Digitale Inlichtingenverzameling

Een onderzoek naar de mogelijkheden van digitale inlichtingenverzameling van de Militaire Inlichtingen- en Veiligheidsdienst aan de hand van de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002

Bachelor Scriptie NLDA Krijgswetenschappen

Auteur: LTZ3. E.N. Zonneveld

1ste begeleider: Kolonel Mr. Dr. P.A.L. Ducheine

2e begeleider: Prof. Dr. B.G.J. de Graaff

Breda, maart 2014

Digitale Inlichtingenverzameling

Een onderzoek naar de mogelijkheden van digitale inlichtingenverzameling van de Militaire Inlichtingen- en Veiligheidsdienst aan de hand van de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002

Door LTZ3 E.N. Zonneveld

Scriptie ter afsluiting van de Bacheloropleiding Krijgswetenschappen aan de Nederlandse Defensie Academie te Breda in het openbaar te verdedigen op 7 april 2014 om 15:00 te Breda tegenover een commissie bestaande uit:

Voorzitter	Dr. F.H. Baudet
Eerste begeleider	Kolonel mr. dr. P.A.L. Ducheine
Tweede begeleider	Prof. Dr. B.G.J. de Graaff

Voorwoord

Ongerichte interceptie van kabelgebonden telecommunicatie, zoals veelvuldig is verschenen in het nieuws, klinkt beangstigend. Het wekt voor veel mensen het gevoel op dat illustratief is beschreven in het boek 1984 van George Orwell, waaruit de uitspraak '*Big brother is watching you'* afkomstig is. Voor mij wekte dit grote interesse naar wat de Militaire Inlichtingen- en Veiligheidsdienst nou precies kan en mag in de huidige digitale samenleving.

Voor u ligt de bachelorscriptie waarmee ik mijn bachelor opleiding Krijgswetenschappen aan de Nederlandse Defensie Academie afrondt. Het vormt mijn eerst mijlpaal in de wetenschappelijke wereld. Met deze achtergrond en de minor Inlichtingen is mijn interesse naar de MIVD enorm gegroeid en deze zal hopelijk nog veelvuldig terugkeren in mijn latere militaire functies.

Een woord van dank wil ik uitspreken aan Kolonel Mr. Dr. P.A.L. Ducheine. De begeleiding die de kolonel geboden heeft is essentieel geweest voor het eindresultaat en de goede afloop van mijn scriptie periode. Het geduld om door al mijn taalkundige fouten heen de inhoud te kunnen lezen, maar zeker ook het geduld om deze fouten te beoordelen, heb ik zeer gewaardeerd.

Op de tweede plaats wil Prof. Dr. De Graaff bedanken voor zijn rol als tweede begeleider en de geleverde feedback op mijn ingeleverde stukken. Daarnaast wil ik Anouk Schagen en Gerben Zonneveld bedanken voor hun steun en de vele uren die zij hebben besteed in het nakijken van mijn scriptie en andere stukken.

E.N. Zonneveld

Luitenant ter Zee derde Klasse

Samenvatting

Dit onderzoek richt zich op de vraag of de beperkingen die de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002 oplegt aan de Militaire Inlichtingen- en Veiligheidsdienst, als het gaat om het toepassen van digitale methoden voor inlichtingenverzameling, zijn verouderd. Het doel van het onderzoek is om een mogelijke aanbeveling te doen betreffende een modernisering van de bijzondere bevoegdheden voor de MIVD.

De MIVD heeft een vijftal taken die de dienst uitvoert die beschreven staan in de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV) 2002. Het gaat hierbij om: de handhaving en bevordering van de internationale rechtsorde; de uitvoering van veiligheidsonderzoeken; onderzoek verrichten in het belang van de nationale veiligheid en ten behoeve van het treffen van maatregelen voor een adequate uitvoering van de taken van Defensie; het bevorderen van het treffen van veiligheidsmaatregelen door andere organisaties en als laatste het verrichten van onderzoek betreffende andere landen.

Bij de uitvoering van deze taken ondersteunt de MIVD de krijgsmachtsonderdelen door hen van inlichtingen te voorzien. Deze inlichtingen kunnen op verschillende wijzen worden verkregen. Er is in dit onderzoek gekeken naar het verzamelen van inlichtingen door middel van het digitale domein. Tijdens het verzamelen van inlichtingen in het digitale domein zijn de bijzondere bevoegdheden, respectievelijk artikel 24 t/m 27 uit de WIV 2002, van toepassing op de MIVD. Deze artikelen staan de MIVD toe om gericht binnen te dringen in een geautomatiseerd werk, gerichte interceptie uit te voeren van niet-kabelgebonden telecommunicatie, het uitvoeren van ongerichte interceptie van niet-kabelgebonden telecommunicatie en als laatste een selectie uit te voeren op de ontvangen telecommunicatie afkomstig van ongerichte niet-kabelgebonden interceptie.

Door de technologische ontwikkeling van glasvezelkabels heeft er een verschuiving plaatsgevonden van de telecommunicatie. Waar deze communicatie eerst verliep via de ether/satelliet is deze in de afgelopen jaren steeds meer gaan lopen via glasvezelkabels. Ook heeft de mobiele techniek, mobiele apparatuur en mobiel internet hier aan bijgedragen. Dit heeft tot gevolg gehad dat nieuwe toepassingen zijn ontwikkeld die het gebruik van deze technologieën vergemakkelijken of ontspanning tot doel hebben. Het gaat hierbij om Cloud computing waarbij mensen en websites hun gegevens en bestanden online opslaan. Social media heeft zijn intreden gedaan doordat mensen in toenemende mate verbonden zijn met het internet en online contact met elkaar kunnen onderhouden vanaf de locatie waar zij dat willen. Op het gebied van inlichtingen zijn er ook ontwikkelingen gedaan.

Zo is er een nieuwe techniek ontwikkeld waarbij met behulp van radiofrequenties toegang kan worden verkregen tot computers en netwerken die niet verbonden zijn met het internet. Ook zijn inmiddels computersystemen en programma's ontwikkeld die grote hoeveelheden gegevens via de kabel kunnen opnemen en analyseren.

De politiek heeft onderkend dat deze technologieën nieuwe dreigingen veroorzaken voor de nationale veiligheid en dat de huidige wet hierdoor mogelijk verouderd zou kunnen zijn. De evaluatiecommissie-Dessens heeft dit vraagstuk onderzocht en kwam met de aanbeveling dat de bevoegdheid tot kabelgebonden interceptie benodigd is.

Door de verschuiving van de telecommunicatie en het toenemende gebruik van glasvezelnetwerken, waar het internet in toenemende mate over verloopt, zal de MIVD mogelijk zijn middelen moeten gaan inzetten om ongerichte interceptie uit te voeren via glasvezelkabel, of te wel ongericht kabelgebonden interceptie. De MIVD wordt hierin echter beperkt doordat deze bevoegdheid niet is opgenomen binnen de huidige wetgeving (WIV 2002).

Summary

This research focuses on the question whether the restrictions imposed by the Law on Intelligence and Security Services from 2002 (LISS 2002), are outdated when it comes to the use of digital methods for collection of intelligence by the Military Intelligence and Security Service (MISS). The purpose of this research is to formulate a possible recommendation for the modernization of the special powers of the MISS.

The five different tasks of the MISS carry's out are described in the Law on the Intelligence and Security Services of 2002. These include: The maintenance and promotion of international justice; conduction of security researches; research in the interests of national security and taking measures for the adequate execution of the main tasks of the armed forces; promoting the safety measures by other organizations and finally conducting investigations concerning other countries.

By carrying out these tasks, the MISS provides the armed forces with intelligence. This intelligence can be obtained in different ways. This study focuses on gathering intelligence through the use of the digital domain. The MISS is bound to article 24 to 27 from LISS 2002 when carrying out its special powers. These articles allow the MISS to perform targeted penetration of computerized systems, to perform undirected interception of non-cable-bound telecommunication, to perform targeted interception of non-cable-bound telecommunication and finally to carry out a selection on the intercepted telecommunication through the use of undirected interception of non-cable-bound telecommunication.

Due to the technological development of fiber optic cables there has been a shift in ways how to perform telecommunications. These telecommunications first made use of satellite. Nowadays these telecommunications are more and more carried out through fiber optic cables. Mobile technology, mobile devices and mobile internet has contributed to this shift in how telecommunications are carried out. This made new developments of applications possible with the main purpose of making technology more user friendly and entertaining. This involves Cloud computing in which people and websites store their files online. Social media has its onset done by the increasing number of people connected to the internet and the online contact they want to have with others from all kinds of different places.

New developments have also occurred in the field of intelligence. A new technique has been developed in which access can be obtained to computers and computer networks, which are not connected to the internet, by means of radio frequencies. Also, new developments of computer systems and computer programs have made it possible to record and analyse large amounts of data which are recorded through the use of cable-bound interception.

Politicians have recognized that these technologies create new threats to national security and deem it possible that the current law is obsolete. The evaluation commission Dessens has considered this issue and has come up with the recommendation that the authority to cable-bound interception is required.

The shift in telecommunications and increasing use of fiber optic networks, which the internet increasingly makes use off, will probably cause the MISS to carry out undirected cable-bound interception. The MISS however is limited because this power is not included in the current legislation (LISS 2002).

Inhoudsopgave

1. Inleiding

'De Nederlandse krijgsmacht wil in het digitale domein een vooraanstaande rol spelen die bij ons land past. De Nederlandse defensie moet een volwaardige cybercapaciteit ontwikkelen. Hier geldt misschien nog meer dan elders dat stilstand achteruitgang is.'

Dat zei minister Hillen bij de opening van het Cyber Symposium van defensie op de Nederlandse Defensie Academie in Breda op 27 juni 2012.[1] De Nederlandse krijgsmacht is al sinds langere tijd bezig met het toepassen van haar cybercapaciteit als uitbreiding op de huidige werkvelden land, lucht, zee en ruimte. De afgelopen jaren is er een extra stap in de richting van een Defensie Cyber Strategie gedaan. Het digitale domein en de toepassing van digitale middelen als wapen of als inlichtingeninstrument zijn sterk in ontwikkeling. Deze ontwikkeling kent in het juridisch veld enkele haken en ogen.

De Wet op de Inlichtingen- en Veiligheidsdiensten (WIV) van 3 december 1987, vormde sinds 1 februari 1988 de wettelijke basis voor Binnenlandse Veiligheidsdienst (BVD) en de Militaire Inlichtingendienst (MID). Op 16 juni 1994 werd door de Afdeling bestuursrechtspraak van de Raad van State geconcludeerd, door een tweetal uitspraken in de zaken Van Gaggum en Valkenier, dat de WIV 1988 niet voldeed. De reden hiervoor was dat de wet niet voldeed aan (de eisen van) het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM) en jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM). Op basis hiervan werd besloten een nieuwe wet op te stellen. Aanpassingen in de bestaande wet zouden niet voldoende zijn.[2] Als uitgangspunt voor de nieuwe wet – de WIV 2002 – werd een gelijkwaardig takenpakket en bevoegdheden van de diensten nagestreefd.

De huidige indeling van verwervingsmethoden van inlichtingen bij de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) bestaat uit een twaalftal onderdelen. Dit zijn: Acoustic intelligence (ACINT); Measurement and signature intelligence (MASINT); Radar intelligence (RADINT); Technical intelligence (TECHINT); Human intelligence (HUMINT); Imagery intelligence (IMINT); Open source intelligence (OSINT); Signals intelligence (SIGINT) met daaronder vallend Communications intelligence (COMINT) en Electronical intelligence (ELINT)[3]; Geospatial intelligence (GEOINT)[4] en als laatste en meest relevante voor deze thesis, de Cyber intelligence (CYBERINT). Deze indeling is gebaseerd op de klassering van bronnen en verzamelorganen.

[1] Ministerie van Defensie (2012a).
[2] Kamerstukken II 1997/98, 25 877, nr.3, p.1.
[3] Leidraad Inlichtingen Koninklijke Landmacht LD5 p.25-28.
[4] MIVD (2013). p.16.

Gedurende het inlichtingenproces wordt er getracht zoveel mogelijk verschillende bronnen aan te wenden om een zo compleet mogelijk inlichtingenbeeld te creëren.[5]

De Militaire Inlichtingen- en Veiligheidsdienst heeft tot taak, met behulp van de verwervingsmethoden inlichtingen te verzamelen over het potentieel van andere mogendheden voor de juiste opbouw en inzet van de eigen krijgsmacht. Het voorziet de departementsleiding en krijgsmachtdelen van inlichtingen. Door deze inlichtingen kan de departementsleiding beslissen over het mogelijk starten en/of voortzetten van crisisbeheersings-, vredes- en humanitaire operaties.[6] Voor de MIVD is het van belang om te beschikken over juiste technologieën en bevoegdheden om deze taak adequaat uit te kunnen (blijven) voeren. Om de uitvoering van de MIVD te controleren wordt er toezicht gehouden op zijn werkzaamheden. In artikel 2 van de WIV 2002 staat dat de MIVD zijn taak verricht in gebondenheid aan de wet en in ondergeschiktheid aan de betrokken minister.[7] Door deze bepaling is de minister verantwoordelijk voor het beleid, de aansturing en de interne controle van de MIVD. Naast de interne departementale controle zijn er ook diverse andere organen die betrokken zijn bij de sturing en controle op de MIVD. Dit zijn: Coördinator Inlichtingen- en Veiligheidsdiensten, de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) en de Nationale Ombudsman. De vaste Kamercommissies, de Commissie voor de Inlichtingen- en Veiligheidsdiensten en de Algemene Rekenkamer voeren daarnaast ook een controlerende functie uit over de MIVD.[8]

Door de huidige wetgeving van de WIV 2002 en de taken en bevoegdheden van de MIVD, op het gebied van digitale inlichtingenverzameling en de technologische ontwikkelingen sinds 2002, te onderzoeken, kan er mogelijk een bijdrage worden geleverd aan een effectievere en efficiëntere werkwijze van de MIVD.

Aanleiding voor het onderzoek zijn de technologische ontwikkelingen in het digitale domein. Hierbij moet gedacht worden aan de introductie van glasvezelkabels en het mobiele internet, waar 47% van de Nederlandse bevolking in de leeftijdscategorie 12 t/m 75 jaar ondertussen beschikking over heeft.[9] De MIVD heeft door de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002 niet de onbegrensde mogelijkheid om alle mogelijke kanalen aan te wenden om inlichtingen te verzamelen.

[5] Ministerie van Defensie. (2013a).
[6] Ministerie van Defensie. (z.d.).
[7] Staatsblad 2002, nr.148, p.2.
[8] Commissie Dessens (2013). p.47.
[9] Centraal Bureau voor de Statistiek (2012). p.3.

De regelgeving omtrent de mogelijk aan te wenden kanalen, ten behoeve van inlichtingenverzameling die destijds in de WIV 2002 zijn opgenomen, was bedoeld ter bevordering van maatregelen in het belang van de staatsveiligheid en van andere gewichtige belangen van de staat.[10] Ruim tien jaar later zijn er nieuwe en veranderde dreigingen, maar daarnaast is er ook de beschikking over nieuwe technologieën. Hierdoor is de wetgeving mogelijk toe aan een modernisering, zodat militairen te veld gesteund worden door een inlichtingendienst die werkt onder een passende wetgeving.

In dit onderzoek zal de WIV 2002 worden gespiegeld aan de MIVD op het gebied van digitale inlichtingen om de huidige beperkingen te onderkennen in relatie tot hedendaagse technologieën. Door deze beperkingen te onderkennen kan er wellicht een bijdrage worden geleverd aan de modernisering van de WIV 2002 op het gebied van digitale inlichtingenverzameling. Deze modernisering van de WIV 2002 heeft in de politiek ook de aandacht. In het verslag van een algemeen overleg, op 7 augustus 2013, zegt de VVD dat zij het belangrijk vindt dat de wetgeving gemoderniseerd wordt, zodat militairen in het veld zich gesteund weten door moderne passende regelgeving.[11] Het digitale domein is onmiskenbaar sterk in ontwikkeling. Digitalisering gebeurt op toenemende schaal in de civiele, maar ook in de militaire wereld. Hierdoor wordt de samenleving steeds meer afhankelijk van deze middelen. Dit brengt kwetsbaarheden met zich mee, zo zal de impact van een cyberaanval enorm zijn op de huidige samenleving. In het militaire domein kunnen de infrastructuur en wapensystemen zodanig worden aangetast dat een betrouwbare verdediging verleden tijd zal zijn. De Nederlandse krijgsmacht en politiek zijn daarom gebaat bij een modern en passende wetgeving op het gebied van digitale inlichtingenverzameling.

1.1 Probleemstelling

Door de jaren heen worden nieuwe technologieën ontwikkeld en de complexiteit daarvan stijgt in een ongelofelijk hoog tempo. Deze ontwikkeling is te zien op alle technologische gebieden in onze samenleving. Het gaat van medische apparatuur tot aan het mobieltje dat iedereen op zak heeft. Deze constante ontwikkeling van nieuwe technologieën heeft naast zijn goede kanten ook implicaties op het juridisch gebied. Vraagstukken over de rechtmatigheid van het gebruik van technieken zijn hier voorbeelden van. Zo heeft de MIVD te maken met deze implicaties.

[10] Staatsblad 2002, nr.148, p.1.
[11] Kamerstukken II, 2012/13, 29 924, nr.100.

In een Tweede Kamerbrief is in juni 2013 gevraagd naar een wettelijke uiteenzetting van de bevoegdheden van de Nederlandse inlichtingen- en veiligheidsdiensten en hoe deze zich verhouden tot het zogeheten PRISM-programma (Planning tool for resource Integration Synchronization and Management) en andere vergelijkbare methoden van informatievergaring.[12] Dit PRISM-programma is gebruikt door de Amerikaanse National Security Agency (NSA) om gericht onderzoek te doen naar niet-Amerikaanse burgers.[13] De Nederlandse inlichtingen- en veiligheidsdiensten werden, nadat dit bekend werd, ook verdacht van het gebruik maken van dit programma. De Nederlandse inlichtingen- en veiligheidsdiensten zijn gebonden aan de WIV 2002, deze dicteert wat hun taken en bevoegdheden zijn. Deze wet is ondertussen twaalf jaar oud en zou mogelijk lacunes kunnen bevatten. Deze mogelijke lacunes zouden invloed kunnen hebben op de MIVD.

De MIVD heeft naast nieuwe technologieën en methoden, die zij zelf kunnen gebruiken, ook te maken met nieuwe technologieën en methoden die de opponent gebruikt.
Ook kan de wijze van optreden van andere mogendheden veranderen, waardoor de MIVD mogelijk beperkt wordt in zijn effectiviteit.
In de afgelopen twaalf jaar zijn er wetsvoorstellen gedaan om dit probleem te ondervangen. In een Algemeen Overleg, op 1 februari 2012, bracht Tweede Kamerlid dhr. A. Elissen (PVV) naar voren dat de WIV 2002 nog nooit was geëvalueerd. Hierop volgend is een motie ingediend waarbij de regering werd verzocht een evaluatie uit te voeren op de WIV 2002.[14] Uit deze evaluatie, uitgevoerd door Commissie-Dessens, is naar voren gekomen dat de WIV 2002 niet omsluitend genoeg is en aanpassing behoeft.[15]
Vanuit deze probleemstelling is de volgende onderzoeksvraag opgesteld:
Zijn de beperkingen die de Wet op de Inlichtingen- en Veiligheidsdienst uit 2002 oplegt aan de Militaire Inlichtingen- en Veiligheidsdienst, als het gaat om het toepassen van digitale methoden voor inlichtingenverzameling, verouderd?
Deze onderzoeksvraag zal worden beantwoord aan de hand van een hypothese. Als eerste hypothese geldt dat de WIV 2002 verouderd is door nieuwe technologieën die in de afgelopen jaren zijn verschenen op het gebied van digitale inlichtingenverzameling. Dit wordt de H_0 genoemd. Indien de H_0 verworpen wordt zal de H_1 aangenomen worden. In de H_1 wordt er vanuit gegaan de WIV 2002 niet verouderd is.

[12] Kamerstukken II 2012/13, 30 977, nr.56, p.1.
[13] Kamerstukken II 2012/13, 30 977, nr.56, p.1-3.
[14] Kamerstukken II 2011/12, 29 924, nr.76, p.1.
[15] Dessens, C.W.M. (2013).

1.2 Doelstelling

Het doel van het onderzoek is het analyseren van de bevoegdheden van de Militaire Inlichtingen- en Veiligheidsdienst op het gebied van digitale inlichtingenverzameling uit de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002, het analyseren van de ontwikkelingen van nieuwe technologieën vanaf 2002 in het digitale domein voor de MIVD en daarnaast het belichten van de behoeftes van de MIVD om vervolgens deze te spiegelen aan de huidige wet om de mogelijke beperkingen van deze wetgeving te belichten.

1.3 Opzet

Om tot de beantwoording van de onderzoeksvraag te komen zal gebruik gemaakt worden van een literatuuronderzoek. Aan de hand van deelvragen zal door middel van onder andere relevante vakliteratuur, kamerstukken en krantenartikelen de onderzoeksvraag worden beantwoord.

De eerste deelvraag die behandeld zal worden is: *Wat zijn de taken van de MIVD en welke bevoegdheden hebben zij ten behoeve van inlichtingenverzameling via het digitale domein op grond van de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002?* Deze vraag zal beantwoord worden in hoofdstuk twee. In hoofdstuk drie zal de volgende vraag worden beantwoord: *Welke technologieën, op het gebied van digitale inlichtingenverzameling zijn beschikbaar sinds het opstellen van de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002 en wat betekent dit voor het verzamelen van inlichtingen voor de MIVD?* In deze hoofdstukken zullen de belangrijkste begrippen worden uitgelegd. De basis die hierbij gevormd wordt zal fungeren als theoretisch kader.

Vervolgens zal in hoofdstuk vier de laatste deelvraag worden beantwoord. De vraag is: *Welke behoeftes zijn er voor de Militaire Inlichtingen- en Veiligheidsdienst op het gebied van digitale inlichtingenverzameling, waar de dienst momenteel niet bevoegd toe is gelet op de taakstelling in de Wet voor de Inlichtingen- en Veiligheidsdiensten uit 2002?*

Uit deze beantwoording zullen resultaten komen die van toepassing zijn op de centrale vraag. In hoofdstuk vijf zullen de resultaten uiteengezet worden, om daaruit tot een conclusie te komen en antwoord te kunnen geven op de onderzoeksvraag. Door dit te doen kunnen er mogelijk aanbevelingen worden gedaan voor wetswijziging of vervolgonderzoek.

1.4 Afbakening

In deze thesis wordt de MIVD onderzocht aan de hand van de WIV 2002. Uit de probleemstelling komt naar voren dat deze thesis gericht is op het digitale domein en de toepassing hiervan binnen de MIVD ten behoeve van inlichtingenverzameling. Het gaat binnen dit onderzoek te ver om ook de andere werkgebieden van de MIVD te onderzoeken aan de hand van de WIV 2002. Daarnaast is de WIV 2002 ook van toepassing op de AIVD, in verband met de grootte van dit onderzoek zal deze buiten beschouwing worden gelaten. In eventueel vervolgonderzoek is het interessant om ook deze erbij te betrekken.

2. MIVD binnen Cyber

In de inleiding zijn de verschillende verwervingsmethoden tot inlichtingenverzameling van de MIVD behandeld. Nu bekend is over welke verwervingsmethoden de MIVD de beschikking heeft, kan er dieper worden ingegaan op het concept cyber en welke digitale methoden er zijn toegestaan om via het digitale domein inlichtingen te verzamelen. Het begrip cyber wordt steeds vaker gebruikt in het nieuws en in de volksmond, maar wat is het nu precies? Recente berichtgevingen in *NRC Handelsblad* spraken over NSA-achtige praktijken, in het digitale domein, waar de MIVD zich ook mogelijk schuldig aan maakt.[16] Hieruit volgt de vraag, welke taken en mogelijkheden heeft de MIVD binnen het digitale domein? Aan de hand van deze vragen is de volgende deelvraag ontstaan die in dit hoofdstuk behandeld zal worden:

Wat zijn de taken van de MIVD en welke bevoegdheden heeft de dienst ten behoeve van inlichtingenverzameling via het digitale domein op grond van de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002?

Bij de beantwoording van deze deelvraag zullen verschillende onderdelen worden uitgelicht. Allereerst zal gekeken worden naar de taken die de MIVD heeft en wat deze inhouden. Vervolgens zal het begrip digitale domein uitgelicht worden en zal er gekeken worden wat dit inhoudt voor defensie. Als laatste subvraag zal de vraag gesteld worden welke bevoegdheden de MIVD heeft om zijn taak, digitale inlichtingenverzameling, uit te voeren. Het hoofdstuk zal afgesloten worden met een subconclusie over bovenstaande deelvraag.

[16] NRC Handelsblad (2013).

2.1 Taken van de MIVD

De MIVD dient de hoofdtaken van defensie die beschreven staan in de grondwet artikel 97.[17] Deze dicteert dat er een krijgsmacht is ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk. Ook is deze krijgsmacht er om zorg te dragen voor de handhaving en de bevordering van de internationale rechtsorde. De inzet van operationele cybercapaciteiten dient de hoofdtaken van de krijgsmacht te ondersteunen. Dit wordt onderstreept doordat voor de welvaart van Nederland met haar sterk internationaal georiënteerde logistieke en dienstensector een veilig en goed functionerend digitaal netwerk essentieel is.[18]

De MIVD heeft verschillende taken met betrekking tot het verzamelen van inlichtingen. Met de invoering van de WIV 2002 heeft de MIVD een extra taak gekregen, ten opzichte van de MID, namelijk de inlichtingentaak die gericht is op het buitenland. In de WIV 2002 zijn de huidige taakomschrijvingen van de AIVD en de MIVD opgenomen, respectievelijk in artikel 6 en 7. In verband met de afbakening van deze thesis zal alleen de taakomschrijving van de MIVD worden toegelicht. De belangrijkste punten uit de taakomschrijving van de MIVD zijn;

A-taak: Het handhaven en bevorderen van de internationale rechtsorde,
B-taak: Uitvoeren van veiligheidsonderzoeken,
C-taak: Onderzoek verrichten in het belang van de nationale veiligheid en ten behoeve van het treffen van maatregelen,
D-taak: Bevorderen van het treffen van veiligheidsmaatregelen door andere organisaties,
E-taak: Verrichten van onderzoek betreffende andere landen (‘buitenlandtaak’).

A-taak

De A-taak heeft als kernzin; het handhaven en bevorderen van de internationale rechtsorde, zoals beschreven in artikel 7 lid 2a:

“1°. Het verrichten van onderzoek omtrent het potentieel en de strijdkrachten van andere mogendheden, ten behoeve van een juiste opbouw en een doeltreffend gebruik van de krijgsmacht;

[17] Grondwet (1815).
[18] AIV/CAVV. (2011). p.11.

2°. Het verrichten van onderzoek naar factoren die van invloed zijn of kunnen zijn op de handhaving en bevordering van de internationale rechtsorde voor zover de krijgsmacht daarbij is betrokken of naar verwachting betrokken kan worden."[19]

De manier waarop de MIVD deze taak vorm geeft begint met het samenstellen van een dreigingsanalyse. Wat is er aan de hand, waar komt de dreiging vandaan en wie is er verantwoordelijk voor deze dreiging?[20] Voordat de MIVD een onderzoek start voor het opstellen van deze dreigingsanalyse, moet er reden zijn tot daadwerkelijke dreiging wat betreft de nationale veiligheid. Dit is van belang, aangezien de MIVD gegevens uitbuit, die zijn verkregen tijdens het onderzoek, om zo belangen en doelen te beschermen waarvoor de MIVD is opgericht.
Wanneer de dreigingsanalyse helder is dient deze bijgevoegd te worden bij het advies over de besluitvorming van een mogelijk komende missie.

B-taak

De B-taak is het uitvoeren van veiligheidsonderzoeken die vallen onder de Wet Veiligheidsonderzoeken (WVO).[21]

C-taak

Onder de C-taak valt het verrichten van onderzoek in het belang van de nationale veiligheid en ten behoeve van het treffen van maatregelen. Voordat er onderzoek wordt gestart wordt er, net als bij de A-taak, eerst gekeken of er aanleiding is tot het ernstig vermoeden dat de te onderzoeken persoon of organisatie een risico vormt voor een gewichtig belang van de staat. De informatie die de MIVD heeft verkregen door middel van verschillende inlichtingenverwervingstechnieken, wordt gemeld aan de instanties over wie dit gaat, zoals beschreven in artikel 36 van de WIV 2002. Deze instanties (de belangendragers) zijn verantwoordelijk en kunnen aan de hand van de informatie van de MIVD preventieve of repressieve beschermingsmaatregelen treffen[22]. Daarnaast moet de MIVD operationele inlichtingen inwinnen voor de Nederlandse militairen die worden en zijn uitgezonden naar een operatiegebied. Dit om ervoor te zorgen dat ongestoord voorbereidingen kunnen worden getroffen ter inzet van de krijgsmacht als bedoeld in het tweede lid onder a, ten 2e.[23]

[19] Staatsblad 2002, nr.148, p.3.
[20] MijnWetten.nl (z.d.).
[21] Dessens, C.W.M. (2013). p.33.
[22] Kamerstukken II 1997/98, 25 877, nr.3, p.57.
[23] Kamerstukken II 1997/98, 25 877, nr.3, p.12.

D-taak

De D-taak houdt in dat de MIVD verantwoordelijk is voor het bevorderen van het treffen van veiligheidsmaatregelen door andere organisaties. Dit houdt in dat zij de onder de C-taak genoemde belangendragers beschermd, waarbij gegevens wat betreft geheimhouding over de krijgsmacht gewaarborgd blijven. De MIVD richt zijn adviezen aan de overheid, maar ook aan de defensie-industrie.[24]

E-taak

Onder de E-taak behoort het onderzoek verrichten naar landen ten aanzien van onderwerpen die direct of indirect van enige relevantie zijn voor defensie. Deze onderzoeken worden uitgevoerd in opdracht van Minister-president, in samenspraak met andere betrokken ministers.[25] Deze taak is in 2002 toegevoegd aan het takenpakket van de MIVD.

Bij de totstandkoming van de WIV 2002 zijn er belangrijke aanvullingen gedaan vanwege de veranderende rol van de krijgsmacht. Waar zij eerst gericht was op conventionele oorlogvoering, werd de focus na de Koude Oorlog gericht op een nieuwe wijze van inzet. Gedurende de Koude Oorlog was de inlichtingenbehoefte vooral gebaseerd op de klassieke algemene verdedigingstaak van de krijgsmacht in koninkrijks- en bondgenootschappelijk verband. Dit veranderde na de Koude Oorlog. Een omwenteling van type operaties vond plaats, waardoor de krijgsmacht zich meer toelegde op internationale crisisbeheersings- en vredesoperaties. De E-taak is hierdoor toegevoegd.[26]

[24] Dessens, C.W.M. (2013). p.32.
[25] Kamerstukken II 1997/98, 25 877, nr.3, p.10.
[26] Graaf, B.A. et al. (2010). p.43.

2.2 Het digitale domein

Wat is het digitale domein of anders gezegd, wat is cyberspace? De normale domeinen waarbinnen militairen operaties uitvoeren zijn duidelijk. Het gaat over land, lucht, zee en ruimte. Het digitale domein onderscheidt zich van de andere doordat het niet geografisch of fysiek afgebakend is. De US Department of Defense en NATO's Cooperative Cyber Defence Centre of Excellence geven de volgende definitie:

> *Cyberspace is a global domain within the information environment. It consists of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.*[27]

> *Cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks.*[28]

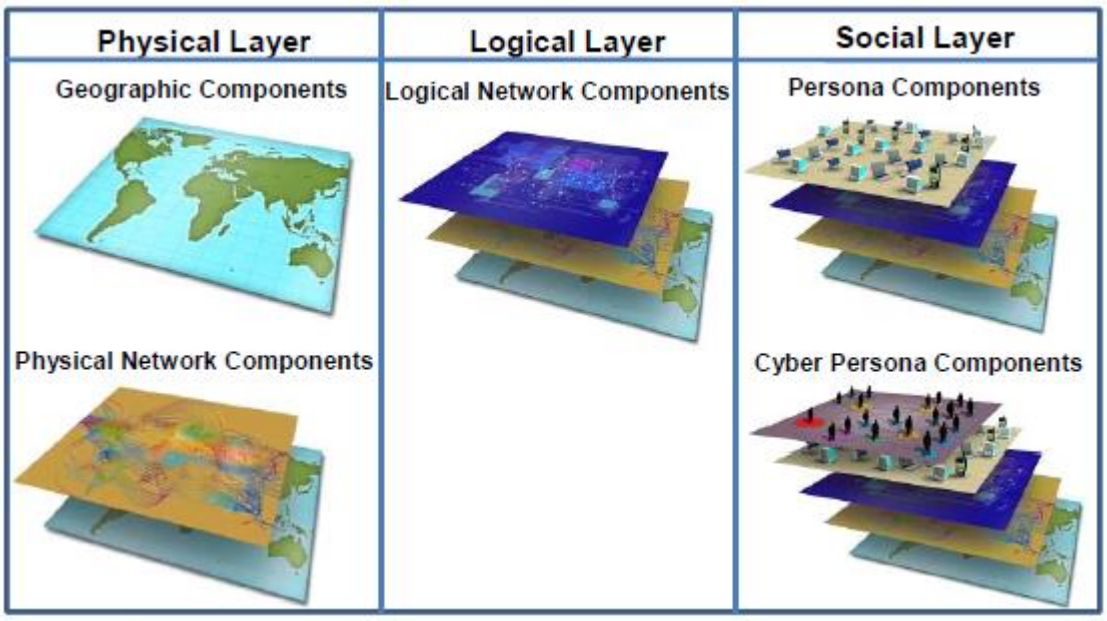
De definitie die wordt gehanteerd door de Adviesraad Internationale Vraagstukken luidt:

> *Het digitale domein wordt gedefinieerd als het geheel van ICT-middelen en ICT–diensten. Hierbij horen ook alle niet met internet verbonden netwerken of andere digitale apparaten.*[29]

De dimensies land, lucht, zee en ruimte zijn natuurlijk, daarnaast zijn land en zee ook tastbaar. De digitale dimensie is daarin tweeledig. Het behelst een fysiek aspect, zoals computers, mobieltjes, routers, netwerkkabels en nog veel meer. Het domein behelst daarnaast ook een niet tastbaar aspect, zoals data. Het digitale domein is gecreëerd door de mens, het wordt steeds groter en neemt nieuwe vormen aan. Ook kunnen delen ervan worden uitgeschakeld, gewist, vernietigd of verdacht worden.[30] Het is een openbare ruimte die niet veroverd kan worden, maar waarin wel tijdelijk een informatie-overwicht kan worden bereikt. Dit is echter alleen mogelijk met behulp van technische hulpmiddelen, zoals virussen en spyware.[31]

[27] Joint Publications 3-0. (2011). p.IV.2.
[28] CCDCOE (2012). p.8.
[29] AIV/CAVV. (2011). p.10.
[30] Ducheine, P.A.L. et al. (2012). p.9.
[31] Ministerie van Defensie (2013). p.97.

De definitie heeft duidelijkheid gecreëerd over wat het digitale domein behelst, maar het is nog niet helder in welke vormen het terug te vinden is.



Het digitale domein kan onderverdeeld worden in drie 'lagen'. [32]

De eerste laag is de fysieke laag. Deze laag bestaat uit de infrastructuur die verbonden is met netwerken van computers en geografische locaties. Het zijn de hardware en de daaraan gelinkte fysieke verbindingen die het netwerk ondersteunen.

De tweede laag is de virtuele laag. Deze bestaat uit de virtuele netwerkcomponenten die technisch van aard zijn en virtuele verbindingen omvatten die bestaan binnen netwerknodes.[33] Hieronder vallen protocollen, software en digitale verbindingen. Deze laag maakt telecommunicatie en dataoverdracht tussen mensen en objecten mogelijk.[34]

De laatste laag is de sociale laag. Deze laag omvat de cyber persona componenten en de persona componenten. De cyber persona componenten zijn de identiteiten van een persoon of een groep op het netwerk. Dit zijn email adressen, IP adressen, mobiele telefoonnummers. De persona componenten zijn de personen die zich daadwerkelijk op het netwerk bevinden of daar gebruik van maken. [35]

[32] TRADOC Pamphlet 525-7-8 (2010). p.8.

[33] De term 'node' betekent in de context van computernetwerken, een computer of ander apparaat dat is aangesloten op een bepaald netwerk. Ook netwerkapparaten zelf worden aangeduid als nodes. Een aantal voorbeelden van nodes in computernetwerken zijn computers, laptops, routers, switches, hubs en draadloze apparatuur zoals draadloze printers, draadloze betaalautomaten en telefoons. Kay, R. (2001).

[34] Ducheine, P.A.L. & Haaster, J. van. (2013). p.368-387.

[35] TRADOC Pamphlet 525-7-8 (2010). p.9.

De lagen zijn onderling met elkaar verbonden en hebben elkaar nodig om bruikbaar te zijn.
Zo werkt de virtuele laag op de hardware, die zich bevindt binnen de fysieke laag. De virtuele laag kan gebruikt worden om veranderingen aan te brengen in de fysieke laag. De virtuele laag, waaronder software valt, reguleert hoe de hardware werkt. Wanneer deze software wordt veranderd, kan dit gevolgen hebben voor de fysieke laag.[36]

Het digitale domein bestaat dus uit veel verschillende netwerken en nodes. Hoewel niet alles onderling wereldwijd fysiek verbonden is met elkaar, groeit de verbondenheid in het digitale domein voortdurend door de toename van draadloze verbindingen en losse netwerken. De eenvoud van het overschrijden van grenzen via het internet is, in vergelijking met andere transmissies of manieren van reizen, uniek. Onze samenleving is tegenwoordig gebouwd op digitale informatievoorziening en communicatie. Internet en mobiele communicatie zijn niet meer weg te denken en ondersteunen in toenemende mate de vitale infrastructuur. Particulieren en banken doen zelf hun betalingen digitaal. Elektriciteitsnetwerken worden op afstand gemonitord, net als het water- en rioolbeheer.[37]

Sommige grenzen zijn binnen het digitale domein niet zomaar te overschrijden. Bepaalde netwerken kunnen softwarematig zijn geïsoleerd door middel van protocollen, firewalls en vercijfering. Scheiding van netwerken kan ook gebeuren door deze volledig los te koppelen van het internet, een zogenoemde 'air gap', waarbij er een elektromagnetische, een elektronische en een fysieke scheiding ontstaat.[38] Ook kunnen netwerken volledig zijn afgesloten van het internet. Fysieke nabijheid is dan benodigd om toegang te hebben tot dit netwerk.[39]

[36] Andress, J. Winterfeld, S. (2014). p.138.
[37] AIVD (2013). p.17.
[38] Janssen, C. (z.d.).
[39] TRADOC Pamphlet 525-7-8. (2010). p.9.

2.2.1 Defensie in het digitale domein

Wat houdt het digitale domein in voor defensie?

Defensie gebruikt het digitale domein voor het behoud van een informatievoorsprong om het initiatief te behouden, verrassing bij de opponent te bewerkstelligen, een superieure inlichtingenpositie te krijgen en om de eigen militaire capaciteiten te beschermen tijdens operaties.

Het verzamelen van informatie gebeurt vaak op heimelijke wijze, zoals door het binnendringen in een geautomatiseerd werk. Het vergaren van informatie tussen computers is geen nieuwe verwervingsmethode voor de MIVD. Signals Intelligence (Sigint) deed dit al op een passieve wijze door te luisteren naar radiosignalen of door het aftappen van communicatielijnen.

Het verkrijgen van inlichtingen in of via het digitale domein wordt ook wel Cyber Intelligence (Cyberint) genoemd. Dit is de techniek om informatie uit of via digitale systemen te verkrijgen. Cyberint onderscheidt zich in de uitvoering van Sigint door juist actief inbraak te plegen in geautomatiseerde werken. De informatie die via Cyberint wordt verkregen is afkomstig van individuen, tegenstanders en overheden. De techniek die hierbij essentieel is wordt ook wel 'hacken' genoemd. Door op deze compleet andere wijze te opereren wordt er een toegang gecreëerd tot andere informatie. Het primaire doel van Cyberint is dan ook het verzamelen van inlichtingen. De techniek die hieraan ten grondslag ligt is afkomstig uit de criminele hackerswereld. Hackers maken gebruik van virussen om gegevens te verzamelen van hun slachtoffers, dit gaat tot en met het niveau van bankgegevens verzamelen om geld te stelen.[40] Inlichtingendiensten die gebruik maken van Cyberint gebruiken vergelijkbare technieken om informatie uit de computers te krijgen van hun doelwit.

Het voordeel van het uitvoeren van digitale inlichtingenverzamelacties is dat deze moeilijk te detecteren zijn. Indien de acties onderkend worden is het voor het slachtoffer eveneens ingewikkeld om concreet te kunnen zeggen door wie of waarvandaan de actie is uitgevoerd.[41]

Voor defensie beperkt het digitale domein zich niet alleen tot het militaire spectrum. De civiele maatschappij dient ook beschermd te worden. Dit gebeurt onder andere door de samenwerking tussen de AIVD en MIVD.

Een goed functionerende justitie, politie en luchtverkeerleiding zijn van groot belang voor de nationale veiligheid. Ook zijn geldstromen en communicatienetwerken een belangrijke factor voor de nationale veiligheid. [42]

[40] Ducheine, P.A.L. et al. (2012). p.149.
[41] Blunden (2010). p 1-16.
[42] Ministerie van Defensie (2013). p.97.

Dit optreden kan op twee manieren gebeuren. Ten eerste kan er defensief worden opgetreden. Het gaat hierbij om de bescherming van de eigen gegevens, netwerken en communicatie- en informatiesystemen tegen cyberdreigingen.[43] Ten tweede, het exploiterend optreden om gegevens, informatie en inlichtingen te verzamelen voor de eigen *situational awareness*.[44]

[43] Ministerie van Defensie (2012). p.9.
[44] Ministerie van Defensie (2013b). p. 98.

2.3 Bevoegdheden van de MIVD binnen het digitale domein

Zoals beschreven in paragraaf 2.1 is de taak van de MIVD het dienen van de Nederlandse defensie. Dit doet de dienst door middel van het verzamelen van inlichtingen. Inlichtingen kunnen worden verzameld via verschillende verwervingsmethoden, zoals beschreven in de inleiding. Het digitale domein wordt naast land, lucht, zee en ruimte beschouwd als de 'vijfde dimensie' waarin militaire operaties kunnen worden ontplooid, zo ook inlichtingenoperaties. De krijgsmacht voert deze digitale activiteiten primair uit in (of door middel van) het digitale domein.[45]

De wijze waarop de MIVD zijn taak uitvoert is afhankelijk van de manier van telecommunicatie. Er zijn hier verschillende manieren van, zoals via een draadloze verbinding (ether). Hieronder vallen radioverkeer, satellietcommunicatie en de moderne mobiele telefonie. Ook kan telecommunicatie lopen via een vaste kabel, zoals glasvezel- en koperverbinding. Daarnaast kan zij ook lopen via een combinatie van beide manieren. Een sprekend voorbeeld hiervan is een telefoongesprek naar Australië, dat zowel via de kabel gaat als via de satelliet.[46]

Er zijn voor de MIVD verschillende bijzondere bevoegdheden voor interceptie als het gaat om telecommunicatie. Deze staan beschreven in de WIV 2002 en mogen alleen worden uitgevoerd na een toetsing op proportionaliteit, subsidiariteit en noodzaak, zoals beschreven in artikel 18, 31 en 32. Deze toetsingen worden vervolgens aan de betreffende minister en/of aan het hoofd van de MIVD overhandigd om hier toestemming voor te verlenen. [47]

De bevoegdheden die benodigd zijn voor het uitvoeren van de taken van de MIVD staan beschreven in de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002. In deze WIV 2002 zijn een aantal bepalingen opgenomen die de algemene en bijzondere bevoegdheden beschrijven. Voor de taken van de MIVD in het digitale domein is artikel 7, lid 2, onder a, b, c, d, e van groot belang. Hierin staat beschreven wat de taken van de MIVD zijn, zoals uitgewerkt in paragraaf 2.1.

De daadwerkelijke bijzondere bevoegdheden van de MIVD op het gebied van digitale inlichtingenverzameling worden behandeld in de artikel 24 t/m 27 van de WIV 2002.

[45] Joint Publications 3-0. (2011). p.xvii.
[46] Ministerie van Defensie (2013c).
[47] CTIVD (2012). p.6.

De bevoegdheden die daar staan beschreven zijn het binnendringen in een geautomatiseerd werk (artikel 24), het uitvoeren van gerichte (artikel 25) en ongerichte (artikel 26) niet-kabelgebonden interceptie en de bevoegdheid tot selecteren van de verzamelde gegevens uit ongerichte niet-kabelgebonden interceptie (artikel 27). Deze bevoegdheden stellen de MIVD in staat zijn taken uit te voeren;

Artikel 24

Artikel 24 betreft het gericht binnendringen in een geautomatiseerd werk (hacken). Dit artikel vindt zijn toepassing in het digitale domein en mag alleen worden uitgevoerd op basis van last. Het doel van deze bevoegdheid is gericht op opgeslagen data en activiteiten op een specifiek geautomatiseerd werk. Dit kunnen (stand-alone) computers zijn van personen, gehele computernetwerken van organisaties of servers van webfora.[48] Deze systemen en netwerken mogen worden binnengedrongen onder de bevoegdheid uit artikel 17 of 21 van de WIV 2002.[49] Hierin staat beschreven dat de MIVD bevoegd is om dit doen, mits het ten behoeve is van een adequate taakuitvoering.

Door middel van een technisch hulpmiddel kan gebruik worden gemaakt van valse signalen, valse sleutels en valse hoedanigheden. Daarbij mogen beveiligingen worden doorbroken, decryptie- en encryptievoorzieningen worden aangebracht, verhaspeling en versluiering worden toegepast om gegevens over te nemen. [50] Dit maakt het voor de MIVD mogelijk om netwerkexploitatie uit te voeren. Dit kan worden gedaan door het plaatsen van een virus of Trojaans paard.

Deze vorm van netwerkexploitatie kan, volgens de Commissie-Dessens, alleen worden uitgevoerd, *'op verzoek van een rechthebbende en moet het juridisch kader dat voor die rechthebbende geldt een dergelijke monitoring toestaan.'*[51]

Daarnaast kan er pas gestart worden met het uitvoeren wanneer er toestemming is verleend door de betrokken minister en door het hoofd van de MIVD. Aan de uitvoering van deze bevoegdheid hangen dus checks en balances.

[48] In een artikel van het NRC Handelsblad van zaterdag 30 nov. stond dat de AIVD, vallend onder dezelfde wetgeving als de MIVD, onrechtmatig een webfora had binnengedrongen. Deze uitspraak van de krant is onjuist volgens AIVD, zie hierover: AIVD & Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (z.d.a).
[49] Dessens, C.W.M. (2013). p.87.
[50] Kamerstukken II 1997/98, 25 877, nr.3, p.39.
[51] Dessens, C.W.M. (2013). p.87.

Artikel 24 stelt expliciet dat er alleen gericht binnengedrongen mag worden in een geautomatiseerd werk. Het artikel biedt echter niet de mogelijkheid voor de MIVD om geplaatste virussen te gebruiken voor een netwerkaanval met militair oogmerk dat het beschadigen van een systeem of netwerk tot doel heeft.[52]

Artikel 25

Artikel 25 betreft de bevoegdheid tot het gericht uitvoeren van interceptie uit de ether en niet-kabelgebonden telecommunicatie. Elke vorm van gesprek, telecommunicatie en gegevensoverdracht via een geautomatiseerd werk mag hierbij gericht worden afgetapt, opgenomen en afgeluisterd met behulp van technische hulpmiddelen.

Gerichte interceptie betekent in dit artikel dat de afzender en/of ontvanger van de communicatie in beginsel bekend is, zodat er gericht op het juiste target onderzoek wordt verricht.[53] De locatie waar het een en ander plaatsvindt is onbelangrijk.

Naast deze bevoegdheid is in dit artikel ook opgenomen dat technische voorzieningen mogen worden gebruikt om het mogelijk te maken versleutelde gesprekken, telecommunicatie of gegevensoverdracht ongedaan te maken. Voor de uitoefening van deze bevoegdheid, wanneer dit plaatsvindt op een locatie anders dan gebruikt door defensie, moet er wel toestemming worden verleend door de verantwoordelijke minister én het hoofd van MIVD.[54]

Niet alleen de uitvoering van artikel 24 wordt gezien als hacken. In het wetsvoorstel Computercriminaliteit III staat dat '*het op afstand binnendringen van een geautomatiseerd werk ('hacken') vergelijkbaar wordt geacht met het afluisteren van telecommunicatie.'*[55]

[52] AIV/CAVV (2011). p.16.
[53] Dessens, C.W.M. (2013). p.74.
[54] Kamerstukken II 1997/98, 25877, nr.3, p.41.
[55] Dessens, C.W.M. (2013). p.83.

Artikel 26

Artikel 26 betreft de bevoegdheid om ongericht niet-kabelgebonden telecommunicatie, zoals al het telecommunicatieverkeer via de ether en satelliet, te ontvangen en op te nemen dat zijn oorsprong kent in het buitenland. Met ongericht ontvangen en opnemen wordt de interceptie van telecommunicatie die niet specifiek afkomstig is van een bepaalde persoon, organisatie of over enige specifieke technische kenmerken beschikt, maar wel van een bepaalde satelliet afkomstig is, bedoeld.

Bij de vaststelling van de WIV 2002 werd de methode *search* gebruikt om het verkeer in kaart te brengen. Dit werd gedaan op *high frequency* radiokanalen. De Nederlandse krijgsmacht gebruikte dit kanaal nog niet geregeld, het werd wel gebruikt door buitenlandse strijdkrachten. Door de toenmalige ministers werd deze methode gezien als het voortraject van gerichte interceptie, zoals beschreven in artikel 25.[56] *Searchen* is een specifieke invulling van het bewust ontvangen en opnemen van telecommunicatie, om zo duidelijkheid te krijgen over de identiteit van de afzender en de technische kenmerken van de telecommunicatie.[57]

Al deze ontvangen telecommunicatie wordt vervolgens digitaal opgeslagen voor later onderzoek. Hierbij wordt nog geen kennis genomen van data. Om deze opgeslagen data te doorzoeken moet eerst een aantal selectiecriteria worden doorlopen, waarvoor de betrokken minister toestemming dient te verlenen. Daarnaast laat artikel 26 het toe om met behulp van technische hulpmiddelen versleuteling van de ontvangen en opgenomen telecommunicatie te verwijderen, wanneer dit nodig is. Het gaat hierbij in het bijzonder om de ontvangen telecommunicatie te ontdoen van de toegepaste cryptografische technieken.[58]

[56] Dessens, C.W.M. (2013). p.75.
[57] Kamerstukken II, 1999/00, 25 877, nr.9, p.21-22.
[58] Kamerstukken II, 1997/98, 25 877, nr.3, p.44.

Artikel 27

Artikel 27 betreft de bevoegdheid voor de MIVD om zich te wenden tot personen, instanties of bedrijven die telecommunicatie verzorgen voor derden. De MIVD mag hen verzoeken tot het verstrekken van gegevens.

'Het gaat hierbij om alle verkeer dat over telecommunicatie-infrastructuur of telecommunicatie-inrichtingen heeft plaatsgevonden, dan wel zal plaatsvinden, ten aanzien van een in dat verzoek aangegeven nummer, dan wel ten aanzien van een in het verzoek aangegeven persoon of organisatie toebehorend technisch kenmerk.'[59]

Op basis van dit artikel kunnen gegevens worden opgevraagd betreffende:

- telecommunicatieverkeer met een specifiek nummer waarmee verbinding wordt gezocht;
- telecommunicatieverkeer met een specifiek nummer vanaf waar verbinding wordt gemaakt;
- gegevens over de identiteit van een persoon of organisatie aan wie een specifiek nummer behoort, zoals naam, woonplaats en gegevens over verbindingstijd.

De bevoegdheid om deze actie te ondernemen is alleen neergelegd bij het hoofd van de MIVD en hoeft niet voor toestemming langs de desbetreffende minister, dit omdat de mate van impact dusdanig lager is dan de bevoegdheid uit artikel 25.[60] Artikel 27 geeft niet de bevoegdheid tot het ongericht intercepteren van kabelgebonden telecommunicatie.

In de hier bovenstaande artikelen wordt gesproken over versleutelingen die zijn aangebracht op de telecommunicatie. Wanneer er sprake is van het ongedaan maken van deze versleuteling, waartegen de interceptie is gericht, is in artikel 24 en 25 vastgelegd dat een ieder die kennis draagt over de versleuteling verplicht is om mee te werken dit ongedaan te maken. Dit is echter niet opgenomen in artikel 26 en 27. Volgens het CTIVD rapport 28 is dit mogelijk per ongeluk niet in de artikelen opgenomen.[61]

[59] Kamerstukken II, 1997/98, 25 877, nr.3, p.46.
[60] Kamerstukken II, 1997/98, 25 877, nr.3, p.47.
[61] CTIVD (2011). p.48.

2.4 Subconclusie

In dit hoofdstuk is gekeken naar de vraag:

Wat zijn de taken van de MIVD en welke bevoegdheden heeft de dienst ten behoeve van inlichtingenverzameling via het digitale domein op grond van de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002?

Ter beantwoording van deze vraag is het hoofdstuk verdeeld in drie onderdelen.
Als eerste is er gekeken naar alle taken die de MIVD ter ondersteuning van de Nederlandse krijgsmacht uitvoert. Onder deze taken vallen:

- Het handhaven en bevorderen van de internationale rechtsorde;
- uitvoeren van veiligheidsonderzoeken;
- onderzoek verrichten in het belang van de nationale veiligheid en ten behoeve tot het treffen van maatregelen;
- bevorderen van het treffen van veiligheidsmaatregelen door andere organisaties;
- verrichten van onderzoek betreffende andere landen ('buitenlandtaak').

Vervolgens is het digitale domein behandeld en is er ingegaan op de eigenschappen van dit domein. De drie lagen - fysiek, virtueel en sociaal - die nauw met elkaar samenhangen en dit steeds meer gaan doen door de toenemende afhankelijkheid van digitale netwerken door defensie en de civiele maatschappij.

Voor het realiseren van deze taken mogen (algemene en bijzondere) bevoegdheden worden toegepast. In het kader van deze thesis is alleen ingegaan op de bijzondere bevoegdheden vanuit de WIV 2002 die de MIVD heeft en die van toepassing zijn in het digitale domein.
Deze bijzondere bevoegdheden zijn gericht op het onderscheppen van berichtenverkeer en datastromen. De digitale bevoegdheden die aan de MIVD zijn toegekend zijn: artikel 24, 25, 26 en 27. Artikel 24 biedt de MIVD het meeste ruimte voor de uitvoering van netwerkexploitatie door het binnendringen van een geautomatiseerd werk en geeft niet de bevoegdheid een netwerk of systeem plat te leggen. Artikel 25 geeft de MIVD de bevoegdheid tot het gericht intercepteren van telecommunicatie uit de ether en de kabel en artikel 26 tot het ongericht intercepteren van niet-kabelgebonden telecommunicatie die zijn oorsprong in het buitenland kent.

Als laatste artikel 27, dat voortborduurt op artikel 26 door selectie uit te voeren op de ongerichte niet-kabelgebonden onderschepte informatie. Voorafgaand aan de uitvoering van deze bevoegdheden moet er eerst toestemming worden verkregen van de desbetreffende minister en/of het hoofd van de MIVD, om zo te zorgen voor een valide optreden binnen de gestelde wetgeving.

3. Technologische ontwikkelingen in het digitale domein

In hoofdstuk twee is ingegaan op de taken en bijzondere bevoegdheden van de MIVD. Daarnaast is de betekenis van het digitale domein gegeven. In komend hoofdstuk zal worden ingegaan op de ontwikkelingen die hebben plaatsgevonden binnen dit digitale domein, sinds de invoering van de WIV in 2002.

Technologische ontwikkelingen worden met open armen ontvangen door de samenleving en de afhankelijkheid van deze techniek wordt steeds groter. De snelheid waarmee nieuwe ontwikkelingen elkaar opvolgen is ongekend. Geavanceerde technologieën worden steeds sneller bereikbaar voor de publieke sector. Ook voor defensie zijn deze technologieën beschikbaar, waardoor nieuwe mogelijkheden ten behoeve van het digitaal verzamelen van inlichtingen en de verwerking hiervan beschikbaar worden. Het volgen van de telecommunicatie van een persoon of organisatie, waarbij een ernstig vermoeden bestaat dat deze een risico vormt voor een gewichtig belang van de staat, kan theoretisch op steeds meer manieren. Dit kan niet alleen door de nieuwe soorten technologie die zijn ontstaan, maar ook doordat de kwaliteit van de (bestaande) technologieën verbetert. Om duidelijk te krijgen welke nieuwe methoden er ontwikkeld zijn sinds de invoering van de WIV 2002, staat in dit hoofdstuk de volgende vraag centraal:

Welke technologieën, op het gebied van digitale inlichtingenverzameling, zijn beschikbaar sinds het opstellen van de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002 en wat betekent dit voor het verzamelen van inlichtingen voor de MIVD?

Om deze vraag te kunnen beantwoorden zijn verschillende nieuwe technologieën uitgewerkt. Vervolgens zijn deze technologieën naast de taken van de MIVD gelegd om een beeld te krijgen wat zij de MIVD voor kansen kunnen bieden.

3.1 Beschikbare ontwikkelingen sinds 2002

De taak van de overheid om haar inwoners te beschermen is groot. Zo is de overheid verantwoordelijk voor de bescherming van bijvoorbeeld de democratische rechtsstaat, grondrechten en veiligheid. Een manier om dit te doen is om de krijgsmacht, door middel van inlichtingenverzameling, op een adequate wijze in te zetten. Hiervoor zet de overheid de AIVD en de MIVD in. Zoals in de afbakening is besproken zal ook hier alleen de MIVD worden behandeld.

De eerder besproken bevoegdheden van de MIVD maken het mogelijk deze taak uit te voeren. Door de komst van nieuwe technologieën kunnen de mogelijkheden om inlichtingen te verzamelen groter worden. Aan de andere kant kan het ook zorgen voor een verschuiving van telecommunicatie naar een, voor de MIVD tot nog toe onbereikbaar, medium. Dit gebeurt nu al door het toenemende gebruik van glasvezelkabels. Een andere manier van telecommunicatie sinds de invoering van de WIV 2002 is het gebruik van het mobiele internet door mobiele apparatuur en het door de NSA ontwikkelde Quantum. Daarnaast hebben zich in de afgelopen twaalf jaar ook andere ontwikkelingen voortgedaan. Het gaat om ontwikkelingen die sociaal van aard zijn, zoals een verandering van communicatie door de vrijheid van mobiele technologie, mobiel internet, social media en cloud computing.

3.1.1 Technologische ontwikkelingen

Deze paragraaf zal een beschrijving geven van de vier, voor de MIVD, interessante technologische ontwikkelingen sinds de invoering van de WIV 2002. Het gaat hierbij om de bovengenoemde ontwikkelingen. Naast de besproken techniek, zal er ook ingegaan worden op eventuele technische en sociale gevolgen van deze nieuwe technologie. Op deze manier wordt een compleet beeld geschept van de nieuwe technologieën die de MIVD mogelijk zou kunnen gebruiken of waar de MIVD tegen aan zou kunnen lopen.

3.1.1.1 Glasvezeltechniek

Een belangrijke ontwikkeling in het digitale domein is de introductie van de glasvezelkabels. In de jaren 80 was de heersende gedachte dat communicatiesatellieten de toekomst voor de communicatie zouden vormen. Het telefoonsysteem dat werd gebruikt was de afgelopen 100 jaar praktisch gezien niet veranderd. Degene die digitale gegevens wilde versturen kon dit doen via een zeer langzame satellietverbinding.

Deze gedachte werd verbroken door telefoonmaatschappijen die hun lange afstand verbinding gingen vervangen met glasvezelkabels eind jaren 80.[62] In 2007 kwam glasvezelverbinding ook beschikbaar voor particulier gebruik.[63]

[62] Tanenbaum, A.S. (2007). p.117.
[63] InterNLnet (z.d.).

Glasvezelverbindingen, ten behoeve van datacommunicatie, vormen een nieuwe technologie waarmee digitale signalen worden verstuurd met de snelheid van het licht door de glasvezelkabels. De capaciteit van glasvezelkabels is aanzienlijk groter dan die van zijn voorganger, de koperen kabel, die overigens nog wel in gebruik is. Glasvezelkabels zijn gebundelde haardunne vezels van zeer helder glas. Zo'n kabel beschikt over de unieke capaciteit om over grote afstanden lichtsignalen te transporten. Dit gebeurt met lasertechnologie, waarbij licht op hoge snelheid wordt in- en uitgeschakeld. Datacommunicatie wordt door deze glasvezelkabels mogelijk met (momenteel) een maximale snelheid van 10 Gigabite per seconde (Gbps).[64] Voor de normale huishoudens die beschikken over een glasvezelverbinding ligt de maximale snelheid nu op 1 Gbps.[65] Door deze enorme capaciteit worden steeds meer koperen kabels, met een maximale downloadsnelheid van 120 Megabite per seconde (Mbps)[66], vervangen door glasvezelkabels. Het internationale dataverkeer verloopt tegenwoordig voor 80 tot 90 procent via glasvezelkabels. De overige 10 tot 20 procent verloopt nu nog via de ether of de satelliet.[67]

De Amsterdam Internet Exchange (AMS IX), het enige internationale internetknooppunt in Nederland, heeft op het moment een maximale capaciteit van 10408 Gbps.[68] De piek van de maximale hoeveelheid internet verkeer via het AMS IX lag in 2002 op 12 Gbps.[69] Dit is uitgegroeid tot een piek van 2742 Gbps in februari 2014.[70] Deze ongeëvenaarde snelheden van datacommunicatie en de hoge bandbreedtes van de technologie maken het mogelijk om diensten, zoals Voice over Internet Protocol (VoIP), videoconferenties en online back-up's, uit te voeren. VoIP zijn telefoongesprekken of videogesprekken die over internet worden gevoerd en dit is in het bijzonder een ontwikkeling die door glasvezel in werking is gezet. In de afgelopen jaren is VoIP in populariteit gegroeid, bijvoorbeeld dankzij programma's als Skype.[71]

De positie van deze technologie in het digitale domein valt onder te delen in de fysieke laag. Glasvezelkabels zijn fysieke verbinding tussen computers en netwerken.

[64] Dufaco ICT (z.d.).
[65] Consumentenbond (z.d.).
[66] Internetten.nl (z.d.).
[67] Dessens, C.W.M. (2013). p.77.
[68] https://www.ams-ix.net/.
[69] AMSix (2003). p.15.
[70] https://www.ams-ix.net/.
[71] Andress, J. Winterfeld, S. (2014). p.176.

3.1.1.2 Mobiele techniek

Op 17 november 1988 kreeg de eerste Nederlander toegang tot het NSFnet. Dit was de toenmalige naam van het huidige internet. Sinds 1988 maakt de Nederlandse samenleving dan ook onderdeel uit van het digitale domein. In ruim 25 jaar is er onwaarschijnlijk veel vernieuwd, verbeterd en ontwikkeld in dit domein.

Zeker ook wat betreft het internet. Oorspronkelijk kon men alleen verbinding maken met het internet via een vaste verbinding. Het gebruik van mobiel internet is rond 2007 gegroeid door de komst van onder andere smartphones en tablets. Mobiel internet is een technologie die bestaat uit de draadloze verbinding van mobiele apparatuur met het internet.

Volgens het Centraal Bureau voor de Statistiek (CBS) bedroeg het internetgebruik op mobiele telefoons in Nederland onder de personen van 12 tot 75 jaar in 2007 8%. Dit gebruik van mobiel internet in dezelfde categorie is in 5 jaar tijd toegenomen tot 47%.[72] Een gevolg van dit mobiele internet en deze groei in gebruikers, is dat het de connectiviteit tussen (individuele of groepen) personen vergroot via het internet. Door deze toename van gebruikers is ook de behoefte aan vernieuwde verbindingen gekomen, waardoor internetbedrijven gingen investeren in hogere mobiele internetsnelheden.

Een tweede technologische ontwikkeling is de mobiele techniek. Mobiele techniek is een techniek waarbij het mogelijk wordt om met elkaar te communiceren aan de hand van draagbare apparatuur. Het is door geavanceerde technologie mogelijk dat communicatiemiddelen zo klein gemaakt worden dat deze zelfs mee te nemen zijn in de broekzak of tas.

Veranderingen die deze technologie met zich mee brengt is bijvoorbeeld het fenomeen dat het niet meer nodig is om op een vaste locatie te zitten om toegang te verkrijgen tot telefonie of het internet. Mensen zijn in toenemende mate online verbonden door het gebruik van mobiele technologie. Hierdoor zijn er meer communicatiemogelijkheden tussen mensen ontstaan. Waar voorheen werd afgesproken om met elkaar te communiceren kan dit nu digitaal en bijna overal gebeuren (mits er verbinding is met het internet of telefonienetwerk).

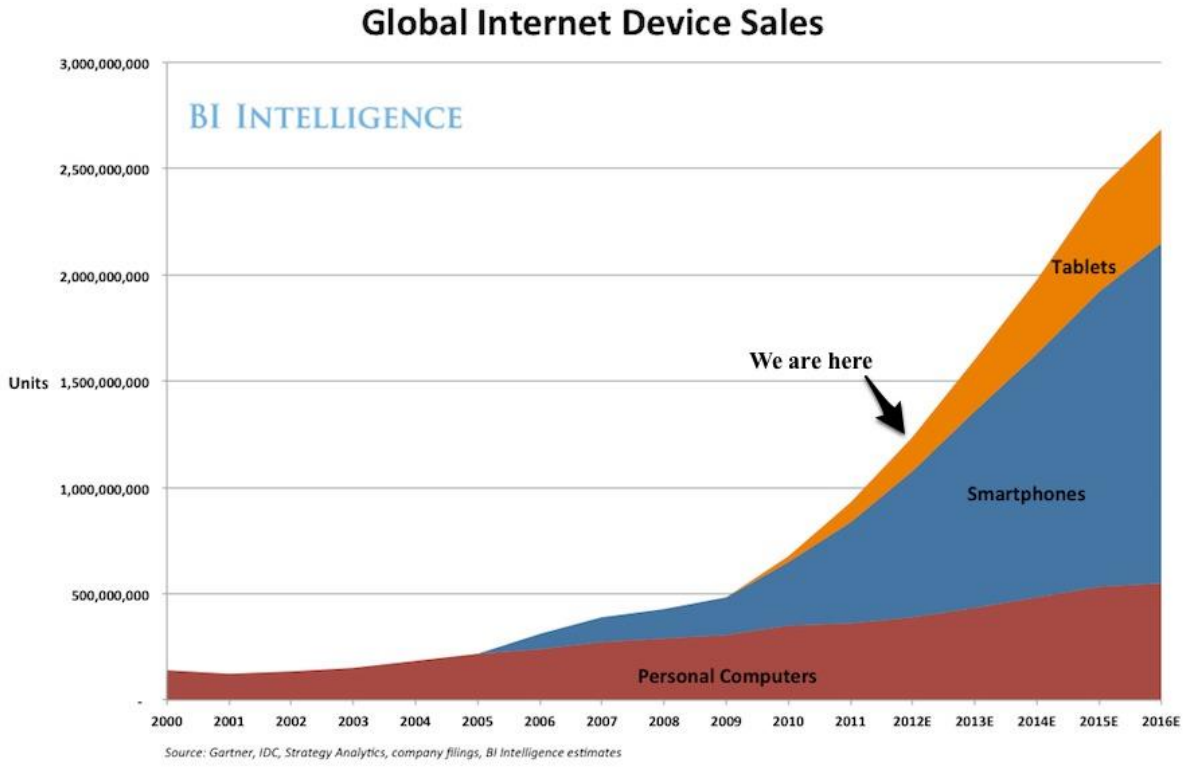
De mobiele technologie brengt in toenemende mate vrijheid met zich mee. Men is vrij om te communiceren waarvandaan hij of zij dat zelf wil. Het brengt tevens een sociale verandering met zich mee. Zo is het mogelijk geworden om thuis te werken in plaats van op kantoor, apparatuur kan meegenomen worden uit het werk mee naar huis.

[72] Centraal Bureau voor de Statistiek (2012). p.3.

Daarnaast gaat men communiceren via social media (internet en telefonie) en zal de persoonlijke interactie minder worden.[73]

Door de ontwikkeling van de mobiele techniek, ontstaan er ook nieuwe vormen van mobiele apparatuur. Mobiele apparatuur kent sinds 2005 een grote sprong voorwaarts als het gaat om de connectiviteit met het internet. Onder mobiele apparatuur vallen onder andere notebooks, netbooks, smartphones, tablets, personal computers (PC), PDA's, spelcomputers en E-readers.

De verkoop van dergelijk apparatuur neemt sinds 2005 steeds meer toe.



Figuur 2. Wereldwijde verkoop van internetapparatuur.[74]

In figuur 2 is te zien hoe de verkoop van smartphones en tablets is gestegen ten opzichte van 2000. Wat opvalt is dat de verkoop van de Personal Computers, waaronder statische computers en notebooks/netbooks, sinds 2002 aanzienlijk lager is dan de verkoop van smartphones en tablets (mobiele apparatuur met toegang tot mobiel internet). Dit zijn echter slechts twee van de nieuwe ontwikkelingen in de categorie mobiele apparatuur.

Desalniettemin geeft dit figuur aan dat de toename van mobiele apparatuur significant is. Ervan uitgaande dat onder de mobiele apparatuur alleen de smartphones en tablets vallen, zijn er in 2013 naar schatting zo'n anderhalf miljard mobiele apparaten verkocht. In 2002 waren deze mobiele

[73] Australian Government (2006). p.2.

[74] Deze grafiek loopt slechts tot 2012. De jaren die daarna zijn weergegeven zijn op basis van verwachting. Zie: UX Magazine (2012).

apparaten nog niet beschikbaar.
Door de toenemende groei van mobiele apparatuur, wordt ook het internet steeds toegankelijker.

Bij de positionering van de mobiele techniek in het digitale domein is een onderscheid tussen mobiele techniek, mobiele apparatuur en mobiel internet nodig. De mobiele techniek valt in de fysieke laag. Het is de hardware dat het mogelijk maakt dat apparatuur klein en draagbaar is. Deze mobiele apparatuur kan vervolgens in alle drie de lagen worden ondergebracht. Zo is de apparatuur zelf hardware. Deze hardware wordt echter pas bruikbaar wanneer software geïnstalleerd is. Deze software valt vervolgens in de virtuele laag. Doordat de apparatuur bruikbaar is door software en draagbaar is door de techniek kunnen mensen het gebruiken op verschillende plekken. Dit zorgt ervoor dat deze mobiele apparatuur ook zijn weerslag kent in de sociale laag. Vanaf deze mobiele apparatuur kunnen mensen, mits zij verbinding met het internet hebben, hun cyber persona component gebruiken om bijvoorbeeld hun email te bekijken. Het mobiele internet valt zowel in de fysieke laag als de virtuele laag. De hardware dat benodigd is om het mobiele internet mogelijk te maken valt in de fysieke laag. Het gaat hierbij om zendmasten en de ontvangers in apparatuur. Het mobiele internet zelf valt in de virtuele laag doordat het een digitale verbinding betreft.
Al deze technologieën maken het mogelijk om vrij te kunnen bewegen en tegelijkertijd de mogelijkheid te behouden om verbonden te zijn met het internet.

3.1.1.3 Quantum

De NSA heeft sinds 2008 gebruik gemaakt van een nieuwe technologie waarbij computers kunnen worden benaderd door middel van radiofrequenties. Met behulp van deze technologie is de NSA in staat om computers en netwerken binnen te dringen en data te verzamelen en te veranderen zonder dat deze systemen zijn verbonden met het internet. Deze techniek heeft de codenaam Quantum en maakt gebruik van covert radiokanalen waarbij radio signalen ongemerkt kunnen worden verzonden door kleine printplaten en USB-sticks die heimelijk in computers zijn geplaatst. Het is tot nu toe succesvol gebruikt om software in Russische militaire netwerken en systemen te implementeren en in die van de Mexicaanse politie en drugskartels.
Wat deze technologie zo bijzonder maakt is de mate van verfijndheid van de inlichtingenorganisatie om via geluid binnen te dringen in losstaande computernetwerken die voordien onbereikbaar waren.[75] Deze printplaten en USB-sticks vallen onder de fysieke laag van het digitale domein. Het doel van deze technologie is om gegevens van bijvoorbeeld de sociale laag heimelijk te verkrijgen.

[75] The New York Times (2014).

3.1.1.4 Super computing

Supercomputers, ook wel High Performance Computing (HPC) genoemd, maakt het mogelijk gigantische hoeveelheden data te analyseren. Dergelijke computers zijn duizenden keren sneller in het uitvoeren van berekeningen, dan laptops. Sinds 2002 is de snelheid van deze computer aanzienlijk gegroeid, door de technologische vooruit op het gebied van ICT.

HPC's voeren berekeningen parallel aan elkaar uit, wat het mogelijk maakt om veelvuldige berekeningen tegelijkertijd uit te voeren. Geschat wordt dat in 2020 de capaciteit van de HPC 50 keer zo groot zal zijn in vergelijking met de snelste HPC in 2013.[76]

Deze technologie valt in het digitale domein in de fysieke laag en wordt bruikbaar door de software die de HPC gebruikt en valt daarom ook in de virtuele laag.

3.1.2 Virtuele ontwikkelingen

Cloud computing, social media, PRISM en Xkeyscore zijn vier virtuele ontwikkelingen die door middel van bovenstaande nieuwe technologieën zijn ontstaan. De MIVD heeft en zal in de toekomst met deze ontwikkelingen te maken krijgen. In deze paragraaf zal beschreven worden wat deze begrippen inhouden en waarom deze van belang zijn.

3.1.2.1 Cloud computing

Datacentra zijn niet per definitie een nieuwe ontwikkeling sinds de inwerkingtreding van de WIV 2002, maar zijn wel noemenswaardig binnen deze context. Datacentra zijn gebouwen met technische installaties en IT-apparatuur die zorgen voor de verwerking, opslag en transport van gegevens via het internet. Datacentra zijn onderling verbonden door middel van glasvezelverbindingen. Ook zijn zij verbonden aan andere kantoor- en productielocaties.[77] Alle data die gegenereerd worden en vervolgens online worden opgeslagen komen in een van de datacentra terecht. Het opslaan van deze gegevens in een datacenter wordt ook wel 'cloud computing' genoemd. Het is een virtuele ontwikkeling die ontstaan is door onder andere glasvezelkabels. Door de toegenomen capaciteit van internetverbindingen, de groei van mobiel internet en mobiele apparatuur met toegang tot dit mobiele netwerk is het mogelijk om cloud computing te bewerkstelligen.[78]

Tot data die worden verzonden via cloud computing, behoren bijvoorbeeld ook alle data van websites, zoals Youtube en Facebook.[79]

Cloud computing is een virtuele ontwikkeling waar de sociale laag gebruik van maakt. Zo worden emailadressen en andere cyber persona componenten opgeslagen in clouds. Dit maakt het mogelijk

[76] European Commission (2013).
[77] Compact (2011). p.1.
[78] Compact (2011). p.3.
[79] The future of the data center (2013).

om vanaf bijna ieder apparaat dat verbonden is met internet, gegevens te uploaden, te bewerken en te downloaden. Het thuiswerken is hier een voorbeeld van waarbij gegevens van een bedrijf vanaf thuis kunnen worden benaderd.

3.1.2.2 Social media

Een belangrijke ontwikkeling in de virtuele laag van het digitale domein is de opkomst van social media. Het is een verzameling van alle internet-toepassingen en wordt ondersteund door nieuwe technologieën. Door social media is het eenvoudig om snel informatie met anderen te delen. De vorm van informatie die gedeeld wordt moet gezien worden in de breedste zin van het woord.
Het betreft namelijk niet alleen tekst, maar ook geluid en video. De meest bekende voorbeelden van internationale social mediasites zijn Wikipedia (2001), Wordpress (2003), Linkedin (2003), Myspace (2003), Facebook (2004), Youtube (2005), Twitter (2006) en Instagram (2010).[80] Een enorm aantal mensen maakt gebruik van deze sites en uploadt zelf nieuwe gegevens. Youtube heeft bijvoorbeeld iedere maand 800 miljoen unieke bezoekers. Twitter heeft meer dan 300 miljoen accounts. Facebook gaat daar zelfs overheen met meer dan 1 miljard leden.

Het bijzondere van deze social media is dat bijna ieder account te linken is aan dat van een ander, doordat ze elkaar hebben aangemerkt als familie of vriend. Daarnaast zijn de verschillende social media platformen ook weer te linken. Dit zorgt ervoor dat zelfs een enkele gebruiker (individu) het middelpunt wordt van een enorm aantal hubs en verbindingen. Social media bevindt zich in alle lagen van het digitale domein. Het maakt gebruik van de fysieke verbindingen, zoals datacentra en het creëert nieuwe cyber persona componenten door de programmatuur in de virtuele laag.

3.1.2.3 PRISM

Op 6 juni 2013 kwam het programma Planning tool for Resource Intergration, Synchronization and Management (PRISM) aan het licht. Edward Snowden, een systeembeheerder die voor de Amerikaanse National Security Agency (NSA) werkte, speelde top secret gerubriceerde PowerPointpresentaties door naar *The Guardian* en *The Washington Post*.[81]
Sinds 2007 is het programma PRISM door de NSA in gebruik genomen.[82] PRISM is een programma dat onder andere samenhangt met cloud computing en social media.

[80] Social-Media (z.d.).
[81] Spiegel Online International (2013).
[82] The Washington Post (2013).

Doordat bedrijven en individuen online gegevens opslaan en communiceren via internet, is de NSA in staat om door middel van PRISM, via ongerichte kabelgebonden interceptie, inlichtingen te verzamelen over deze binnen- en buitenlandse bedrijven en individuen.[83] Dit programma wordt ondersteund in het opslaan van de enorme hoeveelheden verzamelde inlichtingen, door superopslag (veel opslagruimte), supercomputers (met extreem hoge verwerkingscapaciteit en rekenvermogen) en decryptiesoftware.

Een maand nadat Edward Snowden top secret publicaties doorspeelde, verklaarde de NSA dat er naast het onthulde PRISM-programma nog twee versies van hetzelfde programma zijn. Deze programma's lijken veel op elkaar, maar zijn allemaal niet verbonden met elkaar. Één van deze programma's is ingezet voor gebruik binnen de NSA zelf, een ander is gebruikt door het Pentagon tijdens de missie in Afganistan.[84] Wat de programma's verder daadwerkelijk inhouden is niet bekend.

Het PRISM programma zelf is softwarematig van aard en behoort dus in de virtuele laag. Het wordt echter mogelijk gemaakt door componenten uit de fysieke laag en de gegevens uit de sociale laag.

3.1.2.4 Xkeyscore

Naast het door E. Snowden onthulde PRISM programma, gebruikt de NSA ook een ander programma genaamd Xkeyscore. Xkeyscore is de NSA's meest toereikende systeem dat inlichtingen verzameld uit computernetwerken. Dit wordt door de NSA het Digital Network Intelligence (DNI) genoemd. DNI zou mogelijk alles kunnen bekijken wat een standaard internet gebruiker doet op het internet. Hieronder vallen onder andere de inhoud van een email, het gebruikte IP adres en de bezochte websites. Met behulp van Xkeyscore en andere programma's kunnen analisten real-time interceptie uitvoeren tijdens het internetgebruik van een individu.[85]

Deze techniek maakt gebruik van de verschillende lagen van het digitale domein. De essentie van het programma bevindt zich echter, net als bij PRISM, in de virtuele laag. Xkeyscore is een software applicatie dat gebruikt maakt van de hardware uit de fysieke laag en gegevens uit de sociale laag.

Al deze ontwikkelingen in de verschillende lagen van het digitale domein waren niet voorzien in de WIV 2002. De vraag die nu ontstaat is welke voordelen deze technologieën kunnen leveren voor digitale inlichtingenverzameling.

[83] NRC handelsblad (2014).
[84] Spiegel Online International (2013).
[85] The Guardian (2013).

3.2 Gevolgen van de ontwikkelingen

Wanneer men kijkt naar de periode na de inwerkingtreding van de WIV 2002 valt op dat de revolutie in ICT het mogelijk heeft gemaakt om grote hoeveelheden data op te slaan, in enkele seconden te versturen naar de andere kant van de wereld, te verwerken en in toenemende mate te vercijferen. Dit schept talrijke nieuwe opties voor de samenleving. Al deze ontwikkelingen zijn in een sneltreinvaart gekomen in de afgelopen jaren. De impact die dit heeft, op het gebied van veiligheid door de toenemende interconnectiviteit, is ook gegroeid.

Door onder andere gegevensopslag in clouds, social media en het veelvuldig gebruik van mobiele apparatuur is in de samenleving een aantal gevolgen te zien. Er ontstaat bijvoorbeeld een andere manier van communicatie tussen mensen en bedrijven. Ook is de mogelijkheid ontstaan voor mensen om vanaf thuis te werken in plaats van op de werkplek zelf. Door de vele manieren, snelheid en capaciteit van het verzenden van informatie, gaat veel communicatie in deze tijd via het digitale domein. Hierdoor verandert ook de sociale interactie. Aangezien deze interactie nu ook veelal via het digitale domein plaatsvindt.

De digitalisering van communicatie en informatieverwerking zal zich blijven doorzetten. Ook zal de groei van datacentra en communicatienetwerken blijven toenemen deze eeuw. Kabelnetwerken vormen, zoals gezegd, de spil van de Nederlandse elektronische samenleving en ook die van de rest van de wereld.[86] Daarnaast zal het communicatieverkeer steeds meer, en in verschillende samenstelling, afwisselend door de ether en kabelnetwerken worden gevoerd.[87] De gevolgen van de ontwikkelingen op het gebied van informatie en communicatie gaan voor overheden, samenlevingen en individuele burgers in de toekomst leiden tot steeds grotere afhankelijkheid van de digitale snelweg. Het gaat kansen bieden, maar ook uitdagingen, bijvoorbeeld op het gebied van privacy.

[86] Ministerie van Defensie (2013c).
[87] Dessens, C.W.M. (2013). p.71.

3.3 Kansen voor de MIVD

Nederland wordt tegenwoordig geconfronteerd met vele, nieuwe vraagstukken betreffende de nationale veiligheid. Deze vraagstukken waren niet voorzien door de wetgever bij de vaststelling van de WIV 2002. Onder deze vraagstukken vallen de nieuwe technologieën die zijn behandeld in paragraaf 3.1. De ontwikkelingen van nieuwe technieken in het digitale domein bieden nieuwe mogelijkheden voor het verzamelen van inlichtingen. Dit heeft er toe geleid dat er opnieuw aandacht is gekomen voor de noodzaak om nieuwe communicatiemiddelen te kunnen intercepteren door de veiligheidsdienst.[88] Naar aanleiding van de beschreven technologieën en gevolgen hiervan, is de vraag gekomen wat deze technologieën voor kansen bieden voor de MIVD. Om deze vraag te beantwoorden zullen de beschreven technologieën naast de taken van de MIVD gelegd worden.

3.3.1 Glasvezeltechniek

Sinds eind jaren 90 is het data- en communicatieverkeer steeds meer van technische vorm veranderd. De wijziging betreft de verschuiving van ether en satelliet naar glasvezelkabelnetwerken. De interceptiebepalingen, zoals opgesteld in artikel 24 t/m 27 van de WIV 2002, zijn gebaseerd op de situatie die zich twaalf jaar geleden voordeed. De wetgever had niet voorzien dat de technologie zich dusdanig zou ontwikkelen dat een dergelijke verschuiving zou plaatsvinden. Ongerichte interceptie was alleen gericht op niet-kabelgebonden communicatie.[89]

Door de intreding van glasvezelnetwerken en de ontwikkelingen op het gebied van dataverkeer en communicatie is de relevantie van kabelgebonden interceptie gegroeid. Zo gaat 80 tot 90 procent van de telecommunicatie nu via glasvezelnetwerken, waar deze voorheen via satelliet ging. De taak van de MIVD is het waarborgen van de nationale veiligheid. Voor de MIVD geeft deze nieuwe technologie de kans om grote hoeveelheden data te onderscheppen. Aangezien er een enorme capaciteit aan data verzonden kan worden via dit medium. Deze technologie, de hoeveelheid mogelijk te onderscheppen data en de verschuiving van telecommunicatie maken ongerichte kabelgebonden interceptie interessant.

Door de enorme capaciteit van glasvezelnetwerken is cloud computing relevant geworden. De snelheid waarmee bestanden online kunnen worden opgeslagen of gedownload, heeft ervoor gezorgd dat men niet meer gebonden is aan een computer of systeem waarop bestanden zijn opgeslagen. Deze ontwikkeling zorgt ervoor dat er meer digitaal verkeer is en hierdoor mogelijk meer kans op interceptie.

[88] Dessens, C.W.M. (2013). p.9.
[89] Dessens, C.W.M. (2013). p.76.

De voordelen die ongerichte kabelgebonden interceptie voor inlichtingenverzameling met zich mee brengen zijn een verbeterde mogelijkheid tot Computer Network Exploitation (CNE) en VoIP.
Via VoIP worden live gesprekssstromen gestreamd via het internet. In samenwerking met ongerichte kabelgebonden interceptie zouden grote aantallen van dergelijke gesprekken kunnen worden opgenomen.

CNE zorgt voor exploitatie van informatie, de officiële definitie van CNE volgens U.S. Department of Defense luidt:

> *"Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks"*[90]

Deze exploitatie van de informatie, afkomstig van een doel, gaat een grotere betekenis krijgen wanneer er ongericht mag worden geïntercepteerd op de kabel. Doordat ongericht kabelgebonden interceptie kan worden uitgevoerd is de hoeveelheid informatie die wordt ontvangen vele malen groter. De mogelijkheid om vervolgens deze informatie te selecteren en te benutten neemt hiermee ook toe. CNE geeft aan dat zodra er meer mogelijkheden komen om inlichtingen te verzamelen, de mogelijkheid om data of informatie, afkomstig van het doel, uit te buiten voor eigen doeleinden zal groeien.[91]
Een ander voordeel van ongerichte kabelgebonden interceptie via glasvezelkabels ontstaat de mogelijkheid voor het toepassen van programma's, zoals de door de NSA gebruikte PRISM.
Verder zou de MIVD een voordeel kunnen halen uit deze kabelgebonden interceptie aangezien Nederland beschikt over AMS IX, een internationaal internetknooppunt. Op die manier kunnen zowel binnen- en buitenlands dataverkeer worden onderschept vanuit Nederland.

3.3.2 Mobiele techniek

Mobiele apparatuur, zoals mobieltjes en tablets die gebruik maken van mobiel internet, zorgt ervoor dat de mogelijkheid tot het verzamelen van inlichtingen groter wordt. Door de stijging in gebruik van het aantal smartphones en tablets, en daarmee samenhangend de toename van mobiel internet, neemt de hoeveelheid data via de ether en satelliet toe. Het gebruik van mobiel internet gaat ook via kabelnetwerken. In de praktijk gaat telecommunicatie zowel via de kabel als door de lucht.[92]

[90] Joint Publication 1-02 (2010). p.73.
[91] Andress, J. Winterfeld, S. (2014). p.169.
[92] AIVD & Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (z.d.b).

Wanneer iemand bijvoorbeeld met zijn mobiele telefoon of tablet informatie via internet verstuurt, gaat die eerst via de lucht naar een zendmast of thuis via de wifi-router. Vanaf hier gaat de informatie via (glasvezel)kabels naar bijvoorbeeld AMS-IX, waarna de informatie wordt opgeslagen in een datacenter in de Verenigde Staten. In de relatief korte afstand tussen mobiel en zendmast is de MIVD in staat het dataverkeer te ontvangen.
Om echter een betere dekking te hebben om inlichtingen te verzamelen over meer plekken zou een internettap een kans bieden voor de MIVD, omdat al dit dataverkeer uiteindelijk weer via kabelnetwerken zal gaan lopen.[93]

Het gebruik van mobiele apparatuur die verbonden is met het internet zorgt er samen met social media voor dat enorme aantallen verbindingen mogelijk zijn. De interconnectiviteit van social media zorgt voor een enorme hoeveelheid connecties tussen verschillende cyber persona componenten die zijn opgeslagen in datacentra. Zo kunnen Facebook- en Twitteraccounts aan elkaar gekoppeld worden. Ook het plaatsen van berichten op social mediasites gaat via het internet, zowel door de lucht als door de kabel, naar deze datacentra. Deze verbindingen tussen verschillende cyber persona componenten bieden de mogelijkheid om een beter inzicht te krijgen in bijvoorbeeld leden van organisaties en overige connecties. De ontwikkeling van social media netwerken biedt op dit moment voor de MIVD de mogelijkheid om gericht via social media sites binnen te dringen in voor hun relevante netwerken van personen en groepen.
Naast social media heeft de mobiele techniek onder andere ook geleid tot het ontstaan van cloud computing. De snelheid van het mobiele internet is dusdanig snel geworden dat de opslag van data in clouds, via mobiele apparatuur, mogelijk is geworden.
Data ontvangen via het programma PRISM van de NSA biedt voor de MIVD de mogelijkheid om ongericht kabelgebonden data, die worden verstuurd via de social media sites, op te nemen.

Een kans die mobiele techniek de MIVD ook biedt is de mogelijkheid om specifieke personen, groepen en/of staten intensief te volgen. Doordat er veelvuldig gebruik wordt gemaakt van mobiele apparatuur met toegang tot het mobiele internet, is er meer kans op het onderscheppen van inlichtingen.

3.3.3 Quantum

Een andere ontwikkeling die gebaseerd is op mobiele techniek is het Quantum-project van de NSA, waarbij fysieke opnamen- en zendapparatuur worden aangebracht in losstaande systemen. Voor de MIVD zou deze ontwikkeling van toegevoegde waarde kunnen zijn bij het verzamelen van

[93] Kamerstukken II, 2011/12, 30 517, nr.25.

inlichtingen uit fysiek losstaande netwerken en systemen. Het is een technologie die nog verder ontwikkeld kan worden. Voor de MIVD biedt dit een mogelijkheid om hier onderzoek naar te verrichten en eventuele verbeteringen toe te voegen.

3.3.4 Super computing

Door de komst van glasvezelkabels, mobiele techniek en cloud computing is de hoeveelheid digitaal verkeer enorm toegenomen. Als gevolg hiervan is de kans voor de MIVD om inlichtingen te verzamelen eveneens gegroeid. Supercomputers bieden een kans voor de MIVD als er ingezet wordt op kabelgebonden interceptie. De enorme snelheid en hoeveelheid berekeningen die een HPC kan maken zijn benodigd om de opgenomen informatie bruikbaar te maken. Ten behoeve hiervan worden analyses uitgevoerd.

3.4 Subconclusie

In dit hoofdstuk is gekeken naar de vraag:

Welke technologieën, op het gebied van digitale inlichtingenverzameling, zijn beschikbaar sinds het opstellen van de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002 en wat betekent dit voor het verzamelen van inlichtingen voor de MIVD?

Ter beantwoording van deze vraag is dit hoofdstuk in verschillende onderdelen verdeeld. Allereerst is er gekeken naar de technologieën die beschikbaar zijn geworden sinds de invoering van de WIV 2002. De ontwikkelingen die zijn behandeld in deze thesis zijn:

De komst van de glasvezelkabels, de opkomst van mobiele apparatuur die aangesloten is op mobiel internet en het door de NSA ontwikkelde Quantum-project en Xkeyscore programma.

Naar aanleiding van het beschikbaar komen van deze nieuwe technologieën zijn er ook andere ontwikkelingen ontstaan. Bijvoorbeeld het begrip social media, PRISM en cloud computing.
Om antwoord te kunnen geven op de deelvraag van dit hoofdstuk zijn de nieuwe technologieën naast de taken van de MIVD gelegd. Om zo te kijken in hoeverre zij de MIVD kansen bieden voor een nog adequatere manier van inlichtingen verzamelen.

Er kan gezegd worden dat de ontwikkeling van nieuwe technologieën de huidige samenleving als geheel in verbinding heeft gebracht met het internet. Met de komst van het internet zijn nieuwe kansen gecreëerd. De technologieën die de afgelopen jaren zijn ontwikkeld zorgen ook voor meer verbondenheid. Social media draagt hieraan bij met het aantal accounts en de onderlinge verbondenheid tussen de sociale media netwerken. Door de komst van glasvezelnetwerken is de hoeveelheid data gigantisch toegenomen. Ook is het mogelijk om, via de hoge snelheden die glasvezelnetwerken mogelijk maken, steeds meer informatie razendsnel beschikbaar te stellen of te verkrijgen. Deze datastromen zijn sinds 2007 opgevangen door het computerprogramma PRISM om informatie in te winnen.

De belangrijkste kansen die de nieuwe technologieën bieden voor de MIVD en die onderkend zijn in dit hoofdstuk zijn:

- Mogelijkheid tot ongericht kabelgebonden interceptie, door de verschuiving van telecommunicatie, snelheid en capaciteit van glasvezelskabels.
- Social media biedt voor de MIVD de kans om gemakkelijker onderlinge relaties bloot te leggen, waar mogelijk zelfs zonder diepgaand onderzoek.
- Mobiele techniek biedt de MIVD de mogelijkheid tot het ontwikkelen van nieuwe verfijnde technische hulpmiddelen.
- Mobiele techniek biedt de MIVD ook de mogelijkheid tot het intensiever volgen van personen, groepen en staten.
- Cloud computing biedt de MIVD meer kans op interceptie, wanneer er wordt ingezet op ongericht kabelgebonden interceptie. Door het toenemende aantal verbindingen en verkeer zal hierdoor de kans op interceptie worden vergroot.
- Supercomputers biedt de MIVD vervolgens de mogelijkheid om analyses uit te kunnen voeren op de ontvangen informatie door kabelgebonden interceptie.
- Het Quatum project van de NSA biedt de MIVD mogelijkheid om systemen en netwerken te benaderen die niet verbonden zijn met het internet.

Er zijn verschillende kansen die deze technologieën met zich mee brengen voor de MIVD. Echter moeten deze kansen ook mogelijk zijn binnen de huidige wetgeving en moet er behoefte zijn voor aanpassing binnen de MIVD zelf.

4. Nieuwe behoeftes voor digitale inlichtingenverzameling

In hoofdstuk drie is in gegaan op de technologische ontwikkelingen die hebben plaatsgevonden sinds de inwerkingtreding van de WIV 2002. Deze ontwikkelingen zijn gebeurd in een tijdsspan van twaalf jaar. In die periode is ook een groeiend interesse ontstaan voor het digitale domein. De krijgsmacht wil dit domein en de daarbij komende digitale technologieën optimaal kunnen benutten. Defensie is al bezig met een actieve deelname in het digitale domein, maar heeft de MIVD behoefte om meer mogelijkheden te hebben binnen dit domein?

Om hier een antwoord op te kunnen geven staat in dit hoofdstuk dan ook de volgende vraag centraal:

Welke behoeftes zijn er voor de Militaire Inlichtingen- en Veiligheidsdienst op het gebied van digitale inlichtingenverzameling, waar zij momenteel niet bevoegd toe zijn, gelet op de taakstelling in de Wet voor de Inlichtingen- en Veiligheidsdiensten uit 2002?

Om deze vraag te beantwoorden is net als in de voorgaande hoofdstukken het hoofdstuk opgedeeld in verschillende onderdelen. Als eerste zullen de dreigingen en kwetsbaarheden die de MIVD in de nabije toekomst mogelijk zal ondervinden binnen en vanuit het digitale domein behandeld worden. Vervolgens zal de politieke visie over de MIVD in het digitale domein worden behandeld, hierbij zullen de Commissie-Dessens en de CTIVD betrokken worden. Er zal hierbij worden ingegaan op de digitale inlichtingenverzamelcapaciteiten. Als laatste zal er worden afgesloten met een subconclusie.

4.1 Dreigingen en kwetsbaarheden

Vanuit de fysieke wereld komen dreigingen door bijvoorbeeld de wapens die tegenstanders tot hun beschikking hebben. Daarnaast komen ook dreigingen vanuit het digitale domein. Deze worden mede veroorzaakt door nieuwe ontwikkelingen wat betreft de technologie, zoals beschreven in het voorgaande hoofdstuk. Om een beeld te krijgen met welke dreigingen de MIVD te maken krijgt, zullen deze uiteengezet worden in deze paragraaf.

De dreigingen die voortkomen vanuit het digitale domein kunnen worden onderverdeeld in drie categorieën: informatie-gerelateerde dreigingen, systeem-gerelateerde dreigingen en indirecte dreigingen. Deze dreigingen kunnen worden veroorzaakt door verschillende actoren; zoals staten, terroristen, organisaties, criminelen, hacktivisten en scriptkiddies. Deze actoren richten hun activiteiten tegen potentiele doelwitten, zoals private organisaties, burgers en staten.[94]

- Informatie-gerelateerde dreigingen ontstaan wanneer bedreigende groepen, zoals hierboven beschreven, de intentie hebben om informatie te stelen, te bewerken of te misbruiken.
- Systeem-gerelateerde dreigingen zijn gericht op het verstoren of onderbreken van dienstverlening en bedrijfsvoering van een organisatie.
- De indirecte dreiging vanuit het digitale domein omvat alle neveneffecten die worden veroorzaakt vanuit de andere twee categorieën. Het gaat hier om de besmetting van systemen door malware die gebruikt wordt door de dreigende groepen.[95]

Al deze dreigingen vinden plaats bij defensie, maar zeker ook in de civiele maatschappij. Het aantal digitale dreigingen door uiteenlopende incidenten wordt steeds duidelijker zichtbaar. Het gaat hierbij niet alleen om de dreiging tegen de digitale infrastructuur, maar ook ten aanzien van de informatie die digitaal wordt opgeslagen en verwerkt van individueel niveau tot aan bedrijfsniveau.[96]

De nationale veiligheid wordt op het moment het meest bedreigd door staten, terroristen, beroepscriminelen en, in mindere mate, door scriptkiddies en hacktivisten. Hierbij zijn staten en terroristen vanuit operationeel oogpunt het meest relevant voor de MIVD.

[94] Ministerie van Veiligheid en Justitie (2011). p.3
[95] Ministerie van Veiligheid en Justitie (2011). p.4-6.
[96] Ministerie van Veiligheid en Justitie (2012). p.23-30.

4.1.1 Dreiging vanuit staten

De dreiging die andere staten vormen voor Nederland bestaat uit digitale spionage (informatie-gerelateerde dreiging) of offensieve digitale aanvallen (systeem-gerelateerde dreiging). De attributie van dergelijke operaties is zeer moeilijk. Wanneer een staat een niet-statelijke actor inzet kan de attributie mogelijk helemaal worden voorkomen.[97]

Door de inzet van offensieve cybercapaciteiten door staten of door staten gerelateerde actoren kan een verstoring van de ICT in Nederland plaatsvinden. Volgens de defensie cyber strategie gaat het hier om;

"capaciteiten die tot doel hebben het handelen van de tegenstander te beïnvloeden of onmogelijk te maken."[98]

Uit onderzoek van de Nederlandse inlichtingendiensten blijkt dat spionageactiviteiten, die uitgevoerd worden door staten, vooral gericht zijn op de overheidsinstanties, non-gouvernementele organisaties, het bedrijfsleven, de wetenschap en dissidenten- en oppositionele groeperingen. Deze dreigingen worden ook wel Advanced Persistent Threat (APT) genoemd.[99]

Staten die investeren in offensieve cybercapaciteiten kunnen deze capaciteiten inzetten tijdens internationale conflicten. Deze aanvallen zullen voornamelijk gericht zijn op propaganda, spionage observatie, manipulatie, sabotage of disruptie, verkenning, intimidatie van opposanten of gerichte aanvallen.[100] De MIVD heeft geconstateerd dat de defensie-industrie een gewild doelwit is voor spionageactiviteiten. Naast dat de defensie-industrie doelwit is van dergelijke activiteiten zijn ook de partijen die met hen samenwerken een doelwit.[101] De informatie die verkregen wordt bij spionageactiviteiten dient het belang van de vijandige staten. Ook heeft de MIVD bemerkt dat kwaadaardige phishingactitiviteiten worden ondernomen tegen Nederlandse militaire vertegenwoordigingen in het buitenland.[102]

[97] Blunden (2010). p.1-16.
[98] Ministerie van Defensie (2012). p.11.
[99] Ministerie van Veiligheid en Justitie (2013). p.21.
[100] Ministerie van Veiligheid en Justitie (2013). p.21.
[101] Data Protectors (z.d.).
[102] Ministerie van Veiligheid en Justitie (2013). p.25.

Diverse staten hebben de afgelopen jaren veel geld en tijd geïnvesteerd in de ontwikkeling en het bemachtigen van cybercapaciteiten. Deze staten beschikken daardoor nu over meer technologisch geavanceerde mogelijkheden om te opereren in het digitale domein. Hierdoor is het aannemelijk dat deze staten cyberactiviteiten uitvoeren waarvan Nederland geen enkele notie heeft. Op basis van de Nationale Cyber Security Strategie (NCSS) zijn er goede initiatieven en maatregelen getroffen om de weerbaarheid en bewustwording van deze cyberdreiging te vergroten.[103] De dreiging vanuit anderen staten, gericht tegen de Nederlandse overheid, wordt vergroot door tal van gevolgen vanuit nieuwe technologische ontwikkelingen. De toenemende rol van ICT in de samenleving brengt kwetsbaarheden met zich mee. ICT is de hoofdrol gaan spelen in onze huidige netwerksamenleving en is daardoor verantwoordelijk voor de interdependenties tussen talloze systemen, software, telecommunicatie, computers en tal van andere apparaten.[104] Dit maakt ICT gevoelig voor storingen die mogelijk veroorzaakt kunnen zijn door staten, personen of organisaties met kwade bedoelingen.

Ook is de afgelopen jaren het aantal mobiele apparaten en de onderlinge verbondenheid hiervan enorm ontwikkeld en gegroeid. De hoeveelheid data in digitale vorm, die deze apparaten kunnen maken, neemt toe en wordt in toenemende mate in datacentra opgeslagen. Door de hoeveelheid aan opgeslagen data is de dreiging vergroot dat hier informatie uit wordt gehaald die van belang is voor de nationale veiligheid. Defensie zal zich moeten weren tegen de dreiging die uitgaat van staten en hun cybercapaciteiten.

4.1.2 Dreiging vanuit niet-statelijke actoren

Dreigingen kunnen naast staten ook vanuit niet-statelijke actoren voortkomen, zoals terroristen, (beroeps)criminelen, hacktivisten, cybervandalen, scriptkiddies, interne actoren en cyberonderzoekers. De dreigingen die van deze actoren uitgaan zijn uiteenlopend. Zo kan bijvoorbeeld diefstal, verkoop of publicatie plaatsvinden van vertrouwelijke informatie. Daarnaast kunnen deze actoren ook zorgen voor manipulatie van informatie of verstoring van de ICT. Deze handelingen vormen een dreiging voor de nationale veiligheid.[105]

Van de niet-statelijke actoren blijft de grootste dreiging uitgaan van de beroepscriminelen. In 2013 uitte zich dat in diefstal door onlinetransacties en financiële fraude. Daarnaast maakten zij zich veelvuldig schuldig aan digitale inbraak om gegevens te stelen voor criminele doeleinden.[106]

[103] Ministerie van Veiligheid en Justitie (2013a). p.15.
[104] Kamerstukken II 2013/14, 26 643, nr.298, p.3.
[105] Ministerie van Veiligheid en Justitie (2013). p.9.
[106] Ministerie van Veiligheid en Justitie (2013). p.25.

4.1.3 Kwetsbaarheden vanuit het digitale domein

Een kwetsbaarheid van ICT is een beperking voor de beschikbaarheid en betrouwbaarheid van ICT. Deze kwetsbaarheid kan worden veroorzaakt door misbruik. Informatie die opgeslagen is kan hierdoor beschadigd worden. Dit kan ook optreden als gevolg van technisch of menselijk falen.[107]

Het toenemende aantal ICT-apparaten die verbonden zijn met het internet, zoals routers, televisies en webcams, zorgt voor een vergroot risico. De standaardbeveiliging op dergelijke apparatuur is vaak onvoldoende. Hierdoor zijn deze apparaten gevoelig voor digitale spionageactiviteiten.[108]

De risico's van cloud computing zijn aanzienlijk. Zo is de toegang tot deze diensten niet altijd even goed beveiligd en zijn de algemene voorwaarden tot het gebruik van deze diensten uiteenlopend. Zo kunnen enkele cloud-dienstverlenende bedrijven (persoonlijke) informatie inzien die op hun cloud-servers zijn opgeslagen, wanneer er overeenstemming is geweest met de algemene gebruikersvoorwaarden.[109]

Het gebruik van social media zorgt voor het risico dat kwaadwillenden de persoonlijke gegevens van mensen, van bijvoorbeeld een specifiek bedrijf, kunnen gebruiken om gericht digitale aanvallen uit te voeren om zo gegevens te verzamelen.[110]

De voordelen die gebruikers ervaren uit dergelijke ICT apparatuur gaat vaak gepaard met een onbekendheid over de digitale kwetsbaarheid.

[107] Ministerie van Veiligheid en Justitie (2013). p.31.
[108] Ministerie van Veiligheid en Justitie (2013). p.31.
[109] Justitia.nl (z.d.).
[110] Ministerie van Veiligheid en Justitie (2013). p.33.

4.2 Denkwijze over digitale dreiging

De aandacht van security experts is de afgelopen jaren verschoven van preventie naar detectie. In de praktijk is gebleken dat digitale aanvallen niet tegen te houden zijn en in de toekomst ook zullen blijven plaatsvinden. Hierdoor is de focus komen te liggen op detectie. Op deze manier kunnen aanvallen in kaart worden gebracht. Dit is van groot belang wanneer een adequate reactie gewenst is.[111]

Defensie zet ook in op het vergroten van detectie en het analyseren van cyberaanvallen en spionage. De voormalig minister van defensie, drs. J.S.J. Hillen, schreef in juni 2012 een brief naar de Tweede Kamer. Hierin presenteerde hij de Defensie Cyber Strategie. Deze strategie zou in de komende jaren richting en samenhang moeten geven aan de ontwikkeling van het militaire vermogen in het digitale domein. Daarnaast is het van belang dat de focus op een integrale aanpak voor de ontwikkeling van dit vermogen zal komen te liggen.[112]

De Defensie Cyber Strategie omvat zes speerpunten waarop defensie de komende jaren haar doelstellingen in het digitale domein zal gaan ontwikkelen. Zo wordt de digitale weerbaarheid versterkt (defensief), het militaire vermogen ontwikkeld om cyberoperaties uit te voeren (offensief), de cyberinlichtingencapaciteit vergroot en daarnaast wordt het adaptief en innovatief vermogen verbeterd. Ook wordt er geïnvesteerd in een intensieve samenwerking tussen onder andere de AIVD en de MIVD.[113] Deze speerpunten zijn opgesteld om de inzetbaarheid van de Nederlandse krijgsmacht te waarborgen en de effectiviteit, weerbaarheid en inlichtingenpositie te versterken.

Daarnaast is in 2012 Taskforce Cyber opgericht in het kader van cyberintensivering. Er is een uitbreiding gedaan van de capaciteit van het Defensie Cyber Emergency Response Team (DefCERT). Eind 2013 werd het Defensie Cyber Expertise Centrum (DCEC) opgericht.[114] De samenwerking tussen de AIVD en MIVD zal begin 2014 leiden tot de oprichting van de Joint Sigint Cyber Unit en de datum van intreding van het Defensie Cyber Commando is geschat op medio 2014.[115]

Al deze organen van de MIVD en/of de samenwerking tussen de MIVD en de AIVD hebben tot taak het onderzoeken van digitale aanvallen en spionage. In de Defensie Cyber Strategie wordt ook aangegeven dat de MIVD de komende jaren zijn digitale inlichtingen verwervingspositie zal gaan uitbreiden.

[111] Ministerie van Veiligheid en Justitie (2013). p.39.
[112] Kamerstukken II, 2011/12, 33 321, nr.1, p.1.
[113] Kamerstukken II, 2011/12, 33 321, nr.1, p.3.
[114] Rijksoverheid (2013).
[115] Kamerstukken II, 2013/14, 33 750X, nr.6. p.30.

Hieronder vallen de capaciteiten die te maken hebben met het infiltreren in geautomatiseerde werken, het in kaart brengen van de relevante delen van het digitale domein, het monitoren van vitale netwerken en als laatste, het verrichten van onderzoek naar de werking van digitale aanvalstechnieken.[116]

De minister van defensie, mevr. Hennis-Plasschaert, benadrukt wel dat de MIVD op dit moment, onder de huidige wetgeving, in staat is om de Commandant der Strijdkrachten en de minister zelf te voorzien van de noodzakelijke informatie. Daarnaast benadrukt de minister dat de MIVD in een veranderende wereld moet kunnen anticiperen en innoveren. Ten behoeve hiervan moet de MIVD beschikken over adequate mogelijkheden ten behoeve van zijn takenpakket.[117]

[116] Kamerstukken II, 2011/12, 33 321, nr.1, p.8.
[117] Kamerstukken II, 2012/13, 29 924, nr.100, p.14.

4.3 Standpunten van de toezicht- en onderzoekscommissie

Een goedwerkende en stabiele inlichtingenpositie is van belang voor de efficiëntie en effectiviteit van defensie in het digitale domein. Het verzamelen van inlichtingen op verschillende digitale wijzen in het digitale domein neemt toe in belang. Dit is onderkend door de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) en de Commissie-Dessens.

De CTIVD stelt in haar toezichtsrapport, over de inzet van Sigint door de MIVD, dat het onderscheid dat wordt gemaakt in de WIV 2002 tussen kabelgebonden en niet-kabelgebonden interceptie wat gedateerd aan doet. Zij onderkent dat het gebruik van glasvezelkabel bij internationale telecommunicatie enorm is toegenomen door de grote capaciteit van dit medium. Verder komt naar voren in het toezichtsrapport dat de MIVD graag wil dat ongerichte interceptie van kabelgebonden telecommunicatie toegevoegd zou worden aan de bijzondere bevoegden. De MIVD stelt dat de WIV 2002 voldoende bescherming biedt tegen de inbreuk van de privacy-rechten door de toepassing van de bijzondere bevoegdheden. De dienst ziet daarbij geen verschil tussen telecommunicatie via de satelliet of de kabel. De CTIVD laat zich echter niet uit over een nieuw juridische raamwerk dat benodigd is voor de toevoeging van deze bevoegdheid.[118]

In 2002 had de wetgever met de WIV 2002 voor ogen om een formeel wettelijke basis te leggen voor de bevoegdheden van de MIVD. Naast de technologische ontwikkelingen uit hoofdstuk twee hebben ook de gedachten over de uitleg van de wet en bevoegdheden van de MIVD de afgelopen jaren veranderingen doorgemaakt.[119] Op basis hiervan heeft de evaluatiecommissie-Dessens onderzocht of de WIV 2002 nog toereikend is om de hedendaagse dreigingen te weerstaan. In haar onderzoek wordt onder andere geconcludeerd dat de WIV 2002 in het digitale domein toe is aan modernisering.
De evaluatiecommissie stelt in haar onderzoek dat de WIV 2002 omtrent het interceptiebeleid, zoals beschreven in artikel 26 en 27, techniekafhankelijk is opgesteld. Door de technologische ontwikkelingen die zich hebben voorgedaan sinds 2002 en die in de toekomst zullen blijven plaatsvinden zijn deze artikelen echter achterhaald.[120]
Bij de uitoefening van de bijzondere bevoegdheden van de MIVD schiet de huidige interceptiebepaling mogelijk te kort bij de waarborging van de nationale veiligheid. De huidige interceptiebepaling is techniekafhankelijk en laat ongerichte kabelgebonden interceptie niet toe. De evaluatiecommissie is van mening dat ongerichte kabelgebonden interceptie moet worden toegestaan.

[118] CTIVD (2011). p.38.
[119] Dessens, C.W.M. (2013). p.168.
[120] Dessens, C.W.M. (2013). p.171.

Zij vindt dat het belang om kennis te nemen van communicatie leidend moet zijn en niet, zoals de huidige stand van zaken, het medium of techniek bepalend moet zijn. Het onderscheid dat nu gemaakt wordt tussen de ether en kabel, zoals verwerkt in de WIV 2002, kan niet worden gehandhaafd door de ontwikkelingen op het gebied van dataverkeer en communicatie. Tegelijkertijd moet er een wijziging en versteviging van de wettelijke waarborgen komen voor de toestemming en toezicht die verbonden zijn aan de nieuwe interceptiebepaling. [121]

De evaluatiecommissie stelt daarnaast een nieuwe tweedeling voor die de huidige artikelen 25 t/m 27 vervangt. De tweedeling zou gemaakt moeten worden tussen het type activiteit, gericht versus ongericht. Voor ongerichte interceptie activiteiten stelt zij daarbij voor dat een ministeriële toestemming vereist is en directe toezicht en toestemming benodigd is door de Commissie van Toezicht betreffende Inlichtingen- en Veiligheidsdiensten. Voor het huidige artikel 24 zou dezelfde toestemming en toezicht vereisten moeten gaan gelden.[122]

[121] Dessens, C.W.M. (2013). p.172.
[122] Dessens, C.W.M. (2013). p.172.

4.4 Subconclusie

In dit hoofdstuk is gekeken naar de vraag:

Welke behoeftes zijn er voor de Militaire Inlichtingen- en Veiligheidsdienst op het gebied van digitale inlichtingenverzameling, waar de dienst momenteel niet bevoegd toe is gelet op de taakstelling in de Wet voor de Inlichtingen- en Veiligheidsdiensten uit 2002?

Ter beantwoording van deze vraag is het hoofdstuk verdeeld in drie onderdelen.

Als eerste is gekeken of er dreigingen en kwetsbaarheden te onderkennen zijn in en vanuit het digitale domein. De dreigingen zijn onder te verdelen in:

- Informatie-gerelateerde dreigingen;
- systeem-gerelateerde dreigingen en
- indirecte dreigingen.

Deze dreigingen kunnen worden versterkt door de kwetsbaarheden die het toenemende aantal ICT apparaten met zich mee brengt.

Vervolgens is de denkwijze over de digitale dreigingen behandeld. Hierbij werd onderkend dat de denkwijze veranderd is van preventief optreden naar detecteren, omdat men denkt dat digitale aanvallen en spionageactiviteiten zich altijd zullen blijven voortdoen. Defensie gaat hier ook in mee door nieuwe organen op te richten en bestaande uit te breiden. Om zo haar taak, het in kaart brengen van de relevante delen van het digitale domein, het monitoren van vitale netwerken en als laatste, het verrichten van onderzoek naar de werking van digitale aanvalstechnieken, beter uit te kunnen voeren.

Als laatste is er gekeken naar de aanbevelingen die zijn gedaan door de CTIVD en de evaluatiecommissie-Dessens. Zij concluderen dat de MIVD behoefte heeft aan een nieuwe bijzondere bevoegdheid, ten behoeve van digitale inlichtingenverzameling. Het gaat hierbij om de bevoegdheid die het mogelijk maakt om kabelgebonden interceptie uit te voeren. De evaluatiecommissie geeft in haar rapport daarbij ook een mogelijke juridisch kader dat hier ten grondslag aan zou kunnen liggen.

Conclusie

In deze thesis is geprobeerd en antwoord te vinden op volgende onderzoeksvraag:

Zijn de beperkingen die de Wet op de Inlichtingen- en Veiligheidsdienst uit 2002 oplegt aan de Militaire Inlichtingen- en Veiligheidsdienst, als het gaat om het toepassen van digitale methoden voor inlichtingenverzameling, verouderd?

In dit onderzoek werd verondersteld dat de WIV 2002 verouderd is door nieuwe technologieën die in de afgelopen jaren zijn verschenen op het gebied van digitale inlichtingenverzameling.

De huidige wetgeving omtrent het verzamelen van inlichtingen via het digitale domein staat beschreven in de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002. De MIVD valt sinds 2002 onder deze wet. Destijds had de wetgever een situatie voor ogen die toen van toepassing was.
Hierbij is geen of onvoldoende rekening gehouden met de technologische ontwikkelingen die zich de komende jaren zouden voordoen.
De technologieën die sinds 2002 in gebruik zijn genomen of zijn ontwikkeld hebben een grote impact op de manier hoe tegenwoordig de telecommunicatie verloopt. De intreding van glasvezelkabels heeft ervoor gezorgd dat er een snelheid- en capaciteitstoename heeft plaatsgevonden op het gebied van telecommunicatie. Hierdoor zijn programma's die Voice over Internet Protocol gebruiken steeds meer in gebruik genomen, met Skype als sprekend voorbeeld. De toegenomen snelheid en capaciteit van het internet, samen met de mobiele techniek met hieronder vallend de mobiele apparaten en mobiel internet, heeft ervoor gezorgd dat mensen in toenemende mate bereikbaar zijn en niet meer gebonden zijn aan een vaste locatie om toegang te hebben tot het internet. De groei van de beschikbaarheid en het gebruik van het internet heeft voor een verschuiving van telecommunicatie gezorgd. Waar voorheen de telecommunicatie verliep via de ether of satelliet, is deze nu meer gaan lopen via de kabel.
Naast technologische ontwikkelingen zijn er ook andere ontwikkelingen geweest sinds 2002 die aan te merken zijn als virtuele ontwikkelingen. Het gaat hierbij om nieuwe toepassingen op de bestaande technologieën zoals Social Media, Cloud computing. Door de toename in internetgebruik zijn deze toepassingen steeds meer in gebruik genomen.

Ook is er een nieuwe technologie beschreven in het derde hoofdstuk die ontwikkeld is door Amerikaanse National Security Agency. Het gaat hier om het Quantum project. Quantum bestaat uit een chip die geplaatst wordt in een computer of netwerk dat fysiek is gescheiden door een air gap van het internet. Via deze chip kan er toegang worden verkregen tot deze computers of netwerken door verbinding te maken met de chips via radio frequenties.

Andere ontwikkelde toepassingen op de technologie zijn de PRISM en Xkeyscore programma's. Deze programma's maken gebruik van de snelheid en capaciteit van glasvezelnetwerken om telecommunicatieverkeer op te nemen dat onder andere is opgeslagen in datacentra en gegenereerd is op Social Media. Deze programma's zijn in relevantie gestegen door het toenemende aantal internetgebruikers en steeds groter wordende hoeveelheid gegenereerde data.

De Nederlandse overheid heeft onderkend dat de huidige wetgeving voor de MIVD en de AIVD is verouderd en een modernisering mogelijk wenselijk is. De minister van defensie, mevr. Hennis-Plasschaert, heeft aangegeven dat voor een goedwerkende inlichtingen- en veiligheidsdienst er ruimte moet zijn voor innovatie en er geanticipeerd moet kunnen worden op situaties. Door de Motie van Elissen is in de politiek opgemerkt dat de WIV 2002 nog nooit geëvalueerd is. De evaluatiecommissie-Dessens heeft vervolgens een onderzoeksrapport geschreven over WIV 2002. Hierin doet zij onder andere een aanbeveling betreffende digitale inlichtingenverzameling. In het onderzoeksrapport wordt onderkend dat er een verschuiving van telecommunicatie heeft plaatsgevonden van ether/satelliet naar kabel, waardoor de inlichtingen- en veiligheidsdiensten mogelijk doof en blind worden.
De aanbeveling die wordt gedaan door deze commissie betreft de toevoeging van kabelgebonden interceptie aan de bijzondere bevoegdheid in de WIV 2002. Hiervoor wordt ook een mogelijk juridisch raamwerk gegeven.

De aanbeveling van de evaluatiecommissie komt overeen met wat er in dit onderzoek naar voren is gekomen. De verschuiving van telecommunicatie is dusdanig groot dat de behoefte om inlichtingen te verzamelen via de kabel gegrond is. Bij de toepassing hiervan zal ook gekeken moeten worden naar de aanschaf van een HPC om de opgenomen informatie te analyseren en bruikbaar te maken. De andere beschreven ontwikkelingen die zijn gedaan sinds 2002 hebben allemaal betrekking op het gebruik van glasvezelkabels. Doordat ze gebruik maken van het internet. Dit geldt echter niet voor Quantum. De conclusie kan dan ook getrokken worden dat de toevoeging van kabelgebonden interceptie aan de bijzondere bevoegdheden van de MIVD benodigd is.

Quantum is een nieuwe technologie om inlichtingen te verzamelen uit systemen die voorheen onbereikbaar waren. Deze technologie valt echter onder technische hulpmiddelen die gebruikt kunnen worden bij het binnendringen van een geautomatiseerd werk. Dit valt onder artikel 24, die het toelaat om binnen te dringen in een geautomatiseerd werk door middel van technische hulpmiddelen.

Wanneer de beschreven technologieën worden bekeken aan de hand van de drie lagen in het digitale domein kan de conclusie worden getrokken dat er meer bevoegdheden benodigd zijn in de fysieke laag. Als er behoefte is aan meer inlichtingen, is het nodig om kabelgebonden interceptie uit te kunnen voeren. Alle informatie die gegenereerd, verstuurd en gedownload wordt verloopt tegenwoordig via de glasvezelkabel en dus de fysieke laag van het digitale domein.

Op dit moment is de wet de beperkende factor waardoor het nu nog niet is toegestaan om kabelgebonden interceptie uit te voeren. De artikelen 24 t/m 27 beschrijven de bijzondere bevoegdheden die de MIVD op dit moment heeft ten behoeve van digitale inlichtingenverzameling. Artikel 24 geeft de MIVD de mogelijkheid om gericht binnen te dringen in een geautomatiseerd werk. De bevoegdheid tot het gericht intercepteren van niet-kabelgebonden telecommunicatie is beschreven in artikel 25. Artikel 26 geeft de MIVD de bevoegdheid om ongericht niet-kabelgebonden telecommunicatie te intercepteren. Artikel 27 geeft de MIVD de bevoegdheid om een selectie te maken in de ontvangen informatie onder de bevoegdheid van artikel 26.
Deze artikelen staan niet toe dat de MIVD ongerichte interceptie kan uitvoeren op kabelgebonden telecommunicatie.

Uit dit onderzoek is gebleken dat de H_0 kan worden aangenomen. Omdat de H_0 aangenomen wordt kan de onderzoeksvraag positief worden beantwoord. De beperkingen die gelden voor de digitale methode voor inlichtingenverzameling zijn verouderd. Aan de hand van de nieuwe technologieën en de behoeftes die zijn gesteld vanuit de evaluatiecommissie kan kabelgebonden interceptie worden gezien zien als een methode van digitale inlichtingenverzameling waar op dit moment behoefte aan is, maar niet is toegestaan. De MIVD ondervindt hierdoor een beperking op het volledig kunnen exploiteren van dit medium, waarin meer en adequater digitale inlichtingen verzameld kan worden.

Aanbevelingen

Na deze thesis te hebben geschreven, de informatie te hebben onderzocht en hier een conclusie uit te hebben getrokken, is er een aantal punten naar voren gekomen waaruit aanbevelingen voortvloeien. Opvallende aanbevelingen kunnen gedaan worden betreffende de AIVD, kabelgebonden interceptie en vervolgonderzoek. Binnen het vervolgonderzoek is het van belang om verschillende aspecten te onderzoeken of uit te diepen.

AIVD

In dit onderzoek is er gekeken naar de behoefte voor de MIVD aan de hand van WIV 2002. Naast de MIVD valt ook de AIVD onder deze wetgeving. In verband met de grootte van deze thesis is de AIVD in dit onderzoek buiten beschouwing gelaten. Ook de conclusie is nu volledig gericht op de MIVD. Mocht er daadwerkelijk gekeken worden naar aanpassing van de WIV 2002, is het noodzakelijk dat een dergelijk onderzoek ook wordt verricht aan de hand van de taken van de AIVD.

KABELGEBONDEN INTERCEPTIE

Vanuit dit onderzoek volgt de aanbeveling tot het toevoegen van de bevoegdheid tot het gebruik van kabelgebonden interceptie tijdens het inlichtingen verzamelen door de MIVD, om zo de WIV 2002 te moderniseren. Dit, omdat tegenwoordig 80 tot 90 procent van de telecommunicatie verloopt via glasvezelkabels. Een vervolgonderzoek is essentieel om een aantal zaken extra te belichten, zie hiervoor de volgende paragraaf.

VERVOLGONDERZOEK

Aan dit onderzoek hangen een paar beperkingen in verband met de grootte van de thesis, maar zeker ook in verband met de grootte van het onderzoek zelf.

Belangrijk voor vervolgonderzoek is om te kijken naar de focus op het digitaal verzamelen van inlichtingen, de technologische ontwikkelingen die zijn gedaan, een mogelijk juridisch raamwerk en er zal gekeken moeten worden naar de privacy.

Focus digitale inlichtingenverzameling

Binnen dit onderzoek is er gekeken naar de behoeftes van de MIVD op het gebied van digitale inlichtingenverzameling artikel 24 t/m 27 van de WIV 2002. Er is niet verder gekeken naar andere verwervingsmethoden buiten dit domein. Mogelijk behoeft de WIV 2002 voor andere verwervingsmethoden van inlichtingen ook aanpassingen.

Ook hier is het noodzakelijk wanneer er besloten wordt tot modernisering van de wet om eerst deze andere verwervingsmethoden te onderzoeken.

Technologische ontwikkelingen

In dit onderzoek zijn verschillende technologische ontwikkeling genoemd. Hoogstwaarschijnlijk zijn deze technologische ontwikkelingen niet alle technologische ontwikkelingen die zijn gedaan sinds 2002 binnen het digitale domein. Er is in dit onderzoek gekozen voor deze paar, omdat dit de meest bekende technologieën zijn. Verder onderzoek zou moeten uitwijzen in hoeverre er nog andere technologische ontwikkelingen van belang zijn binnen de WIV 2002. Dit geldt voor zowel de MIVD als de AIVD.

Juridisch raamwerk

Dit onderzoek doet een aanbeveling om kabelgebonden interceptie toe te staan, maar biedt geen juridisch raamwerk waar deze aan zou moeten voldoen. De evaluatiecommissie-Dessens doet dit wel. Het is van belang om vervolgonderzoek te verrichten naar dit juridisch raamwerk, voordat er wel of niet besloten kan worden tot de bevoegdheid van het gebruik van kabelgebonden interceptie in de WIV 2002 door de MIVD en de AIVD.

Privacy

Net als hierboven beschreven bij het juridisch raamwerk, wordt er in deze thesis geconcludeerd dat kabelgebonden interceptie van toegevoegde waarde is voor de MIVD. Wat in dit onderzoek niet is gedaan is onderzoek verrichten naar wat dit expliciet inhoudt voor de privacyrechten. Ook dit is belangrijk om verder te onderzoeken voordat er daadwerkelijk gekeken gaat worden tot eventuele modernisering van de WIV 2002.

Reflectie

Waar ben ik tegen aangelopen tijdens het schrijven van deze thesis, wat zijn mijn leerpunten en wat viel mij op?

Het schrijven van deze scriptie is een hele opgave geweest, veel en hard werken. Als ik nu terug kijk naar de afgelopen periode en naar het werk dat ik neergezet heb, kan ik zeggen dat ik trots ben.

Het belangrijkste leermoment dat ik voor mijzelf heb onderkend is dat ik veel meer tijd had moeten steken in mijn Individueel Onderzoeksvoorstel (IOV). Als ik hier beter over nagedacht zou hebben dan zou de structuur van de scriptie van het begin beter in elkaar zitten. Nu heb ik tot drie keer toe mijn werk moeten herschrijven. Dit had kunnen worden voorkomen met een goed uitgedacht IOV. Tijdens het schrijven van deze thesis was het wijzer geweest om beter voor ogen te houden wat de hoofdvraag was waar ik antwoord op moet geven en of de informatie die ik heb hier een bijdrage aan levert. Vervolgens had ik bij het verwerken van de informatie zorgvuldiger om kunnen gaan met het bijhouden van de literatuurlijst. Dit heeft achteraf heel veel tijd gekost. Ook ben ik er bewust van geworden dat mijn dyslectie iets is om rekening mee te houden in de toekomst bij het schrijven van stukken van dit formaat. De tijd die ik kwijt was bij het lezen van bronnen was aanzienlijk meer in vergelijking met mijn collega's. Achteraf gezien had ik hier meer tijd voor moeten inplannen. Wellicht was het slim geweest als ik tijdens het kerstverlof al actief was begonnen. Ik had dan mogelijk eerder klaar kunnen zijn, waardoor ik mijn taalkundige corrector meer tijd had kunnen geven.

Tijdens het schrijven heb ik ondervonden dat het moeilijk was om informatie te vinden over de technologische ontwikkelingen die zijn gedaan sinds 2002. Ik heb dit opgelost door te brainstormen en door collega's te bevragen. Deze heb ik vervolgens gebruikt voor het onderzoek. Ook wilde ik in het begin informatie hebben over welke middelen de MIVD beschikt voor het verzamelen van inlichtingen in het digitale domein. Dit heb ik helaas niet terug kunnen vinden in openbare bronnen.

Ook ben ik tijdens het schrijven achter verschillende aspecten gekomen die nog onderzocht en/of uitgediept dienen te worden voordat er nagedacht kan worden over eventuele modernisering van de wet. Deze aspecten had ik vooraf aan het schrijven van deze thesis nog niet voorzien. Uit deze aspecten heb ik dan ook aanbevelingen gedaan tot vervolgonderzoek.

Door het schrijven van de scriptie ben ik erg nieuwsgierig geworden of en hoe kabelgebonden interceptie mogelijk geïmplementeerd zal worden in de wet en welke gevolgen die zal hebben voor de privacy van de internetgebruiker.

Literatuurlijst

Kamerstukken

Kamerstukken II 1997/98, 25 877, nr.3.

Kamerstukken II 1999/00, 25877, nr.8.

Kamerstukken II 2003/04, 29 241, nr.5.

Kamerstukken II, 2011/12, 30 517, nr.25.

Kamerstukken II 2011/12, 29 924, nr.76.

Kamerstukken II, 2012/13, 29 924, nr.100.

Kamerstukken II 2012/13, 30 977, nr.56.

Kamerstukken II 2013/14, 26 643, nr.298.

Kamerstukken II 2013/14, 30 977, nr.74.

Wet op de Inlichtingen- en Veiligheidsdiensten 2002: zie Staatsblad 2002 nr. 148.

Verslagen

AIV/CAVV. (2011). *Digitale* oorlogvoering. No 77, AIV/ No 22, CAVV. Beschikbaar op: http://www.aiv-advies.nl/ContentSuite/upload/aiv/doc/webversie_AIV_77_CAVV_22_NL(1).pdf. Bekeken op 10-01-2014.

AIVD & Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2013). *Jaarverslag AIVD 2012*. Geraadpleegd op: https://www.aivd.nl/publish/pages/2520/jaarverslag_2012.pdf. Bekeken op: 17-1-2014.

AMSix (2003). *AMSix Annual report 2003.* Beschikbaar op: https://www.ams-ix.net/system/resources/BAhbBlsHOgZmSSIvMjAxMi8wOC8yNy8xNl8xNF8wOF81NjNfQVJfQU1TX0lYXzIwMDMucGRmBjoGRVQ/AR_AMS-IX_2003.pdf. Bekeken op 30-1-2014.

Australian Government (2006). *Mobile and wireless technologies: security and risk factors.* Beschikbaar op: http://www.aic.gov.au/documents/E/9/9/%7BE99293FF-9E0F-4522-8E54-0598720C45B2%7Dtandi329.pdf. Bekeken op: 23-2-2014.

Blunden (2010). *Manufactured Consent and Cyberwar* Beschikbaar op: http://www.cio.wisc.edu/MCaC.pdf. Bekeken op 12-1-2013.

CCDCOE (2012). *National Cyber Security, Framework Manual.* Beschikbaar op: http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf. Bekeken op 25-2-2014.

Centraal Bureau voor de Statistiek (2012). *Verdere groei mobiel internetgebruik.* Beschikbaar op: http://www.cbs.nl/NR/rdonlyres/45D7ACAF-A2D5-43C4-A893-436B5C5A9AAF/0/pb12n060.pdf. Bekeken op 11-2-2014.

Center of Strategic & International Studies (2002). *Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats.* Beschikbaar op: http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf. Bekeken op 26-2-2014.

Compact (2011). *Strategische keuzen rondom datacenters.* Beschikbaar op: http://www.compact.nl/pdf/C-2011-1-Boersen.pdf. Bekeken op 10-2-2014.

CTIVD (2011). *Toezichtsrapport nr.28. Inzake de inzet van Sigint door de MIVD.* Beschikbaar op: http://www.ctivd.nl/?download=CTIVD%20rapport%2028.pdf. Bekeken op: 30-1-2014.

CTIVD (2012). *Toezichtsrapport nr.31. Inzake de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van Sigint door de AIVD*. Beschikbaar op: https://www.aivd.nl/publish/pages/2430/ctivd_rapport_nr_31_over_afluisteren.pdf. Bekeken op 8-2-2014.

Data Protectors (z.d.). *Cyber Security voor de Defensie Industrie in Nederland.* Beschikbaar op: http://dataprotectors.nl/brochures/Sector_Paper_Toeleveranciers_Defensie_Data_Protectors_nl.pd. Bekeken op: 21-2-2014.

Dessens, C.W.M. (2013). *Evaluatie, Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen.* Geraadpleegd op: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2013/12/02/rapport-evaluatie-wiv-2002/b-20546-webeindversie.pdf. Bekeken op 13-12-2013.

Joint Publications 3-0. (2011). *Joint Operations.* Beschikbaar op: http://dtic.mil/doctrine/new_pubs/jp3_0.pdf. Bekeken op 8-01-2014.

Joint Publication 1-02 (2010). *Department of Defense Dictionary of Military and Associated Terms*. Beschikbaar op: http://ra.defense.gov/documents/rtm/jp1_02.pdf. Bekeken op: 30-1-2014.

Ministerie van Defensie (2012). Defensie cyber strategie. Beschikbaar op: http://www.defensie.nl/binaries/defensie/documenten/brochures/2012/09/14/defensie-cyber-strategie/defensie-cyber-strategie.pdf. Bekeken op 12-01-2014.

Ministerie van Defensie (2013). *Nederlandse Defensie doctrine 2013*. Beschikbaar op: http://www.defensie.nl/binaries/defensie/documenten/publicaties/2013/11/20/defensie-doctrine-nl/defensie-doctrine_nl.pdf. Bekeken op: 12-01-2014.

Ministerie van Defensie (2013a). *Jaarverslag MIVD 2012*. Geraadpleegd op: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/jaarverslagen/2013/04/25/jaarverslag-militaire-inlichtingen-en-veiligheidsdienst-2012/jaarverslag-militaire-inlichtingen-en-veiligheidsdienst-2012.pdf. Bekeken op: 17-1-2014.

Ministerie van Defensie (2013b). *Presentatie interceptie van telecommunicatie.* Beschikbaar op: http://www.defensie.nl/binaries/defensie/documenten/publicaties/2013/12/18/presentatie-interceptie-telecommunicatie/presentatie_interceptie_telecommunicatie.pdf. Bekeken op: 9-2-2014.

Ministerie van Veiligheid en Justitie (2011). *Cyber Security Beeld Nederland December 2011.* Beschikbaar op: https://www.ncsc.nl/binaries/nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cyber-security-beeld-nederland/2/Cyber%2BSecurity%2BBeeld%2B2011.pdf. Bekeken op 22-1-2014.

Ministerie van Veiligheid en Justitie (2012). *Cybersecuritybeeld Nederland CSBN-2.* Beschikbaar op: https://www.ncsc.nl/binaries/nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland/1/Cybersecuritybeeld%2BNederland.pdf. Bekeken op: 9-2-2014.

Ministerie van Veiligheid en Justitie (2013). *Cybersecuritybeeld Nederland CSBN-3.* Beschikbaar op: https://www.ncsc.nl/binaries/nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland-3/1/NCSC%2BCSBN%2B3%2B2edruk%2Bseptember%2B2013.pdf. Bekeken op: 22-1-2014.

Ministerie van Veiligheid en Justitie (2013a). *Nationale Cyber Security Strategie 2.* Beschikbaar op: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2013/10/28/nationale-cyber-security-strategie-2/rapport-nationale-cybersecurity-strategie-2-2.pdf. Bekeken op: 25-11-2013.

Ottis, R. & Lorents, P. (z.d.). *Cyberspace: Definition and implications.* Beschikbaar op: http://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf. Bekeken op 8-01-2014.

TRADOC Pamphlet 525-7-8 (2010). *Cyberspace Operations Concept Capability Plan 2016-2028.* Beschikbaar op: http://www.fas.org/irp/doddir/army/pam525-7-8.pdf. Bekeken op 14-01-2014.

Websites

AIVD & Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (z.d.a). *Verdachte webfora zijn legitiem doelwit.* Beschikbaar op: https://www.aivd.nl/@3034/reactie-nrc. Bekeken op 20-1-2014.

AIVD & Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (z.d.b). *Het werk van de AIVD, Interceptie telecommunicatie verkeerd.* Beschikbaar op: https://www.aivd.nl/organisatie/werk-aivd/komt-aivd/interceptie/. Bekeken op: 11-02-2014.

Consumentenbond (z.d.). *Wat is glasvezel?.* Beschikbaar op: http://www.consumentenbond.nl/test/elektronica-communicatie/internet-en-software/glasvezel-internet/extra/wat-is-glasvezel/. Bekeken op: 29-1-2014.
Dufaco ICT (z.d.). *Glasvezel verbindingen.* Beschikbaar op: http://www.dufaco.nl/glasvezel/nieuws/nieuws/glasvezel-verbindingen. Bekeken op 10-2-2014.

European Commission (2013). *Future of High-Performance Computing: Supercomputers to the Rescue.* Beschikbaar op: http://ec.europa.eu/digital-agenda/futurium/en/content/future-high-performance-computing-supercomputers-rescue. Bekeken op: 6-3-2014

The future of the data center (2013). How facebook, Google and the Rest Changed the Data Center. Beschikbaar op: http://futureofthedatacenter.com/how-facebook-google-and-the-rest-changed-the-data-center/ bekeken op: 10-2-2014.

The Guardian (2013). *XKeyscore: NSA tool cellects 'nearly everything a user does on the internet'.* Beschikbaar op: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. Bekeken op 6-3-2014.

Grondwet (1815). Beschikbaar op: www.wetten.overheid.nl. Bekeken op: 2-2-2014.

InterNLnet (z.d.). *Historie.* Beschikbaar op: https://www.internl.net/over-internlnet/over-ns/historie. Bekeken op: 22-2-2014.

Internetten.nl (z.d.). *Snelheid Internetverbindingen.* Beschikbaar op: http://www.internetten.nl/internet/snelheid-internetverbindingen. Bekeken op 19-2-2014.

Janssen, C. (z.d.). *What is an Air Gap?.* Beschikbaar op: http://www.techopedia.com/definition/17037/air-gap. Bekeken op 7-2-2014.

Justitia.nl (z.d.) *Cloudcontract.* Beschikbaar op: http://www.justitia.nl/cloudrecht/cloudcontract.html. Bekeken op 26-2-2014.

Kay, R. (2001).*Wat is een mesh netwerk?* Beschikbaar op: http://computerworld.nl/it-beheer/61959-wat-is-een-mesh-netwerk. bekeken op 10-01-2014.

KPN (z.d.). *Nederland: hart van het internet.* Beschikbaar op: http://www.kpn.com/web/file?uuid=20b0686a-2f4b-41c6-8f32-42d94c594dca&owner=bc24a771-5e12-43a0-90d9-90bbab912306. Bekeken op 29-1-2014.

MijnWetten.nl (z.d.). *Artikel 3.3 Circulaire Bewaking en beveiliging van personen, objecten en diensten.* Beschikbaar op: http://mijnwetten.nl/circulaire-bewaking-en-beveiliging-van-personen-objecten-en-diensten/artikel3.3. Bekeken op: 21-2-2014.

Ministerie van Defensie. (z.d.). *Militaire Inlichtingen- en Veiligheidsdienst, Taken en werkzaamheden*. Beschikbaar op: http://www.defensie.nl/mivd/taken_en_werkzaamheden/. Bekeken op: 20-11-2013.

Ministerie van Defensie (2012a). Minister Hillen presenteert Defensie Cyber Strategie. Beschikbaar op: http://www.defensie.nl/actueel/nieuws/2012/06/27/46197032/ minister_hillen_presenteert _defensie_cyber_strategie. Bekeken op: 22-11-2013.

Ministerie van Defensie (2013c). *Interceptie van Telecommunicatie.* Beschikbaar op: http://www.defensie.nl/mivd/taken_en_werkzaamheden/werkzaamheden/interceptie_van_telecommunicatie/. Bekeken op 9-2-2014.

The New York Times (2014). N.S.A. Devises Radio Pathway Into Computers. Beschikbaar op: http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=0. Bekeken op 19-1-2014.

NRC Handelsblad (2013). *NSA hielp Nederland met onderzoek naar herkomst 1,8 Miljoen.* Beschikbaar op: http://www.nrc.nl/nieuws/2014/02/08/nsa-hielp-nederland-met-onderzoek-naar-herkomst-18-miljoen/. Bekeken op 8-2-2014.

NRC handelsblad (2014). *Snowden: NSA bespioneert ook buitenlandse bedrijven.* Beschikbaar op: http://www.nrc.nl/nieuws/2014/01/26/snowden-nsa-bespioneert-ook-bedrijven/. Bekeken op 30-1-2014.

Posthumus, N. (2013). *25 jaar internet in Nederland – een kwestie van goed 'netwerken'.* Beschikbaar op: http://www.nrc.nl/nieuws/2013/11/17/25-jaar-internet-in-nederland-een-kwestie-van-goed-netwerken/. Bekeken op 28-1-2014.

Rabobank (2013). *En toen belde de bank….* Beschikbaar op: http://www.rabobank.nl/particulieren/servicemenu/nieuws/rabobank_nieuws/phishing. Bekeken op 28-01-2014.

Rijksoverheid (2013). *Rijksbegroting, 4.4 bijlage – overzicht cyber.* Beschikbaar op: http://www.rijksbegroting.nl/2013/voorbereiding/begroting,kst173868_16.html. Bekeken op 19-2-2014.

Social-Media (z.d.). *Social Media.* Beschikbaar op: www.social-media.nl. Bekeken op 10-2-2014.

Spiegel Online International (2013). *Three Different Prisms?.* Beschikbaar op: http://www.spiegel.de/international/germany/merkel-chief-of-staff-testifies-before-parliament-on-nsa-spying-a-913268.html. Bekeken op 30-1-2014.

UX Magazine (2012). *A Primer on Responsive Design: From Content to Development.* Beschikbaar op: http://uxmag.com/articles/a-primer-on-responsive-design. Bekeken op: 10-2-2014.
https://www.ams-ix.net/. Bekeken op 4-2-2014.

The Washington Post (2013). *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program.* Beschikbaar op: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1. Bekeken op: 30-1-2014.

Literatuur

Andress, J. Winterfeld, S. (2014) *Cyber Warfare, Techniques, Tactics an Tools for Security Practitioners.* Elsevier, Amsterdam.

Commandant Landstrijdkrachten (2006). *Leidraad Inlichtingen LD5, Koninklijke Landmacht.* Zwolle: PlantijnCasparie Koninklijke Landmacht LD5.

Dielemans, R.J.I. (2010). *Lexplicatie deel 3.74a. Wet op de inlichtingen- en veiligheidsdiensten 2002; Wet veiligheidsonderzoeken.* Deventer: Kluwer

Ducheine, P.A.L. & Haaster, J. van. (2013). *Cyber-operaties en militair vermogen.* Militaire Spectator, 182(9), p. 368-387.

Ducheine, P. Osinga, F. Soeters, J. (2012) *Cyberwarfare, Critical Perspectives*. T.M.C. Asser Press.

Graaf, B.A. de, Muller, E.R. & Reijn, J.A. van (2010*). Inlichtingen- en veiligheidsdiensten.* Den Haag: Kluwer.

Tanenbaum, A.S. (2007). *Computernetwerken.* Amsterdam: Pearson Education Benelux.

Afbeelding kaft

Wired.co.uk (2013). *Report finds British militairy must 'urgently' draw up cyber security plans.* Beschikbaar op: http://www.wired.co.uk/news/archive/2013-01/10/uk-defence-cybercrime.
Bekeken op 16-1-2014.