgaans geen schending van de soevereiniteit van die staat op. Dit geldt eveneens voor het louter kopiëren (overnemen) van informatie die op de computer (geautomatiseerd werk). De vraag of het installeren van *malware* op computers (geautomatiseerde werken) in een andere staat een schending van de soevereiniteit zal opleveren wordt door geen enkele auteur beantwoord.

De MIVD kan dus de bijzondere bevoegdheid uit artikel 24 toepassen in het buitenland zonder daarmee het non-interventiebeginsel of het soevereiniteitsbeginsel te schenden. Het binnendringen van een geautomatiseerd werk, zelfs als daarvoor enige beveiliging moet worden doorbroken (zoals *firewalls* of wachtwoorden), bevat geen dwangelement en zal derhalve doorgaans geen schending van het non-interventiebeginsel opleveren. Tevens levert dit geen schending van het soevereiniteitsbeginsel op, als het puur gaat om het kopiëren van gegevens die aanwezig zijn in het betreffende geautomatiseerde werk.

Het gebruik maken van bijvoorbeeld de *webcam* van een geautomatiseerd werk waartoe toegang is verschaft zal dan doorgaans ook niet tot een verboden interventie leiden of de soevereiniteit van een staat schenden, mits daarvoor geen aanvullende acties (zoals het gebruikmaken van *malware*) nodig zijn. Als bijvoorbeeld *malware* (als zijnde een technische voorziening) gebruikt dient te worden om toegang te verschaffen tot een geautomatiseerd werk of tot het gebruik van een (al dan niet ingebouwde) *webcam* of microfoon van een geautomatiseerd werk, dan is niet duidelijk of er sprake zal zijn van een verboden interventie of een schending van het soevereiniteitsbeginsel. Hier zal meer onderzoek naar moeten worden verricht.

Met het gebruik van de *webcam*, de microfoon of het navigatiesysteem kan dan, in gevolge van de bijzondere bevoegdheid uit artikel 20 van de WIV, ook extraterritoriaal een persoon worden gevolgd en geobserveerd. Indien, zonder het gebruik van bijvoorbeeld *malware* toegang wordt verschaft tot deze geautomatiseerde werken, zal dit doorgaans geen schending van het non-interventiebeginsel of het soevereiniteitsbeginsel opleveren.

Aangezien het geen verboden interventie oplevert als toegang wordt verschaft tot een geautomatiseerd werk om gegevens te verzamelen en aangezien daarbij enige beveiliging (zoals een wachtwoord) mag worden doorbroken, is het dus ook mogelijk om, op basis van artikel 25 van de WIV, bijvoorbeeld e-mails, SMS-berichten en berichten (waaronder afbeeldingen en films) die via *social media* worden verzonden, te verzamelen zonder dat daarmee het non-interventiebeginsel of het soevereiniteitsbeginsel wordt geschonden.

Zelfs als de gewenste gegevens (in de vorm van bijvoorbeeld e-mails of SMS-berichten) niet aanwezig zijn op het geautomatiseerde werk dat is binnengedrongen, bestaat er op basis van de bijzondere bevoegdheid uit artikel 26 nog een mogelijkheid om deze gegevens te verzamelen. De MIVD kan namelijk niet-kabelbegonden telecommunicatie, vanuit of naar het buitenland, opvangen en opnemen. Daarnaast kan in gevolge van artikel 27 ongericht niet-kabelgebonden telecommunicatie worden ontvangen en opgenomen. Naast het puur verzamelen van de gegevens kan ook, op basis van artikel 25, kennis worden genomen van de inhoud van de berichten. Dit alles levert doorgaans geen schending van het non-interventiebeginsel noch een schending van het soevereiniteitsbeginsel op.

Tot slot kan de MIVD zich op basis van artikel 28 en 29 wenden tot telecommunicatie-aanbieders of aanbieders van telecommunicatiediensten om zogeheten verkeers- en abonneegegevens op te vragen. Uiteraard is dit ook mogelijk bij buitenlandse aanbieders van telecommunicatie(diensten). Als deze bevoegdheden extraterritoriaal worden uitgeoefend dient echter wel een kanttekening geplaatst te worden. Het kan buitenlandse aanbieders namelijk niet verplicht worden gesteld de opgevraagde gegevens te verstrekken.

Als de MIVD dat wel zou doen, dan zou de MIVD handhavende rechtsmacht uitoefenen op het territoir van een andere staat en zou derhalve de soevereiniteit van die staat worden geschonden. Daarnaast zou, in relatie tot het non-interventiebeginsel, een dwangelement (namelijk een verplichting) aanwezig zijn ten aanzien van de instantie die de gegevens kan verstrekken. Desalniettemin kan de MIVD dus wel buitenlandse telecommunicatie-aanbieders benaderen en hen verzoeken de gewenste informatie te verstrekken, verplichten kan de MIVD hen echter niet. Zie tabel 5.1 voor een overzicht van het totaal.

Artikel of bevoegd-heid	Relevant in het cyber-domein	Dwang-element	Beoogde verandering beleid	Veroor-zaakte verandering beleid	Schending non-interventie-beginsel	Fysiek op territoir andere staat	Fysieke effecten op territoir andere staat	Hand-havende rechtsmacht op territoir andere staat	Schending soevereini-teitsbeginsel
Artikel 20	Ja	Nee	Nee	Nee	**Nee**	Nee	Nee	Nee	**Nee**
				Ja	**Ja**			Ja	**Ja**
Artikel 21	Deels	Nee	Nee	Nee	**Nee**	Nee	Nee	Nee	**Nee**
				Ja	**Ja**			Ja	**Ja**
Artikel 22	Deels	Nee	Nee	Nee	**Nee**	Nee	Nee	Nee	**Nee**
				Ja	**Ja**			Ja	**Ja**
Artikel 24	Ja	Nee	Nee	Nee	**Nee**	Nee	Nee	Nee	**Nee**
				Ja	**Ja**			Ja	**Ja**
Artikel 25	Ja	Nee	Nee	Nee	**Nee**	Nee	Nee	Nee	**Nee**
				Ja	**Ja**				
Artikel 26	Ja	Nee	Nee	Nee	**Nee**	Nee	Nee	Nee	**Nee**
				Ja	**Ja**				
Artikel 27	Ja	Nee	Nee	Nee	**Nee**	Nee	Nee	Nee	**Nee**
				Ja	**Ja**				
Artikel 28	Ja	Nee	Nee	Nee	**Nee**	Nee	Nee	Nee	**Nee**
				Ja	**Ja**			Ja	**Ja**
Artikel 29	Ja	Nee	Nee	Nee	**Nee**	Nee	Nee	Nee	**Nee**
				Ja	**Ja**			Ja	**Ja**

Tabel 5.1 Het extraterritoriaal uitvoeren van bijzondere bevoegdheden in relatie tot het non-interventiebeginsel en het soevereiniteitsbeginsel

Naast de mogelijkheid om, op basis van een aantal bijzondere bevoegdheden, extraterritoriaal inlichtingen te verzamelen in het cyberdomein, binnen de grenzen van het internationaal recht, heeft de MIVD een tweetal additionele mogelijkheden tot het (extraterritoriaal) verzamelen van inlichtingen in het cyberdomein.

Ten eerste kan de MIVD zich wenden tot bronnen die voor iedereen toegankelijk zijn, de zogeheten open bronnen. Aangezien de bronnen voor een ieder toegankelijk zijn en geen enkele staat soevereiniteit kan claimen over het internet (een vorm van een open bron in het cyberdomein), zal het non-interventiebeginsel noch het soevereiniteitsbeginsel worden geschonden bij het raadplegen van deze bronnen. Ten tweede kan de MIVD zich (bijvoorbeeld in het cyberdomein) richten tot partner(inlichtingen)diensten om de gewenste inlichtingen te verzamelen. Beide additionele mogelijkheden zullen doorgaans het non-interventiebeginsel noch het soevereiniteitsbeginsel schenden.

Al met al heeft de MIVD genoeg mogelijkheden om extraterritoriaal inlichtingen te verzamelen in het cyberdomein, zonder daarbij de beginselen van non-interventie en soevereiniteit te schenden. Wel dient de MIVD zich, met het uitoefenen van de bijzondere bevoegdheden, altijd te houden aan de voorwaarden die in de WIV worden gesteld aan het uitvoeren van de bijzondere bevoegdheden. Daarnaast dient de MIVD rekening te houden met de ter plaatse geldende wetgeving en mag geen handhavende rechtsmacht op het territoir van een andere staat worden uitgeoefend. Ook mag de MIVD geen dwang uitoefenen en mag er geen beleidsverandering wordt beoogd of teweeg wordt gebracht bij het extraterritoriaal verzamelen van inlichtingen in het cyberdomein. Tot slot dient de MIVD rekening te houden met de soevereiniteit van andere staten door niet fysiek aanwezig te zijn op het territoir van andere staten en geen activiteiten uit te voeren die fysieke effecten (kunnen) hebben op het territoir van andere staten.

Kortom, de MIVD heeft veel mogelijkheden (zes bijzondere bevoegdheden en twee additionele mogelijkheden) om extraterritoriaal inlichtingen te verzamelen in het cyberdomein zonder het non-interventiebeginsel dan wel het soevereiniteitsbeginsel te schenden.

6. Reflectie

In dit laatste hoofdstuk wordt geen (deel)vraag beantwoord die invloed heeft op de inhoud van het onderzoek. In dit hoofdstuk volgt namelijk een terugblik op het gehele scriptieproces. In de eerste paragraaf zal kritisch worden gereflecteerd op de resultaten en de beperkingen van dit onderzoek. In de daaropvolgende paragraaf zal een reflectie van het scriptieproces volgen, waarin onder andere het eigen functioneren als onderzoeker wordt behandeld.

6.1 Reflectie op de resultaten en beperkingen

In dit onderzoek is onderzocht welke mogelijkheden de MIVD heeft voor het extraterritoriaal verzamelen van inlichtingen in het cyberdomein. Het antwoord op deze vraag is in het vorige hoofdstuk, de conclusie, behandeld. Om tot deze conclusie te komen zijn onder andere alle (bijzondere) bevoegdheden van de MIVD bezien in relatie tot het cyberdomein. Er is gekozen om alle bevoegdheden van de MIVD te behandelen om compleet te zijn en om per bevoegdheid te bezien of deze mogelijkheden biedt tot het verzamelen van inlichtingen in het cyberdomein. De bevindingen die hier uiteindelijk uit voort kwamen zijn gebaseerd op een eigen analyse.

Deze eigen analyse was noodzakelijk aangezien een contactpersoon bij de MIVD meldde dat bepaalde informatie (veelal in de vorm van antwoorden op veel door mij gestelde vragen) niet kon worden verstrekt zonder *modus operandi* dan wel het (huidige) kennisniveau van de MIVD prijs te geven. Deze beperking is jammer, aangezien nu niet kon worden voortgebouwd op de kennis van deskundigen in het vakgebied. Derhalve kan het zijn dat er nog meer mogelijkheden zijn met betrekking tot het uitvoeren van de (bijzondere) bevoegdheden in het cyberdomein. De resultaten van het onderzoek hadden wellicht nog uitgebreider (en misschien met meer diepgang) kunnen zijn als de betreffende informatie wel kon worden verstrekt. Denk bijvoorbeeld aan nog meer (cyber)middelen die in het cyberdomein kunnen worden gebruikt om (extraterritoriaal) inlichtingen te verzamelen.

Vanwege bovenstaande, kan het dan ook zijn dat andere onderzoekers die eenzelfde onderzoek verrichten op een andere conclusie uitkomen met andere resultaten. Zo kunnen andere onderzoekers wel over de informatie beschikken (door bijvoorbeeld hun onderzoek te classificeren). Daarnaast kunnen andere onderzoekers een andere eigen analyse loslaten op de (bijzondere) bevoegdheden van de MIVD. Het is goed mogelijk dat andere onderzoekers, wellicht met een andere achtergrond, anders denken met betrekking tot de mogelijkheden in het cyberdomein en daartoe tot andere resultaten komen dan de resultaten in dit onderzoek.

Naast de, tijdens het onderzoek ontstane, beperking met betrekking tot de toegang tot deskundigheid over de (bijzondere) bevoegdheden van de MIVD in relatie tot het cyberdomein, werd in het onderzoek bewust gekozen voor de beperking tot het behandelen van slechts twee internationaalrechtelijke beginselen en het louter behandelen van de MIVD. In dit onderzoek zijn slechts het non-interventiebeginsel en het soevereiniteitsbeginsel behandeld. Deze keuze is gemaakt omwille van de omvang van het onderzoek alsmede omwille het tijdsbestek waarin het onderzoek afgerond diende te worden. Daarom is ook in de inleiding het internationaalrechtelijke geweldsverbod uitgesloten van dit onderzoek, door aan te nemen dat het extraterritoriaal verzamelen van inlichtingen in het cyberdomein doorgaans geen fysiek geweld oplevert. Andere onderzoekers kunnen dit internationaalrechtelijke beginsel misschien wel opnemen in hun onderzoek en derhalve tot andere resultaten komen met betrekking tot de mogelijkheden van de MIVD voor het extraterritoriaal verzamelen van inlichtingen in het cyberdomein, binnen de grenzen van het internationaal recht. Dit geldt overigens ook voor andere onderzoekers die naast de MIVD ook de AIVD of buitenlandse inlichtingendiensten opnemen in het onderzoek.

6.2 Reflectie op het proces

Het scriptieproces begon reeds in 2013, toen een Individueel Onderzoeksvoorstel (IOV) moest worden geschreven. Eerlijkheidshalve dien ik te vermelden dat ik het schrijven van een IOV destijds onnodig vond. Later kwam ik hier op terug, aangezien een goed resultaat start met een goed plan. Uiteindelijk bevatte het opgestelde IOV een plan dat na de jaarwisseling slechts uitgevoerd hoefde te worden.

In het algemeen verliep de onderzoeksperiode goed. De gemaakte tijdsplanning werd nageleefd en de gestelde deadlines werden allen gehaald. Desalniettemin waren er tijdens het proces een aantal momenten waarop zich moeilijkheden voordeden. Zo was het lastig om de hoofdvraag goed te formuleren in één zin. Daarnaast vond in een vroeg stadium van het proces, tijdens het schrijven van het theoretisch kader, een afspraak plaats met een militair jurist. Dit gesprek leverde echter veel verwarring op, aangezien ik door de vele andere invalshoeken afdwaalde van het hoofdonderwerp en de doelstelling van het onderzoek. Gelukkig waren er twee begeleiders die de verwarring wegnamen en mij weer met de neus de goede kant op konden zetten.

Tevens was het, tijdens het schrijven van het theoretisch kader, lastig om goede bronnen te vinden. Dat kwam niet omdat er weinig informatie te vinden was over het non-interventiebeginsel en het soevereiniteitsbeginsel, maar juist omdat er zoveel informatie over deze twee internationaalrechtelijke beginselen te vinden was. Daar het in het verleden van de opleiding soms vervelend was dat er nauwelijks informatie te vinden was over een onderwerp, was de overvloed aan informatie, met betrekking tot het theoretisch kader, in dit scriptieproces juist vervelend.

Bij het onderzoeken en schrijven van de tweede deelvraag, met betrekking tot de mogelijke extraterritoriale werking van de WIV, heb ik geen problemen ondervonden. De wet zelf, de wetsgeschiedenis en de rapporten van de CTIVD en de evaluatiecommissie boden genoeg informatie om de deelvraag te beantwoorden.

Voor het beantwoorden van de derde deelvraag, met betrekking tot de bevoegdheden van de MIVD in het cyberdomein, kon ook gebruik worden gemaakt van de wet zelf, de wetsgeschiedenis en de rapporten van de CTIVD en de evaluatiecommissie. Daarnaast was het gewenst om deskundigen op dit gebied te raadplegen. Helaas kon dit niet, waardoor een eigen analyse werd gemaakt van de bevoegdheden van de MIVD in het cyberdomein. Hierop is in de vorige paragraaf reeds uitvoerig ingegaan.

Hoewel er zich een aantal strubbelingen voordeden tijdens het proces, ben ik toch erg tevreden over zowel het proces als het resultaat. De in het IOV opgestelde tijdsplanning is elke keer gehaald, waardoor ik niet achter de feiten aanliep. Ik heb de termijn van negen weken waarin het onderzoek afgerond diende te worden dan ook als positief ervaren. Tevens is, mijns inziens, de eigen analyse goed uit de verf gekomen. Mede daardoor kon in de conclusie een bevredigend antwoord worden geformuleerd op de centrale vraag van dit onderzoek, zij het met de kanttekening dat meer onderzoek nodig is naar bijvoorbeeld het gebruik van *malware*. Kortom ben ik, ondanks enige strubbelingen en kanttekeningen, erg tevreden over zowel het proces als het resultaat van het onderzoek.

Literatuurlijst

Barkham (2001)

Barkham, J. (2001). Information Warfare and International Law on the Use of Force. *Journal of International Law & Politics*, *34*, 57-113.

Brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties De Vries (2001)

Kamerstukken II 2000/01, 25 877, nr. 59.

Briefing (18 december 2013) AIVD en MIVD aan de Tweede Kamer omtrent interceptie

Algemene Inlichtingen- en Veiligheidsdienst & Militaire Inlichtingen- en Veiligheidsdienst (18-12-2013). *Technische briefing: interceptie, metadata, geautomatiseerd werk, 18 december 2013*. Geraadpleegd op 06 maart 2014 via < https://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CDMQFjAB&url=https%3A%2F%2Fwww.aivd.nl%2Fpublish%2Fpages%2F2525%2Fbriefing_tweede_kamer_door_mivd_aivd_over_interceptie.pdf&ei=T4QYU_zpGaXb7Aau-oCICQ&usg=AFQjCNESUW0HOCzdjl4W8-dnPCBhRNoBpQ&bvm=bv.62577051,d.bGE>

Burci (1996)

Burci, G.L. (1996). United Nations Peacekeeping Operations in Situations of Internal Conflict. In Sellers, M. (ed.), *the new world order: Sovereignty, Human Rights and the Self-Determination of Peoples* (pp. 237-272). Oxford: Oxford International Publishing Ltd.

Canefe (1996)

Canefe, N. (1996). Sovereignty Without Nationalism? A Critical Assessment of MInority Rights Beyond the Sovereign Nation-State Model. In Sellers, M. (ed.), *the new world order: Sovereignty, Human Rights and the Self-Determination of Peoples* (pp. 91-116). Oxford: Oxford International Publishing Ltd.

Cogen (2003)

Cogen, M. (2003). *Handboek Internationaal Recht*. Mechelen: Kluwer uitgevers.

Charter of the United Nations

The Charter of the United Nations (1945). *The Charter of the United Nations*. San Francisco.

Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2007)

Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2007). *Verslag Studiemiddag CTIVD 'Inlichtingenactiviteiten in het buitenland'.* Den Haag.

Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2009)
Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2009). *Nummer 19: Toezichtsrapport inzake de toepassing door de AIVD van artikel 25 WIV 2002 (aftappen) en artikel 27 WIV 2002 (selectie van ongericht ontvangen niet-kabelgebonden telecommunicatie).*

Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2011a)
Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2011). *Nummer 26: Toezichtsrapport inzake de uitvoering van de inlichtingentaak buitenland door de AIVD*.

Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2011b)
Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten (2011). *Nummer 28: Toezichtsrapport inzake de inzet van SIGINT door de MIVD.*

Cronin (2002)
Cronin, B. (2002). Multilateral Intervention and the International Community. In Keren, M. & Sylvan, D.A. (eds), *International Intervention: Sovereignty versus Responsibility* (pp. 147-165). London: Frank Cass & Co Ltd.

Der Spiegel
Spiegel online (03-03-2014). NSA Spying Scandal: Related articles, background features and opinions about this topic. *Der Spiegel* (tot en met 03-03-2014). Geraadpleegd op 03 maart 2014 via < http://www.spiegel.de/international/topic/nsa_spying_scandal/>.

Dinstein (2005a)
Dinstein, Y. (2005). *War, Agression, and Self-Defence*. New York: Cambridge University Press.

Dinstein (2005b)
Dinstein, Y. (2005). Sovereignty, the Security Council and the Use of Force. In Bothe, M., O'Connell, M.E. en Ronzitti, N. (eds), *Redefining Sovereignty: The Use of Force after the Cold War* (pp. 111-122). New York: Transnational Publishers Inc.

Evaluatiecommissie (2013)
Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2002 (2013). *Naar een nieuwe balans tussen bevoegdheden en waarborgen*.

Fleck (2005)

Fleck, D. (2005). National Sovereignty and International Responsibility: Legal and Policy Aspects. In Bothe, M., O'Connell, M.E. en Ronzitti, N. (eds), *Redefining Sovereignty: The Use of Force after the Cold War* (pp. 53-64). New York: Transnational Publishers Inc.

Gellman (2013)

Gellman, B. (16-08-2013). NSA broke privacy rules thousand times per year, audit finds. *Washington Post 16-10-2013*. Geraadpleegd op 29 oktober 2013 via <http://www.washingtonpost.com/world/ national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/ 3310e554-05ca-11e3-a07f-49ddc7417125_story.html>.

Gill (2013)

Gill, T. D. (2013). Non-Intervention in the Cyber Context. In Ziolkowski, K. (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (pp. 217-238). Tallinn: NATO CCD COE Publication.

Hannon (2010)

Hannon, J. (2010). *Software system for denying remote access to computer cameras.* Geraadpleegd op 19 februari 2014 via < http://www.google.com/patents/US20120151606>

Hensel (2004)

Hensel, H.M. (2004). *Theocentric Natural Law and Norms of the Global Community*. In Hensel, H.M. (ed), *Sovereignty and the Global Community: The quest for order in the international system* (pp. 1-53). Aldershot: Ashgate Publicing Limited.

Hes, Hooghiemstra & Borking

Hes, R., Hooghiemstra, T.F.M. & Borking, J.J. (1999). *At face value: On biometrical identification and privacy*. Den Haag: Sdu Grafisch Bedrijf.

Holsti (2004)

Holsti, K.J. (2004). *Taming the Sovereigns: Institutional Change in International Politics*. Cambridge: Cambridge University Press.

International Commission on Intervention and State Sovereignty (2001)

International Commission on Intervention and State Sovereignty (2001). *The Responsibility to Protect*. Ottawa: International Development Research Centre.

Jamnejad & Wood (2009)

Jamnejad, M. & Wood, M. (2009). Current Legal Developments: The Principle of Non-Intervention. *Leiden Journal of International Law, 22*, pp. 345-381.

Judgment Corfu Channel case (1949)

International Court of Justice (1949). *The Corfu Channel case (Merits), Judgment of April 9th, 1949: I.C.J. Reports 1949*.

Judgment Lotus case (1927)

Permanent Court of International Justice (1927). *The Case of the S.S. Lotus (France v. Turkey), Judgment, P.C.I.J. Series A – No. 10.*

Judgment Nicaragua case (1986)

International Court of Justice (1986). *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986*.

Keren & Sylvan (2002)

Keren, M. & Sylvan, D.A. (2002). *International Intervention: Sovereignty versus Responsibility*. London: Frank Cass & Co Ltd.

Kohen (2012)

Kohen, M. (2012). The Principle of Non-Intervention 25 Years after the Nicaragua Judgment. *Leiden Journal of International Law, 25*, pp. 157-164.

Krasner (1999)

Krasner, S.D. (1999). Sovereignty: *Organized Hypocrisy.* Princeton: Princeton University Press.

Krasner (2001)

Krasner, S.D. (2001). Sovereignty. *Foreign Policy, 122*, pp 20-29.

Lubel (2010)

Lubel, N. (2010). *Extraterritorial Use of Force against Non-State Actors.* New York: Oxford University Press Inc.

McCorquodale

McCorquodale, R. (1996). Human Rights and Self-Determination. In Sellers, M. (ed.), *the new world order: Sovereignty, Human Rights and the Self-Determination of Peoples* (pp. 9-34). Oxford: Oxford International Publishing Ltd.

Mostov (2008)
Mostov, J. (2008). *Soft Borders: Rethinking Sovereignty and Democracy*. New York: PALGRAVE MACMILLAN.

Nieuwenhuis(2013a)
Nieuwenhuis, M. (28-10-2013). Cyberaanval zorgt voor grote rampen. *Algemeen Dagblad 28-10-2013*. Geraadpleegd op 29 oktober 2014 via < http://www.ad.nl/ad/nl/5595/Digitaal/article/ detail/3534403/2013/10/28/Cyberaanval-zorgt-voor-grote-rampen.dhtml>.

Nieuwenhuis(2013b)
Nieuwenhuis, M. (28-10-2013). Explosieve stijging van cyberaanvallen. *Algemeen Dagblad 28-10-2013*. Geraadpleegd op 29 oktober 2014 via < http://www.ad.nl/ad/nl/5595/Digitaal/article/ detail/3534364/2013/10/28/Explosieve-stijging-van-cyberaanvallen.dhtml>.

Nollkaemper (2011)
Nollkaemper, P.A. (2011). *Kern van het internationaal publiekrecht*. Den Haag: Boom Juridische uitgevers.

Nota naar aanleiding van het nader verslag (2001)
Kamerstukken II 2000/2001, 25 877, nr. 14.

Nota van Wijziging (1999)
Kamerstukken II 1999/2000, 25 877, nr. 9.

Philpott (2001)
Philpott, D. (2001). *Revolution in Sovereignty: How ideas shaped modern international relations*. Princeton: Princeton University Press.

Pirker (2013)
Pirker, B. (2013). Territorial Sovereignty and Integrity and the Challenges of Cyberspace. In Ziolkowski, K. (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (pp. 189-216). Tallinn: NATO CCD COE Publication.

Simpson (1996)
Simpson, G.J. (1996). *The Diffusion of Sovereignty: Self-Determination in the Post-Colonial Age*. In Sellers, M. (ed.), *the new world order: Sovereignty, Human Rights and the Self-Determination of Peoples* (pp. 35-69). Oxford: Oxford International Publishing Ltd.

Statute of the International Court of Justice

International Court of Justice. *Statute of the International Court of Justice.*

Tallinn Manual (2013)

General editior: Schmitt, M.N. (2013). *Tallinn Manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence.* Cambridge: Cambridge University Press.

The Guardian

Sacha, B., Davis, K., Popovich, N., Powell, K., MacAskill, E., Spencer, R., Van Gelder, L., Ackerman, S., Epstein, K., Lewis, P., Michel, A., Rogers, K. & Rushe, D. (01-11-2013). NSA FILES: DECODED. What the relevations means to you. *The Guardian 01-11-2013*. Geraadpleegd op 03 maart 2014 via: < http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>.

Thomas (1985)

Thomas, C. (1985). *New States, Sovereignty and Intervention*. Aldershot: Gower Publishing Company Limited.

TNO Rapport 35264

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (2010). *TNO rapport 35264: Herkenning van Digitale Informatie*. Geraadpleegd op 05 maart 2014 via < https://rejo.zenger.nl/files/20100331-tno-rapport-herkenning-van-digitale-informatie-ocr.pdf>

Verenigde Naties (2014)

United Nations (2014). *Member States of the United Nations*. Geraadpleegd op 09 januari 2014. Beschikbaar via <http://www.un.org/en/members/index.shtml#text>.

Vienna Convention of the law of treaties

Vienna Convetion of the law of treaties (1969). Vienna.

Wolfrum (2002)

Wolfrum, R. (2002). The UN Experience in Modern Intervention. In Keren, M. & Sylvan, D.A. (eds), *International Intervention: Sovereignty versus Responsibility* (pp. 95-113). London: Frank Cass & Co Ltd.

Ziolkowski (2013a)

Ziolkowski, K. (2013). General Principles of International Law as Applicable in Cyberspace. In Ziolkowski, K. (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (pp. 135-188). Tallinn: NATO CCD COE Publication.

Ziolkowski (2013b)

Ziolkowski, K. (2013). Peacetime Cyber Espionage – New Tendencies in Public International Law. In Ziolkowski, K. (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (pp. 425-464). Tallinn: NATO CCD COE Publication.