Justitie

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Nationaal Coördinator Terrorismebestrijding (NCTb)

Jihadisten en het internet

Jihadisten en het internet

WOORD VOORAF

Terrorismebestrijding is één van de belangrijkste thema's in het internationale en nationale veiligheidsbeleid. De Nationaal Coördinator Terrorismebestrijding (NCTb) is verantwoordelijk voor de beleidsontwikkeling, de analyse van (inlichtingen)informatie en de regie over te nemen beveiligingsmaatregelen bij de bestrijding van terrorisme. Om de hedendaagse terrorismedreiging het hoofd te kunnen bieden, is het van groot belang mee te bewegen met de nieuwste ontwikkelingen. Terroristen maken immers zelf ook slim gebruik van de modernste technologieën en communicatiemiddelen. Het internet heeft daar als vanzelfsprekend een grote rol in.

Jihadistische terroristen en radicalen (jihadisten) gebruiken het internet in ruime mate als middel. Het internet is daardoor onder andere een belangrijk platform voor radicalisering en kan zelfs dienen als virtueel trainingskamp. Jihadisten gebruiken het internet echter niet alleen als middel, maar kunnen zich met terroristische activiteiten ook richten tegen het internet zelf (internet als doelwit) of via het internet tegen andere doelwitten (internet als wapen). Inzicht in deze vormen van internetgebruik is van groot belang voor contra-strategieën én beveiligingsvraagstukken. Deze fenomeenstudie 'Jihadisten en internet' geeft dat inzicht.

Vanuit haar analysetaak maakt de NCTb tal van producten die op strategisch niveau van belang zijn voor de bestrijding van terrorisme. Eén van die producten is het Dreigingsbeeld Terrorisme Nederland (DTN), een landelijke analyse die vier maal per jaar verschijnt. Daarnaast realiseert de NCTb fenomeenstudies zoals deze, waarin een specifiek fenomeen verdergaand wordt onderzocht. Deze studie is tot stand gekomen op basis van literatuuronderzoek, interviews, het monitoren van het internet en een expertmeeting over het thema 'internet als doelwit en wapen'. De uitkomsten van deze meeting - die onderzoekers, overheidsdiensten en bedrijfsleven uit de terrorisme-, telecom- en internetsector bijeenbracht - vormen een belangrijke bouwsteen voor deze studie.

Ik spreek de hoop uit dat deze studie handvatten biedt - voor andere overheidsorganisaties, maar zeker ook voor private partners - om de dreiging te keren van dit internetgebruik door jihadisten. Naar de aard van het verschijnsel terrorisme en het internet is dat niet eenvoudig. Maar dat betekent niet dat we zomaar op onze lauweren moeten rusten. De NCTb zal in ieder geval de bevindingen uit dit onderzoek gebruiken om samen met anderen maatregelen te ontwikkelen om de terroristische dreiging het hoofd te kunnen bieden.

De Nationaal Coördinator Terrorismebestrijding
mr. T.H.J. Joustra

INHOUDSOPGAVE

SAMENVATTING

Jihadistische terroristen en radicalen (jihadisten) gebruiken het internet in ruime mate. Voor contrastrategieën én beveiligingsvraagstukken in het kader van contraterrorisme is inzicht hierin van groot belang. Deze fenomeenstudie, die het resultaat is van een globale, maar brede oriëntatie door de NCTb, probeert dat inzicht te geven. Daarin is onderscheid gemaakt tussen het gebruik van het internet als doelwit en wapen (deel A) en internet als middel (deel B).

A Internet als doelwit en wapen

Bij het *internet als doelwit* richten de terroristische activiteiten zich tegen (de infrastructuur van) het internet zelf. Daarbij kan gedacht worden aan onder andere knooppunten (computerparken), functionaliteiten en verbindingslijnen van het internet of de organisaties die diensten verlenen die cruciaal zijn voor het functioneren van het internet. Een aanval of aanslag tegen het internet kan verschillende vormen aannemen:

- Een cyberaanval door gebruikmaking van computers via het internet. Het internet is in dat geval zowel doelwit als wapen: het internet keert zich tegen zichzelf.
- Een fysieke aanslag door gebruikmaking van conventionele wapens of door sabotageacties van binnen uit.
- Een elektromagnetische aanslag door het gebruik van bijvoorbeeld elektromagnetische energiebronnen.
- Indirecte aanslagen of aanvallen bijvoorbeeld tegen de elektriciteitsvoorziening of koelvoorzieningen.

Bij het gebruik van het *internet als wapen* worden aanslagen tegen fysieke doelen gepleegd via het internet. Te denken valt aan de overname van luchtverkeerssystemen of besturingssystemen van vitale installaties in de chemische sector of de elektriciteitsvoorziening.

Het gebruik van het 'internet als doelwit en wapen' is, veelal onder de noemer van cyberterrorisme, een regelmatig terugkerend thema in de berichtgeving. In die grotendeels internationale berichtgeving divergeren de meningen sterk over de mate waarin hier sprake is van een terroristische dreiging. Begin mei 2006 verschenen enkele berichten over de eenvoud van een (terroristische) aanval/ aanslag op het internet in Nederland. Alle reden daarom om in het kader van deze fenomeenstudie hier aandacht aan te besteden. Juist doordat er relatief weinig geschreven is over de Nederlandse situatie en de kennis over die situatie sterk versnipperd is, heeft de NCTb een expertmeeting georganiseerd met vertegenwoordigers van de inlichtingendiensten, wetenschap, politie, overige overheidsdiensten en de telecom- en internetsector. In deze fenomeenstudie is vanuit uiteenlopende invalshoeken de dreiging beoordeeld. Dit heeft geresulteerd in drie conclusies.

A1 Cyberaanvallen door jihadisten *tegen het internet* zijn niet waarschijnlijk

Een cyberaanval op het mondiale of het Nederlandse internet zélf[1] wordt op dit moment niet waarschijnlijk geacht. Hoewel een cyberaanval laagdrempeliger is dan bijvoorbeeld zelfmoordaanslagen, waardoor potentieel meer jihadisten daartoe zouden kunnen en willen overgaan, gelden als belangrijkste nadelen voor jihadisten dat het uitschakelen van het internet ook de jihadistische infrastructuur op het internet treft en niet appelleert aan het martelaarschap. Verder behoort een succesvolle cyberaanval niet echt tot de mogelijkheden, vooral als gevolg van de al genomen maatregelen hiertegen. Als we al een cyberaanval zouden kunnen verwachten, dan is dat een kleinschalige aanval gedurende een beperkte tijd of een geregisseerde combinatie van kleinschalige cyberaanvallen.

A2 Andersoortige aanslagen door jihadisten *tegen het internet* zijn niet waarschijnlijk

Een andersoortige aanslag tegen het internet, zoals de hierboven genoemde fysieke aanslag, wordt op dit moment evenmin waarschijnlijk geacht. Het mondiale of het Nederlandse internet valt op deze wijze eigenlijk niet uit te schakelen. Er zijn weliswaar mogelijkheden voor kleinschalige aanslagen, maar daartegen zijn wel al maatregelen getroffen om de kans erop te verkleinen en de effecten te beperken. Hoewel dit type aanslag waarschijnlijker lijkt dan een cyberaanval, is de vraag gerechtvaardigd of terroristen niet de voorkeur geven aan bijvoorbeeld een bomaanslag op een soft target in plaats van op een belangrijke internetlocatie.

A3 Cyberaanvallen *via het internet* zijn niet waarschijnlijk

Een aanval via het internet, waarbij het internet als wapen fungeert tegen andere doelwitten, is weliswaar voorstelbaar, maar momenteel niet waarschijnlijk. Desondanks bestaan er wel enkele mogelijkheden hiervoor als gevolg van kwetsbaarheden in bijvoorbeeld software voor procesbesturing (SCADA) waar diverse sectoren gebruik van maken. Bovendien zijn er enkele aantrekkelijke kanten te onderkennen voor jihadisten, maar een dergelijke aanval vereist doorgaans veel (insiders)kennis. Ook zijn klassieke aanvallen zoals bomaanslagen of zelfmoordaanslagen beter publicitair uit te buiten. Een combinatie van één of meer klassieke aanslagen met de inzet van het internet als wapen lijkt meer waarschijnlijk. Hierdoor wordt het effect van die aanval versterkt.

B Internet als middel

Jihadisten gebruiken het internet - net als gewone burgers - voor verschillende doeleinden en beschouwen het internet als een cruciaal middel voor de jihad. In de fenomeenstudie is gekeken naar diverse vormen van internetgebruik en naar de invloed daarvan op radicalisering, uitmondend in de volgende conclusies:

B1 Propaganda via het internet draagt bij aan radicalisering

Propaganda via het internet vindt professioneel plaats, heeft een groot bereik en kent relatief weinig weerwoord. De propaganda blijft niet beperkt tot eenrichtingsverkeer: de jihadisten proberen actief de interactie aan te gaan met geïnteresseerden. Gecombineerd met het feit dat vooral grote groepen jongeren toegang hebben tot het internet en dat intensief gebruiken, dan is duidelijk dat hierdoor een voedingsbodem bestaat voor (verdere) radicalisering. Dat geldt zeker voor moslima's vanwege de aantrekkelijkheid van het internet voor hen (vraagzijde) in combinatie met de actieve rol van radicale moslima's in het aanbod.

1 Hoewel het internet mondiaal is, is tot op zekere hoogte wel degelijk sprake van 'het Nederlandse internet'. Zie hiervoor paragraaf 2.3.

B2 Informatie-inwinning via het internet draagt potentieel bij aan het plegen van terroristische activiteiten

Net als voor iedereen vormt het internet voor jihadisten een onuitputtelijke bron van informatie. Vooral de ontwikkelingen op het terrein van (real-time) satellietbeelden, eventueel gecombineerd met een internetverbinding zoals in het geval van GoogleEarth, zullen snel voortschrijden. Daardoor nemen de mogelijkheden voor informatie-inwinning door jihadisten nog verder toe.

B3 Fondsenwerving via het internet door en voor jihadisten komt nog beperkt voor: verschuiving naar meer heimelijke fondsenwerving is te verwachten

In potentie bestaan vele mogelijkheden voor fondsenwerving door en voor jihadisten en er zijn enkele voorbeelden van bekend, maar het komt in de praktijk nog weinig voor. Deze vorm van fondsenwerving is immers zichtbaar en daardoor kwetsbaar voor overheidsingrijpen. Aangezien het bankieren via het internet steeds eenvoudiger en gebruikelijker wordt, zal ongetwijfeld ook het ge- en misbruik ervan door jihadisten toenemen. Dit, gecombineerd met de toenemende interesse van hackers voor online fraude, zal mogelijk leiden tot een verschuiving van meer openlijke naar meer heimelijke fondsenwerving. Fondsenwerving via het internet zal eveneens kunnen toenemen als gevolg van nieuwe digitale en anonieme betalingsmiddelen.

B4 Internetgebruik resulteert in meer interactieve vormen van rekrutering die nog niet goed te duiden zijn evenals in conscriptie en zelfontbranding

Erg aannemelijk is het niet dat iemand vanuit Nederland zich via het internet rechtstreeks en één-op-één laat *rekruteren* door rekruteurs van internationale terroristische groeperingen. Dit laat onverlet dat van bijvoorbeeld de kern van al Qa'ida een inspirerende werking kan uitgaan, maar het voert te ver om hier te spreken van rekrutering. Op het internet is wel een sterk *interactieve* vorm van *rekrutering* waarneembaar die gekoppeld is aan de interactieve manieren van propaganda bedrijven. Kenmerkend voor het internet is verder dat vooral potentiële strijders zich zelf willen aanmelden voor deelname aan de gewelddadige jihad *(conscriptie)*, wat goed past bij het karakter van het internet. In relatie tot het internet wordt ook wel gesproken van *zelfontbranding*, waarvan sprake is als iemand op zijn eigen houtje op jihad wil gaan of gaat en er geen twee partijen zijn te onderscheiden. Is het in de fysieke wereld al lastig om de overgang van radicalisering naar rekrutering en conscriptie afzonderlijk te bezien, dat geldt zeker voor het internet. Het is wellicht zelfs de vraag of door de opkomst van het internet nog wel sprake is van het klassieke rekruteur/rekruut-concept, en of dit

concept niet langzaam wordt vervangen door een permanente en interactieve mix van top-down en bottom-up informatieverschaffing en -inwinning, vermengd met online aanmoediging, sturing of netwerkvorming.

B5 Gebruik van het internet voor trainingsdoeleinden werkt drempelverlagend voor het plegen van aanslagen

Bereid zijn tot terroristische activiteiten is één ding, maar beschikken over de kennis, vaardigheden en middelen om dat te doen is evenzeer belangrijk. Vooral voor 'homegrown-terroristen' kan het volop beschikbare trainingsmateriaal bijdragen om de intentie tot het plegen van terroristische aanslagen in daden om te zetten. Verspreiding van trainingsmateriaal via het internet door jihadisten draagt bovendien bij aan het snel verspreiden van het geleerde.

B6 Jihadisten gebruiken het internet voor onderlinge communicatie en planning

Er zijn voldoende aanwijzingen dat de jihadisten via het internet onderling communiceren en terroristische activiteiten plannen. Ze maken daarbij gebruik van de mogelijkheden van anonieme en afgeschermde communicatie. Naast voordelen voor jihadisten biedt dit internetgebruik inlichtingen- en opsporingsinstanties de mogelijkheid tot ingrijpen. De jihadisten zijn zich daar goed van bewust.

B7 Virtuele netwerken verhogen de slagkracht van de jihadistische beweging

Door de vorming van virtuele netwerken ontstaat een informele pool van bereidwilligen voor de jihad die in wisselende combinaties met elkaar of individueel geweldsactiviteiten kunnen ontplooien. Lokale en internationale elementen kunnen daardoor meer met elkaar verweven raken.

B8 Internetgebruik ondersteunt het gehele proces van radicalisering

Voor iedere fase van radicalisering is er aanbod beschikbaar. Met behulp van het internet kan een potentiële jihadist processen doorlopen van ideologievorming, ideologieversterking en ideologische indoctrinatie. Nader wetenschappelijk onderzoek naar groepsprocessen via het internet en de invloed van het internetgebruik op radicalisering is echter gewenst.

B9 Vanuit het perspectief van radicalisering gaat de grootste dreiging uit van propaganda via het internet in combinatie met de relatief grote groep jonge moslims die zoekend is.

De propaganda vindt professioneel plaats, heeft een groot bereik, is interactief en kent relatief weinig weerwoord. Combineren we dat met het in potentie grote bereik bij kwetsbare jongeren, dan is duidelijk dat propaganda via het internet het meest bijdraagt aan (verdere) radicalisering, meer dan de andere vormen van internetgebruik.

B10 Vanuit het perspectief van terrorisme gaat de dreiging grotendeels uit van de (mogelijkheden tot) creatie van virtuele netwerken en het gebruik van het internet voor trainingsdoeleinden.

Verhogen virtuele netwerken vooral de slagkracht van de jihadistische beweging, het volop beschikbare trainingsmateriaal kan, zeker voor 'homegrown-terroristen', bijdragen om de intentie tot het plegen van terroristische aanslagen in daden om te zetten.

1

1.1 AANLEIDING

In onze huidige samenleving valt het internet niet meer weg te denken. Het creëert tal van mogelijkheden voor het bedrijfsleven, de overheid en de burgers, maar heeft ook een schaduwzijde. Het internet wordt immers in ruime mate gebruikt als middel door jihadistische terroristen en radicalen (jihadisten) en is daardoor onder andere ook een belangrijk platform voor radicalisering en kan zelfs dienen als virtueel trainingskamp. Jihadisten gebruiken het internet niet alleen als middel, maar kunnen zich met terroristische activiteiten ook richten tegen het internet zelf (internet als doelwit) of via het internet tegen andere doelwitten (internet als wapen). Voor beleidsvorming en -evaluatie ten behoeve van contraterrorisme is inzicht in deze vormen van gebruik van het internet (internetgebruik) door jihadisten daarom van groot belang. Deze fenomeenstudie, die het resultaat is van een globale, maar brede oriëntatie door de NCTb, probeert dat inzicht te geven.

1.2 DOEL, ONDERZOEKSVRAGEN EN AFBAKENING

Het primaire doel van de studie is om op hoofdlijnen inzicht te verkrijgen in het internetgebruik door jihadisten en de dreiging die daar van uitgaat ter beoordeling van mogelijke maatregelen om de dreiging te keren. Het secundaire doel is om onderwerpen te identificeren die verdere analyse en/of onderzoek vergen.

Afgeleid van het doel luiden de onderzoeksvragen:

1. In hoeverre en op welke wijze richten terroristische en radicaal jihadistische netwerken, groepen en individuen zich tegen het internet en gebruiken ze het internet?
   - In hoeverre en op welke wijze kiezen ze het internet als doelwit?
   - In hoeverre en op welke wijze gebruiken ze het internet als wapen?
   - in hoeverre en op welke wijze gebruiken ze het internet als middel?
2. In hoeverre en op welke wijze heeft het internet invloed op radicalisering?
3. In hoeverre gaat er van (welke vormen van) het gebruik een dreiging uit voor de Nederlandse samenleving en waaruit bestaat die dreiging dan?

Zoals blijkt uit het doel en de onderzoeksvragen richt deze studie zich primair op het *jihadistisch terrorisme* en *jihadistische radicalisering*, ook wel aangeduid als *islamistisch terrorisme* en *islamistische radicalisering*. Tenzij anders aangegeven, wordt hiertussen geen verschil gemaakt en hanteren we gemakshalve het begrip jihadisten. In sommige gevallen zal ook het bredere verschijnsel van terrorisme worden meegenomen, al is het maar omdat in de literatuur dat onderscheid niet altijd wordt gemaakt. Voor een definitie van de begrippen wordt verwezen naar het begrippenkader.

Het bredere internetgebruik door criminelen van uiteenlopend pluimage (cybercrime) blijft buiten beschouwing. De aanwezigheid en verspreiding van kinderporno-afbeeldingen op het internet, de vele verschijningsvormen van fraude en oplichting, de verspreiding van virussen, spyware en dergelijke, komen dus niet aan bod, tenzij expliciet gerelateerd aan terrorisme en radicalisering. Het internetgebruik voor economische en industriële spionage, voor militaire doeleinden (cyberwar) en het gebruik door allerlei politieke activisten komen evenmin aan bod.

De studie focust zich verder op het internet en niet op het brede verschijnsel van Informatie Communicatie Technologie (ICT) en nieuwe media. Het gebruik door jihadisten van bijvoorbeeld satelliet- en mobiele telefoons, alsmede het gebruik van satellietzenders wordt dus niet behandeld. Hoewel deze onderwerpen zeker zijn gerelateerd, is het internet al een zodanig complex en omvangrijk studieterrein dat daar bewust van is afgezien.

Een andere afbakening is dat de studie zich primair richt op Nederland, hoewel dat vanwege het karakter van het internet niet altijd eenvoudig en zinvol is. Aan de technische kant van het internet, bijvoorbeeld de gehanteerde technische protocollen, wordt in beginsel geen aandacht besteed, tenzij dat absoluut noodzakelijk is voor het begrip van het gebruik. Evenmin richt de aandacht zich op specifieke strafbare feiten of delicten. Primair wordt gekeken naar de driedeling: doelwit, wapen en middel.

1.3 VERANTWOORDING WERKWIJZE

Het verschijnsel van het internetgebruik door jihadisten is zodanig omvangrijk, dynamisch en complex dat een studie daarnaar werk zou kunnen opleveren voor vele onderzoekers gedurende vele jaren. Zoals eerder is aangegeven is gekozen voor een globale, maar wel brede oriëntatie op basis waarvan vervolgonderzoeken denkbaar zijn. Er is daarbij gekozen voor vier onderzoeksmethoden, namelijk: 1) het houden van interviews en achtergrondgesprekken, 2) een literatuurstudie, 3) een verkenning van het gebruik op enkele Nederlandstalige websites en -fora en 4) een expertmeeting.

Er zijn zeven interviews afgenomen met instanties die zich in Nederland bezighouden met het verschijnsel of het internet in het algemeen. Verder hebben enkele achtergrondgesprekken plaatsgevonden. De interviews en achtergrondgesprekken zijn geanonimiseerd verwerkt. Tevens hebben de auteurs deelgenomen aan congressen en de bevindingen daarvan verwerkt.

De literatuurstudie heeft zich gericht op wetenschappelijke literatuur en andere open bronnen. In de literatuur wordt uitvoerig ingegaan op het internetgebruik door terroristische groeperingen en jihadisten. Het gaat daarbij overwegend om buitenlandse literatuur en vanuit een internationaal perspectief. Specifiek op de Nederlandse situatie toegesneden literatuur is relatief schaars. Dat laatste is ook niet vreemd aangezien het internet en het jihadisme bij uitstek internationaal van aard zijn.

Een op 20 juni 2006 in het kader van deze studie door de NCTb georganiseerde expertmeeting heeft onderzoekers, overheidsdiensten en bedrijfsleven uit de terrorisme-, telecom- en internetsector bijeengebracht, waarbij het onderwerp ‘internet als doelwit en wapen’ centraal stond. De uitkomsten van die expertmeeting zijn verwerkt in hoofdstuk 2.

Er zijn diverse manieren om het internetgebruik door jihadisten in te delen vanuit het perspectief van de doeleinden die zij beogen (zie bijlage 1). In een eerder stadium heeft de NCTb gekozen voor de volgende indeling, rekening houdend met de door anderen benoemde aspecten:

A Het internet als doelwit;
B Het internet als wapen;
C Het internet als middel, nader onderverdeeld in:
- Propaganda;
- Informatie-inwinning;
- Fondsenwerving;
- Rekrutering;
- Training;
- Onderlinge communicatie en planning
- Creatie van virtuele netwerken.

1.4 TOELICHTING STRUCTUUR

Hoofdstuk 2 analyseert het internet als doelwit en wapen en hoofdstuk 3 het internet als middel. Hoofdstuk 4 presenteert de conclusies. Geëindigd wordt met een literatuurlijst, begrippenlijst en enkele bijlagen.

2

INTERNET ALS DOELWIT EN ALS WAPEN

2.1 INLEIDING

Veelal wordt het internet als doelwit en wapen onder *cyberterrorisme* geschaard. Dit is weliswaar een goed klinkende en populaire term voor de dreiging vanuit 'cyberspace', maar deze term is allerminst eenduidig en er bestaan dan ook vele definities voor. Op zich is het niet zo verwonderlijk dat er uiteenlopende definities bestaan voor cyberterrorisme. Hetzelfde geldt voor terrorisme. Als we al het begrip cyberterrorisme zouden willen hanteren, dan moeten we op zijn minst aansluiten bij de definitie voor terrorisme zoals die in Nederland gangbaar is, namelijk:

> *Het plegen van of dreigen met op mensenlevens gericht geweld, danwel het toebrengen van ernstige maatschappijontwrichtende zaakschade, met als doel maatschappelijke veranderingen te bewerkstellingen of politieke besluitvorming te beïnvloeden.*[1]

Vooral de intentie, namelijk het doel om maatschappelijke veranderingen te bewerkstellingen of politieke besluitvorming te beïnvloeden, is in die definitie cruciaal. Tevens moet het gaan om ernstige gevolgen. Bij de auteurs is geen definitie van cyberterrorisme bekend waarin dit voldoende tot zijn recht komt. Daardoor zijn die definities niet één-op-één geschikt voor de Nederlandse situatie. Er is ook nog een andere reden waarom het begrip cyberterrorisme voor deze studie problematisch is. Cyber is het voorvoegsel van cybernetica dat staat voor besturing door middel van automaten, of te wel computers. Cyber betekent dus eigenlijk 'door middel van het gebruik van computers'. Omdat deze studie zich specifiek richt op het internet en niet op het bredere gebruik van computers, is de term cyberterrorisme eerder verwarrend dan verhelderend. Om deze twee genoemde redenen is gekozen voor 'internet als doelwit' en 'internet als wapen' waarbij bovenstaande definitie van terrorisme als uitgangspunt geldt.
Bij het internet als doelwit gaat het om een aanslag tegen (de infrastructuur van) het internet zelf en bij het internet als wapen om een aanval via het internet tegen fysieke doelwitten, zoals de vitale infrastructuur, of online dienstverlening, zoals internetbankieren.

2.2 ACHTERGRONDEN

2.2.1 Toelichting

Allereerst zal deze paragraaf aandacht besteden aan de geschiedenis en aspecten van het internet die van belang zijn voor het vervolg van dit hoofdstuk. Vervolgens wordt ingegaan op enkele methoden die jihadisten zouden kunnen gebruiken voor een aanval tegen of via het internet. Een aanval kan plaatsvinden door het internet of netwerken gekoppeld aan het internet massaal te belasten met als achterliggend doel het functioneren van deze computernetwerken te verstoren of zelfs geheel plat te leggen. Een andere methode is het overnemen of manipuleren van netwerken, databases en besturingssystemen door gerichte hacking. Beide methoden, *massale overbelastingsaanvallen* en *gerichte hacking*, worden afzonderlijk toegelicht.

1 Dit is de definitie van de AIVD die ook wordt gebruikt door de NCTb, en gebaseerd is op het EU-kaderbesluit.

Voor toepassing van beide methoden zijn hackingvaardigheden en/of bekendheid met hacking of toegang tot de hackers-community vereist. In een aparte subparagraaf wordt kort aandacht besteed of er al aanwijzingen zijn dat jihadisten hiervan gebruik hebben gemaakt en/of daar aandacht voor hebben.

2.2.2 Het internet

De Van Dale omschrijft het internet als 'wereldwijd netwerk van computers waarmee men informatie kan uitwisselen'. Eigenlijk is het beter om te spreken van het internet als een wereldwijd netwerk van computernetwerken. In de kern is het internet een communicatie-omgeving of medium, en een onuitputtelijke bron van informatie. Naast een technische dimensie, de netwerken die mondiaal aan elkaar zijn gekoppeld, heeft het internet ook de dimensie van allerlei communicatiediensten/-hulpmiddelen waaronder het world wide web (WWW) en E-mail. Bovendien kent het internet ook een maatschappelijke dimensie: op het internet bestaan tal van sociale gemeenschappen en gebruiken overheden, maatschappelijke groeperingen en niet te vergeten bedrijven het volop. Sommige organisaties bestaan zelfs enkel online.

De geschiedenis van het internet begint in de jaren zestig van de vorige eeuw tijdens de hoogtijdagen van de Koude Oorlog. Er bestond toen de behoefte aan een computernetwerk om te vermijden dat de commandostructuur van het Amerikaanse leger in één klap zou kunnen worden uitgeschakeld.
Er moest een netwerk van computers komen dat immuun zou zijn voor vijandige aanvallen en in ieder geval niet tijdens één aanval, of door een sabotage op één locatie plat gelegd zou kunnen worden. Het Amerikaanse Ministerie van Defensie ontwikkelde daarom het experimentele ARPAnet (Advanced Research Projects Agency network) waarbij - in tegenstelling tot eerdere computernetwerken - er geen mastercomputer werd gebruikt.
Dit computernetwerk moest zowel flexibel als betrouwbaar zijn. Daarom is gekozen voor 'pakketschakelen' (packet switching).[2] Een inhoudelijk bericht bevindt zich in een elektronische envelop (pakket) die vanaf de verzendende computer via verschillende routes naar de eindbestemming(en) wordt verstuurd. Daarbij is geen sprake van een vaste route of van een rechtstreekse verbinding tussen de verzendende en de geadresseerde computer(s).
Grote berichten worden verdeeld over meerdere pakketten, voorzien van een adres en een volgnummer zodat het bericht op de eindbestemming weer kan worden samengevoegd. Door latere ontwikkelingen, waaronder de koppeling van steeds meer netwerken en de terugtrekking van het ministerie van Defensie als sponsor, is het ARPAnet ook opengesteld voor niet-militaire en wetenschappelijke doeleinden en werd daarbij herdoopt tot 'internet'. Het internet is internationaal, er bestaan geen landsgrenzen en het kent geen eigenaar. Dat heeft alles te maken met de open architectuur van de netwerken. Daardoor kan iedereen met de geschikte apparatuur en software aansluiten.[3]

2 Aan het internet liggen twee communicatie-standaarden/-protocollen ten grondslag, namelijk het Internet Protocol (IP) en het Transmission Control Protocol (TCP), samen aangeduid als TCP/IP. In het IP liggen vast: 1) ieder knooppunt op het internet heeft een internetadres, 2) alle berichten worden verdeeld in informatie-pakketjes, 3) ieder berichtpakket wordt in een IP-envelop gestopt en 4) de buitenkant van de envelop bevat het adres van de verzendende computer en de geadresseerde(n). Direct boven op het Internet Protocol draait het TCP en andere protocollen. TCP verdeelt grote berichten onder in meerdere pakketten, voegt deze op de eindbestemming weer samen en heeft mogelijkheden om beschadigde pakketten te 'repareren'. Bang e.a. 1996, p. 13-19, Informatie van TNO medewerker.

Hoewel het internet op uiteenlopende manieren valt onder te verdelen, is voor deze studie het onderscheid naar de verschillende lagen van het internet relevant. Deze zijn:

- de applicatielaag van de internetdiensten zoals surfen, e-mailen, internettelefonie (Voice Over IP - VOIP), et cetera;
- de laag met essentiële diensten voor het functioneren van het internet zelf, waaronder het omzetten van een logisch internetadres zoals 'google.nl' naar een IP-adres;
- de transmissielaag die ten grondslag ligt aan het internetverkeer zoals diverse soorten netwerken, bekabeling et cetera.[4]

Deze lagen zijn onderling sterk met elkaar verweven.

Aannemelijk is dat de afhankelijkheid van de Nederlandse samenleving van het internet nog verder gaat toenemen. De mogelijkheden zijn vrijwel onbegrensd en er komen dagelijks nieuwe toepassingen bij waardoor het internet en de fysieke wereld steeds meer vervlochten raken. Zo is de Nederlandse overheid en zeker de Belastingdienst volop actief met het aanbieden van diensten via het internet. Ook groeien de infrastructuren van het internet, radio, telefonie en televisie verder naar elkaar toe. Een voorbeeld daarvan is telefonie via het internet en het op grote schaal aanbieden van televisie via het internet. Als een zogenaamde 'triple play'-aanbieder uitvalt heeft dit in potentie dus ook drie keer zoveel gevolgen. Daarnaast zal *remote access* van bedrijfsgegevens, besturingssystemen en het internet zelf nog verder toenemen. Illustratief is bijvoorbeeld de mogelijkheid om op enkele NS-stations toegang te verkrijgen tot het internet en de mogelijkheden om in vliegtuigen te kunnen internetten.
Ook de nieuwe ontwikkelingen op het gebied van mobiele telefonie (UMTS) spelen een rol, evenals de ontwikkeling van GPS, file-informatie en controlesystemen in auto's,[5] en virtueel artsenbezoek via webcams. De behoefte aan meer bandbreedte bij gebruikers groeit en leveranciers voorzien daar in. Als gevolg van bovenstaande ontwikkelingen nemen logischerwijze ook de mogelijkheden voor misbruik toe alsmede de complexiteit om daar wat tegen te doen. De ontwikkelingen zelf lijken sneller te gaan dan de aandacht voor de kwetsbaarheid van het internet.[6]

3 Weimann 2006, p. 16-20, Bang e.a. 1996, p. 13-36, Huizer 1998. Voor een uitgebreide geschiedenis van het internet, zie bijvoorbeeld http://www.isoc.org/internet/history/.
4 Thiele & Van Vliet 2005.
5 Luiijf 2006.
6 Dat laatste stellen Thiele & Van Vliet 2005.

2.2.3 Massale overbelastingsaanvallen

Cyberaanvallen tegen of via het internet zijn mogelijk door de computersystemen die websites en andere voorzieningen op het internet faciliteren over te belasten. Dit is te vergelijken met de situatie waarin iedereen in Nederland tegelijkertijd 112 zou bellen. Het telefoonnet zou overbelast raken en de alarmdienst zou onbereikbaar worden. Op het internet kan men een dergelijk effect bereiken door grote hoeveelheden op internet aangesloten computers tegelijkertijd een website - of willekeurig welke andere online dienst - te laten bevragen. De meest gebruikte methode voor deze massale

bevraging is dat individuele of georganiseerde personen zich op volledig geautomatiseerde wijze via het internet onrechtmatig de toegang verschaffen tot vele duizenden computers (soms wel honderdduizenden). Dit gebeurt dikwijls zonder medeweten van de eigenaars van die computers die in sommige gevallen hun computers niet goed hebben beveiligd. De computers waarover de controle is verkregen, kunnen vervolgens als één wapen worden ingezet. Dit noemt men een 'botnet', een netwerk van gehackte computers (robotjes).

Bij massale overbelastingsaanvallen wordt doorgaans gesproken over (de verzamelnaam) DoS-aanvallen.[7] Dergelijke aanvallen vonden en vinden zeer regelmatig plaats en zijn soms succesvol. In februari 2000 werden websites als 'Amazon.com', 'e-Bay' en 'Yahoo!' enkele uren uitgeschakeld.[8] In Nederland zijn sites als 'regering.nl' in oktober 2004 getroffen door dergelijke aanvallen. Naar schatting worden er 4000 overbelastingsaanvallen per week ondernomen.[9] Er zijn veel programma's in omloop waarmee een DoS-aanval kan worden uitgevoerd en daarbij wordt gebruik gemaakt van de hierboven beschreven zombies of bots, die samen een botnet kunnen vormen. Een dergelijk botnet kan ook uit zichzelf doorgroeien door automatisch andere kwetsbare computers te lokaliseren en te besmetten. Dit heeft een groter effect, omdat er meer computers zijn die tegelijkertijd contact zoeken met een bepaalde server. Het is ook moeilijker om de aanvaller te lokaliseren omdat het programma niet rechtstreeks draait vanuit de computer van de aanvaller. Dit neemt niet weg dat een aanvaller uiteindelijk te traceren is.

DoS-aanvallen zijn gericht op aantasting van de beschikbaarheid van het internet. Naast DoS-aanvallen kunnen ook virussen en wormen voor dergelijke ontwrichting van het internetverkeer zorgen. De laatste tijd is minder vaak sprake van grote uitbraken van virussen. Dit neemt niet weg dat er sprake is van een gevaar. De geavanceerde virussen (en andere kwaadaardige software of *malware*) lijken minder gericht op ontwrichting van het gehele internetverkeer en aantasting van de beschikbaarheid , maar meer op het aanrichten van gerichte schade of diefstal van gegevens: aantasting van de betrouwbaarheid en integriteit van het internet en online gegevens-(uitwisseling). De huidige dreiging voor overbelastingsaanvallen lijkt daarmee met name van DoS-aanvallen te komen.

2.2.4 Gerichte hacking

Hacking is een veelomvattende term voor het inbreken op computersystemen of netwerken. Hacken kan plaatsvinden door middel van verschillende technieken, waaronder het raden van wachtwoorden, het uitbuiten van beveiligingslekken in software of het gebruik maken van slecht geconfigureerde computersystemen.
Om een *gerichte en serieuze* hackpoging te laten slagen is diepgaande kennis nodig van bestaande systemen en ICT-beveiliging. Vaak zal een specifieke hackertool geschreven moeten worden om het beoogde doel te bereiken, en is veel voorverkenning, toewijding en volharding nodig. Het is dus zeker niet zo, dat een beveiligd systeem op een achternamiddag kan worden overgenomen. Er zijn bovendien de nodige ontdekkingsmomenten voor systeembeheerders doordat hackers toch een tijd moeten rondddolen en daarbij sporen achterlaten.

7 Er zijn verschillende typen te onderscheiden: 1) de Denial of Service attacks (DoS aanval), 2) Distributed Denial of Service Attack (DDoS-aanval) en 3) Distributed Reflection Denial of Service (DRDoS-aanval). Met een DRDoS-aanval worden de netwerkinfrastructuurservers (die het wereldwijde internetverkeer beheren) bij een aanval betrokken. Deze servers worden niet overgenomen of geïnfecteerd zoals de zombies, maar benut als doorgeefluik ten behoeve van accumulatie. Dit betekent dat de enorme serverparken van zoekmachines als Google en Yahoo onbewust betrokken kunnen raken bij een dergelijke aanval. Dit type aanvaller is nog lastiger te lokaliseren en te detecteren, zoals wordt besproken in Gibson 2002.
8 Weimann 2006, p. 157.
9 Benschop 2006b.

2.2.5 Computerkennis en -vaardigheden van jihadisten

Over het geheel gezien lopen jihadisten verre van achter op het Westen ten aanzien van het gebruik van computers en het internet. Noemenswaardig is bijvoorbeeld dat Khalid Sheik Mohammed (een planner van de aanslagen op 11 september 2001) gechat heeft met aanslagplegers[10] en dat Ramzi Yousef (verantwoordelijk voor de eerste aanslag op het WTC in 1993) al geavanceerde encryptie gebruikte.[11] De aanslagplegers van 11 september 2001 en Madrid in 2004 hebben op slimme wijze gebruik gemaakt van de mogelijkheden die computers bieden, bijvoorbeeld door te werken met het concept van de e-mail *dead-letter box*. Door een hotmail-account aan te maken waarvan meerdere gebruikers het wachtwoord hadden, konden concept-mailberichten worden achtergelaten in de concept- of *draft*-folder, die iedere bezitter van het wachtwoord kon inzien en wijzigen. Dit maakte het risico op ontdekking klein. Daarnaast beheersen de jihadisten onder andere de kunst van het voeren van propaganda via het internet als geen ander. De daarvoor benodigde algemene computervaardigheden zijn ruimschoots voorhanden. Sterker nog, voor deze activiteiten zetten zij vaardigheden in die te scharen vallen onder 'basic' hacking: het kapen van webruimte en websites om het eigen, jihadistische materiaal te promoten.[12] Al met al kan dus zeker worden gesteld dat terroristische groeperingen en jihadisten over kennis beschikken als het gaat om computergebruik en over de middelen. Maar zijn er, naast het hacken met als oogmerk propaganda, nog andere voorbeelden waaruit zou kunnen blijken dat jihadisten beschikken over kennis en middelen van het hacken en er oog voor hebben?

Er zijn diverse voorbeelden bekend van hackergroepen die illustratief zijn in het kader van de virtuele jihad. Er zijn bijvoorbeeld hackergroepen die zich verbonden hebben verklaard met al Qa'ida of de wereldwijde jihad. Deze hackergroepen hebben namen als de *Qaeda Alliance Online* - sinds 9/11 -, de *OBL Crew*, de *Islamic Hackers* en de *Afghan Hackers*.[13] De *World's Fantabulous Defacers* (WFD) hebben tussen 20 november 2001 en 21 maart 2002 334 geregistreerde *defacements* op hun naam gezet, vanuit een pro-Palestijns perspectief. Vooral de verkiezingscampagne-site van Ariel Sharon lag onder vuur. Na een geslaagde defacement werd Sharon als misdadiger gepresenteerd en werden gruwelijke foto's van een kind met littekens geplaatst.[14] Verder zijn er vooral veel hackingactiviteiten geweest tussen pro-Israëlische en pro-Palestijnse hackers.[15] Na 9/11 is er uit naam van Bin Laden gehacked door verschillende hackers.[16] Ondanks dit voorbeeld en de waarschuwingen voor cyber- en hackingaanvallen na 9/11 en met name na de invallen op Afghanistan, was er geen bewijs van een toename van hackingactiviteiten.[17]

10 CRS 2005a, p. 18.
11 Benschop 2006b.
12 Zie voor propaganda hoofdstuk 3, paragraaf 3.4.
13 Weimann 2006, p. 170.
14 Bunt 2003, p. 45.
15 Bunt 2003, p. 48 e.v.
16 Bunt 2003, p. 54.
17 Bunt 2003, p. 55.

Op jihadistische websites wordt de nodige aandacht besteed aan hacken. De *Muslim Hackers Club* - hun website is overigens sinds 1999 niet meer geactualiseerd - had een virus tutorial voor hackers. Het bevatte standaard hacking-tools die toevallig in een cyberislamitische omgeving te vinden waren. Uit een discussie op die site destijds spreekt overigens niet dat er agressief gehacked moet worden.[18] Ook in andere chatrooms is discussie over hacken. Mag het van de islam? Is het crimineel? Bezoekers en de administrator maken zich zorgen over de criminele kanten en het risico om gepakt te worden (waarvan voorbeelden worden genoemd).[19] Verder bevatten veel jihadistische fora een onderdeel dat 'elektronische jihad' heet, waar - naast het voeren van een propaganda-oorlog - hackingmethodes besproken worden.[20] Specifieke doelen die op aan al Qa'ida gerelateerde websites zijn besproken waren de Amerikaanse Centers for Disease Control and Prevention in Atlanta, FedWire (electronisch geldverkeer) en faciliteiten die de informatiestroom via het internet regelen.[21]

Figuur 2.1 Een voorbeeld van aandacht voor hacken

Islam Online produceerde een online fatwa die aangaf dat hacking alleen mag als je (via hacking) zélf aangevallen wordt.
Het aanvallen van websites met islam-vijandige content is weer wel toegestaan volgens een andere fatwa, ontdekt in 2002: "if [...] websites are hostile to Islam and you could encounter its evilness with goodness; And respond to it, refute its falsehood, and show its void content; that would be the option. But if you are unable to respond to it, and you wanted to destroy it and you have the ability to do so, it's ok to destroy it because it is an evil website."
Na deze laatste fatwa werden FBI en Pentagon-sites aangevallen door Saoedische hackers.[22]

Het Global Islamic Media Front (GIMF) is intussen begonnen met het formaliseren en verspreiden van een 74-pagina's omvattend compendium van hacking-methodes en -mogelijkheden. Het nieuwe GIMF-compendium (mede gebaseerd op werk van de in het Verenigd Koninkrijk gearresteerde jihadistische hacker Irhabi007) bevat tevens de gecomprimeerde bestanden van software die nodig is om wachtwoorden te kraken en veiligheidslekken te ontdekken. Het compendium wordt actief via jihadistische fora en websites verspreid.
Op de bij het compendium gevoegde lijst met kwetsbare sites bevindt zich ook een Nederlandse site.[23] Bij dit compendium zijn twee kanttekeningen te plaatsen. Ten eerste is het materiaal verouderd. Dit neemt echter niet weg dat sommige computers, netwerken en websites nog steeds kwetsbaar zijn voor deze technieken. Ten tweede, en zwaarwegender, is dat het compendium gericht is op het benutten van zwakheden in netwerken en websites om materiaal (gratis) te kunnen plaatsen en verspreiden. Welbeschouwd valt dit compendium dan ook onder 'propaganda'. Dit neemt niet weg dat de brede verspreidingsgraad die het materiaal ongetwijfeld zal bereiken door de activiteiten van het GIMF, andere geradicaliseerde of jihadistische personen kan inspireren om verder te gaan dan hacking ten behoeve van verspreiding van materiaal. Ditzelfde geldt voor het mogelijke effect van de specifieke onderdelen op jihadistische webfora.

18 Bunt 2003, p. 38-39.
19 Bunt 2003, p. 45.
20 Rogan 2006.
21 Weimann 2006, p. 113.
22 Bunt 2003, p. 46, Weimann 2006, p.122.
23 Site Institute 2006b.

Als de jihadisten over onvoldoende kennis en middelen zouden beschikken voor het hacken - hoewel er geen aanleiding is om dat te veronderstellen - zouden zij hackingdeskundigheid kunnen inhuren. Ten aanzien van het samenwerken met niet-jihadistische hackers is een poging in 1998 van de Pakistaanse Harkat-ul-Ansar organisatie (volgens de VS gelieerd aan Osama Bin Laden) om software te kopen van hackers, vermeldenswaardig.[24] Vooral in de voormalige Sovjet-Unie en op het Indiase Subcontinent zijn vele hoogopgeleide ICT-specialisten beschikbaar om in te huren, waarbij een deel van deze specialisten moeite heeft om op legale manieren aan betaald werk te komen.[25] Dergelijke 'huurlingen' weten vaak niet door wie ze zijn ingehuurd of naar welk doel ze werken. Échte hackers gaat het om de uitdaging, en niet om de achtergrond van degene die hen uitdaagt tot iets wat eigenlijk onmogelijk zou moeten zijn. Het digitaal inbreken bij een firma als Boeing en blauwdrukken of andere informatie over vliegtuigen ontfutselen kan dan de ultieme uitdaging zijn. De vraag wie daarvoor interesse heeft (en of diegene is wie hij zegt te zijn) is veel minder interessant. En zeker voor jonge hackers is het moeilijk om onderscheid te maken tussen de verschillende personen die interesse hebben in hun vaardigheden.[26] Voor de meer criminele hackers is het overigens puur 'business'.[27] Ook is het voorstelbaar dat hackers activiteiten uitvoeren voor een terroristische organisatie, omdat zij geaccepteerd willen worden door de organisatie, omdat zij het - in algemene zin - eens zijn met de (bijvoorbeeld anti-Amerikaanse of antiwesterse) denkbeelden van deze organisatie of omdat zij langs die weg wraak kunnen nemen op bijvoorbeeld ex-werkgevers of bepaalde bedrijven. Dergelijke hackers hoeven dan ook niet per definitie aan een standaardprofiel te voldoen, maar kunnen ook andere sympathieën hebben.[28]
Toch blijft het de vraag of de gemiddelde hacker daadwerkelijk wil bijdragen aan terroristische activiteiten. Een rapport uit 1999 beweert in ieder geval dat hackers psychologisch en organisatorisch niet 'geschikt' zijn voor terrorisme[29] en uit een gedocumenteerd voorbeeld blijkt dat sommige hackers zich na september 2001 met grote zorg afvroegen of ze niet onbewust hadden meegewerkt aan de aanslagen in de VS, aangezien zij zich hadden laten uitdagen om zich toegang te verschaffen tot specifieke informatie uit de luchtvaartindustrie.[30]

24 Benschop 2006b.
25 Wilson 2006, p. 84.
26 Mitnick 2006, p. 23-47.
27 Interview 2.
28 Interview 3.
29 Weimann 2006, p. 167, verwijzend naar Denning, Cyber-Terror: Prospects and Implications, 1999.
30 Mitnick 2006, p. 23-47.
31 CRS 2005b.
32 Wilson 2006, p. 78, zich baserend op Dan Verton in Black Ice, die put uit een CIA-brief aan de US Senate Select Committee on Intelligence uit april 2002.
33 Interviews 1 en 2.

Twee FBI-kopstukken geven aan dat de technische competenties van terroristen toenemen. Terroristen tonen bovendien aan meer kennis te hebben van de kritieke rol van informatietechnologie in de economie van de Verenigde Staten, en zouden hun rekrutering daarop afstemmen.[31] Al Qa'ida en Hezbollah raken steeds meer vertrouwd met het internet en computertechnologie en deze groepen zouden de intentie en de wens hebben om vaardigheden te ontwikkelen die nodig zijn voor een cyberaanval.[32]
De volgende generatie terroristen groeit op in de digitale wereld, maar dat geldt ook voor de systeembeheerders en overheidsorganisaties. Wie daarbij in het voordeel is, is op voorhand nog niet te voorzien, maar aannemelijk is dat terroristen flexibeler kunnen optreden, niet te maken hebben met lange besluitvormingslijnen en geduldig kunnen zoeken naar fouten. Terroristische organisaties beschikken daarnaast over moderne apparatuur.[33]

2.3 HET INTERNET ALS DOELWIT

2.3.1 Toelichting

Onze samenleving wordt steeds afhankelijker van het internet. Deze afhankelijkheid en daarmee kwetsbaarheid zouden jihadisten op het idee kunnen brengen om het internet zelf als doelwit te kiezen voor terroristische activiteiten. Dat kan verschillende vormen aannemen:

- Een cyberaanval door gebruikmaking van computers via het internet. Het internet is in dat geval zowel doelwit als wapen: het internet keert zich tegen zichzelf.
- Een fysieke aanslag door gebruikmaking van conventionele wapens of door sabotageacties van binnen uit tegen (kern)knooppunten, kernfunctionaliteiten en verbindingslijnen of de organisaties die diensten verlenen die cruciaal zijn voor het functioneren van het internet.
- Een elektromagnetische aanslag door het gebruik van bijvoorbeeld elektromagnetische energie (EMP) tegen (kern)knooppunten, kernfunctionaliteiten en verbindingslijnen.
- Indirecte aanslagen of aanvallen bijvoorbeeld tegen de elektriciteitsvoorziening of koelvoorzieningen waardoor (de infrastructuur van) het internet niet kan functioneren.[34]

Omdat deze fenomeenstudie zich richt op het internetgebruik door jihadisten, ligt de focus op de cyberaanval met een terroristisch oogmerk. Dit behoeft wel een verdere afbakening. Cyberaanvallen die dienen om een politiek statement te maken (het zogeheten *hacktivisme*) vallen hier buiten. Noch de intentie, noch de gevolgen vallen binnen de definitie van terrorisme. Voor dergelijke aanvallen is wellicht de term 'Weapon of Mass Annoyance' geëigend.[35]

Figuur 2.2 Voorbeelden van hacktivisme

In 1997 is de serviceprovider van de ETA, gevestigd in San Fransisco, met e-mails gebombardeerd om te zorgen dat ze web-pagina's van de ETA offline zouden halen (hetgeen een paar dagen later ook gebeurde).[36]
Na de zogeheten Deense cartoon-kwestie vond defacing van Deense websites plaats waardoor ook Deense overheidssites onbereikbaar werden.

2.3.2 Mogelijkheden cyberaanvallen, kwetsbaarheden en weerbaarheid

Het internet is oorspronkelijk ontworpen als een netwerk van computers dat immuun moest zijn voor vijandige aanvallen en in ieder geval niet tijdens één aanval, of door een sabotage op één locatie plat gelegd zou kunnen worden. Desondanks kent het internet uiteraard kernknooppunten, kernverbindingen en kernfunctionaliteiten die het internet wel degelijk een zekere mate van kwetsbaarheid geven. Een potentiële kwetsbare plek voor cyberaanvallen zijn de *Domain Name Servers* (DNS-servers). Deze fungeren als het ware als omgekeerde telefoongidsen: ze zoeken de unieke IP-nummers op die horen bij computers, internet- en e-mailadressen. Hierbij is sprake van een gelaagde opbouw met aan de top dertien rootservers voor het zogenaamde IPv4-protocol en vijf voor het nieuwere protocol IPv6 evenals vele duplicaten daarvan. Een beperkt aantal bevindt zich in Nederland.[37] Er is ook een DNS-server voor het Nederlandse domein en binnen Nederland (evenals in andere landen) hebben providers en grote organisaties hun eigen DNS-server(s). Een andere potentieel kwetsbare plek zijn de zogenaamde Exchanges. Deze zouden we kunnen vergelijken met een groter spoorwegstation. In een station komen vele spoorlijnen samen en kunnen reizigers vanuit diverse richtingen overstappen en een nieuwe richting kiezen. Bestemmingen kunnen echter ook via andere routes worden bereikt. Het station beschikt over de voorzieningen om de reizigersstromen in goede banen te leiden en de verkeersleiding zorgt voor de daadwerkelijke transportbewegingen. Een belangrijke exchange in Nederland is de AMS-IX (Amsterdam Internet Exchange) die zeker een Europese, maar ook mondiale rol vervult. Verder zijn er vier andere exchanges in Nederland.[38] Verder zijn in dit kader nog te noemen de Internet Service providers, KPN en andere telecom- en kabeldienstverleners waarvan de telefoon- of kabelinfrastructuur wordt gebruikt voor het internetverkeer.

De bovengenoemde kwetsbare punten raken vooral de beschikbaarheid van het internet en de eerdergenoemde laag van essentiële diensten en de transmissielaag (zie paragraaf 2.2.2). De applicatielaag wordt door zoveel professionele partijen geleverd dat een totale uitschakeling daarvan nauwelijks reëel te noemen is, terwijl bij uitschakeling van die andere twee lagen ook de applicatielaag niet langer kan functioneren.

Het internet kan ook indirect worden getroffen door het vertrouwen daarin te ondermijnen. Wanneer bijvoorbeeld gedurende enkele dagen van de ene na de andere bank het digitaal bankieren zou worden uitgeschakeld en daar ook nog eens de nodige publiciteit aan zou worden besteed (jihadisten hebben aangetoond daarin zeer bedreven te zijn), dan ondermijnt dat het vertrouwen. Dit element wordt echter beschouwd als aspect van 'het internet als wapen' en zal derhalve in de volgende paragraaf worden behandeld.

Hoewel er potentieel meer aanvalsvormen denkbaar zijn, zal een cyberaanval toch vooral met behulp van de eerder genoemde typen DOS-aanvallen plaatsvinden. Voor zover bekend heeft er één DDoS-aanval plaatsgevonden die écht forse impact heeft gehad op de infrastructuur van het internet. Deze vond plaats op 21 oktober 2002 en was gericht tegen de genoemde DNS-rootservers die het wereldwijde internetverkeer regelen. Zeven van de dertien knooppunten zouden onder de aanval zijn bezweken, en twee servers zouden hebben gehaperd. Technisch gesproken was de aanval mislukt: pas als acht of meer van de DNS-servers bezwijken, wordt de overlast groot. De schaal waarop deze aanval werd uitgevoerd, is tot nu toe ongeëvenaard. Echter, het feit dat kennelijk slechts zes procent van de verzoeken aan de domeinnaamdienst niet beantwoord werden,[39] geeft aan dat de oorspronkelijk voor het internet beoogde robuustheid en mogelijkheden voor het omleiden van dataverkeer gestand werden gedaan. Overigens zijn er geen aanwijzingen dat deze aanval met een terroristisch oogmerk is uitgevoerd. Verder heeft men internationaal inmiddels ruim-

34 CRS 2005a, p. 3, Dasselaar 2006, Planet.nl 2006a, Planet.nl 2006b, Planet.nl 2006c, Nu.nl 2006b, Kwint 2004.
35 Lewis 2002, p. 4.
36 Benschop 2006b.
37 Bron: TNO.
38 Bron voor opsomming exchanges: TNO.
39 Benschop 2006b en http://www.cs.cornell.edu/people/egs/beehive/rootattack.html.

schoots maatregelen getroffen waardoor dit type aanval tegen de rootservers nu niet meer op die manier kan plaatsvinden.[40]

Om bijvoorbeeld een succesvolle DDoS-aanval tegen het internet uit voeren - al dan niet om een land vergaand te isoleren - is een enorm leger bots nodig. Op zich is het relatief eenvoudig en voordelig om via online-handel aan een leger 'bots' te komen.[41] Een prijsindicatie van een dergelijke aanbieding is: 250 dollar voor het huren van 5.000 'voorgeïnfecteerde' machines en soms zelfs grotere aantallen. Het verkrijgen, aanpassen of zélf schrijven van de benodigde kwaadaardige code om een eigen zombie-leger te creëren is betrekkelijk eenvoudig. Op het internet zijn volop tools verkrijgbaar, naar verluidt op ongeveer 400.000 sites.[42] Aanvalslegers zijn dan ook betrekkelijk eenvoudig te creëren of te huren en goed bruikbaar voor personen met gemiddelde vaardigheden.

Hoe kwetsbaar is het internet voor cyberaanvallen? Allereerst geldt natuurlijk dat het internet ooit was bedoeld om aanvallen te kunnen weerstaan. Zo is het internet flexibel in het opvangen van aanvallen: er vindt snel re-routing van pakketten plaats en computers kunnen bij uitval van bijvoorbeeld DNS-servers altijd nog blijven communiceren via IP-adressen. Een DDoS-aanval is niet alleen te pareren door deze snel als zodanig te herkennen met behulp van slimme detectiemethoden, maar ook door het vergroten van servercapaciteit en uitbreiding van het aantal knooppunten. Het uitvoeren van een aanval tegen het internet als geheel is complex. Ten tijde van het schrijven van deze studie is het internet nog nooit volledig uitgeschakeld geweest. De voorbeelden die wel bekend zijn van kleine aanvallen op delen van de infrastructuur, zijn niet toegewezen aan terroristen. Een oefening waarin een massale aanval op de informatie-infrastructuur van het internet werd nagebootst in de VS in juli 2002 onder de naam Digital Pearl Harbor, leidde tot betrekkelijk geruststellende resultaten. Volgens een verslag van die oefening zou voor een succesvolle aanval nodig zijn: "a syndicate with significant resources, including $200 million, country-level intelligence and five years of preparation time".[43] De drempel voor een dergelijke aanval ligt dus hoog.

Toch bestaan er wel degelijk kwetsbaarheden. Zo kunnen delen van de periferie van het internet uitvallen aangezien daar het aantal verbindingen beperkt en de redundantie dus minder groot is. Een gebrek aan transparantie en inzicht bij overheid, aanbieders en gebruikers vergroot het risico van een onvermoed gebrek aan redundantie.[44] Het mondiaal uitschakelen van het internet lijkt echter niet reëel. Daarvoor is het internet te robuust en heeft men geleerd van eerdere aanvallen.[45]

Is het 'Nederlandse internet' meer of minder kwetsbaar voor cyberaanvallen? Hoewel het internet per definitie mondiaal is en het daardoor lastig is om Nederland afzonderlijk te bezien, kan je tot op zekere hoogte wel degelijk spreken van het Nederlandse deel van het internet. Zo is het internet in Nederland deels afhankelijk van de DNS-server die het '.nl-domein' beheert.

40 Expertmeeting.
41 CRS 2005a, p. 20.
42 Interview 2 en Bunt 2003.
43 Weimann 2006, p. 168, onder verwijzing naar een verslag van CNET.com.
44 Kwint 2004, p. 6, Thiele & Van Vliet 2005.
45 Expertmeeting.

Door alle .nl-domeinnamen onbereikbaar te maken vallen alle op .nl eindigende e-mailadressen, websites en onder .nl aangeboden diensten uit. Diverse experts concluderen dat er intussen een dergelijk groot aantal klonen van DNS-rootservers wereldwijd en in Nederland zijn, dat de kans op het uitvallen van grote delen van DNS in Nederland (zowel wat betreft de beschikbaarheid van de .nl-domeinen als de mogelijkheid voor Nederlandse surfers het web te gebruiken) relatief klein is.[46] Bovendien blijven websites en e-mailadressen met een andere extentie, bijvoorbeeld .com, .org en .net, nog functioneren. Voor een isolerende aanval van het .nl-domein zou een voorbereidingstijd nodig zijn van tenminste een half jaar en is vooral veel kennis nodig: de locaties en systemen moeten van tevoren worden verkend.[47] Verder zouden de routers kunnen worden overbelast, maar dat vergt veel kennis en er is sprake van redundantie. Hooguit zouden providers kunnen worden getroffen die hun zaakjes niet op orde hebben. Bij een cyberaanval zal sprake zijn van een geleidelijke uitval. Eventuele aanvallen zien de providers daarom gebeuren. De Computer Emergency Response Teams (CERTs) hebben onderling contacten en kunnen snel tegenmaatregelen treffen. Aan de ene kant maakt de hoge penetratie van het internet in Nederlandse huishoudens en organisaties Nederland extra kwetsbaar ten opzichte van andere landen. Gebruikers treffen lang niet altijd adequate beveiligingsmaatregelen, waardoor ze betrokken kunnen raken bij een botnet. Aan de andere kant zijn er in Nederland zoveel dienstverleners die cruciaal zijn voor het functioneren van het internet, dat Nederland daardoor weer minder kwetsbaar is voor geslaagde cyberaanvallen. Het platleggen van het Nederlandse deel van het internet lijkt al met al niet reëel, hoewel het iets reëler is dan het uitschakelen van het gehele internet.[48]

Wel denkbaar is een mix van speldenprikken die symbolisch pijn doen en het vertrouwen in het internet aantasten. Dat kan bijvoorbeeld doordat terroristen enkele malen bepaalde onderdelen van het internet niet of minder goed laten functioneren. Ook een relatief klein succes zou als succes kunnen worden beschouwd en breed worden uitgemeten. Een dergelijke kleine aanval raakt dan niet zozeer de beschikbaarheid, maar vooral het vertrouwen in het internet. Daar moet dan wel een gerichte strategie achterzitten (zie verder paragraaf 2.3.7) en bovendien is discutabel of het in het laatste geval wel gaat om een terroristische activiteit. Eerder zou het moeten worden beschouwd als een niet-terroristisch wapen in een asymmetrische strijd. Het is immers helemaal niet zeker dat de samenleving wordt ontwricht wat wel het uitgangspunt is om iets als terroristische activiteit te bestempelen. Verder is denkbaar dat jihadisten (eventueel vanuit Nederland) proberen cyberaanvallen te plegen tegen overheden in de brandhaarden in de wereld. In het Midden Oosten is bijvoorbeeld de redundantie in het internet veel minder groot.[49]

De afhankelijkheid van het internet zal de komende jaren verder toenemen door nieuwe toepassingen zoals telefonie en televisie en meer bandbreedte (zie paragraaf 2.2.2). Daardoor neemt ook de kwetsbaarheid verder toe.

46 Kwint 2004, p. 4-5, ook interview 3.
47 Interview 2.
48 Expertmeeting.
49 Expertmeeting.

2.3.3 Intentie van jihadisten bij cyberaanval

De intentie van de jihadisten om het internet als doelwit te kiezen is ingesloten in de definitie van terrorisme, namelijk om maatschappelijke veranderingen te bewerkstellingen of politieke besluitvorming te beïnvloeden. Uiteraard kan dat op vele en uiteenlopende wijzen en de vraag is daarom relevant waarom ze zich nu juist op het internet zouden willen richten en wel met een cyberaanval. Waarom zou dat aantrekkelijk zijn? Veelal wordt immers gesteld dat het de jihadistische terroristen vooral te doen is om zoveel mogelijk onschuldige slachtoffers te creëren en dat de activiteiten angst moeten aanjagen. Zijn daar niet betere manieren voor dan een cyberaanval?

Hoofdargumenten waarom het internet als doelwit aantrekkelijk is voor jihadisten met behulp van een cyberaanval zijn:

1. Dit type aanval past binnen de algemene strategie van al Qa'ida. Een cyberaanval kan in potentie resulteren in grote economische schade en past daarmee in de strategie van al Qa'ida, waar ook economische doelen voorop staan, zoals onlangs nog bevestigd door al-Zawahiri.[50] Bin Laden heeft in een van zijn vele toespraken gezegd: "America [...] needs further blows. The young men need to seek out the nodes of the American economy and strike the enemy's nodes".[51] Gelet op het huidige dreigingsbeeld is voorstelbaar dat jihadisten ook economische doelen anders dan in de Verenigde Staten willen raken. Bovendien zijn er signalen dat strategen van al Qa'ida het internet als strategisch veld hebben ontdekt.
2. Een cyberaanval sluit goed aan bij een asymmetrische strijd. Bijvoorbeeld DDoS-aanvallen worden uitgevoerd met beperkte bronnen tegen een groot, geavanceerd computersysteem. Dit is een zogeheten 'asymmetrische aanval', die qua strategie vergelijkbaar is met het plegen van een zelfmoordaanslag tegen de onderdrukker die over een grote legermacht beschikt.[52] In principe zou één jihadistische hacker in staat zijn om een natie tijdelijk of gedeeltelijk te ontregelen.
3. Het psychologische effect als gevolg van de onvoorspelbaarheid van een cyberaanval is groot. Gezien de complexiteit van het internet is niet goed voorspelbaar en voorstelbaar wat de effecten kunnen zijn, waardoor ontwrichtende consequenties niet volledig kunnen worden uitgesloten. Zo is de uiteindelijke omvang van een zombie-netwerk bijvoorbeeld niet altijd te overzien.[53] Vooraf bestaat daardoor altijd de onzekerheid of er afdoende maatregelen zijn getroffen tegen een dergelijke aanval en die onvoorspelbaarheid heeft ook een psychologisch effect.
4. De combinatie van het onbekende van cyberspace en terrorisme vergroot de psychologische angst. De onbekendheid met de (on)mogelijkheden van computers en het internet om aanslagen te plegen of de maatschappij te ontwrichten is een factor die bij velen angst aanjaagt. Computers en het internet worden nog steeds gewantrouwd en spookverhalen staan garant voor 'cyberfear'. Daarom zullen ook plaagstoten een verhoudingsgewijs grote impact kunnen hebben.

50 NCTB 2006A.
51 Weimann 2006, p. 45.
52 Interview 6.
53 Interviews 2 en 6. Dit bleek ook in het geval van de Nederlandse scheppers van een dergelijk netwerk voor criminele doeleinden.

5. Jihadisten kunnen gebruik maken van de vele berichten over de kwetsbaarheden van het internet. Juist de vele berichtgeving over kwetsbaarheden van het internet hebben terroristen op het spoor gezet dat de (westerse) economie een doelwit kan zijn en bieden handreikingen voor een effectieve aanslag.[54]
6. Een cyberaanval tegen het internet heeft enkele operationele voordelen. Er is bijvoorbeeld geen sprake van eigen verliezen, zoals bij een zelfmoordaanslag. Computers, internettoegang en hacking-tools zijn voor iedereen bereikbaar en aanzienlijk eenvoudiger beschikbaar dan wapens of explosieven. De terroristen kunnen verder de tijd, de locatie en de omstandigheden zelf bepalen en op afstand opereren: het is een slimme bom die bovendien lastig te detecteren is en op afstand (zelfs vanuit een ander land) kan worden bediend wat de ontdekking en arrestatie bemoeilijkt. Het (relatief) anonieme karakter bemoeilijkt de ontdekking en arrestatie van de aanslagpleger. De pakkans is in vele landen relatief laag omdat het daar ontbreekt aan cybercrime-wetgeving en voldoende kennis bij de politie.
7. Een cyberaanval is laagdrempeliger dan een gewone aanslag en zeker laagdrempeliger dan een zelfmoordaanslag. Hoewel het terroristen er om te doen is zoveel mogelijk slachtoffers te creëren of schade te berokkenen, werpt dit toch een drempel op. Uit onderzoek onder militairen is bijvoorbeeld gebleken dat een groot percentage als het er op aankomt anderen niet durft te doden. Ook oplichting via het internet wordt als laagdrempeliger ervaren dan oplichting via de telefoon of op basis van fysiek contact. En hoewel menig jihadist in woord het martelaarschap nastreeft en goedkeurt, bestaat er wel degelijk een grote kloof tussen woord en daad. Een cyberaanval is wat dat betreft psychisch veel eenvoudiger uitvoerbaar dan een zelfmoordaanslag of een andere aanslag waarbij grote aantallen doden en gewonden vallen door het eigen handelen.[55]

Niet alleen zijn er argumenten vóór, er zijn ook argumenten tégen:

1. De effecten van een cyberaanval zijn onvoorspelbaar. Ook voor de aanvallende partij kan de onvoorspelbaarheid problemen opleveren, bijvoorbeeld waar het gaat om sneeuwbal- of neveneffecten. Zo hebben in 2000 Palestijnse hackers Israëlische ISP's succesvol uit de lucht gehaald. Later bleek dat ook de site van de Palestijnse autoriteit door deze actie onbereikbaar werd.[56] Hoewel in potentie de economische schade groot kan zijn, is de werkelijke schade slecht voorspelbaar. Dit mede doordat het internet robuust is en juist ontworpen is om klappen op te vangen.[57]
2. Een cyberaanval levert geen spectaculaire beelden op. Een cyberaanval levert geen spectaculaire beelden op van rokende puinhopen, doden en gewonden. Dit in tegenstelling tot bijvoorbeeld zelfmoordaanslagen.
3. Een cyberaanval is niet in het belang van terroristen. Terroristen snijden zich in de vingers gelet op hun intensieve gebruik van het internet voor andere doeleinden. Zij hebben zelf belang bij een goed functionerend internet. Daar is overigens tegen in te brengen dat terroristen zich hierover wellicht niet veel zorgen maken en dergelijke consequenties voor lief nemen om een hoger doel te bereiken. Al Qa'ida zal er ook rekening mee hebben gehouden dat de aanslagen in 2001 gevolgen zouden hebben voor hun eigen bewegingsvrijheid.

54 CRS 2005b, p. 4.
55 Expertmeeting.
56 Bunt 2003, p. 46.
57 Weimann 2006, p. 168.

4. Een cyberaanval vergt een lange voorbereidingstijd, is complex en wordt bemoeilijkt door de dynamiek van het internet. Een cyberaanval vergt een strategische visie, training en beschikbaarheid van geld en middelen. Daartegen is in te brengen dat ook de aanslagen van 11 september 2001 een lange voorbereidingstijd kenden en training vergden. Een belangrijk verschil is echter wel dat gebouwen lange tijd staan en een lange voorbereidingstijd dus geen probleem vormt. De dynamiek van het internet is daarentegen zodanig dat de voorbereiding wel eens achterhaald zou kunnen zijn tegen de tijd dat de aanval staat gepland als gevolg van de ontwikkelingen. Dit neemt niet weg dat terroristische organisaties in het algemeen hebben aangetoond een groot aanpassingsvermogen te kennen.
5. Het gebruik van het internet laat sporen na. Hoewel er vele mogelijkheden bestaan om anoniem te opereren op het internet, laat het gebruik van het internet toch sporen na en is daardoor de anonimiteit slechts relatief. Zij die bijvoorbeeld actief zijn met kinderporno op het internet gebruiken geavanceerde technieken om anoniem te blijven. Gelukkig voor opsporingsinstanties is een foutje snel gemaakt en kunnen zij tot op heden nog wel degelijk worden opgespoord, mede door intensieve internationale samenwerking op dit terrein. Er is geen reden om aan te nemen dat dit niet geldt voor terroristisch gebruik.
6. Een cyberaanval past niet bij het streven naar het martelaarschap van jihadisten. Hoewel dit zeker zo is, valt daar het eerder genoemde argument tegen in te brengen dat een cyberaanval laagdrempeliger is waardoor potentieel meer (ook jonge, onervaren) jihadisten zich geroepen voelen om woorden in daden om te zetten.
7. De hoge weerstand maakt het geen aantrekkelijk domein. Iets aanvallen dat is ontworpen om aanvallen te overleven is een uitdaging, maar de hoge weerstand van het internet kan uiteindelijk ook zorgen dat jihadisten liever andere doelen kiezen.

2.3.4 Benodigde en beschikbare kennis en middelen cyberaanval bij jihadisten

In paragraaf 2.2 zijn twee methoden beschreven, namelijk massale overbelastingsaanvallen en gerichte hacking. Voor cyberaanvallen is de eerste methode de meest voor de hand liggende. Verder is aangegeven dat er voorbeelden van terroristisch computergebruik bekend zijn en dat ze beschikken over moderne apparatuur. Tevens is aangegeven dat er voorbeelden zijn van jihadistische hackers(groepen) en dat kennis over het hacken wordt verspreid via jihadistische websites. De focus ligt daarbij vooralsnog meer op het optimaal gebruik van het internet, dan op het aanvallen van het internet. Ook is gesproken over mogelijke samenwerking tussen terroristen en hackers.

Wanneer jihadisten zouden (kunnen) infiltreren binnen de internetbranche, dan zou dat de mogelijkheden voor een cyberaanval doen toenemen. Om echt effect te sorteren zouden zij dan bij de grote partijen moeten infiltreren. Dit lijkt weinig kans van slagen te hebben omdat de technici die over de juiste kennis beschikken erg close zijn en elkaar goed kennen. Vrij snel zou traceerbaar zijn wie iets op zijn geweten heeft.[58]

58 Expertmeeting.

2.3.5 Gevolgen cyberaanval

De kans dat er direct doden of gewonden vallen als gevolg van een cyberaanval op het internet is klein. Evenmin zullen er dieren omkomen of het milieu worden aangetast.[59] Het gaat immers om een aanval op computers en computernetwerken. Indirect zouden er wel doden en gewonden kunnen vallen wanneer bijvoorbeeld het telefoonverkeer via het internet komt stil te liggen en mensen in noodsituaties niet kunnen bellen, medici geen gegevens meer kunnen uitwisselen of ambulancediensten niet meer kunnen communiceren.[60] Niet aannemelijk is dat het dan zal gaan om grote hoeveelheden doden en gewonden.

Wanneer het internet niet meer zou functioneren, heeft dat grote economische schade tot gevolg. Door bijvoorbeeld alle .nl-domeinnamen onbereikbaar te maken, vallen alle op .nl eindigende e-mailadressen, websites en onder .nl aangeboden diensten uit. Bij abrupte uitval zou (stand eind 2003) direct maatschappelijk productieverlies ontstaan bij dienstenaanbieders op het internet van ruim één miljoen euro per dag, door het wegvallen van verkeersminuten en online advertenties. De noodzaak voor veel bedrijven en overheidsinstellingen om bij abrupte uitval direct om te zien naar een andere domeinnaam (en deze namen en e-mailadressen kenbaar maken) heeft 490 miljoen euro kosten tot gevolg.[61] GOVCERT.nl stelt echter dat deze, in feite indirecte, gevolgen niet goed zijn in te schatten.[62]

GOVCERT verwacht dat de immateriële gevolgen van een cyberaanval meer dan 40% van de Nederlandse bevolking raken en wellicht zelfs 75%.[63] De aard van de gevolgen en de mate waarin gevolgen zich manifesteren zijn uiteraard mede afhankelijk van de periode dat het internet niet functioneert. Wanneer het jihadisten daadwerkelijk zou lukken om het internet plat te leggen, dan is de verwachting dat het herstel weinig tijd vergt.[64] Uiteraard is dat afhankelijk van de situatie en de mate waarin de jihadisten er in zouden slagen om de aanval door te zetten.

2.3.6 Beoordeling dreiging cyberaanvallen

Alles afwegend beoordeelt de NCTb de dreiging van cyberaanvallen tegen het internet als laag. Een aanval op het mondiale of Nederlandse internet zélf wordt niet waarschijnlijk geacht. De belangrijkste argumenten daarvoor zijn dat de voordelen niet substantieel opwegen tegen de nadelen en dat een succesvolle cyberaanval niet echt tot de mogelijkheden behoort met name vanwege de grote weerstand en redundantie.

Hoewel een cyberaanval laagdrempeliger is dan bijvoorbeeld zelfmoordaanslagen, waardoor potentieel meer jihadisten daartoe zouden kunnen en willen overgaan, geldt als belangrijkste contra-argument dat het platleggen van het internet ook de jihadistische infrastructuur op het internet uitschakelt. Andere gewogen argumenten zijn dat andere aanslagen, zoals een bomaanslag in het openbaar vervoer, een groter effect sorteren en dat de gevolgen

59 Deze conclusie is mede ontleend aan Thiele & Van Vliet 2005.
60 Zie voor de indirecte gevolgen onder andere Planet.nl 2006b.
61 Stratix 2004, p. 1, Planet.nl 2006a, Planet.nl 2006b.
62 Thiele & Van Vliet 2005, p. 16-17.
63 Thiele & Van Vliet 2005, p. 18.
64 Expertmeeting.

van een cyberaanval weliswaar aanzienlijk kunnen zijn, maar garanties daarop (bezien vanuit terroristisch standpunt) zijn er niet. Als er een geslaagde aanval zou plaatsvinden, kunnen de gevolgen groot zijn, met name de economische gevolgen, maar niet aannemelijk is dat het internet voor lange tijd niet zou functioneren. Er zijn mogelijkheden voor cyberaanvallen en kwetsbaarheden die te benutten zijn, maar er zijn vergaande maatregelen te treffen om het internet minder kwetsbaar te maken en die worden ook getroffen. Bovendien verloopt een succesvolle cyberaanval gradueel: na de lancering breidt de cyberaanval zich uit. Daardoor bestaan er voldoende detectiemomenten en bovendien functioneren er samenwerkingsverbanden om tegenmaatregelen te treffen. Er is slechts één voorbeeld van een cyberaanval zoals hier bedoeld bekend, maar er zijn geen aanwijzingen dat die met een terroristisch oogmerk is gepleegd. Als we al een cyberaanval zouden kunnen verwachten, dan is dat een kleinschalige aanval gedurende een beperkte tijd of een geregisseerde combinatie van kleinschalige cyberaanvallen. Dit kan het vertrouwen in het internet aantasten, zeker wanneer het met een publiciteitscampagne gepaard gaat, maar ernstige gevolgen voor het functioneren van het internet zijn moeilijk voorstelbaar.

2.3.7 Andersoortige aanslagen en aanvallen tegen het internet

Naast cyberaanvallen zijn ook andersoortige aanvallen en aanslagen tegen het internet zelf mogelijk, namelijk een fysieke aanslag, een elektromagnetische aanslag en indirecte aanvallen waardoor (de infrastructuur van) het internet niet kan functioneren. Wat zijn de kwetsbare plekken en onderdelen in Nederland voor dit type aanslagen? In Nederland bevinden zich kernknooppunten, kernfunctionaliteiten en verbindingslijnen die van belang zijn voor het internet in Nederland, maar soms ook voor het Europese of zelfs het mondiale internet. Eerder is al gewezen op de (duplicaten van) rootservers die zich in Nederland bevinden, de DNS-server die het '.nl-domein' beheert en de exchanges in Nederland, zoals AMS-IX die een mondiale functie vervult. Daar komen nog bij de Internet Service providers, KPN en andere telecom- en kabeldienstverleners waarvan de telefoon- of kabelinfrastructuur wordt gebruikt voor het internetverkeer. Binnen Nederland bevinden zich tal van glasvezel- en andere kabels voor gegevenstransport, maar ook kabels voor toegang tot het internet voor Nederlandse gebruikers waarvoor veelal gebruik wordt gemaakt van de genoemde telefoon- of kabelinfrastructuur. Gezien de geografische ligging van Nederland, komen veel transatlantische kabelverbindingen binnen in Nederland en verbindt Nederland met kabels Europese landen met elkaar. Een deel van het gegevenstransport vindt plaats via straalverbindingen. De apparatuur die wordt gebruikt op de (kern)knooppunten, door de genoemde organisaties en ten behoeve van de kernfunctionaliteiten is afhankelijk van stroom, kan niet goed tegen water en elektromagnetische straling en vereist koeling. Hoewel er een landelijke dekking is, is sprake van een concentratie van bedrijven, knooppunten, servers en kabels in het westen van het land.[65] Kortom, er zijn: a) diverse soorten organisaties, b) servers en serverparken, c) kabels en d) verbindingsmiddelen kwetsbaar voor dit type aanslagen en daarbij is sprake van een concentratie in het westen van het land. Verder zijn de apparatuur en kabels waar het internet op draait afhankelijk van andere apparatuur en dienstverlening wat een extra kwetsbaarheid creëert.

65 Expertmeeting, Dasselaar 2006, Planet.nl 2006a, Planet.nl 2006b, Planet.nl 2006c, Nu.nl 2006b, Kwint 2004.

De organisaties die een cruciale rol spelen bij het functioneren van het internet zijn zich uiteraard bewust van die kwetsbaarheden. Zij werken bijvoorbeeld vanuit diverse co-locaties, hebben extra waarborgen ingebouwd voor een ongestoorde stroomvoorziening, beschikken over noodaggregaten en bijbehorende brandstofvoorraden, hebben redundante apparatuur en tot op zekere hoogte reserve-apparatuur.[66] Toch blijven er risicofactoren. Zo had de AMS-IX bijvoorbeeld ook last van een stroomstoring in Amsterdam op 29 mei 2006. Na acht minuten is alles langzaam weer opgestart. Hierdoor waren een aantal mensen afgesloten van het internet en ging er wat meer verkeer via andere netwerken. Ook de andere exchanges hebben wat meer verkeer afgehandeld.[67] Hieruit blijkt enerzijds dat er toch wel eens wat op kleine schaal kan gebeuren, maar anderzijds ook dat zelfs als de AMS-IX volledig van de aardbodem zou verdwijnen, wat als zeer onwaarschijnlijk valt te betitelen, het internet nog steeds doordraait, zij het dat er wel her en der vertraging zal ontstaan en de performance wat minder is. De bij de AMS-IX aangeslotenen hebben immers ook andere alternatieven om het internetverkeer af te handelen. Ook bij andere partijen is naar de mening van de deelnemers aan de expertmeeting sprake van voldoende voorzorgsmaatregelen, zeker bij de grotere partijen. Een kwetsbaar punt is wel dat fysieke kabels zouden kunnen worden gesaboteerd, kapot getrokken et cetera. Er zijn echter vele kabels in Nederland en zogenaamde re-routing kan snel plaatsvinden. Dit neemt niet weg dat er single points of failure in Nederland kunnen zijn. De mate waarin er effecten ontstaan, is uiteraard mede afhankelijk van de capaciteit van de betreffende kabel en de mate waarin die kabel een unieke, en moeilijk vervangbare, rol speelt. Een zorgpunt is of de diverse overheden zich wel voldoende bewust zijn van het belang van de dienstverleners die cruciaal zijn voor het functioneren van het internet. Wanneer er een calamiteit is in de omgeving van een cruciale locatie, bijvoorbeeld een bomaanslag of afzetting in verband met de vogelgriep, moeten de medewerkers wel toegang hebben tot die locatie. Dat geldt zeker voor de situatie dat de dienstverlener ook zelf getroffen is. Noodaggregaten moeten bijvoorbeeld af en toe worden bijgevuld. Bovendien is een adequaat hek vaak wenselijk, maar wijst een deelnemer van de expertmeeting er op dat gemeentelijke overheden moeilijk (kunnen) doen over de bouwvergunning daarvoor.[68]

66 Expertmeeting, Planet.nl 2006a.
67 Computable 2006. Kort daarna - op 11 juni - heeft de AMS-IX een blackout-test gedaan waarna de problemen met het back-up systeem zijn verholpen.
68 Expertmeeting, Dasselaar 2006, Planet.nl 2006a, Planet.nl 2006b, Planet.nl 2006c, Nu.nl 2006b, Kwint 2004.

Voor dit type aanslagen gelden enkele aantrekkelijke kanten die eerder zijn benoemd voor cyberaanvallen (paragraaf 2.3.3). Deze aanvallen/ aanslagen a) passen binnen de strategie van de jihadisten, b) zij combineren de angst voor het onbekende van cyberspace en terrorisme en c) er is veel bekend over kwetsbaarheden van het internet. Andere daar genoemde voordelen (relatief eenvoudig en goedkoop, asymmetrische strijd, onvoorspelbaarheid, operationele voordelen en laagdrempeliger) zijn voor deze categorie niet van toepassing. Extra aantrekkelijk van dit type aanslagen ten opzichte van cyberaanvallen is dat er wel degelijk spectaculaire beelden denkbaar zijn die

passen binnen de propagandastrategie van de jihadisten. Daarnaast kunnen dergelijke aanvallen - vanwege de zichtbaarheid ervan, en omdat essentiële diensten of gegevens vernietigd kunnen worden - het vertrouwen in het medium internet aantasten. Daarmee draagt het bij aan het aanjagen van angst door terroristen.

Twee minder aantrekkelijke kanten van een cyberaanval gelden ook hier, namelijk de onvoorspelbaarheid van de effecten en dat een aanval niet in het belang is van terroristen. De andere negatieve punten (geen spectaculaire beelden, lange voorbereidingstijd en complexiteit en het nalaten van sporen) gelden hier niet. Wel geldt als extra nadeel dat het platleggen van het Nederlandse internet, laat staan het mondiale, op deze wijze vrijwel zeker niet zal slagen. Daarvoor zijn wel heel veel gelijktijdige en succesvolle aanvallen nodig. Dit type aanslagen heeft dus in beginsel een kleinschaliger effect dan een cyberaanval waar het de beschikbaarheid van het internet betreft. Hoewel als onwaarschijnlijk beoordeeld, zou je als individu met behulp van een cyberaanval het Nederlandse deel van het internet kunnen platleggen. Zelfs voor een groep zou het wel heel veel inspanning vergen om dit te bereiken met de andersoortige typen aanslagen. Verder moeten voor dit type aanslagen wel degelijk fysieke voorbereidingshandelingen worden getroffen hetgeen de terrorist kwetsbaar maakt en sporen achterlaat.

De aantrekkelijkheid wordt voor een belangrijk deel ook bepaald door de mate waarin er sprake is van een bewuste strategie. Wat willen ze bereiken en in welke mate kunnen ze de aanslag publicitair uitbuiten? Ziet de terroristische groepering die tot dergelijke aanvallen overgaat het als complementair aan andere typen aanslagen (force multiplier) of als zelfstandige aanslag? Bekend is dat de jihadisten met hun keuze voor het type aanslag rekening houden met het propagandistische effect en de psychologische uitwerking daarvan. Per slot van rekening zou één aanslag met een vliegtuig in de VS ook al veel effect hebben gesorteerd, maar ze kozen voor vier gelijktijdige aanslagen. Hetzelfde gebeurde bij de aanslagen in Madrid en Londen. Vanuit die optiek ligt het voor de hand om een strategie te veronderstellen waarbij er meerdere aanslagen en een mix van aanslagen zouden worden uitgevoerd, waaronder één of meer tegen het internet. Ook bekend is dat men economische doelwitten wil treffen. Vanwege de afhankelijkheid van de economie van het internet sluit een dergelijke aanslag zeker aan op de strategie van de jihadisten.[69]

Ten aanzien van de kennis en middelen die nodig zijn en de mate waarin jihadisten daarover zouden beschikken geldt, dat - los van kennis over de kwetsbare plekken van de infrastructuur - geen bijzondere kennis en middelen nodig ten opzichte van soortgelijke aanslagen tegen andere objecten, zoals stations. We mogen dan ook aannemen dat de kennis en middelen voor dit type aanslagen bij terroristen in principe toereikend zijn. De deelnemers van de expertmeeting wijzen er op dat het niet zo moeilijk is om de kwetsbare en kritieke locaties in Nederland inzichtelijk te krijgen. Bovendien is er op het internet voldoende trainingsmateriaal beschikbaar hoe een en ander uit te voeren. Dat laatste geldt zelfs voor elektromagnetische aanslagen en apparatuur. Op jihadistische websites zijn

69 Mede gebaseerd op expertmeeting.

aanwijzingen te vinden dat men geïnteresseerd is in dergelijke aanvallen. Het is voor zover bekend echter nog niet door terroristen toegepast. De deelnemers van de expertmeeting wijzen er bovendien op dat voor een echt gerichte en grote elektromagnetische aanval er veel kennis en middelen nodig zijn, waardoor een dergelijke aanval (nog) niet voor de hand ligt en zeker niet een succesvolle.

De gevolgen zijn soortgelijk aan die van cyberaanvallen, met dien verstande dat aannemelijker is dat er bij dit type aanslag wel degelijk doden en gewonden kunnen vallen. Verder is de hersteltijd langer. Als immers een locatie echt is getroffen, is deze niet direct herbouwd en is er niet in grote hoeveelheden en op heel korte termijn reserve-apparatuur beschikbaar. Daarentegen werken de dienstverleners wel weer vanuit co-locaties waardoor zelfs bij uitval de effecten toch ook wel weer mee kunnen vallen voor die specifieke dienstverlener. Verder geldt ook hier dat er een grote mate van redundantie bestaat op het internet. Dit type aanslag heeft bovendien een minder groot bereik dan met behulp van een cyberaanval.

2.3.8 Beoordeling dreiging andersoortige aanslagen

De NCTb meent dat de waarschijnlijkheid van een andersoortige aanslag niet hoog is. Er zijn mogelijkheden, maar daartegen zijn wel al maatregelen getroffen om de kans erop te verkleinen en de effecten te beperken. Het uitschakelen van het internet is met deze andersoortige aanslagen in principe niet mogelijk; de gevolgen voor het functioneren zijn kleiner dan van een succesvolle, grootschalige cyberaanval, maar de effecten kunnen zichtbaarder zijn, kunnen ook de beschikbaarheid van (opgeslagen) gegevens betreffen en de hersteltijd van (gebouwen en) apparatuur zal langer zijn. Bovendien zijn de effecten beter uit te buiten in het kader van propaganda. Bij een explosie zijn slachtoffers denkbaar, maar de schade zal met name apparatuur betreffen. De jihadisten kunnen beschikken over de kennis en middelen, zeker waar het bomaanslagen betreft.

Hoewel een andersoortige aanslag op de infrastructuur van het internet waarschijnlijker lijkt dan een cyberaanval, en zijn eigen aantrekkelijkheden kent voor jihadisten, is de vraag gerechtvaardigd - met name gelet op de beperkte effecten voor het functioneren internet - of terroristen niet liever een bomaanslag op een soft target zullen plegen dan op een belangrijke internetlokatie.

2.4 HET INTERNET ALS WAPEN

2.4.1 Toelichting

Het internet raakt steeds meer verweven met allerlei activiteiten in de fysieke wereld en allerlei sectoren, organisaties en personen zijn gekoppeld aan het internet. Daardoor zijn ze ook kwetsbaar voor aanvallen via het internet. Veelgehoorde theoretische scenario's zijn het overnemen van het besturingssysteem van vitale installaties, zoals in de chemische sector, om rampen te veroorzaken. Ook verstoring van communicatiesystemen, openbaar vervoer, de

logistieke sector, de financiële sector en de elektriciteitsvoorziening worden als voor de hand liggende voorbeelden genoemd, evenals het aantasten van (de betrouwbaarheid van) virtuele diensten als internetbankieren. Recent is ook gewezen op de mogelijkheid om via het internet door te dringen in de systemen van ziekenhuizen. Bijvoorbeeld het manipuleren van bloedgroepen in de patiëntengegevens zou in potentie dramatische gevolgen kunnen hebben.[70] Een ander bekend scenario is het uitschakelen van alarmcentrales of crisisorganisaties door bijvoorbeeld *hacking* of door overbelasting te veroorzaken, en daarmee de effecten van een reguliere aanslag, zoals een bomaanslag, te vergroten *(force multiplier)*.

Vooral het internet als wapen is gevoelig voor overreactie en overdrijving. Zo zijn er regelmatig berichten over het hacken van websites. Het betreft dan vaak de publieke websites van organisaties, en niet een intern netwerk.[71] Voor de dreiging maakt dat fundamenteel uit, omdat er daarmee geen risico is dat bijvoorbeeld de stroomvoorziening stil komt te liggen. Anderzijds hoeven er niet altijd 'traditioneel' rampzalige (of zichtbare) consequenties aan terroristisch handelen te zitten en kan het veelvuldig en gelijktijdig hacken van websites van virtuele diensten (vooral elektronisch bankieren) en het (voortdurend) manipuleren of onbereikbaar dan wel onbetrouwbaar maken van gevoelige gegevens wel degelijk een terroristisch effect hebben. Echter, het hacken van de homepage van een internetbank en daar jihadistische kretologie op plaatsen dient als pesterij of hoogstens activisme te worden beschouwd. Daarom is een goede afbakening belangrijk.

Figuur 2.3 Voorbeelden die niet onder internet als wapen vallen.

Stel dat een jihadist infiltreert als IT-specialist in een elektriciteitscentrale, toegang heeft of verkrijgt tot het computergestuurde controlesysteem en een deel van Nederland op maandagochtend 07.00 uur op 'zwart' zet met alle gevolgen van dien. De Nederlandse maatschappij is - in ieder geval tijdelijk - ontregeld, en bij langere uitval kunnen back-up systemen zoals in ziekenhuizen uitvallen. Ondanks dat de dreigingsernst aanzienlijk is en ICT is gebruikt, gaat het hierbij niet om een aanval via het internet.
Daardoor valt dit voorbeeld niet onder 'internet als wapen' zoals gehanteerd in deze fenomeenstudie.

Volgens een bericht van 29 juni 2006 heeft een groep Marokkaanse hackers, nadat het Israëlische leger met tientallen tanks, bulldozers en pantservoertuigen het zuiden van de Gazastrook binnenviel, meer dan 750 Israëlische websites gehackt. "Doelwit waren onder meer sites van banken, autofabrikanten en ziekenhuizen. De groep, die zich Team Evil noemt, steunt het verzet tegen de Israëlische bezetting. [...] De hackers lieten de volgende boodschap achter op de gekraakte sites: "Hacked By Team-Evil Arab hackers u KIll palestin people we Kill Israel servers" (Gehackt door Team-Evil, jullie doden Palestijnen, wij doden Israëlische servers).
Het is de grootste aanval op Israëlische websites tot nu toe.[72]
Dit is typisch een voorbeeld van hacktivisme en niet van internet als wapen.

Ook voor internet als wapen geldt dat cyberaanvallen die dienen om een politiek statement te maken (het zogeheten *hacktivisme*) niet worden meegenomen omdat noch de intentie, noch de gevolgen binnen de definitie van terrorisme vallen. Verder kan verwarring ontstaan met het gebruik van het internet als middel. Een voorbeeld van de inzet van het internet als middel is het verzamelen van informatie over een kerncentrale via het internet met als doel om een terroristische aanslag daartegen te plegen. Een ander voorbeeld is het via het internet kenbaar maken van een dreiging met een aanslag als vorm van angst aanjagen. In deze studie is er de voorkeur aan gegeven om deze vormen van gebruik van het internet als afzonderlijke categorie te beschouwen. Het gaat immers om andersoortige zaken, waarvoor andere kennis en middelen zijn vereist en ook andere aangrijpingspunten bestaan voor beleid (zie hoofdstuk 3).

2.4.2 Mogelijkheden internet als wapen, kwetsbaarheden en weerbaarheid

Een aanval via het internet kan op uiteenlopende manieren, waaronder de eerdergenoemde overbelasting door een DDoS-aanval. De effecten van verstoring of overbelasting van een specifiek netwerk heeft echter maar een beperkt effect, en hoogstwaarschijnlijk géén grote invloed op het functioneren van een vitale sector. Gerichte hacking om systemen te manipuleren of uit te schakelen ligt dan meer voor de hand (zie paragraaf 2.2.4).

Er zijn mondiaal geen concrete gevallen bekend waarin gerichte aanvallen tegen fysieke doelen via het internet met daadwerkelijk als terroristisch te bestempelen schadelijke gevolgen zich hebben voorgedaan,[73] hoewel er een aantal vervelende incidenten is geweest die in potentie tot ernstige gevolgen hadden kunnen leiden. Zo zou een jonge hacker zich toegang hebben verschaft tot het controlesysteem van een dam in de VS en zou hij de *floodgates* hebben kunnen openzetten. Het verhaal bleek uiteindelijk enigszins overdreven. De hacker had zich weliswaar toegang verschaft tot het besturingsnetwerk, maar zou niet in staat zijn geweest om daadwerkelijk te 'sturen'.[74] Maar ook in de EU en Nederland zijn - bijvoorbeeld in de energiesector - incidenten met hackers geweest.[75] Los van de daadwerkelijke gevolgen van hackpogingen tot nu toe, geeft het aan dat écht goede en toegewijde hackers - al dan niet geholpen door infiltranten of gefrustreerde ex-werknemers - altijd kwetsbaarheden zullen ontdekken. Verder zullen veel incidenten niet onderkend of gemeld worden, uit vrees voor imagoschade.

Behalve de vitale infrastructuur kunnen ook (financiële) diensten getroffen worden. Hoewel het de vraag is of dit een 'traditioneel' terroristisch effect zal hebben, kan het wel degelijk de betrouwbaarheid van gegevens en diensten aantasten. Bovendien kan het een dubbel doel dienen: door fraude te plegen kunnen in eerste instantie fondsen worden geworven voor bijvoorbeeld komende acties. In tweede instantie zal het breed bekend raken van een grootscheepse (creditcard)fraude-actie het vertrouwen van de bevolking in elektronisch betalingsverkeer, algemeen gegevensverkeer en wellicht zelfs

70 Interview 3 en Planet.nl 2005.
71 Weimann 2006, p. 158. De website van de NASA was gehacked, waardoor het idee bestond dat de hackers hadden kunnen 'sturen'.
72 Nu.nl 2006a.
73 Weimann 2006, Green 2002.
74 Weimann 2006, p. 166.
75 Luiijf 2006, p.52-53.

het internet kunnen aantasten. Wanneer een dergelijke actie (door phishing, pharming of anderszins, zoals bekend uit ervaringen met cybercrime) wordt gecombineerd met een fysieke aanslag op een storage-provider, waardoor (backup)gegevens van rekeningen en transacties verloren gaan, kan dit tot grote onzekerheid bij de burger leiden. Hoewel het effect subtieler is dan wanneer een elektriciteitscentrale gemanipuleerd wordt met als gevolg een grootscheepse stroomstoring, kan de psychologische impact groot zijn, zeker gelet op de stijgende afhankelijkheid van het internet. Ook in propagandistisch opzicht kunnen jihadisten munt slaan uit dergelijke acties, door publiekelijk aan te tonen dat zij erin geslaagd zijn het Westen in het hart (financiën) te treffen.[76]

Zoals eerder is aangegeven is het niet mogelijk om op een achternamiddag de controle over een compleet systeem of netwerk over te nemen. Een dergelijke aanval heeft in Nederland nog niet plaatsgevonden (dan wel er is niet over gepubliceerd) en is complex, maar uit het buitenland zijn voorbeelden bekend die ook op de Nederlandse situatie van toepassing kunnen zijn. Daarom is het van belang te bepalen waar voor Nederland de kwetsbaarheden liggen, zeker als het gaat om de vitale infrastructuur. Het gaat dan om de volgende aspecten: a) SCADA, b) standaardisatie van systemen en programmatuur, c) schijnveiligheid, d) social engineering, e) nonchalance en menselijk falen en f) dynamiek van het internet, software en netwerken.

A SCADA

SCADA *(Supervisory Control And Data Acquisition)* is een generieke term voor procescontrolesystemen die wordt gebruikt door veel bedrijfssectoren, waaronder water- en energiebedrijven, de transportsector en de chemische industrie. Een SCADA-systeem monitort en beheert veelal complete installaties. SCADA kent de nodige kwetsbaarheden die te maken hebben met de opzet ervan, nonchalance en mensen falen. Daardoor is SCADA kwetsbaar voor gerichte hacking, waardoor uiteindelijk aan de knoppen van een installatie gedraaid kan worden. Het is echter de vraag in hoeverre anderen dan het eigen personeel de specifieke technische kennis bezitten om een SCADA-systeem te bedienen. Hacken is één, het daadwerkelijk sturen is een tweede.[77] De SCADA-software is weliswaar standaard, maar de individuele configuraties verschillen per bedrijf. Voor het overnemen van een systeem lijkt infiltratie of inside informatie noodzakelijk. Zonder dergelijke specifieke kennis krijgt een aanval het karakter van een loterij. Er zijn meer dan veertig praktijkgevallen bekend van hackaanvallen tegen SCADA.

B Standaardisatie van systemen en programmatuur

Aan de ene kant is er veel voor te zeggen om systemen en de beveiliging ervan vergaand te standaardiseren met software en volgens vaste protocollen. Hobbyisme wordt daardoor bijvoorbeeld voorkomen. Aan de andere kant biedt standaardisatie kansen voor personen met de verkeerde bedoelingen. Bedrijven schaffen steeds vaker Commercial Off the Shelf-software (COTS) aan.

76 Expertmeeting.
77 Zie voor dat laatste Green 2002.

Figuur 2.4 Voorbeelden van kwetsbaarheid voor internet als wapen.[78]

De Slammer-worm uit 2003 nestelde zich ook in het netwerk van een telecommunicatieaanbieder. Communicatie met een SCADA-systeem in een substation van een elektriciteitsvoorziening was niet meer mogelijk, en het SCADA-systeem was tussen de 6 en 8 uur onbruikbaar.

In augustus 2005 legde een worm 23 fabrieken in de VS plat. Vanuit dat netwerk werd een fabriek in België geïnfecteerd. Ook een fabriek in Australië was een aantal uren buiten bedrijf, waarbij het productieverlies op 6 miljoen dollar werd geschat.

Figuur 2.5 Voorbeeld van kwetsbaarheid via SCADA.

Een bekend voorbeeld van ongeautoriseerde toegang tot een SCADA-systeem is de verstoring van een drinkwater- en rioolwaterzuiveringsinstallatie in 2000 door een ex-contractant. Hij schakelde alarmmeldingen uit, verstoorde communicatie, liet pompen niet op tijd aanslaan en zorgde voor het laten vrijkomen van naar schatting een miljoen liter ongezuiverd afvalwater.

Deze software kan iedereen in principe aanschaffen en doorgronden als onderdeel van een verkenning voor een cyberaanval. Wanneer fouten of kwetsbaarheden eenmaal zijn ontdekt, kunnen in principe alle systemen die met diezelfde software werken geëxploiteerd worden. Dat is ook de reden dat een virus als het 'I Love You'-virus zo succesvol was: wereldwijd gezien gebruikt vrijwel iedereen hetzelfde e-mailprogramma.[79]

Inrichting van een netwerk en de bijbehorende beveiliging naar eigen inzicht heeft daardoor, naast uiteraard nadelen, toch ook wel weer voordelen. In dat kader heeft men het dan ook wel eens over *security by obscurity*. Veel software is speciaal voor bepaalde bedrijven geschreven, en is vervolgens in beheer bij één of meer systeembeheerders. Afhankelijk van de kwaliteit van de software en de persoonlijke werkwijze van de systeembeheerders kan sprake zijn van een spreekwoordelijk doolhof. Zo is een voorbeeld bekend waar bij een organisatie is ingebroken in het netwerk, maar waar vervolgens een verkeerde 'afslag' is genomen en er geen kritieke onderdelen zijn bereikt, laat staan gemanipuleerd.[80]

De verwachting is dat de standaardisering in automatisering en netwerkbeheer verder doorgaat. De beveiliging van systemen gaat dan wel omhoog, als een hacker eenmaal toegang heeft zal hij in steeds meer systemen snel zijn weg kunnen vinden. Aan het zogeheten *security by obscurity* komt een einde door 'goed huisvaderschap' en uniformiteit in programmatuur en beheer.

78 Voorbeelden afkomstig uit Luiijf 2006.
79 Thiele & Van Vliet 2005, p.21.
80 Interview 2.

C Schijnveiligheid

Bedrijven controleren vaak alleen op papier of hun systemen veilig zijn. Dat is heel wat anders dan het daadwerkelijk testen of al die papieren maatregelen ook in de praktijk werken. Zo wordt bijvoorbeeld *airgapping* toegepast om aanvallen van buitenaf te voorkomen: kritieke systemen en netwerken worden hierbij niet met het internet of een ander netwerk verbonden. Toch is in 2004 tot twee keer toe een virus doorgedrongen in, middels een airgap beveiligde, computersystemen van het *Army Space and Missile Defense Command*. Op dat systeem zou geen antivirus-software geïnstalleerd zijn geweest. Zodra een dergelijk systeem tegen de afspraak toch aan een ander netwerk wordt gekoppeld, is besmetting een kwestie van tijd. Airgapping heeft ook geen effect wanneer wifi-apparatuur in een geairgapped netwerk worden opgenomen.[81] De op papier getroffen beveiligingsmaatregelen zijn daarmee in één klap ongedaan gemaakt.

Daarnaast zouden ten gevolge van de privatisering weliswaar veel investeringen hebben plaatsgevonden in de betreffende sectoren, doch niet in de ICT-infrastructuur. Ook zou meer moeten worden getest en geoefend in de vitale sectoren. Tenslotte worden fysieke veiligheid en IT-veiligheid - twee verschillende zaken - geregeld door elkaar gehaald.

D Social engineering

Onder social engineering wordt verstaan het bespelen van personen binnen een bedrijf, teneinde gevoelige informatie te verkrijgen. Feitelijk valt een dergelijk onderwerp buiten het bereik van deze fenomeenstudie. Voor een succesvolle cyberaanval kan social engineering echter een noodzakelijk middel in de voorbereidingsfase van hacken zijn. Hiervan zijn gedocumenteerde voorbeelden.[82] Uit een oefening van de NSA in 1997 in de VS zou naar voren zijn gekomen dat het zich voordoen als technicus of hoge officier de tegenpartij kon overhalen bepaalde wachtwoorden te geven.[83]

E Nonchalance en menselijk falen

Een groot risico vormt menselijke nonchalance. Een onderzoek in de VS uit april 2005 toonde aan dat slechts op 9% van alle pc's van 251 onderzochte bedrijven het voor beveiliging van systemen essentiële *Service Pack 2* voor het besturingssysteem Windows XP was geïnstalleerd.[84] Ook voor Nederland geldt ongetwijfeld dat veel systeembeheerders niet in eerste instantie bezig zijn met beveiliging, maar met hun core-business: het (soms 24*7) draaiend houden van een systeem, en daarmee het tevreden houden van de klant of werkgever.[85] Uit een onderzoek in Nederland blijkt dat driekwart van de onderzochte bedrijven een firewall heeft, en software tegen virussen en wormen heeft geïnstalleerd, en dat zestig procent beschikt over software tegen spyware.[86] In hoeverre de geïnstalleerde firewalls correct geconfigureerd zijn en de virusscanners bijgewerkt worden is niet bekend. Hierbij kan bovendien de analogie worden aangehaald, dat het installeren van een firewall hetzelfde is als het plaatsen van een slot op de deur: als je eenmaal toch binnen bent gekomen als gevolg van bijvoorbeeld een slecht slot, kun je vaak overal bij, tenzij kostbare spullen in kluizen zijn geplaatst.[87] Firewalls moeten dus wel goed zijn geconfigureerd en bij voorkeur moeten accounts en bestanden met wachtwoorden zijn beveiligd.

81 Gebaseerd op: interview 3, Weimann 2006, p. 166 en Expertmeeting.
82 Mitnick 2006.
83 Weimann 2006, p. 160 over de oefening 'Eligible Receiver'.
84 CRS 2005b, p. 5 en Wilson 2006, p. 75.
85 Interview 3.
86 EZ 2005.

Menselijk falen kan eveneens de gelegenheid bieden aan terroristen om een cyberaanval in te zetten. Veel netwerken en besturingsinstallaties zijn zoals gezegd niet verbonden met het internet. Een schijnbaar stand-alone systeem van bijvoorbeeld een elektriciteitscentrale kan echter wel degelijk aangevallen worden door een onverwachte connectie met een netwerk dat wél aangesloten is op het internet. Zo is het gedeeld gebruik door twee aparte netwerken van één moderne printer met eigen geheugencapaciteit voldoende voor een ernstig veiligheidsrisico. Een schijnbaar stand-alone netwerk blijkt dan tóch aan het internet te hangen en wordt ongemerkt kwetsbaar. Dit zou bijvoorbeeld ook in een ziekenhuis het geval kunnen zijn, waardoor patiëntgegevens gemanipuleerd kunnen worden.[88] Daarnaast is een risico gelegen in het combineren van kantoorapplicaties (waarin regelmatig nieuwe kwetsbaarheden worden ontdekt) en monitorings- en sturingssystemen, zoals het hiervoor genoemde SCADA.

F Dynamiek van het internet, software en netwerken

Er zullen altijd exploiteerbare kwetsbaarheden in software en systemen zitten. In 2002 werd een ernstige fout ontdekt, waardoor internetrouters eenvoudig hadden kunnen worden overgenomen.[89] Een andere ontdekking van een kwetsbaarheid werd gedemonstreerd tijdens een conferentie over *computer security* in juli 2005 (Black Hat): in de veelgebruikte internet routers van Cisco Systems zat een veiligheidslek. Deze kwetsbaarheid was zodanig ernstig dat zelfs een bekende cyberterrorisme-criticus moest toegeven dat er sprake was een serieus risico voor aanvallen op en gegevensdiefstal uit netwerken door een zeer snel uit te voeren *hack*. Hoewel Cisco Systems al een *patch* (reparatiesoftware) had uitgebracht voor dit lek, waren de klanten hier kennelijk onvoldoende van op de hoogte.[90] Recentelijk zijn nog kwetsbaarheden ontdekt in kantoorapplicaties als Word 2003 en Excel. Dit benadrukt het risico van het combineren binnen één netwerk van kantoorapplicaties en procescontrolesystemen.

Tal van maatregelen zijn getroffen om kwetsbaarheden te verminderen. Netwerken zijn robuuster gemaakt en infrastructuren houden immers ook al rekening met bijvoorbeeld natuurrampen, ongelukkig menselijk handelen en bliksemінslag. Hierdoor veroorzaakte storingen kunnen snel worden hersteld,[91] hetgeen tevens zou moeten gelden voor storingen veroorzaakt door een aanval via het internet. Bovendien kennen systemen van bijvoorbeeld elektriciteitscentrales redundantie en zijn zij vaak voorzien van noodaggregaten.[92]

87 Mitnick 2006.
88 Interview 2.
89 CRS 2005a, p. 9. Het betrof een fout in het Simple Network Management Protocol.
90 Wilson 2006, p. 75.
91 Lewis 2002, p. 11 en Green 2002.
92 Interview 2.

Daarnaast kan niet worden uitgevlakt dat de virtuele wereld niet altijd een volstrekt afgezonderde wereld is, maar deel uitmaakt van onze fysieke wereld: storingen zullen door mensen worden ontdekt en gecorrigeerd of opgevangen. Bij bijvoorbeeld een vergiftigingsscenario waarbij het ijzergehalte van een graanontbijtproduct door een hacker van het productiesysteem zodanig wordt verhoogd dat kinderen ziek worden en sterven,[93] wordt wellicht voorbijgegaan aan het gegeven dat de smaak ook zal veranderen (dat door testers en anderen zal worden geproefd), dat het bewuste ingrediënt in de fabriek opeens veel vaker en eerder moet aangevuld et cetera. De menselijke factor en andere factoren moeten niet opeens volledig worden uitgevlakt wanneer het over een aanval via het internet gaat. Dit geldt ook voor het uitvallen van de luchtverkeersleiding of boordcomputers. Piloten zijn getraind om ook zonder dergelijke hulpmiddelen te navigeren en te landen.[94]

Is Nederland extra kwetsbaar? De breedband- en internetpenetratie in Nederland is enorm, steeds meer bedrijven maken gebruik van het internet voor het aanbieden van diensten of bedienen van installaties en de afhankelijkheid van het internet zal in de toekomst ongetwijfeld toenemen. En waar geen sprake is van een bewuste, rechtstreekse koppeling kan via een achterdeur onbewust toch koppeling met het internet plaatsvinden (zie hierboven onder nonchalance).

Al met al kunnen we de volgende conclusie trekken. Er zijn mogelijkheden om het internet als wapen in te zetten en fysieke doelwitten en virtuele diensten zijn tot op zekere hoogte kwetsbaar. Bij fysieke, vitale doelwitten dient de besturing overgenomen te worden, hetgeen uitgebreide studie of insider-informatie vereist. De ervaringen op het gebied van cybercrime lijken aan te geven dat virtuele diensten eenvoudiger kunnen worden verstoord. Toch zijn er maatregelen daartegen te treffen en ook getroffen. De beveiliging van procescontrolesystemen als SCADA loopt hierbij nog achter. De kwetsbaarheden zijn niet altijd rechtstreeks aan computers of het internet gerelateerd, maar betreffen veeleer menselijke factoren. Een aanval via het internet zoals hier bedoeld is complex. Er zijn geen voorbeelden bekend van grootschalige aanvallen via het internet met grote gevolgen, hoewel het incident met het ongezuiverde afvalwater (zie figuur 2.5) een voorbeeld is van wat er mis zou kunnen gaan als iemand die een systeem kent, dit van een afstand wil manipuleren.

2.4.3 Intentie internet als wapen

Net als het geval is voor internet als doelwit, gelden ook voor internet als wapen zowel voor- als nadelen die bepalend zijn voor de vraag of en in welke mate jihadisten het internet als wapen zouden willen gebruiken. De in subparagraaf 2.3.3 genoemde voordelen gelden grosso modo ook voor internet als wapen. De *onvoorspelbaarheid* van een aanval en dus het psychologische effect is wel groter. Het is voor de verdedigende partij vrijwel onmogelijk om alle gevolgen van een cyberaanval te overzien, omdat het nog niet eerder is gebeurd, het moeilijk te simuleren is en niet alle interdependenties bekend zijn. Hierdoor kunnen allerlei onverwachte effecten optreden.[95] Het is bovendien geen prettige gedachte dat een terrorist van een afstand kan inbreken in het interne netwerk van een onderdeel van de vitale infrastructuur of een ziekenhuis. Het sluiten van bijvoorbeeld een waterkering door manipulatie van het betreffende SCADA-systeem zal geen watersnoodramp veroorzaken, maar kan de scheepvaart wel sterk hinderen, ongelukken tot gevolg hebben en angst teweeg brengen onder de bevolking.

93 Colin 1997, p. 15-18.
94 Denning 1999.
95 De onderbouwing van de extra onvoorspelbaarheid is gebaseerd op Interview 6.

Als extra voordeel kan worden genoemd de *grote variëteit en het grote aantal combinaties* die mogelijk zijn voor aanvallen. De scenario's voor aanvallen lijken eindeloos, en het aantal zal alleen maar toenemen met de groei van het gebruik en de afhankelijkheid van het internet. Bovendien zullen computers, software en netwerken altijd kwetsbaar blijven, er zullen altijd niet-ontdekte onvolkomenheden zijn, en de complexiteit van vitale infrastructuren zal onherroepelijk tot foutjes en gaten leiden.[96]

Net als het geval is bij de voordelen, gelden de in subparagraaf 2.3.3 genoemde nadelen ook voor het internet als wapen. Een belangrijk verschil is dat de jihadisten zich met deze aanslag niet zelf in de vingers snijden omdat het internet zelf gewoon blijft functioneren. Tevens is sprake van extra onvoorspelbaarheid van een aanval en de schade ervan. Die schade kan groter zijn, omdat rechtstreeks doelen worden getroffen, veelal van de vitale infrastructuur. Toch zal de schade als bijvoorbeeld de 'floodgates' van een dam door een cyberaanval worden opengezet relatief beperkt zijn vergeleken met een bomaanslag (al dan niet veroorzaakt door met een vliegtuig tegen de dam te vliegen) waarmee een dam daadwerkelijk zwaar beschadigd raakt.[97] Daarnaast zouden - gelet op mogelijk beperkte effecten of de onvoorspelbaarheid van (de duur van) de effecten - terroristen meerdere doelen tegelijk voor een lange periode moeten aanvallen om een écht 'terroristisch effect' te bereiken.[98] Verder geldt als extra nadeel, bezien vanuit het perspectief van de jihadist, dat de menselijke factor hier niet moet worden onderschat. De mens kan vreemde zaken opmerken en actie ondernemen of kan getraind zijn om te handelen in noodsituaties (zie subparagraaf 2.4.2).

Misschien vormt het plegen van een dergelijke aanval de uitvlucht wanneer conventioneel terrorisme beter bestreden wordt. Wanneer de fysieke beveiliging van vitale objecten wordt verhoogd, kunnen aanvallen via het internet wél verhoudingsgewijs toenemen.[99] De vraag is echter of bij een betere beveiliging niet eerst ándere fysieke doelen met fysieke aanslagen zullen worden getroffen, voordat men op het internet zijn gram gaat halen. Wel is door de opkomst van onder andere virtuele diensten een extra doelwit beschikbaar gekomen voor jihadisten die niet het martelaarschap zoeken. En discussie *(chatter)* in jihadistische webfora over SCADA zou toenemen.[100]

96 Weimann 2006, p. 166.
97 Lewis 2002, p. 4.
98 CRS 2005a, p. 11.
99 Weimann 2006, p. 171, Interview 1.
100 Voor dat laatste, zie Independent 2006a.

2.4.4 Kennis en middelen

In paragraaf 2.2 is aangegeven dat er voorbeelden van terroristisch computergebruik bekend zijn en dat terroristen beschikken over moderne apparatuur. Tevens is aangegeven dat er enkele jihadistische hackers(groepen) bekend

zijn en dat kennis over het hacken wordt verspreid via jihadistische websites. Ook is gesproken over mogelijke samenwerking tussen terroristen en hackers. Voor aanvallen via het internet is gerichte hacking de meest voor de hand liggend methode, aangezien DDoS-aanvallen enkel ingezet zouden kunnen worden voor overlastgevende verstoring, behalve wellicht in het geval van SCADA-systemen. Een serieuze hackpoging kan niet op een achternamiddag worden uitgevoerd. Terroristen zouden een lange voorbereidingstijd in acht moeten nemen en meerdere doelen tegelijk voor een lange periode moeten aanvallen om écht 'terroristisch effect' te bereiken. Een dergelijke strategische planning is wellicht lastig in een dynamische omgeving als het internet met zijn vele nieuwe toepassingen en ontwikkelingen. En zelfs dan zijn de uitkomsten nog onvoorspelbaar. Een aanval via het internet zoals hier bedoeld vergt niet alleen veel kennis, maar ook inzet en toewijding. Échte hackers die de capaciteiten bezitten om werkelijk kwaad te doen zijn zeldzaam, maar een dergelijke hacker van jihadistische signatuur dan wel (onbewust) ingehuurd zal tot het uiterste gaan om te slagen in zijn opzet. Hierbij zal hij eveneens andere middelen dan louter technische inzetten. Te denken valt hierbij aan social engineering, infiltratie en werken onder een dekmantel.

Een feit is echter dat er geen voorbeelden bekend zijn van het gebruik van het internet als wapen door jihadisten, zeker niet tegen vitale sectoren. Wel zijn er aanwijzingen dat jihadisten interesse hebben voor dit type aanvallen. Ook zijn voorbeelden bekend van criminelen die virtuele diensten misbruiken, afpersen of onbetrouwbaar maken. Voor deze variant van het internet als wapen is tot nu toe meer aandacht geweest vanwege het financiële gewin, en kennis daarover kan daardoor eerder bij jihadisten aanwezig zijn dan kennis over manipulatie van een procescontrolesysteem in een Nederlandse sector.

2.4.5 Gevolgen

Via het internet zouden jihadisten onder andere delen van de vitale infrastructuur kunnen aanvallen. Het is niet voor niets dat enkele sectoren daarvan vallen onder het alerteringssysteem. Terroristische activiteiten tegen die sectoren hebben grote en ernstige maatschappelijke gevolgen. Daarbij doet niet ter zake of de aanval via het internet of op andere wijze heeft plaatsgevonden.

Hoewel er ontelbare scenario's denkbaar zijn, is het lastig voorstelbaar dat grote aantallen doden en gewonden daadwerkelijk tot de gevolgen van een cyberaanval zullen behoren. Een uitzondering vormen hierop wellicht ziekenhuizen, waarbij het manipuleren van patiëntgegevens in bepaalde gevallen fatale gevolgen zal kunnen hebben, en personenvervoer, waar verstoring van wissels (trein) in principe ernstige gevolgen kunnen hebben. Wel kan de betrouwbaarheid van het internet en virtuele diensten zoals internetbankieren worden aangetast, hetgeen uiteindelijk van invloed zou kunnen zijn op de bestendiging en doorontwikkeling van dit soort diensten.

Wanneer cyberaanvallen langdurige verstoringen veroorzaken in meerdere sectoren van de economie/samenleving tegelijk zullen daadwerkelijk vervelende effecten voelbaar worden, zal mogelijk paniek onder een deel van de bevolking uitbreken, zal hamstergedrag vertoond worden, kan het de beurshandel verstoren of negatief beïnvloeden, en zal uiteindelijk sprake kunnen zijn van maatschappijontwrichtende schade. Niet alle maatschappelijke en vitale functies zijn echter zodanig afhankelijk van het internet dat een aanval via het internet ook echt als een aanslag gevoeld zal worden. Daarbij komt dat mensen vaak snel herstellen van schrik, en gewend zijn aan storingen met elektriciteit en computers. En er is er nog in andere zin de factor mens: storingen en veranderingen worden opgemerkt door onze zintuigen of anderszins. Wanneer bijvoorbeeld een chemische fabriek die via het internet gemanipuleerd wordt giftige gassen uitstoot, zal de omgeving dit snel merken. Het is niet gezegd dat dit niet tot slachtoffers zal leiden, maar de oorzaak zal ongetwijfeld snel gevonden worden. Dit neemt natuurlijk niet weg dat er ook sluipender gevolgen mogelijk zijn.

2.4.6 Beoordeling dreiging

Een aanval via het internet acht de NCTb op dit moment niet erg waarschijnlijk. De belangrijkste gewogen argumenten daarvoor zijn dat de voordelen niet substantieel opwegen tegen de nadelen (intentie), dat andere aanslagen een groter effect sorteren en dat de gevolgen weliswaar aanzienlijk kunnen zijn, maar garanties daarop (bezien vanuit terroristische standpunt) zijn er niet. Als er een aanslag zou plaatsvinden, kunnen de gevolgen groot zijn, maar niet aannemelijk is dat die doelen voor lange tijd niet zouden kunnen functioneren. Wel kan het vertrouwen van de burger worden aangetast als veelvuldig verstoringen plaatsvinden in bijvoorbeeld de vitale sectoren, of wanneer virtuele diensten en daaraan gekoppelde privacygevoelige gegevens (banken, gezondheidszorg) onbetrouwbaar lijken. De duur van een dergelijke aantasting van vertrouwen is lastig te beoordelen, maar zou via het internet wel eens eenvoudiger te bewerkstelligen kunnen zijn dan een grote ramp in de vitale sectoren. Er zijn maatregelen te treffen en getroffen om de doelwitten minder kwetsbaar te maken voor aanvallen via het internet, maar duidelijk is dat procescontrolesystemen als SCADA hierop nog een uitzondering vormen. Een aanval via het internet in combinatie met een fysieke aanslag, waarbij die als force-multiplier werkt, is aannemelijker dan alleen een cyberaanval.

Interessant is tenslotte de vraag waarom terroristen tot nu toe geen cyberaanval hebben gepleegd. Kennis, middelen en voorbereidingstijd zijn beschikbaar en aanvullende expertise is in te huren. De gevolgen van een cyberaanval zijn weliswaar onvoorspelbaarder dan van een bomaanslag, maar kunnen toch aanzienlijk zijn, en de jihadisten kunnen vervolgens de te verwachten uitbraak van 'cyberfear' optimaal uitbuiten in hun propaganda. Dat het nog niet is gebeurd wordt wellicht veroorzaakt doordat de jihadisten nog onvoldoende bekend zijn met de mogelijkheden, of liever kiezen voor traditionele doelen.

2.5 SLOTBESCHOUWING

In dit hoofdstuk is vanuit uiteenlopende invalshoeken gekeken naar de dreiging die uitgaat van het internet als doelwit en wapen. Daarbij zijn allerlei vormen van aanvallen en aanslagen onderscheiden. Verder is gekeken naar de afzonderlijke dimensies van mogelijkheden en kwetsbaarheden, de mate van aantrekkelijkheid, de mate waarin jihadisten over de kennis en middelen beschikken en de gevolgen. Tot slot is veelal ook gekeken naar andere typen aanslagen die tot het repertoire van terroristen behoren.

Wanneer we met het laatste beginnen, dringt zich toch het beeld op dat andere typen aanslagen, waaronder bomaanslagen, de komende tijd een grotere waarschijnlijkheid hebben dan de in dit hoofdstuk beschreven aanvallen en aanslagen. Zelfmoordaanslagen en bomaanslagen zijn denkbaar met als doel om het internet te verstoren, maar het is toch meer aannemelijk dat terroristen dergelijke aanslagen liever plegen tegen andere doelen, zoals soft targets. Per slot van rekening heeft bijvoorbeeld de Arena in Amsterdam veel meer bekendheid dan een exchange in Amsterdam en een grotere publicitaire waarde zowel nationaal als internationaal. En daar waar jihadisten zeer gevoelig zijn voor de psychologische boodschap achter aanslagen, lijken die meer klassieke aanslagen publicitair beter uit te buiten dan cyberaanvallen en hebben ook een meer voorspelbare uitkomst. Zelfmoordaanslagen zijn voor jihadisten extra aantrekkelijk, omdat het martelaarschap wordt verheerlijkt. Het martelaarschap is niet haalbaar met de in dit hoofdstuk genoemde aanvals- en aanslagvormen. Toch kan dit juist een voordeel zijn voor Nederlandse jihadisten: het gat tussen woord en daad is immers kleiner bij dit type aanvallen dan een zelfmoordaanslag. Een combinatie van een of meer klassieke aanvallen met de inzet van het internet als doelwit of wapen lijkt meer waarschijnlijk. Hierdoor wordt het effect van de klassieke aanval versterkt.

Internet als doelwit en als wapen vormen op dit moment weliswaar een beperkte dreiging voor Nederland, de mogelijkheden voor misbruik zullen echter blijven toenemen evenals de complexiteit om daar wat tegen te doen. Jihadisten hebben interesse voor cyberaanvallen en beschikken al over kennis en middelen daartoe en hebben de intentie om de westerse economieën te raken. Het feit dat het martelaarschap niet bereikt wordt kan bepaalde jihadisten zowel afschrikken als aantrekken, maar rekening dient te worden gehouden met een aanzienlijke aantrekkingskracht voor Nederlandse jihadisten. Hoe groot de dreiging zal zijn, zal vooral afhankelijk zijn van: a) de mate waarin het terrorisme zich mondiaal verder ontwikkelt, b) er effectieve maatregelen zijn te treffen tegen andere typen aanslagen waardoor verschuivingseffecten kunnen ontstaan en c) er maatregelen te treffen zijn tegen de kwetsbaarheden van het internet en van fysieke en virtuele doelen die via het internet zijn gekoppeld.

3

3.1 CONTEXT EN VORMEN VAN INTERNETGEBRUIK

Ondanks dat jihadisten een terugkeer naar de glorietijd van de islam voorstaan en gruwen van de verderfelijke invloeden van het Westen, gebruiken zij het internet als middel - net als gewone burgers - voor verschillende doeleinden. De jihadisten beschouwen het internet zelfs als een cruciaal middel voor de jihad, hetgeen ook wordt gepropageerd. *"Dit is het internet dat Allah in dienst heeft genomen om de jihad en de mujahidin te dienen, dat gekomen is om jullie belangen te dienen - aangezien de helft van de strijd van de mujahidin op internetpagina's wordt uitgevochten - het enige kanaal voor mujahidin-media".*[1] Dat ze het beschouwen als een cruciaal middel komt ook sterk naar voren in een uitspraak van een bekende Syrische islamistische geestelijke prediker en voormalige leider van de Al Muhajiroun die luidt: *"We have no problems with technology. Other people use the Web for stupid reasons, to waste time. We use it for serious things."*[2]

Hoewel deze studie zich specifiek richt op jihadisten, ontkomen we er niet aan om op sommige plaatsen ook te kijken naar het salafisme. Het salafisme kan worden omschreven als een oriëntatie in de soennitische islam. Binnen het salafisme staat de terugkeer van moslims naar de zogenaamde 'zuivere islam' centraal. Salafisten verstaan hieronder de geloofspraktijk, zoals vormgegeven door de salaf, wat letterlijk voorouders betekent. Met de salaf wordt verwezen naar de profeet Mohammed, zijn metgezellen en zijn onmiddellijke opvolgers. De meeste hedendaagse salafisten vullen deze terugkeer naar de zuivere islam op een ultra-orthodoxe, puriteinse wijze in. Zij stellen dat ware gelovigen zich in alles letterlijk dienen te richten naar de Koran en de Soenna. Het salafisme bestaat uit verschillende stromingen. Voor deze studie wordt volstaan met het benoemen van de twee belangrijkste stromingen: de niet-jihadistische en de jihadistische (gewelddadige) vorm van het salafisme. De niet-jihadistische vorm van het salafisme wil 'ketterse' invloeden uit de islam bannen en de moslims terugbrengen tot de 'zuivere islamitische levenswijze'. De jihadistische vorm van het salafisme stelt dat de zuivere islam niet alleen gewaarborgd wordt door het uitbannen van ketterse invloeden uit het persoonlijke leven van elke moslim. Ook dient de gewapende strijd tegen de vijanden van de zuivere islam te worden gevoerd. Wanneer in deze studie wordt gesproken over het salafisme, dan wordt hiermee de niet-jihadistische vorm van het salafisme bedoeld en met 'salafisten' de aanhangers van deze variant. Dit in tegenstelling tot de jihadistische vorm die we rekenen onder het begrip 'jihadisten'.

Het internetgebruik door jihadisten is voor een deel zichtbaar voor iedereen die zich op het internet begeeft. In sommige gevallen kost het iets meer moeite om het internetgebruik door jihadisten waar te nemen, maar is dat wel mogelijk. Daarvoor is bijvoorbeeld een gebruikersnaam en een wachtwoord vereist. Voor een deel echter vindt het internetgebruik door jihadisten

1 Benschop 2006a, onder verwijzing naar S. Ulph, 'Mujahideen to Pledge Allegiance on the Web', in: Terrorism Focus, 2, 22 (29 november 2005).
2 Higgins e.a. 2002.

achter afgeschermde delen van het internet plaats. Dit zijn de heimelijke activiteiten die onzichtbaar blijven zonder de inzet van bijzondere bevoegdheden door opsporings- en inlichtingeninstanties. Het is evident dat meer bekend is over de zichtbare activiteiten dan over de heimelijke activiteiten en dat deze studie zich vooral richt op het zichtbare deel.

Dit hoofdstuk start met algemene achtergronden van jihadistisch internetgebruik (paragraaf 3.2) en een analyse van de Nederlandse situatie (paragraaf 3.3). Vervolgens worden in de paragrafen 3.4 tot en met 3.10 de volgende vormen van internetgebruik uitgediept: propaganda, informatie-inwinning, fondsenwerving, rekrutering, training, onderlinge communicatie en planning, en de creatie van virtuele netwerken. Iedere paragraaf eindigt met een beoordeling van de dreiging van deze vorm van internetgebruik voor Nederland, maar wel bezien in de internationale context. Paragraaf 3.11 analyseert vervolgens in hoeverre en op welke wijze de vormen van internetgebruik invloed hebben op radicalisering. Het hoofdstuk eindigt met een slotbeschouwing.

3.2 ACHTERGRONDEN

3.2.1 Inleiding

Deze paragraaf schetst enkele algemene noties over het jihadistische internetgebruik. Aan de orde komen: a) de voordelen van het internet voor jihadisten, b) de modus operandi die ze hanteren en de mate waarin zij zich bewust zijn van hun veiligheid op het internet en c) de opbouw van de virtuele jihadistische gemeenschap.

Het is van groot belang om te beseffen dat we het internetgebruik door jihadisten niet geïsoleerd kunnen bestuderen van algemene ontwikkelingen in de samenleving, op het internet en in het jihadisme. Zo is het gebruik van het internet in onze samenleving de laatste jaren aanzienlijk toegenomen evenals de bandbreedte van het internet. Was een ADSL-aansluiting enkele jaren geleden nog voor vele particulieren te hoog gegrepen, intussen heeft een groot deel van de huishoudens een permanente en snelle verbinding met het internet. Een ander feit is dat jihadisten in Nederland vaak jong zijn en dat jongeren veelal de eerste gebruikers zijn van de nieuwste ICT. Is het maken van een website voor menig veertigplusser nog omgeven met een hoop mystiek, voor menig jongere is dat geen enkel probleem. Internetgebruik, maar ook het zich afzetten tegen de gevestigde orde en provocerend gedrag, passen binnen de jeugdcultuur, een cultuur waar ook jonge jihadisten op zijn minst door beïnvloed raken en daar onderdeel van uitmaken. En binnen de internationale jihadistische beweging is eerder sprake van elkaar inspireren en kopieergedrag, dan van een centrale aansturing. In deze context is het niet vreemd dat het jihadistische internetgebruik zich blijft ontwikkelen, Nederlandse virtuele jihadisten zich laten inspireren door buitenlandse jihadisten en hun gedrag overnemen zonder dat sprake is van een aansturing van buitenaf.

3.2.2 Voordelen van het internet voor jihadisten

Het internet als nieuw medium heeft enkele unieke kenmerken. Nieuw ten opzichte van de telefoon, televisie en radio is dat zowel ogen, oren als mond tot hun recht komen en het interactieve karakter op het hele spectrum van één-op-één-communicatie tot communicatie van velen met velen zonder beperkingen van plaats en tijd. Nieuw is ook het multimediale karakter: tekst, video, audio en foto's. Een ander aspect is dat de afzonderlijke technieken en infrastructuren zoals die van televisie, radio en datacommunicatie, steeds meer geïntegreerd raken. De voordelen van de afzonderlijke media zijn daardoor gecombineerd voorhanden. Is iemand voor het verzenden van een boodschap via kranten, televisie en radio nog afhankelijk van redacties en journalisten en van de kenmerken van het specifieke medium, via het internet kan iedereen als het ware zijn eigen krant, televisie- of radiostation creëren tegen geringe kosten. Individuen en organisaties zijn zowel consumenten als producenten en kunnen zelf bepalen wat zij ontvangen en zenden. Zowel consumenten als producenten kunnen daarbij ook nog eens (tot op zekere hoogte) anoniem blijven. Een ander aantrekkelijk punt is de beperkte of afwezigheid van regulering, censuur of andere vormen van overheidscontrole.[3]

In dit hoofdstuk zal blijken dat de jihadisten deze voordelen uitbuiten. Zo benutten zij het multimediale karakter volop en richten zich op meerdere doelgroepen. Dat doen ze in de vorm van bijvoorbeeld video-uitzendingen via het internet, digitale magazines, animaties, cartoons en losse berichten en door veelvuldig gebruik te maken van banners, logo's en muziek (strijdliederen) met een jihadistische achtergrond.

3.2.3 (Inter)nationale modus operandi en veiligheidsbewustzijn

Abu Musab as-Suri, strateeg en ideoloog van de jihadistische beweging en al Qa'ida, heeft een model ontwikkeld voor zogeheten virtuele jihadistische verzetsbrigades. Dit model fungeert als inspiratiebron voor de modus operandi van de jihadistische beweging op het internet en kan als volgt worden samengevat. Moslimjongeren die interesse hebben voor aansluiting bij de jihadstrijd moeten eigen totaal onafhankelijke jihadbrigades oprichten. Deze brigades opereren zonder functioneel verband met de centrale leiding. De enige band die ze daarmee onderhouden is de gemeenschappelijke ideologie en doelstelling. Deze verzetsbrigades kunnen in drie soorten worden ingedeeld. De eerste soort vormen de *initiërende* en *oprichtende brigades*. Zij zorgen voor de werving en de initiële opleiding van nieuwe leden op allerlei terreinen: ideologie, veiligheid en militaire technieken. De tweede soort bestaat uit *operationele brigades* die zich direct aansluiten bij het front. De derde soort zijn de *clandestiene mobiliserende brigades*. Personen met een uitstekende toerusting in de islamitische kennisdomeinen, maar ook in politieke, intellectuele en media-aangelegenheden vormen deze jihadbrigades. Het zijn mensen die eveneens veel ervaring hebben in het gebruik van het internet en de ICT-netwerken. Kennis van het internet en de computertechnieken behoort volgens as-Suri tot de basisuitrusting van de jihadstrijder. De initiërende en oprichtende brigades zijn als het ware 'informatiebrigades' waarvan de taak is om de jihadistische boodschap te verspreiden langs literatuur, onderzoek,

3 Kortekaas 2005, p. 98-99, Castells 1998, p. 60-65, Weimann 2006, p. 23-31.

publicaties en met name langs geheime communicatiemiddelen, zoals het internet. Zij vertalen artikelen, publicaties en nieuwsberichten van het verzet in alle talen van moslims en van de wereld. Deze brigades zouden aandacht moeten besteden aan de veiligheid van de verspreiding van materialen. Zij ontwikkelen een eigen werkwijze en passen zich aan aan de lokale omstandigheden van de landen waarin zij opereren.[4]

De virtuele jihadisten opereren op professionele wijze en zijn na verwijdering als gevolg van justitieel ingrijpen weer snel, onder een andere naam en bij een andere provider (in het buitenland), online. Ook verplaatsen sites zich steeds vaker spontaan. Sites die lang hetzelfde adres hebben worden minder druk bezocht, omdat gebruikers vrezen dat inlichtingendiensten ze in de gaten houden of runnen. Verder valt te constateren dat op de meeste jihadistische websites doorgaans veel en actuele informatie te vinden is, bijvoorbeeld in de vorm van kwalitatief hoogwaardige multimediabestanden of commentaar op de actualiteit. Beheer vindt zeer actief plaats, onwelgevallige content wordt verwijderd en er zijn ballotages ten aanzien van de registratie op sites. De meeste islamistische sites waar openlijk steun aan de jihadstrijd wordt gegeven draaien op Amerikaanse servers.[5] Van eenentwintig in 2004 beschreven Hezbollah-sites waarop het martelaarschap en terroristische activiteiten bevorderd worden, maken er bijvoorbeeld negentien gebruik van diensten van Amerikaanse bedrijven.[6] Ook uit andere bronnen blijkt de populariteit van Amerikaanse servers. Deels is dit toe te schrijven aan de betrouwbaarheid, de toegankelijkheid en de geavanceerdheid van dergelijke servers en het feit dat zij veel bezoekers tegelijkertijd kunnen verwerken, deels aan de grondwettelijke vrijheid van meningsuiting. Veel anti-Amerikaans materiaal staat dus op Amerikaanse servers.[7] Daarnaast maakt men ook gebruik van Europese en Aziatische dienstverleners (web-hosting bedrijven), waaronder in Maleisië.

Organisaties maken soms ook misbruik van vrije ruimte op servers die niet aan henzelf toebehoren (zie paragraaf 3.3.3.2), en jihadistische websites blijken steeds vaker gebruik te maken van dienstverleners die gratis (of voor bescheiden prijzen) webruimte aanbieden, de zogenaamde 'third party file-hosting services'. Zij gebruiken dat vooral voor het beschikbaar stellen van audio- en videomateriaal. Door gebruik te maken van dergelijke diensten ontstaat meer continuïteit in het enorme aanbod aan materiaal en ontstaat een schuiladres, aangezien het jihadistische materiaal zich achter een onvermoed en onverdacht internetadres bevindt. Tevens biedt de beschikbare ruimte meer mogelijkheden voor het aanbieden van bestanden in verschillende formats. Zo zijn begin 2006 via een file-hosting service opnames van al-Zawahiri beschikbaar gekomen in drie formaten: mp3 (audio), RealMedia (standaard mediaplayer) en mpg (formaat geschikt voor het branden van video-cd's).[8]

Zowel de aanbieders van jihadistische websites en materialen als de consumerende informatiezoekers beseffen dat het internet weliswaar een vrijplaats is, maar geen volledig anonieme vrijplaats. Veel bedrijven en software-applicaties verzamelen namelijk informatie over gebruikers, hun interesses en hun surfgedrag. Ook politie- en inlichtingendiensten maken gebruik van de mogelijkheden die het internet biedt op dit punt. Wanneer iemand zich op het internet begeeft, is hij in beginsel traceerbaar aan de hand van het unieke IP-adres van zijn computer. De jihadisten doen daarom hun best om anoniem te blijven en gebruiken daarvoor diverse mogelijkheden, waaronder het werken vanuit een internetcafé. Het voert te ver om deze mogelijkheden uitgebreider te behandelen. Feit is wel dat op jihadistische sites gesproken wordt over de mogelijkheden en ook aanwijzingen worden gegeven hoe hiervan gebruik te maken.

Jihadisten doen ook hun best om pottenkijkers buiten de deur te houden. Sommige jihadistische sites beschermen zich zelf met wachtwoorden. Dat is veelal nog laagdrempelig. Een verdergaande vorm van afscherming is dat nieuwe gebruikers moeten worden geïntroduceerd door één of meerdere gerespecteerde gebruikers. Bovendien werpen zij drempels op door elkaar de maat te nemen, waardoor iemand met geringe kennis van het Arabisch en het jihadisme snel door de mand zal vallen. Verder wordt een gebruiker die alleen maar rondkijkt en niet actief deelneemt, of afwijkende meningen verkondigt, verwijderd. Een andere trend is dat een steeds uitgebreider registratieformulier moet worden ingevuld (inclusief motivatie voor deelname, vaak in het Arabisch), en dat wachtwoorden maar een korte periode geldig zijn.

Dat de jihadisten veiligheidsbewust zijn blijkt bijvoorbeeld in 2006 uit meerdere berichten waarin waarschuwingen en tips zijn verschenen. Deze hebben onder andere betrekking op het gebruik van Google, Google-Toolbar[9] en het risico dat die applicatie als spyware ingezet kan worden.[10] Ook wordt aandacht besteed aan de wijze waarop bijvoorbeeld de Saoedische autoriteiten gebruikers van webfora monitoren en traceren, waarbij wordt aangegeven dat e-mail-adressen die eindigen op .sa nooit veilig kunnen zijn, aangezien de Saoedische veiligheidsdiensten daar altijd bij zouden kunnen.[11] Verder zijn jihadisten zich bewust van cyberaanvallen van tegenstanders op hun sites en wisselen tips uit hoe hier mee om te gaan. Ook waarschuwen jihadisten elkaar voor het optreden van opsporings- en inlichtingendiensten op de discussiefora.[12] Een nieuw verschijnsel zou het opzetten van *honeypots* vóór terrorismebestrijders zijn. Daarbij zou bijvoorbeeld een tactiek worden gebruikt als het verspreiden van vooraf afgesproken wachtwoorden, waardoor inlichtingen- en opsporingsdiensten herkenbaar worden op webfora, maar mogelijk ook in fysieke bijeenkomsten. Het zou hen dragers kunnen maken van valse informatie en kwetsbaar maken voor ontvoeringen.[13] Overgens zouden ook anderen zoals onderzoeksjournalisten slachtoffer kunnen worden van dergelijke acties.

Op de publicaties van de jihadistische groepen en geestelijke leiders rusten geen auteursrechten. Integendeel, veel publicaties zijn voorzien van de aanbeveling: 'Auteursrechten gelden niet voor deze publicatie. Gebruik het voor datgene dat God en zijn profeet zint'. Trainingsboeken voor de voorbereiding en uitvoering van jihadistische acties stellen echter een beperking

4 Vertaling uit het Arabisch van as-Suri 2004, p. 1336 en 1408-1410.
5 Bunt 2003, p. 207.
6 Weimann 2006, p. 231.
7 Benschop 2006a.
8 SITE-Institute 2006a
9 SITE-Institute 2006q.
10 Washington Post 2006.
11 SITE-Institute 2006r.
12 Eigen waarneming op een forum op 04-01-2006.
13 Newsbytes 2006.

aan het gebruik. De gebruiker wordt gevraagd om de eed af te leggen dat 'de opgedane kennis niet tegen moslims gebruikt gaat worden'.

3.2.4 Opbouw virtuele jihadistische gemeenschap en voorbeelden

3.2.4.1 Opbouw algemeen

De virtuele jihadistische gemeenschap bestaat uit grote aantallen websites, webfora en weblogs van terroristische groeperingen en sympathisanten. Hoewel uiteenlopende indelingen hiervan denkbaar zijn, beschrijven wij die aanwezigheid aan de hand van de volgende onderverdeling:

1. Officiële sites van jihadistische organisaties;
2. Sites van jihadistische geleerden;
3. Overige websites, fora en weblogs;
4. Distributiekanalen.

De grenzen binnen deze indeling zijn echter niet altijd scherp te trekken. Sommige sites die een belangrijke rol hebben in de distributie van materiaal, hebben bijvoorbeeld tevens de rol van een webforum. Dat geldt zeker voor websites die door sommigen als moedersites worden omschreven. Ze fungeren als stabiele, geautoriseerde bronnen van informatie uit de eerste hand, in het bijzonder voor theologische kwesties, ideologische debatten, strategische kwesties en officiële doctrines en persberichten.[14] De moedersites kennen vaak 'spiegelsites': kopieën die klaar staan om online gezet te worden wanneer nodig. Het online zetten van spiegelsites kan nodig zijn wanneer een (overheids)organisatie ingrijpt en de website offline haalt, of dat ze het slachtoffer worden van een particuliere 'internetwreker'.[15] Het kan ook gebeuren dat de website een *'parasite'* is (zie paragraaf 3.2.3) die betrapt wordt en van de betreffende server wordt verwijderd.

3.2.4.2 Officiële sites van jihadistische organisaties

Vele jihadistische organisaties manifesteren zich op het internet. Enkele daarvan worden hieronder genoemd. De kern van al Qa'ida ontbreekt uiteraard niet. De oorspronkelijke, officiële alneda.com website van al Qa'ida was eind 90-er jaren geregistreerd in Singapore en te vinden op webservers van verschillende providers in Maleisië en de VS (Texas).[16] Al Neda ('De oproep') bevatte redactionele artikelen die door belangrijke leiders van al Qa'ida werden geschreven. Er werd in opgeroepen tot het plegen van terroristische acties en uitgevoerde aanslagen werden uitvoerig gelegitimeerd. Het discussieforum van de site bevatte veel relatief onschuldige berichten waarvan wordt aangenomen dat het gecodeerde signalen waren.
In de multimediasectie stonden foto's, audiobestanden en video's van Osama bin Laden.[17]
Na verwijderd te zijn op verzoek van de Verenigde Saten heeft de site rondgezworven. Eind 2002 verliep de domeinnaam-registratie, waarna de naam in handen kwam van een privé-persoon. Dit had tot gevolg dat de al Qa'ida site een zogeheten 'parasite' werd, waarbij gebruik gemaakt werd van een fout in webserver-

14 Lia 2006.
15 Benschop 2004.
16 Weimann 2006, p. 67.
17 Benschop 2004.

programmatuur om de ruimte van een bestaande, legale site te misbruiken: het soort technieken dat in het hackerscompendium van het GIMF wordt genoemd (zie paragraaf 2.2.5). Dit parasiteren werd geregeld ontdekt, en de parasite heeft daarom rondgezworven van september 2002 tot april 2003. Daarna keerde de site zelfstandig terug onder de naam faroq.com, voorzien van de Al Neda banner. Deze site begon met een focus op de strijd in Irak, maar langzaam verscheen de originele content van alneda.com weer op de site.[18]

Een andere al Qa'ida website was het *Center for Islamic Studies and Relief*. Deze website kende bijdragen van Abu Gaith en al-Zawahiri, die er zijn oorlogsverklaring aan de VS publiceerde. Daarnaast was de website een leverancier van het tweemaandelijkse magazine *Sawat al-Jihad* of *The Voice of Jihad*. De eerste editie was voornamelijk gewijd aan internetpropaganda, en het magazine geeft inzicht in één van de hoofddoelen van al Qa'ida: het genereren van steun van het algemene publiek en legitimiteit bij moslims.[19]

Hoewel 'de' officiële al Qa'ida website momenteel niet bereikbaar is, zou al Qa'ida vertegenwoordigd zijn op ongeveer vijftig sites,[20] die voor propaganda- en distributiedoeleinden worden benut. Deze sites vormen onderdeel van het grote distributie- en communicatienetwerk van deze in de fysieke wereld opgejaagde organisatie, die in cyberspace de dans echter weet te ontspringen.Ook de jihadisten in Irak zijn actief op het internet. De bekendste hiervan zijn *Islamic Army in Iraq* en *The Islamic front of Iraqi resistance*. De website *Islamic Army in Iraq* biedt communiqués, artikelen, boeken, informatie over operaties, en twee online magazines: al-Fursan (De Ridders) en al-Kata'ib (de Bataljons). Er is tevens een onderdeel geheten: 'Vecht met ons', waar bezoekers worden aangemoedigd om deel te nemen aan de jihad.[21]

3.2.4.3 Sites van jihadistische geleerden

Jihadistische geleerden verspreiden hun gedachtegoed in tekst, beeld en geluid, verzorgen *hyperlinks* (elektronische doorverwijzingen) naar andere (in hun ogen) gezaghebbende sites, en kunnen rechtstreeks via e-mail en chatprogramma's, zoals paltalk of instant-messenger, met geïnteresseerden communiceren. Met name as-Suri is populair bij jihadisten. Hij heeft een zeer omvangrijk werk op zijn naam staan, dat ongeveer 1600 pagina's omvat (zie ook paragraaf 3.2.3 en 3.8). Het werk is oorspronkelijk in het Arabisch verschenen, maar enkele delen zijn al vertaald naar het Engels. Gelet op de toename van naar het Nederlands vertaalde materiaal (zie paragraaf 3.3.4), is het waarschijnlijk slechts een kwestie van tijd dat vertalingen van onderdelen van het werk van as-Suri in het Nederlands verschijnen en in Nederland gebruikt gaan worden.[22] Ook Abu Basir al Tartousi is een gezaghebbende jihadistische geleerde die veel informatie en kennis aanbiedt, inclusief commentaar op recente ontwikkelingen in het Midden-Oosten, het Westen en met name het Verenigd Koninkrijk. Vermeld dient te worden dat deze sites regelmatig uit de lucht zijn en dat zij zich vaak verplaatsen. Dit neemt niet weg dat dergelijke sites populair zijn en dat het materiaal op die sites steeds verder verspreid raakt.[23]

18 Weimann 2006, p. 68.
19 Weimann 2006, p. 44, 68.
20 Weimann 2006, p. 65.
21 Rogan 2006, p. 19.
22 Interview 5.
23 Rogan 2006, p. 32.

3.2.4.4 Overige websites, fora en weblogs

Een meer interactieve variant van het jihadistische internetgebruik vindt plaats via webfora en weblogs. De webfora fungeren in eerste instantie als discussieplatform voor het bespreken van uiteenlopende zaken, van actualiteiten tot voorbereiding op de jihadstrijd. Veel fora zijn druk bezocht. Behalve dat er discussie plaatsvindt, worden er *hyperlinks* naar de belangrijke websites, materialen en verhandelingen gegeven.

Naast de zeer populaire webfora zijn er tevens jihadistische weblogs of 'blogs'. Deze hebben vaak niet de oorspronkelijke functie van een *blog*, namelijk het verspreiden en bediscussiëren van actuele meningen. Zij dienen in dat geval meer als een distributiekanaal dat hyperlinks verzorgt naar de populairste jihadistische sites: een soort elektronisch prikbord. Deze *blogs* hebben als voordeel dat ze geen hinder ondervinden van valse, verstorende postings, maar daarmee zijn ze tevens veel minder interactief. Om diezelfde reden zal de populariteit juist kunnen toenemen. Het gedachtegoed kan snel, actueel en ongestoord worden verspreid.[24] Al met al hangen veel jihadistische *blogs* tussen daadwerkelijke interactieve sites en distributiesites (zie hierna) in.

3.2.4.5 Distributiekanalen

De distributiekanalen kunnen nader worden onderverdeeld, namelijk in die van directory-sites, fansites of supportsites en productiebedrijven. Professionele *directory-sites* bevatten met name zeer uitgebreide en zeer actuele *hyperlinks* naar jihadistische websites zoals locaties voor het downloaden van bestanden, forums, nieuwssites, sites van sjeiks, sites met lijsten van martelaren et cetera. Een voorbeeld van een professionele en stabiele directory is Dalil Meshawir die een Engelse en een Franse versie kent.[25] De distributiekanalen hebben een ongeorganiseerd karakter zoals gebruikelijk op het internet. Er schuilt derhalve geen centrale aansturing of regie achter.

Sommige distributiekanalen worden gevormd door *fansites* of *supportsites*, die door liefhebbers (en computerkenners) zijn opgezet. De sites zien er ontwerptechnisch vaak goed uit, maar zijn soms ook duidelijk opgezet door amateurs, en daarom niet altijd even stabiel of actueel. De primaire taakopvatting van fansites en supportsites lijkt te zijn het zo breed mogelijk distribueren van het materiaal dat afkomstig is van moedersites en andere locaties, zoals de online al Qa'ida magazines *Sawat al-Jihad* en *al-Battar*. Ze kunnen soms enkel als 'portal' fungeren, hetgeen inhoudt dat met name *hyperlinks* naar andere websites of downloadlocaties worden aangeboden. Andere bieden een soort encyclopedie van specifieke bestanden of *hyperlinks* naar dergelijke bestanden, bijvoorbeeld gericht op training en wapens. Sommige fansites of supportsites functioneren dus als directories.

Een derde variant van distributiekanalen zijn de *productiebedrijven*, ook wel aangeduid als mediagroepen, zoals het Global Islamic Media Front (GIMF) en as-Sahab, het (vermeende) mediabedrijf van al Qa'ida. Zij verspreiden

24 Rogan 2006, p. 22.
25 Rogan 2006, p. 22, 'Dalil' betekent: 'mijn index'.

Figuur 3.1 Voorbeelden van supportsites

al-Muhajiroun (UK). Deze website bevat secties inzake de ramadan en conferenties, maar tussen die informatie valt een stuk te bespeuren over 'Aqd Al Amaan': The Convenant of Security. Dit convenant houdt in dat Moslims in het Westen hun land van verblijf niet mogen aanvallen. Andere moslims mogen dezelfde ongelovigen echter wél aanvallen. De website spreekt op diverse locaties over "the magnificent contemporary Mujahideen and Martyrs", "the magnificent 19 of 9/11", "the domination and influence of the kufr states" en "This book....gives an Islamic solution to the Cancer known as America".

Supporters of Shareeah: de site van Abu Hamza al Masri. Dit is een erg moderne site, die gebruik maakt van flash-technieken en multimedia. De site heeft een sterk propagandistisch karakter, en lijkt zelfmoordaanslagen te steunen of te verheerlijken.[26]

Tajdeed.org.uk, een supportsite van de Saoedische dissident Mohammed al-Masari, geregistreerd in Londen. Deze website noemde de bomaanslagen in de Londense metro een 'overwinning voor fundamentalisten'.[27]

het materiaal van de moedersites, maar maken tevens zélf mediaproducties, veelal gebaseerd op geautoriseerd materiaal, bijvoorbeeld in de vorm van compilaties of compendiums zoals het hackerscompendium.

Het GIMF is één van de belangrijkste spreekbuizen van al Qa'ida, en is onder meer verantwoordelijk voor het professioneel geproduceerde jihadistische internetjournaal *'Voice of the Caliphate'*. De status van het GIMF is mede af te lezen aan het feit dat al Qa'ida zou hebben aangegeven dat sympathisanten alleen informatie serieus dienen te nemen die getoetst, goedgekeurd en bevestigd is door het GIMF op Yahoogroups.com.[28] Het GIMF presenteert zichzelf in ieder geval als knooppunt (men gebruikt het woord Qa'ida, basis) voor jihadistische, anti-joodse propaganda op het internet. Dat zij hun werk serieus nemen blijkt uit het feit het GIMF mensen met ervaring op het gebied van videoproducties en het redigeren van websites (zoals IT- en communicatie-experts, filmproducenten en fotografen) heeft opgeroepen om hun bijdrage te leveren.[29] Het GIMF vertaalt haar producties veelal in het Engels en Frans, maar heeft onlangs ook bepaalde statements van de *Mujahideen Shura Council* en videoproducties van as-Sahab in het Duits vertaald, die geplaatst zijn op een website.[30]

De mediagroep as-Sahab is onder meer verantwoordelijk voor de video *"A letter to the people of the West, in occasion of the four year anniversary of the attacks of New York and Washington"*, een 45 minuten durend interview met *al-Zawahiri*, gemaakt in september 2005, uitgegeven in december 2005. Alle acht de videoboodschappen van al-Zawahiri die in 2005 werden

26 Beide voorbeelden afkomstig van Weimann 2006.
27 Cops@Cyberspace 2006a.
28 Weimann 2006, p. 228.
29 Benschop 2004.
30 SITE-Institute 2006e.

uitgezonden droegen het logo van as-Sahab. De opnames zijn steeds professioneler geworden, met gebruikmaking van logo's en Engelse ondertiteling. In de eerste helft van 2006 zijn al drie audio-opnamen van Bin Laden en zes opnames van *al-Zawahiri* via as Sahab verschenen.[31] Begin juli werd een video ter gelegenheid van de 'verjaardag' van de aanslagen in Londen van 7 juli 2005 aangekondigd.[32]

3.3 JIHADISME OP HET NEDERLANDSE INTERNET

3.3.1 Inleiding

Evenals veel andere westerse landen heeft Nederland sinds enkele jaren te maken met virtueel jihadisme op het *Nederlandse internet*. We kunnen spreken van het Nederlandse internet wanneer een website, forum (et cetera): 1) Nederlands als voertaal heeft, 2) op de een of andere manier georiënteerd is op Nederland of 3) fysiek dan wel virtueel vanuit Nederland wordt gefaciliteerd of in Nederland draait. De criteria voor een jihadistische site zijn opgenomen in bijlage 2.

De informatie in deze paragraaf is vooral gebaseerd op waarnemingen tijdens het monitoren van het internet en de inhoudsanalyse van het aangetroffen materiaal op sites die (in ieder geval tot en met mei 2006) in de lucht waren evenals op open bronnen. Het overzicht van jihadistische sites is niet volledig. De besproken sites zijn wel toonaangevend voor de afgelopen vier jaar omdat zij breed bekend waren en op gezette tijden de aandacht kregen van de media en de politiek. Vermelding van een site vindt bovendien alleen bij naam en toenaam plaats wanneer deze niet langer bestaat: dit om te vermijden dat actuele sites opeens veel extra bezoek zouden krijgen. Eerst wordt een typering gegeven van salafistische Nederlandse sites. Daarna worden de jihadistische sites op het Nederlandse internet beschreven en vervolgens de Nederlandse virtuele jihadisten. Afgesloten wordt met een overzicht van de bevindingen.

3.3.2 Salafistische sites in Nederland

Het Nederlandse internet kent een groot aantal sites met een islamitische identiteit en karakter. Naast enkele neutrale sites, is het leeuwendeel salafistisch. De salafistische sites kunnen globaal in drie categorieën worden ingedeeld. In de eerste plaats de sites die zich hoofdzakelijk richten op de salafistische leer in de dogmatiek, erediensten en ethiek. Het zijn als het ware a-politieke sites, die doelbewust trachten om politieke vraagstukken, en derhalve onderwerpen die te maken met de jihadstrijd, te mijden. De tweede categorie bestaat uit een beperkt aantal salafistische sites die kritische geluiden tegen de regimes in het Midden Oosten vermijden en waarschijnlijk zijn gestimuleerd vanuit de Saoedische staat. Het merendeel daarvan staat in het teken van de Da'wa, de verspreiding van het islamitische geloof en de bekering van autochtone Nederlanders. Een belangrijke functie van deze sites is de totstandbrenging van een salafistische geloofsgemeenschap. Voor zover deze sites een actualiteitenrubriek hebben, besteedt men aandacht aan de Palestijnse kwestie, de oorlog in Irak en Afghanistan. Daarbij wordt de berichtgeving van de westerse media zonder commentaar overgenomen. Een derde categorie kan omschreven worden als 'hybride' sites. Het zijn sites die het salafistische gedachtegoed propageren, maar impliciet de jihadstrijd goedkeuren of daar in ieder geval niet expliciet afstand van nemen.

31 NRC-Next 2006.
32 SITE-Institute 2006k.

De jihadistische internetsites in Nederland onderscheiden zich van de salafistische door het expliciet politiseren van de theologische, dogmatische, liturgische en ethische grondslagen en het oproepen tot de (gewapende) jihadstrijd.

3.3.3 Jihadistische sites in Nederland

3.3.3.1. Drie perioden

De eerste manifestatie van jihadistische terroristische bewegingen in Nederland vond plaats rond het jaar 2000. De terroristische dreiging voor Nederland was een afgeleide van de internationale dreiging.[33] In 2002 sloeg de terroristische dreiging om van exogeen naar endogeen. En in 2003 richtten de jihadstrijders zich nadrukkelijk op Nederland als doelwit. De ontwikkeling van jihadistische sites volgde in grote lijnen dit patroon.

De eerste jihadistische sites waarmee Nederland te maken kreeg waren in het buitenland gevestigd of op het buitenland georiënteerd. De gebruikte taal was vooral Arabisch. In de loop van het jaar 2001 trad echter een verschuiving op. Er kwamen sites die zich specifiek op Nederland richtten of waren opgezet door Nederlandse jihadisten, maar nog wel met een buitenlandse oriëntatie. Weer later, rond 2003, kwamen Nederlandse jihadistische sites die waren gericht op de jihadstrijd in Nederland. Er zijn dus drie, deels overlappende, categorieën te onderkennen, die deels ook te bezien zijn als perioden:

1. op het buitenland georiënteerde jihadistische sites in Nederland;
2. Nederlandse jihadistische sites met een buitenlandse oriëntatie;
3. Nederlandse jihadistische sites gericht op Nederland.

3.3.3.2. Op het buitenland georiënteerde jihadistische sites in Nederland

Vóór het jaar 2001 was er geen jihadistische site die zich qua taal, inhoud en oriëntatie specifiek op Nederland richtte. Onder deze categorie zijn - voor zover bekend - een drietal sites te scharen waarbij sprake is van een zekere relatie met Nederland, namelijk:

- *www.qoqaz.com*, een site in het Arabisch die de jihadstrijd in Tsjetsjenië steunde. In het jaar 2002 hebben jihadistisch georiënteerde personen uit Nederland postings geplaatst op die website en in juni 2002 hebben twee personen uit Nederland korte bijdragen gezet op het discussieforum.
- Een site die werd gehost door een Nederlands bedrijf.
- *www.alneda.com*, een site van al Qa'ida, die op een bepaald moment gebruikmaakte van de via hacking verkregen webruimte van een Nederlandse voetbalclub. Eén van de documenten daarop was een toespraak van Bin Laden.

33 AIVD 2002a, p. 21.

3.3.3.3. Nederlandse jihadistische sites met een buitenlandse oriëntatie

De jihadistische actoren achter deze sites opereerden vanuit Nederland, ontwierpen diverse Nederlandstalige internetomgevingen, richtten zich op het Nederlandse publiek en riepen Nederlandse jongeren expliciet op tot deelname aan de jihadstrijd. Van deze categorie behandelen we twee sites.

De site *www.qoqaz.nl* geldt als eerste volwaardige jihadistische site met alle daarbij behorende functionaliteiten: audiovisueel aanbod, nieuwsrubriek en interactieve toepassingen (e-mail en forum). Aanvankelijk was deze site georiënteerd op de jihadstrijd in Tsjetsjenië en publiceerde artikelen, foto's en video's daarover. Maar in maart 2001 publiceerde deze site een artikel waarin moslimjongeren in Nederland worden opgeroepen tot deelneming aan militaire trainingen als voorbereiding op de jihadstrijd. Geïnteresseerde jongeren werden verwezen naar bijvoorbeeld de banenwinkels van de Koninklijke Landmacht en er werden tal van adviezen gegeven. In april 2001 werd de website gesloten, maar dook weer op in 2003 en april 2004.

De site *www.geocities.com/sluitjeaan* is vermoedelijk van start gegaan in het voorjaar van 2003. De naam 'sluit je aan' verwijst naar een publicatie van Abdullah Azzam, een vooraanstaande jihadist en de medeoprichter van al Qa'ida. Deze website richt zich duidelijk op de jihadstrijd in Afghanistan, Tsjetsjenië en Palestina. De site startte met algemene ideologische en politieke verhandelingen in het Nederlands en het Engels. Het was in feite een Nederlandse versie van de in Groot-Brittannië gevestigde jihadistische site: *www.azzam.com*. De aandacht verschoof langzaam naar gerichte oproepen tot voorbereiding van en deelname aan de jihadstrijd. In september 2003 verscheen een oproep aan moslimjongeren om deel te nemen aan de jihadstrijd. De site had geen zelfstandig domein op het internet, maar maakte gebruik van een subsidiaire ruimte aangeboden door een internetbedrijf. De interactieve functionaliteiten waren beperkt, maar de site nodigde de bezoekers nadrukkelijk uit tot bijdragen en stimuleerde hun inbreng. Na commotie in de media en de politiek over de publicaties van deze site is hij even verdwenen, om vervolgens weer op een andere internetlocatie te verschijnen. Meteen daarna werd deze website weer uit de lucht gehaald.

3.3.3.4. Nederlandse jihadistische sites gericht op Nederland

In de loop van het jaar 2003 was een aantal jihadisten actief op het internet. Zij waren met name actief onder de zogeheten msn-groepen. In het voorjaar van 2004 doken een nieuwe msn-groep, twee websites met een uitgesproken jihadistisch karakter (MuwahhidinDeWare-Moslims, 5434_, Tawheed_wal_Jihaad) en andere statische internetpagina's van beperkte omvang op.

De diverse msn-groepen en sites richtten zich qua inhoud op zowel de theoretische en dogmatische als op de praktische en operationele aspecten van de jihadstrijd. Qua inhoud leken zij in veel opzichten op elkaar. De proliferatie van jihadistische msn-groepen in het jaar 2004 en het veelvuldige gebruik ervan is wellicht te verklaren door de eenvoud van de toepassing

van deze faciliteit en het veelvuldige gebruik van msn bij jongeren. De msn-groepen werden geboren en gedoopt met expliciete jihadistische namen. Zij verdwenen gedurende een korte periode om weer elders op te duiken met een nieuwe naam en met een nieuw uiterlijk.
De msn-groepen gaven het ontwikkelingsniveau, de internetvaardigheden, maar ook de strategische oriëntatie aan van de virtuele Nederlandse jihadisten op dat moment.
Zij hebben het mogelijk gemaakt om ervaring op te doen met ontwerp en inhoud van een jihadistische site.

Figuur 3.2 Overzicht van jihadistische MSN-groepen (m.u.v. twee die nog in de lucht zijn)

Naam	**Periode**
De Basis	*januari 2003 - maart 2004*
De Basis2	*maart 2004 - juli 2004*
MuwahhidinDeWareMoslims	*juli 2003 - januari 2004*
	juli 2004 - september 2004
ElKhatab	*augustus 2003 - september 2004*
al-ansaar	*maart 2004 - juli 2004*
Shareeah	*april 2004 - september 2004*
*5434_*	*maart 2004 - oktober 2004*
Tawheedwaljihad	*augustus 2004 - oktober 2004*
Tawheedwalqitaal	*augustus 2004 - oktober 2004*
NIboeken	*december 2004 - februari 2005*
Ahloetawheed	*oktober 2004 - februari 2005*

De jihadisten ontwikkelden zich, maakten gebruik van nieuwe internetfunctionaliteiten en gingen in 2004 over tot het gebruik van de gratis tk.domeinen en Freewebs om eigen websites op te richten. Het .tk-domein kan verbonden worden met iedere andere website, webpagina, homepage, web profile, weblog, blog of web gallery. De registratie is eenvoudig uit te voeren. Het gebruik is gratis, maar er wordt wel reclame gemaakt op de webpagina's. Ook op Freewebs kunnen private personen, bedrijven en instellingen een gratis hosting nemen inclusief domeinnaam. Dit brengt geen verplichtingen of kosten met zich mee en men krijgt geen reclame opgedrongen. Het is voor iedereen vrij eenvoudig om via Freewebs een website online te krijgen.

Het gebruik van gratis tk.domeinen en freewebs door de jihadistische groepen in Nederland biedt vanzelfsprekend een financiëel voordeel, maar ook voordelen in termen van veiligheid. Het onderhouden van een eigen, betaalde site vraagt immers om registratie, administratie en beveiliging. Een gratis hostingprovider vergt vaak geen (correcte) registratie en de gebruiker profiteert van de professionaliteit van het hostingbedrijf qua beveiliging, technische know-how en stabiliteit van de dienstverlening. In figuur 3.3 zijn enkele tk.domeinen en freewebs opgesomd.

Figuur 3.3 jihadistische tk.domeinen en freewebs (m.u.v. twee die nog in de lucht zijn)

Naam	Periode
www.twaheedwaljihaad.tk	juni 2004 - september 2005
www.tawheedwalqitaal.tk	september 2004 - mei 2005
www.ahloetawheed.tk/	mei 2004 - november 2004
www.freewebs.com/aqeeda	januari 2005 - april 2006
www.freewebs.com/poldermujahideen/	februari 2005 - november 2005
www.freewebs.com/overigeinfo	september 2004 - februari 2005

In de tweede helft van 2005 is de eerste Nederlandse zelfstandige jihadistische website van start gegaan die gaandeweg verder werd opgebouwd en gediversifieerd qua rubrieken en aandachtsvelden. Begin 2006 was deze site niet meer operationeel en iets later werd aangekondigd dat de website definitief offline zal blijven. Deze site overtrof de voorgaande in alle opzichten en richtte zich zowel op de jihadstrijd als op de verspreiding van het salafistische gedachtegoed in Nederland. De site predikte en promootte duidelijk de jihadstrijd zonder zich schuldig te maken aan het aanzetten tot geweld of expliciet haat te zaaien, en bood een goed overzicht van de lopende salafistische activiteiten in Nederland. In één van de forumrubrieken werd de literatuur van de Hofstadgroep (met name de vertalingen en geschriften van Mohammed B.), maar ook nieuwe vertaalde literatuur verspreid. De site was qua vorm en inhoud professioneel opgezet. De kwaliteit van het Nederlands was goed tot zeer goed te noemen. Het ontwikkelen, runnen en onderhouden van een degelijke site veronderstelt het bestaan van een gedreven, onderlegd en professioneel kader.

Een ander fenomeen in de Nederlandse jihadistische context zijn weblogs en het gebruik van Paltalk. De eerste weblog met een expliciete jihadistische oriëntatie dateert van medio 2005, maar is in december 2005 volledig uit de lucht gegaan. Op deze weblog stonden een aantal publicaties en verklaringen van de 'Leeuwen van Tawhied'. Daarnaast bestaat een aantal weblogs waarvan de inhoud niet expliciet is gericht op de jihadstrijd, maar de daarin geplaatste artikelen hebben betrekking op de gangbare thema's van de jihadistische ideologie. Daarnaast bevatten ze ook liederen over de jihadstrijd in het Arabisch. Ook maken salafistische en jihadistische groeperingen in toenemende mate gebruik van Paltalk. Dit is een gratis spraakondersteunend chatprogramma. Hiermee kan men deelnemen aan of anoniem luisteren naar discussies. In een aantal zogeheten *Paltalkrooms* wordt vaak Arabisch gesproken, terwijl Paltalk het spreken in vele andere talen mogelijk maakt.
Door in het Arabisch te communiceren, worden de niet Arabisch sprekende personen bewust of onbewust uitgesloten van de discussies.

Naast het zelf oprichten van sites is opvallend dat de Nederlandse jihadisten ook hun pijlen richten op neutrale bij de potentiële doelgroep populaire websites en fora. Voorbeelden daarvan zijn postings in rubrieken waar het publiek kan reageren op stellingen of nieuwsitems en op willekeurige websites. Daarnaast nemen virtuele jihadisten constant deel aan de discussies. Op sommige fora worden afwijkende ideeën en salafistische geluiden door enkele 'forumoverheersers' van een felle tegenreactie voorzien. Opvallend is de verspreiding langs discussiefora van de recent naar het Nederlands vertaalde literatuur van de politieke, ideologische, strategische kopstukken van al Qa'ida. Deze worden eerst op diverse discussiefora gepubliceerd als losse postings of artikelen. De bedoeling daarbij is dat er een discussie ontstaat bij het bezoekerspubliek. Vervolgens worden de publicaties breed verspreid via andere fora en internetlocaties. Later verschijnt de vertaalde literatuur als publicatie, uitgegeven door een virtuele uitgeverij of persoon/groep. De eenmaal vertaalde publicaties worden herhaaldelijk op diverse fora en sites gepubliceerd. Zo worden de stukken van de Hofstadgroep nog steeds op het internet gezet, hetzij in een tekstbestand, hetzij in een nieuwe lay-out en vormgeving.
Vanaf begin 2006 is een trend ontstaan van het massaal op neutrale sites plaatsen van *hyperlinks* naar Arabischtalige jihadistische audiovisuele producties. Dit opereren op neutrale sites biedt enkele voordelen, namelijk het:

- voorkomen van detectie van personen en structuren die achter de website zitten;
- voorkomen van schade als gevolg van verwijdering en acties van opsporing en inlichtingendiensten;
- verkrijgen van legitimiteit en legaliteit zonder zich bloot te stellen aan publieke veroordeling;
- vergroten van de bekendheid bij een breder publiek;
- onderhouden van contacten en het communiceren met een breder publiek.

Dat deze tactiek wellicht noodzakelijk is om een groter publiek te bereiken kan worden opgemaakt uit een onderzoek waaruit naar voren komt dat Marokkaanse en Turkse jongeren in Nederland met name algemene Nederlandse sites alswel sites voor Turken en Marokkanen in Nederland bezoeken. Slechts 5 procent van het surfen bestaat uit het bezoeken van Turkse, Marokkaanse of andere internationale sites.[34] Hoewel dit misbruik van neutrale websites en fora geen eigen gezicht op het internet oplevert, is het wel een slimme wijze van propaganda en werving. Met een beperkter gevaar voor ingrijpen door overheden, bereikt de jihadistische boodschap een veel breder publiek en kan er zelfs nieuwe aanwas plaatsvinden.

3.3.3.5 Typering Nederlandse jihadistische sites

Al eerder is aangegeven dat het van groot belang is om te beseffen dat het internetgebruik door jihadisten niet geïsoleerd kan worden bezien van algemene ontwikkelingen in de samenleving, op het internet en in het jihadisme. Daarbij is in het bijzonder gewezen op het feit dat het internetgebruik van veelal jonge jihadisten niet los gezien kan worden van de jeugdcultuur en dat binnen de internationale jihadistische beweging eerder sprake is van elkaar inspireren en kopieergedrag, dan van een centrale aansturing.

De Nederlandse jihadisten richten zich tot nu toe vooral op het ordenen, aanbieden en verspreiden van informatie en materialen van jihadistische geestelijken en

34 Holst 2006, p. 12.

strategische en operationele leiders evenals het verwijzen naar dat materiaal op Engelse en Arabischtalige sites. Zij fungeren daarmee vooral als intermediair tussen de oorspronkelijke makers van het materiaal (producenten) en de eindgebruikers, hoewel zij op hun beurt ook eindgebruiker kunnen zijn. Bij de overdracht van informatie sluiten zij aan bij de taal, cultuur, mentaliteit en belevingswereld van vooral Marokkaanse jongeren. Dit zorgt voor een effectieve overdracht van de jihadistische boodschap. In toenemende mate bieden de sites ook vertaalde werken aan, wat de overdracht aan de specifiek Nederlandse doelgroep sterk vereenvoudigt. Die informatie dient vooral propagandadoeleinden, maar is deels ook gericht op training, aspecten die verder in dit hoofdstuk nog uitvoerig aan bod komen. Deze sites zijn primair te bezien als distributiekanalen (zie paragraaf 3.2.4.5).

Naast distributiekanaal bieden vele sites de mogelijkheid van interactie tussen jihadisten en een breed en divers publiek van geïnteresseerden evenals tussen jihadisten onderling. De inbreng van bezoekers, deelnemers en leden wordt actief gestimuleerd. De informatie kan zo heel gericht en op maat worden uitgewisseld met geïnteresseerden en aan de hand van specifieke vragen of actualiteiten. Bovendien kunnen op die wijze virtuele netwerken ontstaan van moslims en niet moslims (potentiële bekeerlingen) die geïnteresseerd zijn in de jihadstrijd. Uiteindelijk biedt dit zelfs de gelegenheid tot rekrutering van werkelijk in de jihadstrijd geïnteresseerden (zie ook de paragrafen 3.10 en 3.7).

Er is een duidelijke ontwikkeling te signaleren dat de jihadisten ook het multimediapotentieel van het internet steeds meer benutten ter ondersteuning van de activiteiten in Nederland. Voorbeelden daarvan zijn een Nederlandse bewerking van één van de videofilmpjes van al Qa'ida in Irak en een kort videofilmpje over Wilders. Van echte zelfstandige productiebedrijven (paragraaf 3.2.4.5) is echter nog geen sprake.

De virtuele Nederlandse jihadisten hebben zich dus in de opzet van de Nederlandse sites laten inspireren door het door as-Suri ontwikkelde model voor de virtuele jihadistische informatiebrigades (zie paragraaf 3.2.3). Ook sluit bijvoorbeeld het produceren van audiovisuele materialen aan bij de modus operandi van al Qa'ida in Irak en Saoedi-Arabië. Deze bestaat erin dat de moederorganisatie die terroristische acties voorbereidt, plant en ten uitvoer brengt daarnaast een parallelle mediaorganisatie opricht. De mediaorganisatie richt zich daarbij op informeren van de achterban en de werving van nieuwe leden. Het is niet uitgesloten dat deze werkwijze ook in de Nederlandse situatie zal worden geïmiteerd. Juist op basis van deze (buitenlandse) inspiratiebronnen voor de Nederlandse jihadisten kunnen we anticiperen op hetgeen we op het Nederlandse internet kunnen verwachten.

Er zijn aanwijzingen dat veel personen die in bestaande jihadistische netwerken in de fysieke wereld actief zijn, tevens actieve internetgebruikers zijn. In ieder geval blijkt uit de studie van Peters naar de literatuur van de Hofstadgroep en de analyse van het verspreidingspatroon van deze documentatie op het internet dat de Hofstadgroep ook als virtuele organisatie

optrad door het aanbieden van buitenlandse producties, het verzorgen van vertalingen/-ondertiteling, en - veelal in de vorm van kopieergedrag - het zelf ontwikkelen van producties. Deze virtuele manifestatie was complementair aan de fysieke groep. Ook maakte men handig gebruik van de mogelijkheden van het internet en ICT, zoals het opzetten van eigen websites, verspreiding van informatie via openbare websites en het toepassen van encryptie.
Een virtuele jihadistische organisatie kan dus de reële jihadistische organisatie indiceren.

3.3.4 Nederlandse virtuele jihadisten

Achter de omvangrijke jihadistische productie op het internet schuilen uiteraard individuen, groepen of netwerken waarvan de Hofstadgroep één van de belangrijkste was. Enkele leden van de Hofstadgroep hebben een aantal msn-groepen opgericht en onderhouden. Zo maakten zij eigen webpagina's bij MSN groups, bijvoorbeeld onder de naam '5343', de 'tawheed-waljihad' en de MSN-group Muwahidin/dewaremoslims. Op basis van de eerdergenoemde analyse van Peters van de literatuur van de leden van de Hofstadgroep en de analyse van het verspreidingspatroon van een aantal documenten uit deze literatuur kan gesteld worden dat veel van de eerder beschreven msn-groepen en sites die actief waren van 2002 tot 2004 duidelijk onder de directe of indirecte invloedssfeer van de Hofstadgroep vielen. De door de leden van de Hofstadgroep geproduceerde informatie werd niet alleen op de 'eigen' sites geplaatst, maar werd door hen tevens verspreid in diverse discussiefora.[35] Ook werd een aantal gematigde salafistische sites gebruikt om de teksten met een jihadistische strekking te publiceren. De ideologische literatuur van de Hofstadgroep werd in de loop van 2003, maar ook nu nog, gepost op diverse discussiefora van de bestaande gematigde salafistische sites en in diverse onschuldige msn-groepen gepubliceerd. Naast de theoretische artikelen over de jihadstrijd in het algemeen werden op deze locaties eveneens berichten geplaatst over de jihadstrijd in Irak en Afghanistan, alsmede toespraken van Bin Laden, al-Zawahiri en al-Zarqawi. Twee andere msn-groepen, al-ansaar en shareeah, werden onderhouden door Bilal L., de bedreiger van Geert Wilders.

Uit het monitoren van het internet blijkt dat er in de loop van het jaar 2005 als het ware een virtueel internationaal vertaalnetwerk van jihadistische literatuur uit het Arabisch, Engels en Frans is ontstaan dat intensief gebruik maakt van het internet. De virtuele Nederlandse jihadisten hebben hierbij aansluiting gevonden. Enerzijds bieden Nederlandse sites *hyperlinks* naar deze vertalingen. Anderzijds nemen de virtuele Nederlandse jihadisten zelf deel aan het vertalen van jihadistische literatuur in het Nederlands. Hieruit blijkt dat de virtuele Nederlandse jihadisten in hun ideeënproductie zich laten inspireren door anderen in het buitenland, die het initiatief nemen voor een vertaalprogramma. Die anderen zoeken naar actuele informatie en zijn vertrouwd met de vindplaatsen van informatie op Arabischtalige jihadistische websites. De selectie van de te vertalen stukken getuigt van de aanwezigheid van specialistische kennis. Dat nog geen sprake is van autonomie in de ideologische know-how en productie bij de Nederlandse jihadisten blijkt ook uit een tekstanalyse. Het conceptueel- en abstractieniveau evenals de competenties om kennis

35 Benschop 2004, p. 17, 27.

en inzichten op de Nederlandse situatie toe te passen, zijn nog onvoldoende ontwikkeld. Bijna alle vertaalde stukken in het Nederlands zijn reeds vertaald in het Engels en vervolgens naar het Nederlands. Op die Engelstalige sites heeft al een selectie van het vertaalde, aangeboden materiaal plaatsgevonden. Ook de uit het Arabisch vertaalde stukken zijn werken van anderen en dus niet van de hand van de Nederlandse jihadisten. Voor het merendeel blijkt hieruit dat de beheersing van het Arabisch niet goed is.

In vergelijking met andere Europese landen zoals Groot-Brittannië, Frankrijk en België, onderscheiden de virtuele Nederlandse jihadisten zich door een actieve rol van vrouwen. De moslima's fungeerden in eerste aanleg als deelnemers in het netwerk rond de Hofstadgroep. In de tweede plaats droegen de moslima's bij aan de ontwikkeling van Nederlandstalige jihadistische literatuur. Zij verrichtten documentatieresearch op de Engelstalige jihadistisch georiënteerde sites en vertaalden dat vervolgens in de Nederlandse taal. Momenteel komt het merendeel van de in het Nederlands vertaalde jihadistische literatuur van de hand van vrouwen.[36] De 'moslima's' spelen verder een prominente rol in zowel de inhoudelijke ontwikkeling van de msn-groepen/sites als in de interactie met het publiek. Aan meer algemene islamitische websites, maar zeker ook aan salafistische en jihadistische, nemen moslima's actief deel aan discussies, stellen vragen en plaatsen er berichten. Tijdens het verhoor van Soumaya S., die tegelijk met Nouredine el F. en Martine van der O. in Amsterdam werd opgepakt, zou zij onder meer hebben verklaard dat ze regelmatig internetcafes bezocht in Amsterdam en Den Haag en daarbij hotmail-adressen gebruikte. Ook dat ze daarbij nicknames gebruikte en bepaalde websites frequenteerde om informatie te krijgen over haar geloof. Ze verklaarde verder dat ze regelmatig met Nouredine chatte via MSN.[37] De moslima's romantiseren in hun bijdragen de rol van moslima's in de geschiedenis en hun rol in de gewelddadige jihad. En daarmee geven zij tot op zekere hoogte blijk van behoefte aan emancipatie. Verder proberen zij (discussie)bijeenkomsten te organiseren op het internet of daarbuiten.[38]

Het internetgebruik van de Nederlandse jihadisten moet, zoals eerder is verwoord, wel worden bezien in de bredere context van het internetgebruik onder jongeren. Met het plaatsen van postings en het deelnemen aan discussies proberen ('vermeende') jihadisten ook erkenning en aanzien te krijgen. Daarbij kunnen ze zich veel radicaler uiten, dan dat ze werkelijk zijn. Een ander opmerkelijk punt is de wisseling van rollen. Iemand kan zich voordoen als deskundige op het ene forum onder een nickname, terwijl hij op een ander forum of onder een andere nickname vragen stelt aan andere 'deskundigen' om vervolgens de opgedane kennis weer uit te venten. De kenmerken van het internet maken het immers eenvoudig om in korte tijd krediet en een bepaalde status op te bouwen, zelfs op jonge leeftijd en zonder jarenlange studie. Niet van iedereen die radicale standpunten uitdraagt, gaat dus per definitie een dreiging uit. Inlichtingen- en opsporingsinstanties hebben de moeilijke taak om het kaf van het koren te scheiden.

36 Bron voor dat laatste: Volkskrant 2005.
37 KRO Reporter, 18 juli 2005, vermeld in Cops@Cyberspace 2006b.
38 Mede gebaseerd op Nationaal 2006 en Nieuwsblad 2006. Zie voor de rol van vrouwen ook AIVD 2006, p. 40 en 48.

3.3.5 Bevindingen

Bevindingen op basis van de analyse in deze paragraaf zijn:

1. De Nederlandse jihadisten richten zich tot nu toe vooral op het ordenen, aanbieden en verspreiden van jihadistische informatie en materialen. Die informatie dient vooral propagandadoeleinden, maar is deels ook gericht op training.
2. Vele sites bieden de mogelijkheid van interactie tussen jihadisten en een breed en divers publiek van geïnteresseerden evenals tussen jihadisten onderling. Niet alleen kan informatie zo heel gericht en op maat worden uitgewisseld met geïnteresseerden en aan de hand van specifieke vragen of actualiteiten, op die wijze kunnen ook virtuele netwerken ontstaan of kunnen werkelijk in de jihadstrijd geïnteresseerden worden gerekruteerd.
3. Het virtuele jihadisme op het Nederlandse internet kan aanwijzingen geven over de reële jihadisten in Nederland.
4. Nederlandse virtuele jihadisten laten zich inspireren door een internationaal virtueel vertaalprogramma en vertalen vooral materiaal uit het reeds door anderen 'voorgesorteerde' aanbod van materiaal.
5. Moslima's zijn zeer actief als vertalers, in de ontwikkeling van sites en in de interactie met het publiek.
6. Nederlandse virtuele jihadisten opereren structureel of sporadisch op diverse neutrale discussiefora van niet-jihadistische signatuur. Met een beperkter gevaar voor ingrijpen door overheden, bereikt de jihadistische boodschap zo een veel breder publiek en kan zelfs nieuwe aanwas plaatsvinden.

3.4 PROPAGANDA

3.4.1 Toelichting

Terroristische groeperingen proberen met hun activiteiten een politiek doel te realiseren. Dat doen zij door bijvoorbeeld aanslagen te plegen waarbij doden en gewonden vallen. Maar zij proberen zeker ook om over de hoofden van de slachtoffers een breder en gemengd publiek te bereiken om zo bijvoorbeeld angst in te boezemen, besluitvorming te beïnvloeden, de groepering op de kaart te zetten en potentiële sympathisanten en rekruten te mobiliseren. Op de beruchte opnames die in november 2001 werden uitgezonden, waarin Bin Laden sprak over de aanslagen van 11 september 2001, gaf hij aan dat de aanslagplegers niet zozeer een daad hadden gepleegd, alswel een 'toespraak' hadden gehouden die andere toespraken overschaduwde, en die door de hele wereld *("Arabieren, niet-arabieren en zelfs Chinezen")* werd verstaan. Hieruit valt op te maken dat Bin Laden het terrorisme vooral lijkt te zien als een communicatiemiddel.[39] Propaganda vormt dan ook een wezenlijk aspect van terrorisme doordat het in grote mate de effecten van de aanslagen zelf versterkt.[40] Ook jihadisten beschouwen propaganda als wezenlijk onderdeel van hun strategie.

Veelal wordt een onderscheid gemaakt tussen propaganda en psychologische oorlogsvoering. Onder jihadistische propaganda kan worden verstaan het

39 Weimann 2006, p. 40, onder verwijzing naar Nacos, Terrorist Calculus.
40 Muller e.a. 2004, p. 57-70, Weimann 2006.

aan diverse doelgroepen verkopen van het antiwesterse, jihadistische gedachtegoed. Daarbij is overduidelijk wie de verspreider is en het materiaal wordt daarnaast op een presenteerblaadje aangeboden. In sommige gevallen moet iemand daarentegen zelf bijvoorbeeld iets downloaden en vindt propaganda op meer subtiele wijze plaats. Psychologische oorlogsvoering wordt gebruikt als term voor het aanjagen van angst ter beïnvloeding van de vijand en het publiek van de vijand. In jihadistische termen hebben ze het dan over: angst aanjagen in de harten van de ongelovigen. Propaganda is dus vooral gericht op het zieltjes winnen en het indoctrineren van de eigen potentiële achterban en aanhangers, terwijl psychologische oorlogsvoering vooral is gericht op het aanjagen van angst om zo de gewenste politieke veranderingen te bewerkstelligen. Doordat propaganda en psychologische oorlogsvoering dicht tegen elkaar aan liggen en psychologische oorlogsvoering een beladen term is, wordt in deze studie hier geen onderscheid tussen gemaakt.

In de verdere bespreking wordt stilgestaan bij de volgende vormen van propaganda:

A het verwerven of behouden van de directe aanhang en (de grotere) achterban (zie paragraaf 3.4.3);
B het beïnvloeden van de internationale publieke opinie (zie paragraaf 3.4.4);
C het beïnvloeden van de vijand en het publiek van de vijand (zie paragraaf 3.4.5)
D het aanjagen van angst (paragraaf 3.4.6);
E hacktivisme (paragraaf 3.4.7).

Het onderscheid tussen deze vormen van propaganda is niet altijd scherp doordat één boodschap uiteenlopende doelen kan dienen en gericht kan zijn op diverse doelgroepen. Dit wordt ook wel aangeduid als zogeheten multi-target berichten. Van het aanjagen van angst kan bijvoorbeeld ook een wervende werking uitgaan. En soms geven terroristische organisaties nadrukkelijk een vredelievende, diplomatieke boodschap af, om tegenstanders op het verkeerde been te zetten en om legitimatie te kweken wanneer de vijand vervolgens - ondanks het vredelievende voorstel - niet wenst te onderhandelen.[41] Zo heeft Osama Bin Laden een aantal keer een ultimatum gesteld, en een vorm van onderhandelingsperspectief geboden, waaronder op 19 januari 2006. Dat deze methode effect kan hebben blijkt uit verschillende reacties waaruit blijkt dat het goed denkbaar zou zijn als het Westen met al Qa'ida zou gaan onderhandelen.[42] De beelden op jihadistische sites van Abu Ghraib, de Iraakse gevangenis waar gevangenen door Amerikaanse soldaten zijn mishandeld, zijn tevens een voorbeeld van multi-target berichten, waarbij vriend en vijand in één bericht worden aangesproken.[43] Voor de broeders vormen de beelden het zoveelste bewijs van de verderfelijkheid van het Westen, en dat het Westen moslims als minderwaardig beschouwt en haat. Voor de vijanden kunnen de beelden een twijfelzaaiend effect hebben. Voor het neutrale publiek kan het betekenen dat zij sympathie ontwikkelen voor de standpunten en/of de strijd van de jihadisten, die zich als slachtoffer presenteren. Te verwachten valt dat jihadisten bij het plannen van aanslagen meer en meer rekening zullen houden met de 'propageerbaarheid' van hun acties, al dan niet 'live' uitgezonden via het internet.

41 Weimann 2006, p. 59.
42 Volkskrant 2006 en Zerkin 2006.
43 Weimann 2006, p. 61-64.

De volgende paragraaf schetst de voordelen van propaganda via het internet. Vervolgens wordt in afzonderlijke paragrafen verder ingegaan op de verschillende vormen van propaganda. Geëindigd wordt met een beoordeling van de dreiging.

3.4.2 Voordelen van het internet voor propaganda

In paragraaf 3.2.2 zijn al de voordelen van het internet besproken. Vooral voor propaganda gelden er nog enkele aanvullende voordelen ten opzichte van de reguliere media. In de meeste landen maken media als televisiezenders en kranten zelf de keuze óf en zo ja in welke mate en vorm terroristische boodschappen via bijvoorbeeld televisie-uitzendingen het publiek bereiken. Het materiaal dat via de reguliere media wordt uitgezonden is in veel gevallen daarbij onderhevig aan framing, editing en mogelijk ook censuur.

Framing is het selecteren van bepaalde delen van een ervaren realiteit en het meer saillant maken daarvan in een tekst op een dusdanige manier dat een bepaalde probleemdefinitie, causale oorzaak en morele evaluatie en oplossing voor het betreffende onderwerp worden gepromoot.[44] In het geval van bijvoorbeeld het NOS-journaal zou in ruime mate sprake zijn van het plaatsen van al Qai'da video's in een westers frame. Een voorbeeld hiervan is de video uit december 2001 waarop Bin Laden onder andere aangeeft dat de aanval op het WTC alles heeft opgeleverd wat hij had kunnen hopen. De focus van het journaal (en van de aanwezige gast/specialist) is vrijwel volledig gericht op de authenticiteit van de opname enerzijds en de betrouwbaarheid van de vertaling anderzijds. Dit wordt veroorzaakt door de hunkering van het Westen destijds om bewezen te krijgen dat Bin Laden achter de aanslagen zit.[45] Uitzendingen via het internet hebben van framing geen last.

Een ander verschijnsel bij reguliere media is *editing*, de redactionele bewerking van de boodschap. Eén van de productiemaatschappijen van al Qa'ida, as-Sahab, bracht op 26 april 2006 een 52 minuten durende audio-boodschap van Bin Laden uit. Al-Jazeera zond hiervan slechts 5:45 minuten uit, en verzorgde commentaar bij de niet-uitgezonden delen van de toespraak.[46] Jihadisten gaan creatief te werk om editing tegen te gaan door korte voorgefragmenteerde boodschappen te verspreiden, opdat dergelijke stukjes boodschap wél steeds in zijn geheel worden uitgezonden. Uitzendingen via het internet hebben van editing geen last omdat de jihadisten de uitzending volledig zelf in de hand hebben.

Daarnaast is (overheids)censuur of -controle op uitzendingen via het internet moeilijk, hoewel dat wel plaatsvindt in landen zoals Singapore, China en Saoedi-Arabië. In Singapore wordt bijvoorbeeld onder de noemer van het voorkomen van cyberaanvallen al het internetverkeer gemonitord, controleert de overheid de drie ISP's, en worden alle websites gescreend op bezwaarlijke of staatsgevaarlijke inhoud. In China is registratie van iedere internetgebruiker bij een plaatselijk beveiligingsbureau nodig, waardoor de overheid kan nagaan wie welke internetpagina's bezoekt.[47]

44 Van Yperen 2005, onder verwijzing naar de definitie van Entman, 1953 - vertaling uit het Engels.
45 Van Yperen 2005.
46 SITE Institute 2006d.
47 Weimann 2006, p. 180.

Nog een voordeel van het internet is dat de inhoud van de boodschappen eenvoudig kan worden aangepast aan verschillende doelgroepen om een zo krachtig mogelijk profiel op te bouwen. Jihadisten verstaan deze kunst, ook wel aangeduid als *narrowcasten*, goed. Zij richten zich bijvoorbeeld op kinderen, moslima's en het publiek in specifieke westerse landen.

Ten slotte is er de mogelijkheid van herhaling van preken, berichten en video's. Herhaling is belangrijk voor het erin hameren van boodschappen. De jihadisten gaan hier erg ver in. Aanstaande herhalingen en terugblikken worden zelfs aangekondigd, zoals in het geval van berichtgeving rond de terugblik op de aanslagen in Londen op 7 juli 2005.[48] Deze inzet van dergelijke aankondigingen *(teasers)* vindt ook plaats voor het aankondigen van nieuwe items, statements of publicaties.[49]

Al Qa'ida komt openlijk uit voor het gebruik van het internet als propagandamiddel, zoals in 2004 in een online al Qa'ida magazine waar promotie voor het gebruik van het internet voor dat doel plaatsvindt.[50] Voor zover bekend wijst al Qa'ida al sinds 2000 moslims op hun 'heilige plicht' om nieuws en andere zaken over de jihad zo spoedig mogelijk verder te verspreiden in andere nieuwsgroepen, fora en sites. Er wordt daarbij zelfs gedreigd met religieuze sancties: moslims zullen verantwoording moeten afleggen aan Allah, wanneer een website met materiaal van al Qa'ida plotseling gesloten wordt vóórdat zij de moeite hebben genomen om de inhoud verder te verspreiden.[51]

3.4.3 Verwerven of behouden van aanhang en achterban

Wanneer we het over deze vorm van propaganda hebben, dan moeten we breder kijken dan uitsluitend de jihadisten. Ook de salafisten (vaak ook als islamisten aangeduid) proberen actief zieltjes te winnen voor hun gedachtegoed en moslims en ongelovigen te indoctrineren. We kunnen hier spreken van 'digitale dawa', waarbij in de Nederlandse context sprake is van een soort Nederlandse variant van de radiale islam. Deze leidt overigens niet automatisch tot een oriëntatie op religieus gelegitimeerd geweld, maar verlaagt wel de drempel voor het propageren van de jihad.[52] Bij deze *digitale dawa* is dus niet echt sprake van jihadistische propaganda, maar het kan individuen wel ontvankelijk maken voor de jihad en drempelverlagend werken (zie verder paragraaf 3.11).

Met de propaganda die is gericht op het verwerven of behouden van aanhang en achterban beogen de jihadisten om: 1) oude strijders en huidige supporters in algemene zin een hart onder de riem te steken en hun bestaande beelden van het verderfelijke Westen te bevestigen, 2) jonge nieuwe (potentiële) jihadisten te inspireren en 3) de bredere achterban te overtuigen van de noodzaak van het bestaan en de handelingen van de organisatie. Deze vorm van propaganda kent diverse manifestaties. Enkele hiervan zijn:

1. Officiële sites in de plaatselijke taal. Deze sites bevatten gedetailleerde informatie over de interne politiek en relaties met andere groepen.
2. Islamistische preken, speeches, alsmede videobeelden van successen van de jihad, en kwaadaardigheden van de westerse, zionistische, christelijke vijand.
3. Trainingsmateriaal of handleidingen. Deze kunnen een propagandistische werking hebben doordat deze aan personen het gevoel kan geven dat men slimmer is dan de vijand en dat men onverwacht kan toeslaan: men kan iets betekenen, en zich 'meerderwaardig' voelen. Iets waarnaar vele - vooral jonge - moslims op zoek zijn. Op dergelijk trainingsmateriaal wordt vanuit andere optiek nog separaat ingegaan.
4. Materiaal gericht op interne disciplinering en versterking van de moraal van de (potentiële) 'harde kern', teneinde twijfel of afwijkende meningen te voorkomen.[53]
5. Materiaal dat aspecten van de jihadstrijd legitimeert. Zo is er veel materiaal en zijn er veel teksten waarmee getracht wordt om zelfmoordaanslagen en het als 'collateral damage' doden van moslims te rechtvaardigen.
6. Materiaal gericht op specifieke doelgroepen onder wie moslima's en kinderen.

In de afgelopen jaren kwam verhoudingsgewijs veel propagandamateriaal uit Irak, wat in propagandistisch opzicht een goudmijn is voor de jihadisten. Recentelijk is veel propagandamateriaal afkomstig van de moedjahedien uit Afghanistan.

Figuur 3.4 Voorbeelden van propaganda gericht op eigen aanhang en achterban

In een opname van Osama Bin Laden uit december 2001 geeft hij aan dat de Verenigde Staten bijna op de knieën gedwongen zijn. De boodschap is bedoeld om de moraal van de Afghaanse strijders, die op dat moment Afghanistan uitgejaagd worden, op te vijzelen.[54]

In januari 2004 werd door leden van de Hofstadgroep verkondigd: 'Beste broeders en zusters, Zoals jullie wellicht al weten hebben de mojahidien hun oorlogstactiek aangepast. Wanneer wij de moeshrikien [ongelovigen] op Iraaks, afgaans bodem gaan bestrijden zijn het vooral de moslimburgers die hier het slachtoffer van worden, dit is ook de reden dat de Taliban in 2002 uit de grote steden zijn weggetrokken. Wij streven ernaar om de ongelovigen op hun eigen grondgebied te verslaan[...]. Net zoals in Amerika Engeland en andere Europese landen hebben wij inshallah [Met Godswil] ook hier de middelen om een begin te maken aan grootschalige bomaanslagen, liquidaties en guerrilla-acties. [...] Het zal Inshallah niet lang meer duren voordat de eerste klappen vallen en de grond onder de ongelovigen zal beven'.[55]

De jihadisten plaatsten op diverse discussiefora op het internet politieke verklaringen waarin zij standpunten innemen over de actualiteit, met het oog op mobilisering van moslims tegen de Nederlandse overheid en samenleving als zijnde 'ongelovigen'. De gepubliceerde communiqués zijn nadrukkelijk gericht op moslims in de Nederlandse samenleving. Recente voorbeelden in 2006 waren:

- *een pamflet tegen de deelname aan de gemeenteraadsverkiezingen van 4 maart 2006,*
- *een verklaring van de 'Leeuwen van Tawhied' op de vooravond van de uitspraak van de rechter over de Hofstadgroep en*
- *een pamflet, dat moslims in Nederland oproept om de Nederlandse rechtbanken te boycotten.*[56]

48 SITE-Institute 2006k.
49 SITE-Institute 2006o.
50 Weimann 2006, p. 105 over het Sawt al-Jihad-magazine van februari 2004.
51 Weimann 2006, p. 66.
52 AIVD 2006, p. 29-30.
53 Hoffman 2006, p. 3, en Interview 6.
54 Hoffman 2006, p. 7.
55 Foxtrot 2004.
56 Eigen waarnemingen.

3.4.4 Beïnvloeden van internationale publieke opinie

De jihadisten beogen met deze beïnvloeding dat het grote publiek sympathie krijgt voor de jihad en de jihadisten. Ook deze vorm van propaganda kent diverse manifestaties.

Het internationale publiek is, in tegenstelling tot de eigen aanhang en achterban, niet per sé actief op zoek naar informatie. Voor dit publiek verschaffen tal van terroristische groeperingen basisinformatie over de eigen organisatie in verschillende talen. Ook brengen diverse terroristische groeperingen algemene persberichten en videoboodschappen uit, gericht op de pers in andere landen. Met bepaalde videoboodschappen wordt tevens geprobeerd om informatie 'wit te wassen',[57] door ze in de mainstream-pers te brengen, die deze vervolgens als zelfstandige berichtgeving doorzetten naar het grote publiek. Veel terroristische websites bezigen begrippen als 'vrijheid van meningsuiting', 'politieke gevangenen', 'mensen- en vrouwenrechten', omdat het westerse publiek erg gevoelig is voor dergelijke onderwerpen. Men presenteert zich graag als slachtoffer en vergroot daarbij daden van de vijand uit. Dit alles kan de acceptatiegraad verhogen en verzorgt een algemene rechtvaardigingsgrond voor politieke actie.[58] Dit kan door onder meer verplaatsing van verantwoordelijkheid (wij zijn het slachtoffer, we moeten dit wel doen, maar het is niet onze schuld of verantwoordelijkheid), ontmenselijking van doelen (honden, apen, varkens), gunstige vergelijkingen (het Westen pleegt gruwelijkere daden dan wij) en verdraaiing van feiten en gebeurtenissen in de tijd (9/11 was een reactie op VS-agressie in het Midden-Oosten en Afrika).[59] Overigens wordt deze tactiek gedeeltelijk ook toegepast bij andere vormen van propaganda.

Figuur 3.5 Voorbeeld van propaganda gericht op de internationale publieke opinie

Herhaling van gruweldaden van het Westen vindt veelvuldig plaats. Zo zijn beelden van de aanslagen in de Verenigde Staten op 11 september 2001 en de foto's van de mishandelingen in de Abu Ghraib-gevangenis niet van het internet te branden. Dit bleek ook weer tijdens de zogeheten 'cartooncrisis' van begin 2006. In de video die op vele gehackte Deense sites verscheen waren opnieuw foto's van Abu Ghraib gemonteerd.

3.4.5 Beïnvloeden van (het publiek van) de vijand

De jihadisten beogen met deze vorm van propaganda, die is gericht op de vijand en het publiek van de vijand, om de steun voor het overheidsbeleid te verzwakken door demoralisatie, beschadiging van de (geloofwaardigheid van de) media, overheid en haar personeel.[60] Daarnaast trachten zij te bewerkstelligen dat het (militaire) personeel zélf minder gemotiveerd raakt om de strijd voort te zetten. Dit kan bereikt worden door desinformatie te verspreiden, of juist door verkeerd gepresenteerde beelden actief te corrigeren. Ook moet rekening worden gehouden met infiltratie van reguliere westerse webfora door (groepen) personen, die middels argumentatie zullen proberen draagvlakvermindering onder de westerse bevolking te bewerkstelligen. Een oproep hiertoe heeft plaatsgevonden via het GIMF.

57 Hoffman 2006, p. 4.
58 Weimann 2006 p. 53.
59 Weimann 2006, p. 55, verwijzend naar de theorie van Bandura.
60 Weimann 2006, p. 61-64.

De groepen zouden moeten bestaan uit 'internet-jihadisten' die de Engelse, Spaanse, Franse of Duitse taal machtig zijn. Deze personen zouden goed moeten kunnen debatteren, en over 'methoden voor overtuiging' moeten beschikken.[61] Nederlandse jihadisten benutten deze tactiek van het misbruiken van neutrale sites veelvuldig (zie paragraaf 3.3.3.4).

Figuur 3.6 Voorbeelden van propaganda gericht op (het publiek van) de vijand

Nadat Tsjetsjeense rebellen een Russische SU-24 uit de lucht hadden gehaald, probeerden de Russische autoriteiten dit gegeven te ontkennen. Zij werden echter ingehaald door de publiciteitscampagne van de rebellen met beelden van de wrakstukken van het betreffende vliegtuig.[62]

Via het internet waarschuwt de Taliban Afghanen die samenwerken met de coalitietroepen voor de laatste keer: als zij nu niet tot inkeer komen is er geen weg terug tijdens een aanstaand Taliban-offensief tegen de coalitietroepen.[63]

Via het GIMF is een 42 minuten durende video uitgegeven, die een montage vormt van enerzijds een bestaande Amerikaanse HBO-documentaire 'Baghdad ER' over Amerikaanse soldaten in Irak en medische ingrepen die zij moeten ondergaan en anderzijds beeld- en geluid-materiaal van o.a. al-Zarqawi en al-Zawahiri. De inleidende tekst luidt: "They [American soldiers] are injured... taken by ambulances, then to the emergency room and at last... they die like dogs".[64]

3.4.6 Aanjagen van angst

Het aanjagen van angst kan bijvoorbeeld door bedreigingen te uiten via de massamedia, door zichzelf groter en gevaarlijker voor te doen dan men in werkelijkheid is, of door extreme, gewelddadige video's beschikbaar te stellen en extreme uitspraken te doen, bijvoorbeeld in de vorm van zelfmoordtestamenten. De reeds genoemde, belangrijke speler in het verspreiden van jihadistisch materiaal, het GIMF, heeft verklaard dat het hun recht is om de vijand angst aan te jagen.[65]

Dat het aanjagen van angst het grote publiek bereikt is onder andere af te meten aan de interesse voor misschien wel het bekendste voorbeeld hiervan: de door de Irakese Ansar al-islam op het internet geplaatste onthoofdingsvideo's van Nick Berg en Paul Johnson. In mei 2004 was - na *'American Idol'* - 'Nick Berg' namelijk de populairste zoekterm op Google, in juni 2004 was dat 'Paul Johnson'.[66]

61 SITE-Institute 2006g.
62 Weimann 2006, p. 61-64.
63 SITE-Institute 2006n.
64 SITE-Institute 2006p.
65 SITE-Institute 2005b.
66 Weimann 2006, p. 110.

Figuur 3.7 Voorbeelden van het aanjagen van angst

De Abu Hafs-Brigade heeft de verantwoordelijkheid opgeëist voor de grote stroomstoring in de zomer van 2003 in delen van de Verenigde Staten. Hoewel getwijfeld kan worden aan het feitelijke bestaan van de Abu Hafs entiteit, en al helemaal aan de door hen gedane claims, is het zeker ten opzichte van het grote publiek een poging om zich te manifesteren en dat publiek te doen vrezen voor verdere aanslagen. De claims van Abu Hafs worden ook qua naamgeving spectaculair verpakt. Zo werden de 'aanslag' die de stroomstoring zou hebben veroorzaakt "Operation Quick Lightning in the Land of the Tyrants of this generation" genoemd.[67]

Eind 2005 verscheen er een artikel dat beschreef hoe moslims ("blond or black") eenvoudig duizenden Amerikanen zouden kunnen vermoorden door toe te slaan tijdens de Superbowl: door een paar explosies in het stadion te veroorzaken zou dusdanige paniek ontstaan dat men elkaar onder de voet zou lopen, en tribunes zouden bezwijken, met gevolgen die uiteindelijk groter zouden zijn dan het drama in het Belgische Heizel-stadion.[68]

Een Candid Camera / Funniest Home Videos -achtige compilatie verschijnt begin september 2005, met als ondertitel: Bloody comedy. Het betreft een snel gemonteerde compilatie van opnames van aanslagen op Amerikaanse militairen, die ondersteund worden door een lach-machine en 'grappige' (dieren)geluiden.[69]

In een video van Bilal L. uit januari 2005 werd het Tweede-Kamerlid Wilders bedreigd. Deze professionele videoboodschap begint met een steunbetuiging aan de moordenaar van Theo van Gogh, Mohammed B. en eindigt met de volgende boodschap: "En tenslotte. Een cadeautje voor Geert Wilders. We hebben onze zwaarden al geslepen, hond." Op de achtergrond is het geluid hoorbaar van messen die worden geslepen. De aftiteling van de boodschap luidt: "Dit is een productie van Leeuwen van de Tawhied (de polder mujahideen) (beter bekend als Hofstad-netwerk.)".[70]

3.4.7 Hacktivisme

Bij hacktivisme gaat het om cyberaanvallen die dienen om een politiek statement te maken. Dat kan bijvoorbeeld door cyberaanvallen uit te voeren op websites van vijandige of 'aan de vijand gelieerde organisaties' door die in een kwaad daglicht te stellen of door die het zwijgen op te leggen.

Behalve door aanvallen van websites is het ook mogelijk om een politiek statement te maken via een Google-bom. Een Google-bom is een poging om het zoekresultaat van Google te beïnvloeden en zo een bepaalde pagina hoog op de resultatenlijst van deze zoekmachine te laten verschijnen. Het programma indexeert pagina's door ze af te 'grazen'. Daarbij wordt onder andere gekeken naar *hyperlinks* naar andere sites. Op deze manier werd

67 Weimann 2006, p. 55.
68 SITE-Institute 2006l.
69 SITE-Institute 2005a.
70 Het TV-programma Zembla besteedde op 10 februari 2005 aandacht aan deze video.

George Bush ooit het 'slachtoffer' van een Google-bom. Wie de woorden 'miserable' en 'failure' intypte kreeg als eerste zoekresultaat de website van Bush.[71] Er zijn nog geen gevallen van een jihadistische Google-bom bekend.

In hoeverre de bekende vormen van jihadistisch hacktivisme, waaronder de hackaanvallen tijdens de cartoonrel en van Israël (zie paragraaf 2.2.5), de voorbode zijn geweest van grotere aanvallen in de toekomst is nog niet te zeggen. De computervaardigheden van de jihadisten lijken in ieder geval toe te nemen en de intentie voor dergelijke aanvallen blijkt in ieder geval aanwezig.

Figuur 3.8 Voorbeelden van hacktivisme

Het particuliere initiatief 'Internet Haganah' in de Verenigde Staten, dat tracht jihadistische websites offline te krijgen is slachtoffer geworden van denial of service-attacks waardoor de eigen site niet meer toegankelijk werd.

In juli 2006 is de website van het kamerlid Wilders voor de tweede keer gehackt door islamitische hackers. Zij lieten een bericht achter op zijn website.[72]

Tijdens de Deense cartoonrel woedden niet alleen felle discussies over de kwestie, maar werden ook vele Deense sites gehacked met als resultaat een defacement: de inhoud van de betreffende internetpagina's was vervangen door jihadistische afbeeldingen, video's en kreten. Het effect van zulke defacements is over het algemeen gering. Vervelender was het dat de Deense overheid overspoeld werd door e-mails waardoor het reguliere e-mailverkeer van en naar de Deense overheid gehinderd werd.

3.4.8 Beoordeling dreiging propaganda

Het internet biedt tal van mogelijkheden voor propaganda. Salafisten en jihadisten gebruiken het internet daartoe volop. Er zijn zeer vele voorbeelden bekend van propaganda via het internet. Zij werken daarbij op professionele wijze, richten hun boodschap op een breed en divers publiek en daarbinnen op specifieke doelgroepen, waarbij zij uiteenlopende talen hanteren. Er zijn enkele voorbeelden gedocumenteerd van via het internet geradicaliseerde personen. Imam Samudra, die is veroordeeld als *field coördinator* voor de aanslagen op Bali op 12 oktober 2002, verklaarde bijvoorbeeld dat hij tot zijn overtuiging was gekomen door het lezen van een aantal standaardwerken en artikelen op radicale websites. En in de autobiografische schetsen van Samir A., die onder de titel 'Deurwaarders' door de Nationale Recherche werd aangetroffen op diens huiscomputer, staat onder meer uitgebreid zijn zoekproces op het internet en de rol die het internet heeft gespeeld bij zijn radicaliseringsproces beschreven.[73] Verder beschouwen de jihadisten zelf propaganda als nuttig voor realisatie van hun doelen. De vele herhalingen in de boodschappen en compilaties van oudere video's en

71 Nu.nl 2006d.
72 Nu.nl 2006c.
73 AIVD 2006, p. 46.

preken zijn enerzijds een onmisbaar en noodzakelijk kenmerk van propaganda, maar geven - in ieder geval voor buitenstaanders - tegelijkertijd blijk van een soort armoede. Al met al kunnen we dus stellen dat propaganda via het internet bijdraagt aan radicalisering.

3.5 INFORMATIE-INWINNING

Het internet is een virtuele bibliotheek met een vrijwel oneindige hoeveelheid informatie die bovendien merendeels openlijk toegankelijk is. Overheden, bedrijven en individuen plaatsen grote hoeveelheden informatie op het internet zoals plattegronden, vertrek- en aankomsttijden van vliegtuigen en adresgegevens. Deze informatie kan behulpzaam zijn bij het plegen van aanslagen op gebouwen en voor allerlei voorbereidingsactiviteiten.

De jihadisten zijn zich goed bewust van de mogelijkheden van het internet voor informatie-inwinning en benutten het internet als virtuele bibliotheek en bron van informatie voor voorbereidingsactiviteiten.

> *"Uit AIVD-onderzoek werd duidelijk dat ook in Nederland aanwezige jihadisten op het internet actief op zoek gingen naar deze operationele kennis. In een aantal gevallen werden bij huiszoekingen en arrestaties zelfgemaakte explosieven aangetroffen waarvan de fabricage waarschijnlijk (deels) was gebaseerd op kennis verkregen via het internet."*[74]

Zo zijn na de aanhouding van Samir A. foto's, schetsen en plattegronden over de kerncentrale Borssele, de gebouwen van de Tweede Kamer, het Binnenhof en het AIVD-gebouw aangetroffen die voor een groot deel door hem via het internet zijn vergaard. Samir A. heeft de virtuele verkenning van het AIVD-gebouw vervolgd door een fysieke verkenning van dit gebouw.[75] Ook zijn er bijvoorbeeld bouwtekeningen van een dam aangetroffen op computers van al Qa'ida die in beslag zijn genomen.[76] Kort na een oproep van al-Zawahiri aan jihadisten om olie-installaties aan te vallen, waren er Arabischtalige jihadistische sites te vinden die informatie verschaffen over locaties en omvang van olievelden en -installaties, met de nodige hyperlinks naar andere informatiebronnen. Het plaatsen en zoeken van informatie laat echter wel digitale sporen na, hetgeen een belemmering voor terroristen kan vormen. Zoals eerder is aangegeven zijn zij zich hier goed van bewust en nemen zij tegenmaatregelen.

Dat het internet zich bij uitstek leent om op legale wijze aan veel informatie te komen, is evident. Bijvoorbeeld bij het geven van vertrektijden doen vliegmaatschappijen dat bewust. Toch plaatsen organisaties veelal ook informatie op het internet zonder te beseffen dat deze voor tal van doeleinden kan worden misbruikt. De Amerikaanse Minister van Defensie waarschuwde zijn personeel in januari 2003 dat er teveel ongerubriceerd en in potentie voor terroristen bruikbaar materiaal op Defensie-websites te vinden was. Hij herinnerde zijn personeel er aan dat in een in Afghanistan aangetroffen al Qa'ida handboek te lezen viel dat 80% van de benodigde informatie over de vijand via open bronnen te verkrijgen is.[77] Kennelijk blijft het Amerikaanse Ministerie van Defensie zich ook in 2005 bewust van de risico's: "The enemy is actively searching the unclassified networks for information,

74 AIVD 2006, p. 51.
75 Uitspraak van het Gerechtshof 's-Gravenhage op 18 november 2005 inzake het hoger beroep tegen Samir A. te vinden op www.rechtspraak.nl.
76 Benschop 2006a.
77 Conway 2005, p. 14.

especially sensitive photos, in order to obtain targeting data, weapons systems vulnerabilities and [tactics] for use against the coalition."[78] Het Nucleair Regulatory Commission's (NRC) Office of Nuclear Security and Incident Response uit de VS heeft kort na de aanslagen van 11 september haar gehele website offline gehaald. Een aantal weken later kwam de site terug online, geschoond van ongeveer duizend gevoelige documenten.[79]

Het intern houden van informatie heeft slechts betrekkelijk nut wanneer vervolgens de beveiliging van het interne netwerk ontoereikend is, of wanneer organisaties het toestaan dat *file-sharing* of *peer-to-peer-programma's* door personeel worden gebruikt. Zo blijkt dat bijvoorbeeld via het programma *Limewire* veel informatie kan weglekken, omdat meer bestanden via het internet met andere Limewire-gebruikers worden gedeeld dan de eigenaar van de informatie zich bewust is.

Figuur 3.8 Voorbeelden van op legale wijze te verkrijgen gevoelige informatie

Op de website state.nv.us was - als materiaal voor een contraterrorisme trainingssymposium in 1996 in Nevada - een uitgebreide beschrijving te vinden van de methodes die gebruikt worden voor het verschepen van nucleair afval, welke routes gebruikt worden voor het transport, en zelfs met welke wapens die transporten zouden kunnen worden aangevallen. Op de jihadistische site almoltaqa.org is - in de sectie 'explosieven' - een link naar de site in Nevada te vinden: de informatie is dus gevonden, gekopieerd en verder verspreid.[80]

In Nederland vormen de gemeentelijke risicokaarten een openbare bron van informatie met behulp waarvan elke burger via het internet kan opzoeken welke potentieel gevaarlijke locaties zich in zijn woonomgeving bevinden. Op verzoek van minister Remkes hebben de provincies besloten informatie over de effecten van calamiteiten weg te laten. De informatie die wordt weggelaten, is via de betreffende gemeenten overigens nog wel opvraagbaar.[81]

Een andere vorm van informatie-inwinning via het internet kan plaatsvinden via *geospatial information*, zoals Google Earth. In de vorm van satellietfoto's, vaak gecombineerd met informatie van luchtfoto's, vormt dit een rijke en betrekkelijk gedetailleerde bron van informatie. Terroristen kunnen geholpen zijn met dergelijke informatie in publieke databases voor algemene doelwitselectie en -locatie: het biedt immers op een snel toegankelijke manier informatie aan over de omgeving en ook soms de structuur van gebouwen. Maar voor het daadwerkelijk voorbereiden van aanslagen zullen zij meer gedetailleerde en actuele informatie nodig hebben die ze kunnen verkrijgen door observatie en andere bronnen.[82] De informatie afkomstig van Google Earth is ook via andere kanalen vrij of commercieel verkrijgbaar.[83] Er zijn inderdaad de nodige andere aanbieders van dergelijk materiaal. Overigens is Google ontvankelijk voor verzoeken om bepaalde gedeelten onzichtbaar te maken. Waar het geen satellietbeelden maar luchtfotografie betreft, is Google zelfs verplicht om op dergelijke verzoeken in te

78 Military.com 2005.
79 Conway 2005, p. 15.
80 Weimann 2006, p. 113.
81 Planet.nl 2006b.
82 RAND 2000.
83 Justitie 2005b.

gaan.[84] Wanneer satellietbeelden ook real-time en/of nog gedetailleerder dan nu bekeken kunnen worden, kan dit gevaren met zich meebrengen voor verkeerd gebruik. Volgens antwoorden op kamervragen valt niet in algemene zin te beantwoorden in hoeverre deze effecten positief of negatief zullen zijn.[85] Voorstelbaar is dat het zowel voor terroristen als voor inlichtingen- en veiligheidsdiensten voordelen zal hebben, die elkaar mogelijk opheffen. De ontwikkelingen gaan echter zeer snel en anticipatie op die mogelijke dreiging lijkt geboden.

Hoewel de informatie die in de voorbeelden is genoemd niet altijd bestemd was voor het grote publiek, was deze wel vrijelijk beschikbaar. De informatie waarover tot nu toe is gesproken werd dan ook op legale wijze verkregen, door het zoeken in open bronnen. Ook door íllegale methoden te gebruiken kan informatie worden ingewonnen. Daarnaast moet rekening gehouden worden met infiltratie in bedrijven met gevoelige klant- en internetinformatie. Een infiltrant bij Google of een ISP zou grote schade kunnen aanrichten door gegevens over klanten, IP-adressen en surfgedrag te ontvreemden en te analyseren, en vervolgens daarop door te rechercheren. Gegevens over IP-adressen leveren soms bijzondere kennis op: zo zouden gegevens over de naam en aanlegplaatsen van een Amerikaans vliegdekschip bekend zijn geworden omdat de bemanning toegang had tot het internet.[86] In hoeverre terroristen informatie op illegale wijze hebben verworven - al dan niet door zelf te hacken, of door hackers in te huren of te verleiden tot uitdagende opdrachten of door infiltratie - is niet bekend. Dit heeft uiteraard eveneens te maken met het feit dat hackers geen visitekaartjes achterlaten. Het is echter zeker waarschijnlijk dat zij deze methode toepassen.

Hackers zouden verder kunnen proberen om informatie te verkrijgen over de werkwijze van inlichtingen- en opsporingsinstanties ter voorbereiding op een actie of juist om de eigen organisatie te beschermen of af te schermen. Hierbij zouden pogingen kunnen worden ondernomen om in te breken op bijvoorbeeld de informatiesystemen van de politie.

Een andere mogelijkheid om aan informatie te komen is via datamining: het ontdekken van patronen, associaties, veranderingen en structuren in grote hoeveelheden gegevens die opgeslagen zijn in een database. Niet bekend is of jihadisten zich hiermee bezighouden. In veel publicaties wordt ofwel aangenomen dat jihadisten aan datamining doen, ofwel wordt kennelijk geen onderscheid gemaakt tussen informatie-inwinning en datamining.

Hoe moeten we de dreiging van informatie-inwinning via het internet beoordelen? Net als voor iedereen vormt het internet voor jihadisten een onuitputtelijke bron van informatie, die op zowel legale als illegale wijze kan worden verkregen en met behulp van professionele hulpmiddelen zoals datamining kunnen worden gecombineerd. Deze informatie kan bruikbaar zijn bij de voorbereiding en uitoefening van terroristische activiteiten. Hoewel deze informatie potentieel ook op andere wijze zou kunnen worden verkregen, zijn de mogelijkheden voor het inwinnen van informatie via het internet laagdrempeliger, goedkoper, eenvoudiger, minder arbeidsintensief en grootschaliger. Met name de ontwikkelingen op het terrein van real-time satellietbeelden, eventueel gecombineerd met een permanente internetverbinding, zullen snel voortschrijden. Daarmee is informatie-inwinning via het internet een zeer bruikbaar middel voor jihadisten en draagt dat potentieel bij aan het daadwerkelijk uitvoeren van terroristische activiteiten.

84 NCTb 2006b.
85 Justitie 2005b.
86 Newsbytes 2006.

3.6 FONDSENWERVING

Fondsenwerving via het internet kent diverse varianten.[87] Een *eerste variant* van fondsenwerving betreft rechtstreekse en openlijke fondsenwerving via websites. Bedoeld als wervende teksten, wordt op verschillende sites toegelicht dat de kosten voor het runnen van een terroristische organisatie niet mals zijn. Zo gaat Hamas in op de prijzen van kogels, aanschaf van andere goederen en kosten voor omkoping, toont Hezbollah op de al-Manar site van Hezbollah drie bankrekeningen voor donaties, en wijst daarnaast op de kosten die verbonden zijn aan de zorg voor gewonde martelaren en hun gezinnen (voor 360 dollar per jaar kun je een weeskind en voor 300 dollar de weduwe van een martelaar sponsoren), en doet de Pakistaanse LeT aan openlijke fondsenwerving met verzoeken om geld en computerhardware. Dergelijke donaties zijn voor moslims met name een optie indien zij zelf niet fysiek kunnen deelnemen aan de jihad.[88] Bij veel terroristische groeperingen spreken de websites hun bezoekers rechtstreeks aan om geld over te maken of hun bank- of creditcardgegevens achter te laten dan wel een internet-betalingswijze te kiezen *(zoals PayPal)*. In de Verenigde Staten zijn personen in staat van beschuldiging gesteld wegens het onderhouden van dergelijke websites tussen 1998 en 2002.[89] Ook nemen openlijke fondsenwervingsactiviteiten soms de vorm aan van kettingbrieven die oproepen tot het doneren van geld. Deze worden via e-mail aan gelijkgestemden verstuurd. Ook hierbij worden bankrekeningnummers op radicale websites vermeld en kunnen donateurs door middel van financiële internetdiensten, zoals PayPal en CashU, geld overmaken.[90] Een ander voorbeeld van een openlijke oproep is de oproep in 2004 tot financiele steun voor de vrouw van Samir A. na zijn arrestatie.[91]

Een *tweede variant* van fondsenwerving is de benutting van profiling, e-commerce tools en het plegen van fraude. Bezoekers van websites kunnen worden geprofiled via gebruikersgegevens. Dergelijke gegevens kunnen gegenereerd worden uit registratieformulieren of online-questionnaires, op grond waarvan potentiële donateurs aangeschreven kunnen worden. Een veelvoorkomende vorm van fondsenwerving via websites is de online-winkel waar boeken, CD's, DVD's, vlaggen en t-shirts aangeschaft kunnen worden.[92] Zo werden in Kopenhagen in februari 2006 zeven personen gearresteerd of in staat van beschuldiging gesteld die via een internet winkel T-shirts verkochten waarvan de opbrengst bestemd was voor terroristische organisaties die op de EU lijst voorkomen.[93]

Behalve rechtstreekse oproepen of online-winkels kunnen niet-vrijwillige bijdragen gegenereerd worden via online-creditcardfraude, *phishing* en *pharming*. De voorbeelden hiervan zijn schaars.[94] Aangezien in algemene

87 Conway 2005.
88 Weimann 2006, p. 135-138.
89 Apuzzo 2006.
90 Thomas 2003.
91 Afkomstig uit het Requisitor van de Officier van Justitie (www.om.nl/de_hofstadgroep).
92 Conway 2005.
93 BBC Monitoring 2006a.
94 Conway 2005 die zich baseert op Libbenga, Terrorists grow fat on email scams 28-9-2004.

zin op het terrein van cybercrime toenemende aandacht lijkt te zijn van hackers voor fraude, valt niet uit te sluiten dat jihadistische hackers eenzelfde pad bewandelen en dat fraude in toenemende mate een belangrijk instrument wordt voor fondsenwerving.

Een *derde variant* van fondsenwerving is die van exploitatie en misbruik van liefdadigheidsinstellingen. Het 'geven van aalmoezen' (zakat) is één van de vijf zuilen van de islam. De zakat beslaat 2,5% van het vermogen en is bestemd voor de armen, weduwen, wezen, zieken of reizigers. Naast de zakat kan de gelovige meer vrijwillige giften doen, wat binnen de islam als zeer verdienstelijk geldt. Jihadistische organisaties lijken misbruik ter maken van deze 'zuil' door hun wijze van fondsenwerving, die vaak via liefdadigheidsorganisaties loopt.

Het doen van donaties is door de opkomst van het internet bij wijze van spreken met een muisklik te regelen. Voorbeelden van liefdadigheidsinstellingen die actief zijn/waren op of via het internet zijn: *Mercy International, Wafa al-Igatha al-Islamiya, Rabita Trust, Al Rasheed Trust, Global Relief Fund, Benevolence International Foundation,* en *Help The Needy*. Deze liefdadigheidsorganisaties adverteren op Islamitische websites en chatrooms, en plaatsen verwijzingen naar hun eigen internetpagina's. Ook heeft infiltratie plaatsgevonden van jihadisten in bestaande organisaties, waardoor er sprake is van geheime agenda's van dergelijke sites. Sommige van dergelijke organisaties verwijzen op hun websites op verdekte wijze naar die agenda.[95] In april 2006 werd om donaties gevraagd voor de Palestijnen op verschillende jihadistische fora. "Do not be lazy.... Do not stay behind. Make your move now, time passes and the situation gets worse. Transit for help and medical aid will not be prohibited, even in all the doors are locked in front of us. We will never abandon our brothers in Palestine. Put an effort to spread the campaign." Het bericht bevatte de namen en rekeningnummers van enkele liefdadigheidsinstellingen.[96] Soms wordt ook gevraagd om andere donaties dan financiële.

Er is voor jihadisten één belangrijk nadeel aan online-fondsenwerving: het vindt relatief openlijk plaats, en is daardoor principe zichtbaar, traceerbaar en rechercheerbaar. Bovendien is men veelal afhankelijk van het bancaire betalingsverkeer hetgeen niet alleen sporen achterlaat, maar ook internationaal goed in de gaten wordt gehouden in verband met alle beleidsmaatregelen op het terrein van het tegengaan van financiering van terrorisme. Buiten de sfeer van liefdadigheid zijn waarschijnlijk daarom weinig echt serieuze voorbeelden van fondsenwerving te noemen. Daar waar fondsenwerving voor terroristische activiteiten wel herkenbaar was, verdwenen die sites weer snel uit de lucht, vermoedelijk door overheidsingrijpen. Relatief nieuw zijn echter de anonieme betalingsmethoden zoals éénmalige 'CASH U-cards', die eigenlijk debitcards zijn. Deze verminderen het zicht op betalingen en de sympathisanten in potentie sterk. Een toename van fondsenwerving is daarom voorstelbaar.

Hoe moeten we de dreiging van fondsenwerving via het internet beoordelen? In potentie bestaan vele mogelijkheden voor fondsenwerving en er zijn enkele voorbeelden van bekend, maar het komt in de praktijk nog weinig voor. Deze vorm van fondsenwerving is immers zichtbaar en daardoor kwetsbaar voor overheidsingrijpen. Aangezien het bankieren via het internet steeds eenvoudiger en gebruikelijker wordt, zal ongetwijfeld ook het ge- en misbruik ervan door jihadisten toenemen. Dit, gecombineerd met de toenemende interesse van hackers voor online fraude, zal mogelijk leiden tot een verschuiving van meer openlijke naar meer heimelijke fondsenwerving. Fondsenwerving via het internet zal eveneens kunnen toenemen als gevolg van nieuwe digitale en anonieme betalingsmiddelen.

95 Conway 2005.
96 Site Institute 2006t.

3.7 REKRUTERING

Is propaganda nog vooral gericht op zieltjes winnen, rekrutering probeert individuen actief te betrekken bij terroristische activiteiten en gaat duidelijk een stap verder. Het voert te ver in het kader van deze fenomeenstudie om heel uitgebreid in te gaan op rekrutering. Voor meer achtergronden wordt verwezen naar onder andere AIVD-rapporten die (mede) over rekrutering gaan.[97] Toch wordt bij het internetgebruik door jihadisten menigmaal gewezen op (de mogelijkheden voor) rekrutering. Daarom wordt ook in deze fenomeenstudie daar expliciet aandacht aan besteed.

Onder *rekrutering* wordt verstaan: het in beeld brengen en vervolgens controleren en manipuleren van personen om een geïnternaliseerde radicaal politiek-islamitische overtuiging bij deze personen te bewerkstelligen, met als uiteindelijk doel om deze personen op enigerlei wijze te doen participeren in de gewelddadige jihad.[98] Rekrutering is dus gericht op het 'vangen' van personen die bereid zijn én aan te zetten zijn tot het uitvoeren van een gewelddadige actie. Er wordt een proces ingezet door een rekruteur dat is gericht op potentiële *rekruten*. Bij rekrutering zijn dus twee partijen betrokken waarbij het initiatief uitgaat van de rekruterende partij.

Zoals eerder al is aangegeven, is het merendeel van de jihadistische groeperingen present op het internet en doen zij op tal van manieren hun best om niet alleen zieltjes te winnen, maar ook personen zo ver te krijgen dat zij op enigerlei wijze gaan participeren in de gewelddadige jihad. Zo heeft de militaire tak van Hamas een eigen site genaamd *alqassam.com* die is gericht op rekrutering. Daarbij worden de bekende beloftes van het martelaarschap gedaan. De site dient tevens als virtueel monument voor de gestorven martelaren.[99]

Theoretisch is denkbaar dat iemand vanuit Nederland zich via het internet rechtstreeks en één-op-één laat rekruteren door rekruteurs van internationale terroristische groeperingen, zoals Hamas. Erg aannemelijk is dat echter niet. Radicalisering in het Westen, mogelijker wijze uitmondend in rekrutering, is immers een proces dat veelal start vanuit een zoekproces naar antwoorden op levens- en religieuze vragen. Er zijn tal van westerse en Nederlandse sites die hier veel beter en gerichter op inspelen dan die van terroristische groeperingen uit 'verre landen' (zie paragraaf 3.11) en de dreiging voor Nederland gaat vooral uit van lokaal autonome netwerken.

97 AIVD 2002b, AIVD 2004, AIVD 2006.
98 AIVD 2004.
99 Voor dat laatste Weimann 2006, p. 82.

Dit laat onverlet dat van bijvoorbeeld de kern van al Qa'ida wel een inspirerende werking kan uitgaan bij de vorming van virtuele netwerken. Een voorbeeld daarvan wordt genoemd in figuur 3.10 van paragraaf 3.10. Toch voert het te ver om hier te spreken van rekrutering door al Qa'ida.

Op het internet is een sterk interactieve vorm van rekrutering waarneembaar van lokaal autonome netwerken die sterk gekoppeld is aan de interactieve manieren van propaganda bedrijven. De AIVD zegt hierover:

> *"Aanvankelijk verloopt de communicatie geheel open, vervolgens meer vertrouwelijk in beperkte kring en in de laatste fase is duidelijk sprake van conspiratief gedrag. In eerste instantie vindt een posting plaats op een website of een nieuwsgroep, waarbij wordt verwezen naar een bepaalde site, waarop via een chatprogramma met een grotere groep medestanders of op individuele basis kan worden gediscussieerd over (geloofs)zaken. Vervolgens wordt aan sommigen voorgesteld om in een één-op-één chatsessie verder op zaken in te gaan. In zo'n bilaterale sessie wordt vaak duidelijk toegewerkt naar rekrutering. Bepaalde charismatische of ideologisch meer geschoolde jongeren krijgen door medestanders kandidaten toegespeeld die mogelijk vatbaar zijn voor zo'n rekrutering via het internet. Deze zelfbenoemde ideologen en rekruteurs, onderhouden vaak bilaterale internetcontacten met een aanzienlijke groep potentiële rekruten."*[100]

Kenmerkend voor het internet is echter vooral dat potentiële strijders zich zelf willen aanmelden voor deelname aan de gewelddadige jihad (conscriptie). Net zo min als het gebruik van het begrip rekrutering impliceert dat er sprake is van een hiërarchische legerorganisatie, impliceert het begrip conscriptie dat. Conscriptie (in dit kader) is gericht op het mogen deelnemen aan de activiteiten van een netwerk of groepering die bereid en in staat is tot het uitvoeren van een gewelddadige actie. Het *proces* wordt in dit geval niet ingezet door een *rekruteur*, maar door de potentiële strijder die voor zich zelf als het ware de knop al heeft omgezet. Wel komt er een selecteur aan te pas die moet bepalen of de strijder wordt opgenomen in de gelederen van het netwerk of de groepering en daar ook eventueel een training voor krijgt. Feitelijk is dus bij conscriptie geen sprake van rekrutering in formele zin, hoewel er nog wel steeds twee partijen betrokken zijn.

Conscriptie past goed bij het karakter van het internet waar sprake is van een grote dynamiek en potentieel sterk wisselende rollen. Geïnteresseerden in de jihad nemen bijvoorbeeld deel aan discussies op het internet. Als ze na verloop van tijd ontvankelijk zijn geraakt voor de jihadistische boodschap en steeds verder radicaliseren, kan een moment ontstaan waarin zij zich zelf aanbieden aan iemand die bij hen hoog in aanzien staat. Zij geven daarmee invulling aan het algemene appèl op het internet om zich aan te sluiten bij de 'karavaan der martelaren'.[101] Het kan ook gaan om een meer algemene oproep. Een buitenlands voorbeeld van een dergelijk proces is

100 AIVD 2006, p. 48.
101 Eén van de eerste jihadistische sites die zich op Nederland richtte had de naam 'sluit je aan' (bij de karavaan der martelaren) en Azzam, één van de grondleggers van al Qa'ida, heeft een werk met deze titel geproduceerd (zie paragraaf 3.3.3.3). Zie voor dit proces van 'zelf aanmelden' ook AIVD 2006.

uitgeschreven in de New York Post. In een met een wachtwoord beschermde chatroom vond eind september 2003 een discussie plaats. Een persoon schrijft: *"Brother, how do I go to Iraq for Jihad? [...]"*. Na vier dagen komt er een antwoord en een advies om iemand op te zoeken die hij vertrouwt om op die manier de eerste stappen te zetten op de weg die wijd open is. Na een vervolgvraag stuurt de antwoordgever een propagandistische video en geeft instructies om PalTalk-software te downloaden. Daarna verdwijnt de potentiële rekruut uit beeld voor het publiek.[102] Een ander voorbeeld is het volgende. In 2003 plaatste ene Abu Thur de volgende boodschap op een islamistisch webforum:

> *"Dear Brothers,*
> *I have already succeeded with the grace of Allah and his help, to go to Kurdistan for Jihad through one of the brothers in this forum. Praise be to Allah, I have fought there, by the grace of God and his bounty. But Martyrdom was not granted to me, and therefore I ask Allah to give me more lifetime and to make my deeds good. I ask anyone who has the capacity to organize for me to go to another Jihad front to correspond with me."*[103]

Kenmerkend voor het internet is verder dat de rollen snel kunnen wijzigen. Bij gebrek aan 'een karavaan om zich bij aan te sluiten', kan de potentiële strijder bijvoorbeeld besluiten er zelf maar één te vormen. De potentiële strijder wordt dan 'rekruteur' voor zijn eigen nog te vormen groep of kan deel gaan nemen aan een virtueel netwerk dat beoogt om aanslagen te plegen. Overigens valt daarbij de vraag te stellen of er wel sprake is van conscriptie als je lid bent van een virtueel netwerk van gelijkgestemden die gewelddadige acties niet zeggen te schuwen. Feitelijk is eerder sprake van een geleidelijk groepsproces van onderlinge beïnvloeding.

In relatie tot het internet wordt ook wel gesproken van *zelfontbranding*. Daarvan is sprake als iemand die zonder duidelijke contacten met rekruteurs of zonder dat hij regelmatig een radicale moskee bezoekt of zonder andere vormen van fysieke beïnvloeding, vanachter het computerscherm de gewelddadige jihad omarmt en uit eigen beweging op jihad probeert te gaan of in eigen land aanslagen voorbereidt.[104] Bij zelfontbranding is geen sprake van twee partijen: de zelfontbrander wil immers op zijn eigen houtje op jihad gaan en heeft de knop al omgezet. Van rekrutering in formele zin kan dan ook geen sprake zijn.

De zelfontbrander consumeert het radicale materiaal via het internet en kan (zowel passief als actief) discussies op het internet volgen en zich daardoor laten inspireren.[105] Van contact met een (virtuele) rekruteur, selecteur of conscriptie is geen sprake.

> *"In Nederland werd eind september 2004 de 18-jarige scholier Yahya K. uit Sas van Gent aangehouden, die bedreigingen had geuit op het internet tegen onder meer het Kamerlid Hirsi Ali en de AIVD. Tijdens zijn arrestatie bleek hij in het bezit van zelfgemaakte explosieven die hij met kennis afkomstig van het internet in elkaar had gezet. Ook het proces van radicalisering had hij geheel doorlopen vanachter zijn beeldscherm in de virtuele wereld".*[106]

102 Weimann 2006, p. 102- 121.
103 Rozen 2003.
104 Onder andere: Van Leeuwen 2005, p. 87.
105 Mede gebaseerd op AIVD 2006, p. 50.
106 AIVD 2006, p. 50.

Is het in de fysieke wereld al lastig om de overgang van radicalisering naar rekrutering en conscriptie afzonderlijk te bezien, dat geldt zeker voor het internet. Rollen kunnen snel wisselen en het gemak om virtuele netwerken te vormen (zie paragraaf 3.10) vertroebelt het beeld nog meer. Is er immers wel sprake van rekrutering of conscriptie als je lid bent geworden van een virtueel netwerk van gelijkgestemden die gewelddadige acties niet zeggen te schuwen? Of is eerder sprake van een geleidelijk groepsproces van onderlinge beïnvloeding? Het is zelfs de vraag of door de opkomst van het internet nog wel sprake is van het klassieke rekruteur-/rekruut-concept, en of dit concept niet langzaam wordt vervangen door een permanente en interactieve mix van top-down en bottom-up informatieverschaffing en -inwinning, vermengd met online aanmoediging, sturing of netwerkvorming, die uiteindelijk tot hetzelfde resultaat leidt: aanwas voor de jihadstrijd. Kortom, rekrutering, conscriptie en zelfontbranding via het internet zijn nog relatief nieuwe verschijnselen die nog niet geheel kunnen worden doorgrond.

Wat is nu de dreiging die hier van uitgaat? Het internetgebruik door jihadisten resulteert in meer interactieve vormen van rekrutering die nog niet goed te duiden zijn evenals in conscriptie en zelfontbranding. Het onderscheid met radicalisering is niet eenvoudig te maken. Wel kunnen we stellen dat het internetgebruik voor dit type doeleinden de stap van aanhanger van het jihadistische gedachtegoed naar terrorist kan verkleinen en bespoedigen, zeker in combinatie met het aanbod van propaganda- en trainingsmateriaal en de vorming van virtuele netwerken.

3.8 TRAINING

Onder het begrip training valt het opzoeken of produceren en/of verspreiden van educatiemateriaal, handleidingen, films en dergelijke over aspecten die van belang zijn voor de jihadstrijd. Voorbeelden daarvan zijn materialen hoe jihad te voeren in dichtbevolkte steden, explosieven te maken, wapens te hanteren of veilig te communiceren.

Er is veel jihadistisch trainingsmateriaal beschikbaar op het internet. Dit is mede gestimuleerd door het verdwijnen van de fysieke trainingskampen in Afghanistan. Nieuwe zijn niet snel opgezet hoewel er nog steeds signalen zijn van fysieke trainingskampen, bijvoorbeeld in Afrika. Als gevolg van het verdwijnen van de kampen in Afghanistan is de behoefte aan virtuele trainingskampen toegenomen. Een aantal jihadistische webfora kent dan ook symbolische namen van beroemde trainingskampen in Afghanistan.[107]
Het belang van het internet voor training wordt ook ondersteund door uitspraken als *"It is not necessary... for you to join in a military training camp, or travel to another country... you can learn alone, or with other brothers, in [our arms] preparation program."*[108]

Training via het internet manifesteert zich met name door uitgifte van handleidingen, bijvoorbeeld voor het maken van explosieven. Tussen 2000 en 2005 is het aantal verwijzingen naar sites met terrorisme-geörienteerde handboeken verdubbeld.[109] Een belangrijk werk voor de huidige jihadisten is dat van de eerder genoemde as-Suri. Zijn omvangrijke werk bestaat uit vele (strategische) handleidingen (zie ook paragraaf 3.2.3) en trainingsmateriaal. Het boek is in het Arabisch, maar enkele delen zijn al vertaald in het Engels.

107 Rogan 2006, p. 26.
108 Al Qa'ida-kopstuk Abu Hadschir al Muqrin tijdens een interview met Der Spiegel online.
109 Weimann 2006, p. 124.

Naast handleidingen zijn video's in opmars. Het gaat dan bijvoorbeeld om instructievideo's hoe een bomgordel te maken, of buskruit of slagpijpjes te maken. Dit materiaal is in het algemeen zeer professioneel van opzet.[110] Het risico dat van dit laagdrempelig beschikbare trainingsmateriaal uitgaat is aanzienlijk te noemen, zeker wanneer daarvan in het Nederlands vertaalde versies beschikbaar komen. Gelet op de algemene toename van naar het Nederlands vertaalde materiaal, is het waarschijnlijk slechts een kwestie van tijd wanneer Nederlandse vertalingen van materiaal verschijnen.[111]

Maar niet alleen explosieven krijgen aandacht in de voorbereiding op de strijd. Actueel en regelmatig verschijnt het *online* tijdschrift *Al-Battar*. Al-Battar plaatst veel en breed geörienteerd instructiemateriaal, wordt toegeschreven aan al Qa'ida en is in 2004 van start gegaan. Alle aspecten van terrorisme komen aan bod. De achtste editie van Al-Battar (april 2004) bevat uitgebreide, geïllustreerde instructies voor het gebruik van een sluipschutter-geweer, kennelijk geschreven door een expert.[112] De tiende editie (mei 2004) legt weer de nadruk op ontvoering en gijzeling, met daarbij de mogelijke motiveringen voor ontvoeringen: eisen doen inwilligen, politieke schade door verstoring verhouding tussen staten, informatie van de gegijzelde, losgeld en een zaak onder de aandacht brengen. Tenslotte wordt op Al-Battar aandacht besteed aan het ontdekken van infiltranten en agenten, reizen, valse documenten, schuilplaatsen, communicatie en maatregelen voor het geval men gearresteerd wordt. Onlangs is een compilatie geproduceerd van het Al-Battar materiaal.[113] Vaak worden professionele methodieken overgenomen uit militaire handboeken of uit instructieboeken voor inlichtingenofficieren.[114] Ook de gegevensdragers van de Hofstadgroep bevatten dergelijke militaire handleidingen en op de weblog van de Leeuwen van Tawhied werd in juli 2005 het document 'Lessen in veiligheid' gepubliceerd, dat gaat over hoe te handelen bij arrestaties en verhoor.

Ook de nieuwste ontwikkelingen worden kennelijk nauwgezet door terroristen gevolgd, zoals blijkt uit een bijdrage op een jihadistisch forum. In die bijdrage wordt een geavanceerd antiraketsysteem voor militaire voertuigen gedemonstreerd. De mujahideen in Irak hebben kennelijk geëxperimenteerd hoe deze actieve bescherming te omzeilen.[115]
Het Simon Wiesenthal Center rapporteert dat in de vele trainingsdocumenten die zij in het kader van een onderzoek hebben aangetroffen, tevens instructies voor het maken van massavernietigingswapens te vinden zijn, inclusief doelwitselectie.[116] Ook aan biologische wapens wordt gedacht. Zo verscheen er op jihadistische webfora een handleiding over het gebruik van botulisme en werd over de toepassing ervan gediscussieerd.[117]

110 Resultaat van voorleggen materiaal aan deskundigen. Zie ook Telegraaf 2006.
111 Interview 5.
112 Jamestown 2006.
113 Interview 1.
114 AIVD 2006, p. 51.
115 SITE-Institute 2006u.
116 National Post 2006.
117 SITE-Institute 2006v.

Onlangs is er een nieuwe compilatie van trainingsmateriaal verspreid op jihadistische fora, 'verstopt' in een bestand dat *Nemo* heet. De compilatie bevat - naast scènes uit de tekenfilm '*Finding Nemo*' - materiaal aangaande onder andere vervalsingen, explosieven, gif en nucleaire wapens. Verder worden *hyperlinks* gegeven naar zeventien andere relevante documenten.[118] Het toekennen van een naam als Nemo aan dergelijke compilaties is extra verraderlijk, omdat kinderen dergelijke bestandsnamen als zoekterm invoeren bij het gebruik van moderne file-sharing-programma's om films te downloaden. Op die manier kunnen zij geconfronteerd worden met gewelddadig materiaal.

In het Verenigd Koninkrijk hebben reeds enkele veroordelingen plaatsgevonden van 'aan al Qa'ida geliëerde' personen die instructies van het internet hadden gehaald, bijvoorbeeld voor het opblazen van vliegtuigen.[119] Bij de in augustus 2006 in het VK gearresteerden in het kader van het verijdelde complot om meerdere vliegtuigen op te blazen, zouden eveneens via het internet verkregen handleidingen zijn aangetroffen.[120] Uit AIVD-onderzoek is duidelijk geworden dat ook in Nederland aanwezige jihadisten op het internet actief op zoek gingen naar operationele kennis. In een aantal gevallen werden bij huiszoekingen en arrestaties zelfgemaakte explosieven aangetroffen waarvan de fabricage waarschijnlijk (deels) was gebaseerd op kennis verkregen via het internet.[121] De gegevensdragers van de verdachten van de Hofstadgroep bevatten literatuur afkomstig van het internet die onder andere betrekking had op militaire handleidingen.[122]

Uiteraard is niet al het materiaal dat op het internet te vinden realistisch, betrouwbaar en (veilig) uitvoerbaar. Experts geven aan dat dit materiaal lang niet toereikend is om bijvoorbeeld op veilige wijze een aanslag te plegen, explosieven te vervoeren en het explosief op het juiste moment met het gewenste effect tot ontploffing te brengen. Daar is toch meer expertise voor nodig, die gelukkig schaars is. Een fysiek trainingskamp levert toch meer kennis en vooral ervaring op dan handleidingen en video's via het internet.[123]

Hoe moeten we de dreiging van online trainingsmateriaal en training via het internet beoordelen? Het internet staat vol handboeken, instructies en tips voor personen die een aanslag willen plegen, of zich in meer algemene zin willen voorbeiden op de jihadstrijd. Het internet biedt in deze vooral laagdrempelig gemak in het zoeken en aanbieden van het materiaal, zodanig dat je zou kunnen spreken van een groot virtueel trainingskamp. Als belangrijke kanttekening valt bij het beschikbare materiaal en het concept van een virtueel trainingskamp te plaatsen, dat je de instructies nog altijd zélf goed moet kunnen begrijpen, oefenen, toepassen en uitvoeren en dat de discipline die benodigd is of voor succesvolle strijd of het uitvoeren van een grootschalige aanslag in een feitelijk trainingskamp vele malen beter zal kunnen worden ontwikkeld. Ook kunnen bij bepaalde instructies ongetwijfeld vraagtekens geplaatst worden ten aanzien van 'gebruiksgemak' en veiligheid. Voor een kleinschaligere aanslag (explosies of vergiftigingen) is de dreiging die uitgaat van het beschikbare online-materiaal om vier redenen echter wel degelijk aanzienlijk:

- tenminste een deel van de beschrijvingen is expliciet en compleet, en de kwaliteit en beschikbaar ervan neemt toe;
- er wordt steeds meer naar het Engels, Frans, Duits maar ook naar het Nederlands vertaald materiaal op het internet aangetroffen;
- ook personen die geen concrete plannen hadden voor een aanslag kunnen door de veelheid van het rijk geïllustreerde materiaal geïnspireerd raken;
- er is materiaal beschikbaar voor diverse soorten aanslagen, waaronder die met chemische, biologische, radiologische en nucleaire middelen.

118 Site Institute 2006c.
119 Guardian 2005.
120 Independent 2006b, Telegraaf 2006.
121 AIVD 2006, p. 51.
122 Rechtspraak.nl 2006.
123 Eigen navraag bij deskundigen. Zie ook Washington Post 2005.

3.9 ONDERLINGE COMMUNICATIE EN PLANNING

Het internet is, naast de andere functies die het vervult, bij uitstek een communicatieomgeving. Het is daardoor niet vreemd dat de jihadisten het internet gebruiken voor onderlinge communicatie binnen de eigen groepering of het netwerk en voor planning van terroristische activiteiten. Hoewel daartussen een onderscheid valt te maken, is dat slechts gradueel. Onderlinge communicatie (binnen een terroristische groepering of netwerk) kan over van alles gaan. In het kader van een beoordeling van de dreiging gaat het dan natuurlijk niet om elkaar te informeren over het wel en wee van de familie, maar om communicatie die is gerelateerd aan terroristische activiteiten. En dan hebben we het al gauw over planning van terroristische activiteiten.

Het internet speelt niet voor niets een grote rol als mondiale communicatieomgeving. Een reden daarvoor is onder andere de eenvoudige toegang tot het medium en de geringe kosten. Overigens geldt wel als nuancering dat velen in de traditionele moslimlanden nog geen toegang hebben tot het internet, hoewel dit de afgelopen jaren wel sterk is toegenomen, vooral door een stijging van het aantal internetcafé's. Een ander aantrekkelijk punt is dat het internet als het ware als het elektronische zenuwstelsel kan fungeren van een netwerk en daardoor inherente nadelen van netwerken, namelijk het moeizame karakter van coördinatie van activiteiten en doelgerichte taakuitvoering, kan neutraliseren. Extra aantrekkelijk voor de jihadisten is dat de communicatie en operationele informatie-uitwisseling grotendeels anoniem kunnen plaatsvinden en dat bewijsvoering voor opsporingsinstanties tal van complicaties kent. En daar is het internet in het voordeel ten opzichte van andere communicatiemiddelen, zowel voor de kern van al Qa'ida als voor de door al Qa'ida geïnspireerde netwerken. Ook binnen een klein netwerk kan het internet daarbij voordelen hebben. Bij fysiek contact kunnen immers eventuele observatieteams zicht krijgen op het netwerk en op gerichte wijze afluisteren.

Toch gelden voor jihadistische netwerken de genoemde voordelen van het internet maar ten dele. Communicatie en informatie-uitwisseling zijn en blijven immers een riskante aangelegenheid, omdat de informatie ongewild terecht kan komen bij anderen. Particuliere organisaties die het internet afspeuren op illegale activiteiten kunnen bijvoorbeeld informatie onder-

scheppen en dat doorgeven aan opsporingsinstanties. Weisburd in de VS, die als een soort Simon Wiesenthal het internet afspeurt naar jihadisten, heeft wat dat betreft al een naam opgebouwd.[124] De deelnemers moeten informatie en kennis delen wil het netwerk kunnen functioneren. Dit biedt weliswaar voordelen, maar ook mogelijkheden voor misbruik en ongewenste verspreiding van cruciale en kwetsbare informatie. Zeker virtuele netwerken zijn wat dat betreft niet goed beheersbaar. Een deelnemer kan de informatie immers doorgeven aan andere deelnemers, al dan niet van andere netwerken. Er bestaat bovendien geen garantie dat opsporingsinstanties de communicatie niet onderscheppen en daardoor blijft oog-in-oog-communicatie soms noodzakelijk. Hoewel er dus voor netwerken voordelen zijn om via het internet te communiceren en informatie uit te wisselen, zowel binnen als tussen bestaande netwerken, blijven er ook nadelen.[125]

Wegen de voordelen zwaarder dan de nadelen? Zoals eerder is vermeld, beschikt de jihadistische beweging in het algemeen over gedegen computerkennis en vaak over de nieuwste programmatuur en voldoende apparatuur. Deze gebruiken zij ook voor communicatie en planning van terroristische activiteiten (zie figuur 3.9). De jihadisten zijn zich daarbij goed bewust van het risico dat communicatie kan worden onderschept en communiceren in toenemende mate achter 'gesloten virtuele deuren' (zie paragraaf 3.2.3). De Bundesverfassungsschutz zou hebben aangegeven dat mobiele telefoons nauwelijks meer een rol spelen in de communicatie, en dat zij vrezen dat er een systeem van heimelijke communicatie via het internet bestaat, waarbinnen planning en coördinatie voor aanslagen plaatsvindt.[126] Overigens zijn daarbij wel vraagtekens te plaatsen.

Figuur 3.9 Voorbeelden van communicatie via het internet

Gedetailleerde plannen voor een aanslag op de Saoedische minister van Binnenlandse Zaken werden gevonden op een site van al Qa'ida-operatives in Saoedi-Arabië.

Er zijn aanwijzingen dat het internet is gebruikt voor de strategische planning van de aanslagen in Madrid in maart 2004. In een strategisch document uit december 2003 op de GIMF-site wordt Spanje als meest geschikte kandidaat voor een aanslag aangeduid, om te zorgen dat Spanje de coalitie verlaat en de coalitie wordt verzwakt. Zelfs de timing (verkiezingen in maart) en methode ('several attacks or blows') staan in het document vermeld.[127]

Gelet op de algemene internetvaardigheden van jihadisten zullen zij ook telefonie via het internet (VOIP) en andere moderne toepassingen (gaan) benutten om afluisterbaarheid en traceerbaarheid van hun communicatie te bemoeilijken. Toch verschijnen er nog steeds berichten dat vooral de top van 'kern al Qa'ida' gebruik maakt van koeriers. De berichten worden weliswaar op een pc gemaakt en geprint, maar fysiek verstuurd.

Al met al kunnen we dus concluderen dat jihadisten het internet gebruiken voor onderlinge communicatie en planning. Ze maken daarbij gebruik van de mogelijkheden van anonieme en afgeschermde communicatie. Naast voordelen voor jihadisten biedt dit internetgebruik inlichtingen- en opsporingsinstanties de mogelijkheid tot ingrijpen. De jihadisten zijn zich daar goed van bewust.

3.10 CREATIE VAN VIRTUELE NETWERKEN

Jihadisten opereren veelal in lokaal en internationaal opererende netwerken.

> *"Een jihadistisch netwerk is een fluïde, dynamische, vaag afgegrensde structuur die een aantal personen (radicale moslims) omvat die onderling een relatie hebben, zowel op individueel als geaggregeerd niveau (cellen/groepen). Zij worden ten minste tijdelijk door een gemeenschappelijk belang verbonden. Dat belang is het nastreven van een aan jihadisme (inclusief terrorisme) te relateren doel.*
> *Personen die deel uitmaken van het netwerk worden geduid als lid. Men is lid indien men binnen de grenzen van het netwerk actief en bewust een bijdrage levert aan de realisering van het bovengenoemde doel."*[128] [129]

Als groot voordeel van het internet zou kunnen worden genoemd dat het mogelijk is om virtuele netwerken te vormen, in de zin dat leden daarvan elkaar online hebben 'ontmoet' en elkaar vervolgens enkel online treffen. Deze virtuele netwerken kunnen variëren van geheel nieuwe netwerken, een combinatie van een nieuw met een bestaand netwerk en een combinatie van bestaande netwerken. In potentie kunnen via het internet wereldwijd netwerken worden gecreëerd, hoewel de traditionele moslimlanden in toegang tot het internet nog achterlopen. Door personen te volgen tijdens bijvoorbeeld chatroomsessies, elkaar de maat te nemen en één-op-één te communiceren in afgesloten omgevingen (zie paragraaf 3.7), kan een goede indruk ontstaan van iemands betrouwbaarheid en toewijding aan de goede zaak.

De AIVD noemt aanvullend nog enkele andere voordelen. In virtuele netwerken kunnen individuen uit lokale netwerken snel wereldwijd contacten leggen om bijvoorbeeld logistieke ondersteuning of strijdmiddelen te organiseren bij de voorbereiding van aanslagen. De deelnemers aan het netwerk kunnen betrekkelijk anoniem participeren.

> *"Aangezien het netwerk slechts bestaat in de virtuele wereld en er in de reële wereld geen enkel contact hoeft te bestaan tussen de verschillende deelnemers, zijn dergelijke netwerken moeilijk te onderkennen en de personen die erin participeren onder een soms snel wisselende virtuele nickname niet eenvoudig te identificeren voor politie en inlichtingen- en veiligheidsdiensten. [....] De virtualisering van de jihad biedt op deze manier enorme mogelijkheden voor internationale samenwerking tussen netwerken en individuen en verhoogt zo de slagkracht van de jihadistische beweging."*[130]

124 Zie voor Weisburd bijvoorbeeld Labi 2006.
125 Geïnspireerd door Kortekaas 2005, p. 51-55, 69-70, 103-107 en 123-129.
126 BBC Monitoring 2006b.
127 Weimann 2006, p. 130 en p. 134.
128 AIVD 2006, p. 14.
129 Voor meer achtergrondinformatie over terroristische netwerken, zie AIVD 2006, p. 13-19.
130 AIVD 2006, p. 49.

Er kleven ook nadelen aan virtuele netwerken. Een kenmerk van virtuele gemeenschappen en netwerken is namelijk de *vluchtigheid van contacten en identiteiten*. Doordat individuen zeer uiteenlopende achtergronden kunnen hebben, is communiceren onderling in die virtuele netwerken lang niet altijd eenvoudig. De drempels om uit de gemeenschap te stappen, zijn bijvoorbeeld laag. Als gevolg van die vluchtigheid weet je eigenlijk niet met wie je contact hebt en diegene kan weer snel verdwijnen. Personen kunnen bovendien nog eens vele identiteiten (nicknames) aannemen en deze snel veranderen. Daarnaast is het aanbrengen van een scheiding tussen een elektronische en een natuurlijke identiteit eenvoudig. Een virtuele persoon kan opsporingsambtenaar of inlichtingenmedewerker blijken te zijn. Juist binnen illegale netwerken is cruciaal dat iemand te vertrouwen is. Op grond van bovenstaande kanttekeningen is dat bij virtuele personen nog maar de vraag. En daar waar netwerken überhaupt inherent een zekere mate van vrijblijvendheid kennen, geldt dat zeker voor virtuele netwerken waarin men elkaar niet (fysiek) kent en fysiek heeft ontmoet. Dit alles maakt het functioneren van virtuele netwerken er niet eenvoudiger op.[131]
De AIVD stelt in dat kader dat:

> *"[....] het onderlinge wantrouwen en het grote veiligheidsbewustzijn onder jihadisten ook een rem kan zijn op snelle virtuele netwerkvorming. Pas indien er daadwerkelijk onderling vertrouwen bestaat, kunnen er via het internet gezamenlijke activiteiten worden ontplooid. Dit betekent dus dat men elkaar vaak reeds kent uit de fysieke wereld of kan verwijzen naar gemeenschappelijke kennissen, clan- of familieleden. Vaak vinden gedetailleerde ideologische discussies plaats om elkaar de maat te nemen, of wordt streng geselecteerd bij het toelaten van deelnemers tot bepaalde gesloten (delen van) websites die meestal slechts via bepaalde (soms snel wisselende) wachtwoorden te benaderen zijn."*[132]

Hoe reëel is de creatie van virtuele netwerken in het licht van bovenstaande voor- en nadelen? En, wanneer men elkaar al kent uit de fysieke wereld, is dan nog wel sprake van een virtueel netwerk? Feit is dat er voorbeelden van virtuele netwerken zijn gedocumenteerd. Eerder in dit hoofdstuk is aangegeven dat de Nederlandse jihadisten bewust de interactie zoeken met geïnteresseerden in de islam en de jihadstrijd. Op die wijze kunnen totaal nieuwe virtuele netwerken ontstaan en een virtuele jihadistische gemeenschap op het internet worden gecreëerd. Er zijn zeker indicaties dat dat ook het geval is. Verder is verwoord dat de Nederlandse jihadisten gebruik maken van vertalingen van anderen en naar andere sites verwijzen. Ook dat kan worden gezien als een virtueel netwerk. Er zijn ook twee voorbeelden openbaar van een virtueel netwerk dat voorbereidingshandelingen trof voor aanslagen (zie figuur 3.10). Op te merken is wel dat nu de betreffende netwerken zijn opgerold, dit niet bijdraagt aan het vertrouwen in virtuele netwerken bij jihadisten.

131 Kortekaas 2005, p. 107-114 die zich daarbij baseert op andere auteurs op het terrein van georganiseerde criminaliteit.
132 AIVD 2006, p. 49.
133 Washington Times 2006, Bell 2006.
134 SITE-Institute 2006h.
135 Scheuer 2006.

Figuur 3.10 Voorbeelden van virtuele netwerken

Diverse operaties die de afgelopen maanden tot aanhoudingen in Europa en Noord Amerika hebben geleid, wijzen op de aanwezigheid van virtuele netwerken. De in Canada gearresteerde jihadistische verdachten maakten deel uit van een internationaal virtueel netwerk, waarvan verschillende leden ook fysiek met elkaar in contact traden.[133] *Twee Amerikanen van het (vermeende) netwerk hebben doelwitverkenningen uitgevoerd in Washington DC in de lente van 2005. Deze verkenningen vonden plaats minder dan een maand nadat de twee Amerikanen in Canada drie van de zeventien onlangs in Canada gearresteerde extremisten hadden ontmoet. Het materiaal van de verkenningen zou zijn aangetroffen bij Irhabi007 (een bekende jihadistische hacker) in het Verenigd Koninkrijk. En het netwerk bleek een grotere spanwijdte te hebben, want één maand voorafgaand aan de arrestatie van Irhabi007, werd een handlanger van hem - een in Zweden geboren man - gearresteerd in Bosnië wegens het plannen van een aanslag. Deze arrestatie leidde weer tot de aanhouding van vier Denen, die van hetzelfde netwerk deel zouden uitmaken.*
Volgens het SITE-institute is het duidelijk dat deze personen elkaar zonder het internet waarschijnlijk nooit zouden hebben ontmoet, laat staan samengewerkt.[134]

Recent is een plan verijdeld "to destroy an underwater tunnel connecting New Jersey and New York City and inundate lower Manhattan". [....] The plot that was disrupted in the first week of July was still in the planning stages and was led by a 31-year-old Lebanese national named Assem Hammoud. Living in Beirut when arrested, Hammoud is a 2002 graduate in commerce of Concordia University in Montreal and was teaching economics, business ethics and human resources at the Lebanese International University. [....] Hammoud was living a normal life, had no police record and had an extended family, none of whom seems to have known of his radical tendencies.

Assem Hammoud-who was using the alias Amer al-Andalusi-appears to have been the leader of an entirely 'virtual' would-be terrorist operation. Accounts to date show that Hammoud and seven other individuals had joined together to plan a suicide attack on a tunnel connecting New Jersey and lower Manhattan. The group had never met as a unit, and instead had communicated via the internet and was spread over three continents. Three of the eight are now under arrest: Hammoud, an unnamed Syrian and an individual of undisclosed nationality. [....]
The FBI has said that the five others involved in the plot-a Saudi, a Yemeni, a Jordanian, a Palestinian and an Iranian Kurd-have been 'largely identified' but have not been apprehended. [....] The FBI and the U.S. Department of Homeland Security (DHS) have underscored that the Hammoud-led plot was very much still in the planning stages; no explosives had been acquired, financial support was not apparent and none of the plotters had visited New York. [....] While there is not yet any information showing a direct connection between the plotters and al-Qaeda, Assem Hammoud told his Lebanese interrogators that he had been motivated by the example of Osama bin Laden and al-Qaeda's attacks, and that he was acting 'on a religious order from bin Laden.' For instance, Hammoud told the Lebanese: "I am proud to carry out his orders." [135]

Voor relatief onschuldige en niet strafbare activiteiten, zoals het discussiëren over bepaalde onderwerpen, zal de noodzaak van vertrouwen minder wegen dan voor echt strafbare feiten zoals het plegen van terroristische activiteiten. Immers de gevolgen bij niet strafbare activiteiten zijn beperkter wanneer het vertrouwen wordt geschaad, de informatie uitlekt, of blijkt dat een lid van het netwerk een opsporingsambtenaar is die zich virtueel uitgaf voor een ander. Toch bestaat de indruk dat het bij martelaarsacties niet altijd gaat om het succesvol ten uitvoer brengen van een actie, maar vooral om het feit dat men daartoe bereid was. De Profeet zegt immers dat niet de daad zelf belangrijk is, maar de intentie. In dat opzicht zou zelfs een actie die virtueel is beraamd en wordt verijdeld, toch nog succesvol zijn. Ontdekking maakt dan niet zoveel meer uit. In die zin is het dus ook denkbaar dat enkele personen die elkaar uitsluitend virtueel kennen, op enig moment samen komen voor een aanslag. Op het internet heeft zich dan een soortgelijk groepsproces voltrokken als in fysieke netwerken.

Verder kent een deel van de actieve jihadisten op het internet elkaar al via fysieke contacten of netwerken. Kunnen we dan eigenlijk wel spreken van een virtueel netwerk? Het feit dat men elkaar al fysiek kent, betekent nog niet dat men in de fysieke wereld even vrijelijk over bepaalde zaken praat, zich bewust is van gelijke idealen en denkbeelden en deel uitmaakt van dezelfde virtuele netwerken. Denkbaar is dat twee personen elkaar kennen uit bijvoorbeeld dezelfde moskee, maar pas interactief en via nicknames met elkaar communiceren over deelname aan de jihad zonder te weten dat men elkaar kent. Het feit dat men elkaar kent, is dus niet doorslaggevend voor het verschil met gewone netwerken en de dreiging die daar van uitgaat: het verschil is er.

Als het gaat om de creatie van virtuele netwerken concludeert de AIVD dat op langere termijn er met name door de virtualisering een ongedifferentieerde informele pool van bereidwilligen voor de jihad kan ontstaan

> *"[....] die in wisselende combinaties met elkaar of individueel geweldsactiviteiten ontplooien. Het risico dat lokale en internationale elementen meer met elkaar verweven raken wordt daarmee groter. Met name het internet maakt het gemakkelijk om op korte termijn contacten te leggen, zowel nationaal als over de grenzen heen, en een tijdelijk virtueel netwerk te creëren voor het voorbereiden van acties.*[136]

In dat geval geldt dat, in de bewoordingen van de AIVD, de slagkracht van de internationale jihadistische beweging aanzienlijk wordt verhoogd.[137]

3.11 INVLOED INTERNET OP RADICALISERING

De NCTb spreekt in zijn dreigingsbeelden over 'het internet als katalysator voor radicalisering' en de AIVD over 'het internet als de turbo van de jihadbeweging'.[138] Maar, op welke wijze heeft het internet invloed op radicalisering? Radicalisering wordt vooral gezien als een proces dat ergens start en in het ergste geval eindigt doordat het overgaat in terrorisme. Er is echter niet exact aan te geven wanneer radicalisering start en eindigt en bovendien bestaan daarover verschillende normatieve standpunten. Wat zijn nu mogelijke verklaringen achter de rol die het internet speelt bij de start van de radicalisering?

136 AIVD 2006, p. 61.
137 AIVD 2006.
138 NCTb 2006b, AIVD 2006, p. 43.

Uiteraard zijn er twee zijden aan de 'radicaliseringsmedaille' te onderkennen: de *vraagzijde* en de *aanbodzijde*. Radicalisering kent een *vraagzijde* van individuen die, al dan niet latent, op zoek zijn naar materiaal over de islam, het leven van een moslim in een westers niet-moslimland, maar ook eventueel naar radicaal materiaal. Radicalisering kent aan de *aanbodzijde* de salafisten en de jihadisten.

Er is sprake van een grote groep ontheemde, vooral jongere, moslims in westerse-niet-moslimlanden. Zij voelen zich geïsoleerd in de samenleving waarin ze leven. Doordat deze jongeren zich, anders dan hun ouders, voor hun toekomst oriënteren op het Westen, maar zich tegelijkertijd ook in die samenleving sterk gewantrouwd voelen, zijn zij zoekende naar hun identiteit en een positionering in de westerse samenleving en kampen met tal van levensvragen en religieuze vragen. Op zoek naar antwoorden op die vragen komen ze uit in een omgeving die ze goed kennen en een laagdrempelige toegang kent, namelijk het internet. Daar kunnen ze niet alleen veel informatie vinden, maar bovendien onderdeel gaan uitmaken van een virtuele (moslim)gemeenschap en daarin met andere gelijkgestemden en lotgenoten van gedachten wisselen en stoom afblazen door het uiten van frustraties. Zij ervaren het internet als "[...] één van de weinig beschikbare middelen in hun 'strijd' en zij voelen zich relatief veilig tijdens het gebruik van internet. Veilig ten aanzien van de politie en inlichtingen- en veiligheidsdiensten maar ook veilig ten aanzien van familie- en traditionele invloeden. De corrigerende invloed van ouders en culturele normen en waarden zijn tijdens hun gebruik van internet voor een groot deel verdwenen."[139] Dat het internet een veilige omgeving is, geldt zeker voor moslima's.

> *"Deze moslima's ondergaan internet als een warm bad. Het is de plek waar ze ongestoord zichzelf kunnen zijn, op een anonieme manier in contact kunnen komen met andere moslima's en op een islamitisch sociaal geaccepteerde manier in contact kunnen komen met het andere geslacht. Hiermee wordt internet voor moslima's, die bij het bereiken van de puberteit hun bewegingsruimte sterk beperkt zien, een verlengstuk voor het fysieke leven."*[140]

De combinatie van ontheemde moslims in westerse-niet-moslimlanden en de mogelijkheden van het internet voor creatie van virtuele gemeenschappen en informatievergaring, zijn redenen waarom het internet een rol kan spelen aan de vraagzijde van radicalisering. Toch vervult het internet binnen deze context eerder een belangrijke maatschappelijke functie, dan dat het een katalysator of turbo voor radicalisering is. Er ontbreekt dus nog een belangrijk aspect dat verklaart waarom en hoe het internet kan bijdragen aan radicalisering. Daarvoor moeten we kijken naar de aanbodzijde.

139 Roy 2005, p. 153-170, AIVD 2006 en interview 4.
140 Pels 2003.

De salafisten en jihadisten spelen handig in op de levensvragen van ontheemden door de islam en jihadstrijd in one-liners te verpakken en te verkopen.

De salafisten beogen met hun aanwezigheid op het internet om via informatieverschaffing en propaganda moslims te mobiliseren voor hun visie op de islam. Hoewel de salafisten deelname aan de gewapende jihad niet voorstaan, kan hun visie op de islam sommigen wel ontvankelijk maken voor de gewapende jihad. Afhankelijk van de ontvankelijkheid van de betreffende individuen, kan het salafistische materiaal echter ook juist een buffer vormen.[141]

De jihadisten gaan een stap verder en proberen via propaganda, rekrutering en het aanbieden van trainingsmateriaal andere moslims te mobiliseren voor de jihad en hen kennis aan te reiken hoe ze de strijd zouden kunnen voeren. Door het universele en mondiale karakter van de (beoogde) virtuele gemeenschap, de ruimte tot het zelf interpreteren van de islam, gekoppeld aan de onwetendheid bij een groot deel van de Europese moslimjongeren op godsdienstig terrein en hun gebrek aan kennis van de Arabische taal, is de informatie normatief, fundamentalistisch/orthodox, eenvoudig van aard, conceptueel arm en de onderliggende ideologie vaak niet-coherent. Het aanbod schetst een moslimidentiteit die losstaat van nationale of etnische oorsprong en een ideaalbeeld dat ver af staat van de concrete samenleving waarin de ontheemden leven. Bovendien ontbreekt een kritische reflectie en informatie over de context en geschiedenis. Van echte discussie tussen voor- en tegenstanders is weinig sprake, hoewel er op het internet in Nederland wel in beperkte mate een religieus-ideologisch geïnspireerde discussie valt te bespeuren. Het internet is verder de plaats bij uitstek voor de zelfbenoemde meester die anderen religieuze uitleg geeft en voor de autodidact.[142]

Het probleem van het internet is daarom dat het aanbod merendeels is gebaseerd op een beperkte, eenzijdige en eenduidige (lees orthodoxe en/of radicale) uitleg van de islam en dat het aanbod er niet op is gericht om de ontheemden beter te laten functioneren in de samenleving waarin zij leven, maar te mobiliseren voor de zuivere islam of de mondiale jihad. Door bepaalde boodschappen en video's keer op keer uit te zenden, en door rechtvaardigende teksten steeds opnieuw als de waarheid te presenteren, ontstaat er een cultuur waarin sommigen ontvankelijk kunnen worden voor de jihad of de jihad als gewoon wordt ervaren. En daarmee speelt het internet, naast de genoemde nuttige functie, wel degelijk een rol bij de start van radicalisering.

De propaganda van de jihadisten richt zich echter niet alleen op mobilisatie van gewone moslims, maar ook op verdere radicalisering. Met hyperlinks op discussiefora worden geïnteresseerden gelokt naar radicalere sites. Ook richt de propaganda zich op al geradicaliseerden en voorziet hen van zwaarder materiaal. Websites bieden de gelegenheid tot chatten met jihadisten en communicatie tussen geradicaliseerden onderling en faciliteren daarmee ook groepsvorming. Uit onderzoek blijkt dat anonieme communicatie per computer leidt tot een sterkere groepsidentiteit, sterkere verantwoordelijkheidsgevoelens voor de groep, en dat makkelijker groepspolarisatie optreedt. Dit zou inhouden dat groepen op het internet juist sneller kunnen radicaliseren. Eenzijdige propaganda en herhaling van boodschappen via het internet zullen hieraan verder

141 Buijs e.a 2006, p. 275.
142 Roy 2005, p. 153-170, AIVD 2006.

bijdragen.[143] "Aanvankelijk verloopt de communicatie geheel open, vervolgens meer vertrouwelijk in beperkte kring en in de laatste fase is duidelijk sprake van conspiratief gedrag. In eerste instantie vindt een posting plaats op een website of een nieuwsgroep, waarbij wordt verwezen naar een bepaalde site, waarop via een chatprogramma met een grotere groep medestanders of op individuele basis kan worden gediscussieerd over (geloofs)zaken. Vervolgens wordt aan sommigen voorgesteld om in een één-op-één chatsessie verder op zaken in te gaan. In zo'n bilaterale sessie wordt vaak duidelijk toegewerkt naar rekrut ring."[144] De jihadisten beogen via het internet dus ook individuen te werven voor daadwerkelijke acties en bij te dragen aan verdere radicalisering. Verder verschaffen ze trainingsmateriaal en proberen zo individuen kennis te geven op welke wijze en met welke middelen de strijd gevoerd kan worden. Dat kan variëren van relatief onschuldige acties, zoals het hacken van bepaalde websites, tot terroristische aanslagen. Omgekeerd kunnen geradicaliseerde personen zich zelf aanbieden voor het plegen van gewelddadige activiteiten (conscriptie) of geheel zelfstandig verder radicaliseren, uitmondend in zelfontbranding.

Illustratief voor de invloed van het internet op verdere radicalisering is dat het internet in de groepsvorming van de aanslagplegers in Londen van juli 2005 een belangrijke rol heeft gespeeld en daarmee bij het plegen van een aanslag. "Het begint gewoon met een stel jongens [...]. Ze voelen zich kwaad of beledigd, willen ergens bijhoren, zoeken een doel in het leven. Op internet vinden ze gelijkgestemden, waardoor ze geen idee meer hebben hoe klein hun wereld eigenlijk is. 'Internet is buitengewoon stimulerend. Wat je ook doet, je krijgt het idee dat je de wereld aan het veranderen bent.'"[145] Illustratief is ook dat Imam Samudra, veroordeeld als field coördinator voor de aanslagen in Bali op 12 oktober 2002, verklaarde dat hij tot zijn overtuiging was gekomen door het lezen van een aantal standaardwerken en artikelen op radicale websites.[146] Ook in Nederland is er een voorbeeld bekend van een persoon die vergaand via het internet is geradicaliseerd, namelijk die van de eerder genoemde zelfontbrander uit Sas van Gent. Verder is het internet van invloed geweest op de radicalisering van Samir A. En de twee hoofdverdachten van de mislukte aanslagen op Duitse treinen eind juli 2006 zouden pas na hun aankomst in Duitsland zijn geradicaliseerd door propaganda van al Qa'ida op het internet. Eveneens via het internet kwamen de twee aan instructies voor het vervaardigen van de bommen. De bommen in de gevonden koffers kwamen voor 90 procent overeen met die instructies.[147]

Al met al is de conclusie dat het internet het gehele proces van radicalisering faciliteert. Voor iedere fase van radicalisering is er aanbod beschikbaar om "[...] belangstellenden, onder begeleiding dan wel zelfstandig, stap voor stap [te] indoctrineren in de jihadistische ideologie". Het aanbod is bovendien vaak multimediaal en interactiever dan andere bronnen en daarmee aantrekkelijker voor jongeren.[148] Op deze wijze kan een potentiële jihadist processen doorlopen van ideologievorming, ideologieversterking en ideologische indoctrinatie. Het draagt bovendien bij aan groepsvorming en tot netwerk-

143 Meertens e.a. 2006.
144 AIVD 2006, p. 48.
145 Persson 2005.
146 Weimann 2006, p. 106.
147 ANP 2006.
148 Dat laatste is gebaseerd op NRC 2005.

vorming van gelijkgestemden. Individuen en groepen kunnen zich daardoor gaan keren tegen de samenleving, eerst ideologisch en mogelijk op termijn activistisch-gewelddadig.

De vraag in hoeverre en op welke wijze het internet daadwerkelijk een rol speelt bij radicalisering en uiteindelijk tot terrorisme kan in deze fenomeenstudie niet volledig worden beantwoord, en blijft een interessante onderzoeksvraag. Start de reis naar het aanhangen van het radicale gedachtegoed op het internet, of is dat slechts een tussen- of eindstation? In hoeverre spelen radicale moskeeën en imams daarbij nog een rol? Is het geval van de zelfontbrander uit Sas van Gent een uitzonderlijk geval, of zijn er meer gevallen van zelfontbranding te verwachten in de toekomst? Nader onderzoek moet over deze vraagstukken uitsluitsel geven.

3.12 SLOTBESCHOUWING

De dreiging die uitgaat van het internet als middel is vooral een indirecte dreiging. In tegenstelling tot het gebruik van het internet als doelwit en wapen gaat het niet om terroristische activiteiten op zich. Het gaat om creatie van de randvoorwaarden waardoor de jihadisten een bredere doelgroep kunnen bereiken, beter kunnen functioneren, relevante kennis kunnen verspreiden en tot zich nemen en onderling kunnen communiceren. Het internetgebruik kan ook het voorbereiden en uitvoeren van terroristische activiteiten vereenvoudigen dankzij bijvoorbeeld de mogelijkheden om informatie in te winnen en virtuele netwerken te creëren.

Bezien vanuit het perspectief van radicalisering, gaat op dit moment de grootste dreiging uit van propaganda via het internet in combinatie met de relatief grote groep, vooral jonge moslims, die zoekend is naar antwoorden op tal van levensvragen en religieuze vragen. De propaganda vindt professioneel plaats, heeft een groot bereik en kent relatief weinig weerwoord. De propaganda blijft niet beperkt tot eenrichtingsverkeer: de jihadisten proberen actief te interacteren met geïnteresseerden. Combineren we dat met het feit dat vooral grote groepen jongeren toegang hebben tot het internet en dat intensief gebruiken, dan is duidelijk dat propaganda via het internet bijdraagt aan (verdere) radicalisering. Dat geldt zeker voor moslima's vanwege de aantrekkelijkheid van het internet voor hen (vraagzijde) in combinatie met de actieve rol van radicale moslima's in het aanbod. Hierdoor wordt potentieel een grote groep moslims bereikt die nu nog niet zijn geradicaliseerd. En juist de bijdrage van propaganda aan radicalisering is zorgelijk, omdat radicalisering niet alleen drempelverlagend werkt voor rekrutering voor de jihad, maar ook in de toekomst zou kunnen leiden tot meer terroristische activiteiten.

Bezien vanuit het perspectief van terrorisme, gaat de dreiging momenteel grotendeels uit van de (mogelijkheden tot) creatie van virtuele netwerken en het gebruik van het internet voor trainingsdoeleinden. Bereid zijn tot terroristische activiteiten is één ding, maar beschikken over de personen, kennis, vaardigheden en middelen om dat te doen is evenzeer belangrijk. Verhogen virtuele netwerken vooral de slagkracht van de jihadistische beweging, het volop beschikbare trainingsmateriaal kan, zeker voor de categorie die wordt aangeduid als 'home-grown-terroristen', bijdragen om de intentie tot het plegen van terroristische aanslagen in daden om te zetten. Zeker wanneer daarbij wordt betrokken dat het internet ook voor informatie-inwinning volop wordt gebruikt en er veel informatie over potentiële doelen voor terroristen toegankelijk is. Verspreiding van kennis via het internet door jihadisten in de vorm van trainingsmateriaal en via virtuele netwerken draagt bovendien bij aan het snel verspreiden van het geleerde. Praktijkervaringen opgedaan in bijvoorbeeld Irak vinden snel hun weg via het internet en zijn binnen korte tijd mondiaal toegankelijk.

Minder concreet of (voor de NCTb) zichtbaar is de dreiging die uitgaat van de andere vormen van internetgebruik, zoals voor onderlinge communicatie, planning, rekrutering of fondsenwerving. Deze komen minder vaak voor en/of zijn minder zichtbaar, dan wel het medium internet vertroebelt het klassieke beeld ervan, zoals in het geval van rekrutering.

4

CONCLUSIES

Alvorens de conclusies te presenteren, is een opmerking over de houdbaarheid van de conclusies op zijn plaats. De ontwikkelingen op het internet gaan bijzonder snel en jihadisten spelen daar niet alleen op in, maar reageren ook op 'bedreigingen' vanuit overheden.
De dynamiek van het internetgebruik door jihadisten is daardoor groot. De conclusies zijn gebaseerd op het inzicht van nu (eind oktober 2006), waarbij daar waar mogelijk rekening is gehouden met voorzienbare ontwikkelingen. Eventuele ontwikkelingen waardoor de beoordeling van de dreiging er anders uit komt te zien, zullen in het periodiek uit te brengen Dreigingsbeeld Terrorisme Nederland (DTN) worden gerapporteerd, evenals de eventuele nieuwe beoordeling van de dreiging.

1 Cyberaanvallen door jihadisten tegen *(de infrastructuur van)* het internet zijn niet waarschijnlijk

Een cyberaanval op het mondiale of het Nederlandse internet zélf wordt niet waarschijnlijk geacht. Hoewel een cyberaanval laagdrempeliger is dan bijvoorbeeld zelfmoordaanslagen, waardoor potentieel meer jihadisten daartoe zouden kunnen en willen overgaan, gelden als belangrijkste contra-argumenten dat het platleggen van het internet ook de jihadistische infrastructuur op het internet uitschakelt en niet appelleert aan het martelaarschap. Andere gewogen argumenten zijn dat andere aanslagen, zoals een bomaanslag in het openbaar vervoer, een groter effect sorteren en dat de gevolgen van een cyberaanval weliswaar aanzienlijk kunnen zijn, maar garanties daarop (bezien vanuit terroristisch standpunt) zijn er niet. Verder behoort een succesvolle cyberaanval niet echt tot de mogelijkheden, vooral als gevolg van de al getroffen maatregelen hiertegen. Als we al een cyberaanval zouden kunnen verwachten, dan is dat een kleinschalige aanval gedurende een beperkte tijd of een geregisseerde combinatie van kleinschalige cyberaanvallen.

2 Andersoortige aanslagen door jihadisten tegen *(de infrastructuur van)* het internet zijn niet waarschijnlijk

Een andersoortige aanslag tegen het internet - a) een fysieke aanslag, b) een elektromagnetische aanslag en c) indirecte aanslagen zoals via de stroomvoorziening - wordt niet waarschijnlijk geacht. Het mondiale of het Nederlandse internet valt op deze wijze eigenlijk niet uit te schakelen. Er zijn weliswaar mogelijkheden voor kleinschalige aanslagen, maar daartegen zijn wel al maatregelen getroffen om de kans erop te verkleinen en de effecten ervan te beperken. Hoewel een andersoortige aanslag op de infrastructuur van het internet waarschijnlijker lijkt dan een cyberaanval en zijn eigen aantrekkelijkheden kent voor jihadisten, is de vraag gerechtvaardigd of terroristen niet de voorkeur geven aan een bomaanslag op een soft target in plaats van op een belangrijke internetlocatie.

3 Cyberaanvallen via het internet zijn niet waarschijnlijk

Een aanval via het internet, waarbij het internet als wapen fungeert tegen andere doelwitten, is weliswaar voorstelbaar, maar niet waarschijnlijk. Desondanks bestaan er wel enkele mogelijkheden hiervoor als gevolg van kwetsbaarheden in bijvoorbeeld software voor procesbesturing (SCADA) waar diverse sectoren gebruik van maken. Bovendien zijn er enkele aantrekkelijke kanten te onderkennen, maar een dergelijke aanval vereist doorgaans (insiders)kennis. Ook zijn klassieke aanvallen zoals bomaanslagen of zelfmoordaanslagen beter publicitair uit te buiten. Een combinatie van één of meer klassieke aanslagen met de inzet van het internet als wapen lijkt meer waarschijnlijk. Hierdoor wordt het effect van die aanval versterkt.

4 Propaganda via het internet draagt bij aan radicalisering

Propaganda via het internet vindt professioneel plaats, heeft een groot bereik en kent relatief weinig weerwoord. De propaganda blijft niet beperkt tot eenrichtingsverkeer: de jihadisten proberen actief de interactie aan te gaan met geïnteresseerden. Combineren we dat met het feit dat vooral grote groepen jongeren toegang hebben tot het internet en dat intensief gebruiken, dan is duidelijk dat hierdoor een voedingsbodem bestaat voor (verdere) radicalisering. Dat geldt zeker voor moslima's vanwege de aantrekkelijkheid van het internet voor hen (vraagzijde) in combinatie met de actieve rol van radicale moslima's in het aanbod.

5 Informatie-inwinning via het internet draagt potentieel bij aan het plegen van terroristische activiteiten

Net als voor iedereen vormt het internet voor jihadisten een onuitputtelijke bron van informatie die bovendien met behulp van professionele hulpmiddelen zoals datamining kunnen worden gecombineerd. Deze informatie kan bruikbaar zijn bij het plegen van terroristische activiteiten. Hoewel deze informatie ook op andere wijze kan worden verkregen, zijn de mogelijkheden voor het inwinnen van informatie via het internet laagdrempeliger, goedkoper, eenvoudiger, minder arbeidsintensief en grootschaliger. Met name de ontwikkelingen op het terrein van (real-time) satellietbeelden, eventueel gecombineerd met een internetverbinding zoals in het geval van Google Earth, zullen snel voortschrijden. Daarmee is informatie-inwinning via het internet een zeer bruikbaar middel voor jihadisten en draagt dat potentieel bij aan het plegen van terroristische activiteiten.

6 Fondsenwerving via het internet door en voor jihadisten komt nog beperkt voor: verschuiving naar meer heimelijke fondsenwerving is te verwachten

In potentie bestaan vele mogelijkheden voor fondsenwerving door en voor jihadisten en er zijn enkele voorbeelden van bekend, maar het komt in de praktijk nog weinig voor. Deze vorm van fondsenwerving is immers zichtbaar en daardoor kwetsbaar voor overheidsingrijpen. Aangezien het bankieren via het internet steeds eenvoudiger en gebruikelijker wordt, zal ongetwijfeld ook het ge- en misbruik ervan door jihadisten toenemen. Dit, gecombineerd met de toenemende interesse van hackers voor online fraude, zal mogelijk leiden tot een verschuiving van meer openlijke naar meer heimelijke fondsenwerving. Fondsenwerving via het internet zal eveneens kunnen toenemen als gevolg van nieuwe digitale en anonieme betalingsmiddelen.

7 Internetgebruik resulteert in meer interactieve vormen van rekrutering die nog niet goed te duiden zijn evenals in conscriptie en zelfontbranding

Erg aannemelijk is het niet dat iemand vanuit Nederland zich via het internet rechtstreeks en één-op-één laat *rekruteren* door rekruteurs van internationale terroristische groeperingen, zoals Hamas. Dit laat onverlet dat van bijvoorbeeld de kern van al Qa'ida een inspirerende werking kan uitgaan bij de vorming van virtuele netwerken, maar het voert te ver om hier te spreken van rekrutering door al Qa'ida. Op het internet is wel een sterk *interactieve* vorm van *rekrutering* waarneembaar die sterk gekoppeld is aan de interactieve manieren van propaganda bedrijven. Kenmerkend voor het internet is vooral dat potentiële strijders zich zelf willen aanmelden voor deelname aan de gewelddadige jihad *(conscriptie)*. Feitelijk is bij conscriptie geen sprake van rekrutering in formele zin, hoewel er nog wel steeds twee partijen betrokken zijn. In relatie tot het internet wordt ook wel gesproken van *zelfontbranding*, waarvan sprake is als iemand op zijn eigen houtje op jihad wil gaan of gaat en er geen twee partijen zijn te onderscheiden. Van rekrutering in formele zin is bij zelfontbranding geen sprake. Is het in de fysieke wereld al lastig om de overgang van radicalisering naar rekrutering en conscriptie afzonderlijk te bezien, dat geldt zeker voor het internet. Het is wellicht zelfs de vraag of door de opkomst van het internet nog wel sprake is van het klassieke rekruteur/rekruut-concept, en of dit concept niet langzaam wordt vervangen door een permanente en interactieve mix van top-down en bottom-up informatieverschaffing en -inwinning, vermengd met online aanmoediging, sturing of netwerkvorming. Zeker rekrutering via het internet, maar ook conscriptie en zelfontbranding, zijn nog relatief nieuwe verschijnselen die nog niet geheel kunnen worden doorgrond.

8 Gebruik van het internet voor trainingsdoeleinden werkt drempelverlagend voor het plegen van aanslagen

Bereid zijn tot terroristische activiteiten is één ding, maar beschikken over de kennis, vaardigheden en middelen om dat te doen is evenzeer belangrijk. Vooral voor 'homegrown-terroristen' kan het volop beschikbare trainingsmateriaal bijdragen om de intentie tot het plegen van terroristische aanslagen in daden om te zetten. Zeker wanneer daarbij wordt betrokken dat het internet ook voor informatie-inwinning volop wordt gebruikt en er veel informatie over potentiële doelen voor terroristen toegankelijk is. Verspreiding van trainingsmateriaal via het internet door jihadisten draagt bovendien bij aan het snel verspreiden van het geleerde. Het gebruik van het internet voor trainingsdoeleinden werkt al met al drempelverlagend voor het plegen van aanslagen.

9 Jihadisten gebruiken het internet voor onderlinge communicatie en planning

Er zijn voldoende aanwijzingen dat de jihadisten via het internet onderling communiceren en terroristische activiteiten plannen. Ze maken daarbij gebruik van de mogelijkheden van

anonieme en afgeschermde communicatie. Naast voordelen voor jihadisten biedt dit internetgebruik inlichtingen- en opsporingsinstanties de mogelijkheid tot ingrijpen. De jihadisten zijn zich daar goed van bewust.

10 Virtuele netwerken verhogen de slagkracht van de jihadistische beweging

Door de vorming van virtuele netwerken ontstaat een informele pool van bereidwilligen voor de jihad die in wisselende combinaties met elkaar of individueel geweldsactiviteiten kunnen ontplooien. Lokale en internationale elementen kunnen daardoor meer met elkaar verweven raken, hetgeen de slagkracht van de internationale jihadistische beweging aanzienlijk verhoogt.

11 Internetgebruik ondersteunt het gehele proces van radicalisering

Voor iedere fase van radicalisering is er aanbod beschikbaar. Met behulp van het internet kan een potentiële jihadist processen doorlopen van ideologievorming, ideologieversterking en ideologische indoctrinatie. Nader wetenschappelijk onderzoek naar groepsprocessen via het internet en de invloed van het internetgebruik op radicalisering is echter gewenst.

12 Vanuit het perspectief van radicalisering gaat de grootste dreiging uit van propaganda via het internet in combinatie met de relatief grote groep jonge moslims die zoekend is.

De propaganda vindt professioneel plaats, heeft een groot bereik, is interactief en kent relatief weinig weerwoord. Combineren we dat met het in potentie grote bereik bij kwetsbare jongeren, dan is duidelijk dat propaganda via het internet het meest bijdraagt aan (verdere) radicalisering, meer dan de andere vormen van internetgebruik. En juist de bijdrage van propaganda aan radicalisering is zorgelijk, omdat radicalisering niet alleen drempelverlagend werkt voor rekrutering voor de jihad, maar ook in de toekomst zou kunnen leiden tot meer terroristische activiteiten.

13 Vanuit het perspectief van terrorisme gaat de dreiging grotendeels uit van de (mogelijkheden tot) creatie van virtuele netwerken en het gebruik van het internet voor trainingsdoeleinden.

Verhogen virtuele netwerken vooral de slagkracht van de jihadistische beweging, het volop beschikbare trainingsmateriaal kan, zeker voor de categorie die wordt aangeduid als 'home-grown-terroristen', bijdragen om de intentie tot het plegen van terroristische aanslagen in daden om te zetten.

Tot slot nog de bevindingen op basis van de analyse van het jihadisme op het Nederlandse internet:

1. De Nederlandse jihadisten richten zich tot nu toe vooral op het ordenen, aanbieden en verspreiden van jihadistische informatie en materialen. Die informatie dient vooral propagandadoeleinden, maar is deels ook gericht op training.
2. Vele sites bieden de mogelijkheid van interactie tussen jihadisten en een breed en divers publiek van geïnteresseerden evenals tussen jihadisten onderling. Niet alleen kan informatie zo heel gericht en op maat worden uitgewisseld met geïnteresseerden en aan de hand van specifieke vragen of actualiteiten, op die wijze kunnen ook virtuele netwerken ontstaan of kunnen werkelijk in de jihadstrijd geïnteresseerden worden gerekruteerd.
3. Het virtuele jihadisme op het Nederlandse internet kan aanwijzingen geven over de reële jihadisten in Nederland.
4. Nederlandse virtuele jihadisten laten zich inspireren door een internationaal virtueel vertaalprogramma en vertalen vooral materiaal uit het reeds door anderen 'voorgesorteerde' aanbod van materiaal.
5. Moslima's zijn zeer actief als vertalers, in de ontwikkeling van sites en in de interactie met het publiek.
6. Nederlandse virtuele jihadisten opereren structureel of sporadisch op diverse neutrale discussiefora van niet-jihadistische signatuur. Met een beperkter gevaar voor ingrijpen door overheden, bereikt de jihadistische boodschap zo een veel breder publiek en kan zelfs nieuwe aanwas plaatsvinden.

LITERATUUR

AIVD 2002a
AIVD, *Jaarverslag 2002 Algemene Inlichtingen- en Veiligheidsdienst,* 2003.

AIVD 2002b
AIVD, *Rekrutering in Nederland van incident naar trend*, 's-Gravenhage: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2002.

AIVD 2004
AIVD, *Van dawa tot jihad. De diverse dreigingen van de radicale islam tegen de democratische rechtsorde*, 's-Gravenhage: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2004.

AIVD 2006
AIVD, *De gewelddadige jihad in Nederland: Actuele trends in de islamistisch-terroristische dreiging,* 2006.

ANP 2006
ANP, *Mohammed-spotprenten motief voor kofferbommen*, 2 september 2006.

Apuzzo 2006
M. Apuzzo, *'Britisch man indicted on terrorism charges over Internet sites'*, Associated Press Newswires, 20 juli 2006.

As-Suri 2004
As-Suri, *Oproep tot het universeel islamitisch verzet,* 2004.

Bang e.a. 1996
S. Bang e.a., *Het complete internet handboek*, Schoonhoven: Academic Service, 2e geheel herziene uitgave, 1996.

BBC Monitoring 2006a
'Seven to be charged in Denmark over terror-support T-shirts', BBC Monitoring Service, 20 februari 2006.

BBC Monitoring 2006b
'Authorities concerned about Hezbollah, Hamas presence in Germany', BBC Monitoring European, 24 juli 2006.

Bell 2006
S. Bell, *'Two Toronto suspects took part in discussions. Web forum linked cells'*, National Post, 15 juni 2006.

Benschop 2004
A.Benschop, *Kroniek van een aangekondigde politieke moord - Jihad in Nederland*, 2004 (www.sociosite.org/jihad_nl.php)

Benschop 2006a
A. Benschop, *CyberJihad Internationaal: Waarom terroristen van internet houden*, http://www.sociosite.org/ 2006.

Benschop 2006b
A. benschop, *CyberTerrorisme: Dodelijk geweld vanaf het toetsenbord*, http://www.sociosite.org/ 2006.

Buijs e.a 2006
F.J. Buijs, F. Demant, A. Hamdy, *Strijders van eigen bodem*, Amsterdam: University Press, 2006.

Bunt 2003
G.R. Bunt, *Islam in the Digital Age. E-Jihad, Online Fatwas and Cyber Islamic Environments*, London: Pluto Press, 2003.

Castells 1998
M. Castells, *The Rise of the Network Society. Volume 1 of the Information Age*, Blackwell Publishers Inc., 1998.

Colin 1997
B. Colin, *'The Future of Cyberterrorism'*, Crime and Justice International, maart 1997, p. 15-18.

Computable 2006
'Ook AMS-ix heeft last van stroomstoring Amsterdam', Computable.nl, 30 mei 2006.

Conway 2005
M. Conway, *Terrorist 'use' of the internet and fighting back*, Dublin: Department of Political Science College Green Trinity College, 2005.

Cops@Cyberspace 2006a
Cops@Cyberspace, jaargang 9, nr. 31, 2006.

Cops@Cyberspace 2006b
Cops@Cyberspace, Jaargang 9, nr. 29, 2006.

CRS 2005a
C. Wilson, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CRS-report for Congress, 1 april 2005.

CRS 2005b
J. Rollins, C. Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, CRS-report for Congress, 20 oktober 2005.

Dasselaar 2006
A. Dasselaar, *En toen lag alles plat*, Planet.nl, 8 mei 2006.

Denning 1999
D. E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Georgetown University, 1999.

EZ 2005
Ministerie van Economische Zaken, *Vragen van het lid Gerkens (SP) aan de Minister en de Staatssecretaris van Economische Zaken over onderschatte cybercrime*, Antwoorden op Kamervragen d.d. 7 juli 2005, TK 2004-2005, 2023

Foxtrot 2004
'Jihaad planning deel 2', Foxtrot.messageboard.nl, 2004 (foxtrot.messageboard.nl/2767/viewtopic.php?t=108, Jihaad planning deel 2, 020104).

Gibson 2002
S. Gibson, *The distributed reflection DoS-attack*, 2002 (http://grc.com/dos/drdos.htm)

Green 2002
J. Green, *'The Myth of Terrorism'*, Washington Monthly, november 2002.

Guardian 2005
'Algerian guilty of downloading bomb data', The Guardian, 25 november 2005.

Higgins e.a. 2002
A. Higgins, K. Leggett, A. Cullison, *'How al Qaeda put Internet to use'*, The Wall Street Journal, 11 november 2002.

Hoffman 2006
B. Hoffman, *The Use of the Internet by Islamic Extremists*, Testimony presented to the House Permanent Select Committee on Intelligence, mei 2006.

Holst 2006
R. van Holst, *'Mediagebruik van allochtonen in Nederland'*, Mira Media, januari 2006.

Huizer 1998
E. Huizer, *Structuur en organisatie van het internet*, 1998, http://nieuws.surfnet.nl/nieuws/snn-archief/achtergrond/jg97-98/internet.html.

Independent 2006a
'The new breed of cyber-terrorist', The Independent, 1 juni 2006.

Independent 2006b
'Tight security as suspects accused of airline bomb plot appear in court', The Independent, 23 augustus 2006.

Jamestown 2006
'Jihadi forums marvel at new role of snipers', Jamestown Terrorism Focus, 4 april 2006.

Justitie 2005a
Minister van Justitie, *Antwoorden op Kamervragen van het lid De Wit (SP) aan de minister van Justitie over de voorgestelde bewaarplicht van dataverkeergegevens,* 6 september 2005.

Justitie 2005b
Minister van Justitie, *Antwoorden op Kamervragen van de leden Weekers (VVD) en Wolfsen (PvdA) aan de ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties over programma's op internet die mogelijk terroristen helpen,* 6 oktober 2005.

Kortekaas 2005
J. Kortekaas, *Risico-analyse georganiseerde criminaliteit. Uitwerking instrumentarium en toepassing op de ICT-ontwikkelingen*, 's-Gravenhage: Elsevier overheid, 2005.

Kwint 2004
Projectgroep KWINT *Continuïteit, Rapportage Internationale Kwetsbaarheden NL Internet,* 23 november 2004.

Labi 2006
N. Labi, *'Rapportage terroristen op het internet. Jihad 2.0'*, Vrij Nederland, 1 juli 2006.

Lewis 2002
J.A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, CSIS, december 2002.

Lia 2006
B. Lia, *'Al-Qaeda online: understanding jihadist internet infrastructure'*, Jane's Intelligence Review 18, januari 2006, p. 14-19.

Luiijf 2006
H.A.M. Luiijf, R. Lassche, *SCADA (on)veiligheid: een rol voor de overheid?*, TNO, 15 april 2006.

Meertens e.a. 2006
R.W. Meertens, Y.R.A. Prins en B. Doosje, *In iedereen schuilt een terrorist*, Schiedam: Scriptum, 2006.

Military.com 2005
'Army to Crack Down on Military Bloggers', Military.com, 31 augustus 2005. (www.military.com/NewsContent/0,13319,76350,00.html).

Mitnick 2006
K. D. Mitnick, W.L. Simon, *The Art of Intrusion*, Wiley Publishing, 2006.

Muller e.a. 2004
E.R. Muller, R.F.J. Spaaij, A.G.W. Ruitenberg, *Trends in terrorisme*, Alphen aan den Rijn: Kluwer, 2004.

Nationaal 2006
'Jihad krijgt girlpower op; Radicale moslima's tokkelen nieuw', Nationaal (Vlaanderen), 3 juli 2006.

National Post 2006
'Online hate growing rapidly', National Post, 6 april 2006.

NCTb 2006a
NCTb, *Dreigingsbeeld terrorisme Nederland nr.5*, 2006.

NCTb 2006b
Google Earth, 2006.

Newsbytes 2006
Newsbytes News Network, *New Internet Threat Emerges: 'website cloaking'*, 9 maart 2006.

Nieuwsblad 2006
'Ik zoek een bruid voor mijn man', Het Nieuwsblad, 4 juli 2006.

NRC 2005
'Het ronselen voor de jihad gaat volop door', NRC-Handelsblad, 3 januari 2005.

NRC-Next 2006
'Mediamachine wapen van terreur, op basis van een interview van K. Gannon met een cameraman van As-Sahab', NRC-Next, 26 juni 2006.

Nu.nl 2006a
'Marokkanen hacken Israëlische websites', Nu.nl, 29 juni 2006.

Nu.nl 2006b
'Terreuraanval op internet blijkt heel eenvoudig', Nu.nl, 8 mei 2006.

Nu.nl 2006c
'Website Geert Wilders opnieuw gehackt', Nu.nl, 16 juli 2006.

Nu.nl 2006d
'Verdonk getroffen door Google-bom', Nu.nl, 3 maart 2006.

Pels 2003
T. Pels, *'Respect van twee kanten, over socialisatie en lastig gedrag van Marokkaanse jongens'*, Migrantenstudies, themanummer Jeugd, 19 (4) 2003, p. 228-239.

Persson 2005
M. Persson, *'Het begint met een stel jongens; Terrorisme'*, de Volkskrant, 23 juli 2005.

Planet.nl 2005
'Meer dan een miljoen patiëntengegevens op straat', Planet.nl, 2 september 2005.

Planet.nl 2006a
'Reacties: Grotere én andere gevaren', Planet.nl, 12 mei 2006.

Planet.nl 2006b
'Leven na de internetaanslag', Planet.nl, 11 mei 2006.

Planet.nl 2006c
'24 uur internet onder vuur', Planet.nl, 9 mei 2006.

RAND 2000
RAND, *Mapping the risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information*, 2000.

Rechtspraak.nl 2006
'Rechtbank heeft uitspraak gedaan in zaken verdachten Hofstadgroep', Rechtspraak.nl, 2006, (http://www.rechtspraak.nl/Gerechten/Rechtbanken/s-Gravenhage/Actualiteiten/Rechtbank+heeft+uitspraak+gedaan+in+zaken+verdachten+Hofstadgroep.htm).

Rogan 2006
H. ROGAN, *Jihadism online- A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes*, Kjeller: Forsvarets Forskningsinstitutt Norwegian Defence Research Establishment (FFI/Rapport-2006/00915), 2006.

Roy 2005*
O. Roy, *De globalisering van de islam*, Amsterdam: Van Gennep, 2e druk, 2005.

Rozen
L. Rozen, *'Forum point the way to jihad'*, Wired News, 6 augustus 2003, (http://www.wired.com/news/culture/1,59897-0.html)

Scheuer 2006
M. Scheuer, *'The New York Plot: The Impact of Bin Laden's Campaign to Inspire Jihad'*, Terrorism Focus, 3 (28), 18 juli 2006.

SITE-Institute 2005a
SITE-Institute, *Global Islamic Media Front Issues 'Jihad Candid Camera' Video of Insurgency in Iraq*, 6 september 2005.

SITE-Institute 2005b
SITE-Institute, *Al-Qaeda university for jihad subjects*, 10 oktober 2005.

SITE-Institute 2006a
SITE-Institute, *Zawahiri video exemplifies latest jihadi media distribution trends*, 12 maart 2006.

SITE-Institute 2006b
SITE-Institute, *The Global Islamic Media Front Circulates 'The Comprehensive study on how to Hack the Crusaders' and the Zionists' websites, as was authored by Irahbi 007*, 2 mei 2006.

SITE-Institute 2006c
SITE-Institute, *The 'Nemo Document' of Comprehensive Mujahid Training for Jihad - Explosives, Poisons, Physical Preparation, Nuclear Weapons, and Guns*, 26 mei 2006.

* Het Franstalige boek is gepubliceerd in 2002.

SITE-Institute 2006d
SITE-Institute, *Complete Audio Message of Usama bin Laden from 4/23/06,* 26 april 2006.

SITE-Institute 2006e
SITE-Institute, 12 mei 2006.

SITE-Institute 2006g
SITE-Institute, *The Global Islamic Media Front announces the initiation of infiltrating western internet forums, and issues a call to able muslims to join the information jihad,* 12 januari 2006.

SITE-Institute 2006h
SITE-Institute, *Canadian arrests portray the value of the internet in global networks,* 6 juni 2006.

SITE-Institute 2006k
SITE-Institute, *A Forthcoming Video for the First Anniversary of the July 7 London Bombing,* 6 juli 2006.

SITE-Institute 2006l,
SITE-Institute, *Plan to inexpensively kill Thousands of American Citizens,* 6 februari 2006.

SITE-Institute 2006n
SITE-Institute, *Final Warning from the Taliban to the Afghanis in the Armed Forces and Police in Afghanistan to Remove Themselves from the Battlefield,* 25 juli 2006.

SITE-Institute 2006o
SITE-Institute, *A Forthcoming Message from Ayman al-Zawahiri,* 26 juli 2006.

SITE-Institute 2006p
SITE-Institute, *The Global Islamic Media Front Presents a Film of the Condition of the American Soldier: 'They are Hurting',* 4 augustus 2006.

SITE-Institute 2006q
SITE-Institute, *Jihadist Forum Member Advocates Users Beware of Google and its Software Applications,* 28 maart 2006.

SITE-Institute 2006r
SITE-Institute, *A Guide for Internet Safety and Anonymity Posted to Jihadist Forum*, 24 maart 2006.

SITE-Institute 2006t
SITE-Institute, *A Flyer Providing Information How One May Send Donations to Palestinians Posted to Jihadist Forums,* 25 april 2006.

SITE-Institute 2006u
SITE-Institute, *Jihadist Forum Member Provides a Video of an Advanced Protection System to Military Vehicles and How to Circumvent its Effectiveness*, 3 mei 2006.

SITE-Institute 2006v
SITE-Institute, *A manual instructing in the use of clostridium microbe and clostridium botulinum toxin as biological weapons*, 27 januari 2006.

Stratix 2004
H. Rood, *Gevolgen uitval .nl domein*, Stratix Onderzoek, Schiphol, 2004.

Telegraaf 2006
'Algerijn Abbas Boutrab mogelijk al in Nederland bezig met 'Operatie Bojinka 2006', De Telegraaf, 19 augustus 2006.

Thiele & Van Vliet 2005
V. Thiele, E. Van Vliet, *Kwetsbaarheid van internet voor bewust menselijk handelen*, Den Haag, 2005.

Thomas 2003
T.L. Thomas, *Al Qaeda and the Internet: the danger of 'cyberplanning'*, Parameters, 2003, p. 112-123.

Van Leeuwen 2005
Van Leeuwen, *'Ronselen in Europa voor de Heilige Oorlog'*, in: Justitiële Verkenningen, 31, 2/2005.

Van Yperen 2005
S. van Yperen, *Al-Qa'ida-video's in het NOS-journaal*, Master's Thesis, Erasmus-universiteit Rotterdam, Faculteit Historische en Kunstwetenschappen, 1 september 2005.

Volkskrant 2005
'Vijver voor extremisten', De Volkskrant, 26 november 2005.

Volkskrant 2006
'Praten met Al Qa'ida en Hamas, er zit niks anders op; Het debat in: de Verenigde Staten', De Volkskrant, 13 mei 2006.

Washington Times 2006
'Nobles & Knaves', The Washington Times, 10 juni 2006.

Washington Post 2005
'*Al Qaeda and the Internet (Evan Kohlmann, interview transcript)*', The Washington Post, 8 augustus 2005.

Washington Post 2006
'*Even terrorists worry about Internet security*', The Washington Post, 13 april 2006.

Weimann 2006
G. Weimann, *Terror on the Internet. The New Arena, the New Challenges*, Washington D.C.: United States Institute of Peace Press, 2006.

Wilson 2006
C. Wilson, *Terrorist Capabilities for Cyberattack*, CIIP Handbook, 2006.

Zerkin 2006
A. J. Zerkin, *Thinking the unthinkable: Negotiating with terrorists*, Lezing Universiteit van Amsterdam, mei 2006.

BEGRIPPENLIJST

Amsterdam Internet eXchange (AMS-IX): hierop zijn de netwerken van bijna alle internetproviders in Nederland aangesloten. Er wordt nationaal en internationaal verkeer uitgewisseld. De AMS-IX is het grootste internetknooppunt in Nederland.

Commercial-off-the-shelf: Commercial-off-the-shelf (COTS) software is software die ontwikkeld is voor een hele markt in plaats van voor individuele klanten. Een voorbeeld hiervan is Microsoft Office.

Computer Emergency Response Team (CERT): Een CERT is een team dat assisteert bij het oplossen van beveiligingsinbreuken. Sommige grotere CERT's (als GOVCERT.NL) hebben ook een belangrijke voorlichtingsfunctie en brengen zogenaamde advisories uit met waarschuwingen over recentelijk ontdekte softwaregaten en methoden waarop de problemen opgelost kunnen worden.

Dawa: letterlijk 'oproep' tot de islam, thans in de discours over radicale islam betekent het het uitdragen van de radicaal islamitische ideologie.

Defacement: defacement (of: defacing) betreft het zonder toestemming veranderen, vervangen of vernielen van een website dan wel het door middel van een DNS-hack of spoofing doorgeleiden van internetverkeer naar een andere website.

Denial of Service (DoS): Het beperken of frustreren van de werking van een systeem, applicatie of netwerk.

Distributed Denial of Service (DDoS): Het beperken of frustreren van de werking van één of meer netwerken, systemen, of toepassingen daarop, door misbruik te maken van een groot aantal computers.
Een 'controller' zet de computers ertoe aan om massaal en gelijktijdig een netwerk, systeem of toepassing aan te vallen.

Domain Name Server (DNS): het internet kan zijn taken niet vervullen zonder ondersteunende diensten. Zo is er een koppeling tussen het op internet gebruikelijke IP-adres (een nummer) en de voor de gebruiker bekende naamgeving door een hiërarchisch georganiseerde dienst. Dit is de Domain Name Server (DNS). Deze dienst werkt als een telefoonboek. Diensten als het www, bestandsoverdracht en e-mail zijn sterk afhankelijk van het goed functioneren van deze voorziening.

Encryptie: Encryptie is het proces, waarmee gegevens met behulp van een wiskundig algoritme en een uit een reeks getallen bestaande sleutel worden versleuteld, zodat deze voor onbevoegden onleesbaar worden. Op die manier kunnen partijen op vertrouwelijke wijze met elkaar communiceren.

Firewall: afscherming tussen het internet en een intern (bedrijfs)netwerk. Dit ter voorkoming van computerinbraak en de verspreiding van virussen.

Gewelddadig politiek activisme: onderscheidend punt ten opzichte van terrorisme is de afwezigheid van een doelbewust streven naar menselijke slachtoffers of het nadrukkelijk incalculeren dat bij acties mensenlevens te betreuren zijn.

Internet als doelwit: Bij het internet als doelwit richt het geweld danwel het toebrengen van ernstige maatschappijontwrichtende zaakschade zich tegen (de infrastructuur van) het internet zelf. Dit kan verschillende vormen aannemen:

- een cyberaanval: door gebruikmaking van computers via het internet;
- een fysieke aanslag: door gebruikmaking van conventionele wapens tegen computerhardware of communicatielijnen;
- een elektromagnetische aanslag: door het gebruik van bijvoorbeeld elektromagnetische energie (EMP);
- overige indirecte aanvallen bijvoorbeeld tegen de elektriciteitsvoorziening waardoor (de infrastructuur van) het internet niet kan functioneren.

Internet als wapen: Bij het gebruik van het internet als wapen worden aanslagen tegen fysieke doelen gepleegd met gebruik van het internet. Te denken valt aan de overname van luchtverkeerssystemen of besturingssystemen van vitale installaties in de chemische sector. Een ander voorbeeld is om de alarmcentrales of crisisorganisaties uit te schakelen door bijvoorbeeld hacking of door overbelasting te veroorzaken.

Internet Service Provider (ISP): een organisatie die haar klanten toegang tot het internet aanbiedt. Om dit te doen onderhoudt de ISP een of meer POP's, toegangspunten tot het internet voor abonnees van de ISP. Naast het verlenen van toegang bieden veel ISP's tegenwoordig ook andere diensten aan. Voorbeelden hiervan zijn nieuwsdiensten, transactieoplossingen en entertainmentdiensten.

IP: IP betekent Internet Protocol. IP lijkt op het systeem van de post. Een pakketje gegevens kan worden geadresseerd (middels een 'IP-adres' of 'IP nummer'), verstuurd over het internet en tenslotte 'afgegeven' op het juiste computersysteem. IP-adressen worden uitgedeeld door daartoe bevoegde instanties, bijvoorbeeld providers. Elke domeinnaam heeft een corresponderend IP nummer. Het IP-adres van bijvoorbeeld surfopsafe.nl is 213.156.7.44. Een IP-adres kunt u invoeren in het 'adres' veld van uw browser. U komt dan ook op de internetpagina's van het domein terecht.

Jihad (in dit kader in de betekenis van gewapende strijd): het ontplooien van geweldsactiviteiten tegen gepercipieerde vijanden van de islam ter verwezenlijking van een wereld die een zo zuiver mogelijke afspiegeling is van hetgeen men meent dat in de eerste bronnen van het islamitische geloof staat vermeld.

Jihadisten: samentrekking van jihadistische terroristen en jihadistische radicalen.

Malware: samentrekking van malicious (Engels voor kwaadaardig) en software. Verzamelnaam voor slechte software zoals virussen, trojans, spyware, adware, browserhijackers en dialers.

Phishing: een verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen. Door middel van een nepsite of e-mail probeert de oplichter (visser) persoonlijke gegevens als creditcardnummers, pincode, sofinummer et cetera te achterhalen.

Radicale islam (of islamisme): het politiek-religieus streven om, desnoods met uiterste middelen, een samenleving tot stand te brengen die een zo zuiver mogelijke afspiegeling is van hetgeen men meent dat gesteld wordt in de oorspronkelijke bronnen van de islam.

Radicalisering (AIVD): de (groeiende) bereidheid tot het nastreven en/of ondersteunen van diep ingrijpende veranderingen in de samenleving, die een gevaar kunnen opleveren voor (het voortbestaan van) de democratische rechtsorde (doel), eventueel met het hanteren van ondemocratische methodes (middel), die afbreuk kunnen doen aan het functioneren van de democratische rechtsorde (effect).

Radicalisering (Justitie): een geesteshouding waarmee de bereidheid wordt aangeduid om de uiterste consequentie uit een denkwijze te aanvaarden en die in daden om te zetten. Die daden kunnen maken dat op zichzelf hanteerbare tegenstellingen escaleren tot een niveau waarop de ze de samenleving ontwrichten, doordat er geweld aan te pas komt, het tot gedrag leidt dat mensen diep kwetst of in hun vrijheid raakt of doordat groepen zich afkeren van de samenleving. (Deze definitie is breder en omvat in tegenstelling tot de AIVD-definitie ook de effecten van radicalisering op integratie en niet uitsluitend het aspect van de bedreiging van de democratie.)

Rekrutering: het in beeld brengen en vervolgens controleren en manipuleren van personen om een geïnternaliseerde radicaal politiek-islamitische overtuiging bij deze personen te bewerkstelligen, met als uiteindelijk doel om deze personen op enigerlei wijze te doen participeren in de gewelddadige jihad.

Root server: is een server op het hoogste niveau van het hiërarchische Domain Name System (zie DNS) en vormt dus een essentiële functie in het'adresboek' van het internet.

Router: stuurt pakketjes informatie over een netwerk naar het juiste adres.

Salfisme/salafisten: Wanneer in deze studie wordt gesproken over het salafisme, dan wordt hiermee de niet-jihadistische georiënteerde vorm van het salafisme bedoeld en met 'salafisten' de aanhangers van deze variant. Dit in tegenstelling tot de jihadistische vorm die we rekenen onder het begrip 'jihadisten'.

SCADA: omvat het geheel aan automatisering, elektrotechniek en informatie- en communicatietechnologie dat ingezet wordt voor het monitoren (supervisory), besturen en bewaken (control) van processen, en het verzamelen van gegevens (data acquisition)

Single Point of Failure: is een enkelvoudig onderdeel van een systeem dat bij uitval de werking van het gehele systeem aantast.

Spoofing: techniek om de herkomst van berichten te versluieren of veranderen. Met behulp van spoofing kan de identiteit van een entiteit (b.v. persoon of systeem) aangenomen worden waardoor misbruik van een (bestaande) vertrouwensrelatie mogelijk wordt.

URL (Uniform Resource Locator): eenduidige plaatsaanduiding van een bestand, webpagina, programma, dienst of iets willekeurig anders op het internet, waarin naast de lokatie ook het protocol vermeld is waarmee het bestand, de webpagina, het programma, de dienst of dat 'willekeurige anders' aangesproken kan worden. Vaak wordt de benaming URL gebruikt om het webadres aan te geven, bijvoorbeeld http://www.surfopsafe.nl/.

Terreur: schrikbewind van een staat tegen haar eigen onderdanen, veelal met als doel de macht van de heersende politieke, religieuze of etnische elite te handhaven.

Terrorisme: het plegen van of dreigen met op mensenlevens gericht geweld, dan wel het toebrengen van ernstige maatschappijontwrichtende zaakschade, met als doel maatschappelijke veranderingen te bewerkstellingen of politieke besluitvorming te beïnvloeden.

Weblog: pagina's waarop de eigenaar (de weblogger) zijn vondsten tijdens surftochten over het web rapporteert. Dit gebeurt meestal in de vorm van korte berichtjes, die al dan niet gepaard gaan met een korte opmerking of omschrijving van de hand van de weblogger. Zo wordt een lijst van interessante links gevormd, die het de nieuwsgierige surfer makkelijker maken om specifieke sites te vinden. Een weblog bevat over het algemeen geen links naar hoofdpagina's of domeinen, maar er wordt rechtstreeks gelinkt naar pagina's binnen een site.

World Wide Web (WWW): Het world wide web is evenals het 'surfen' daarop inmiddels een ingeburgerd begrip. Protocol-technisch is de belangrijkste dienst die hieraan ten grondslag ligt het hypertext transfer protocol (http), dat zorg draagt voor het transport en het raadplegen van de webpagina's. In de loop der jaren is de functionaliteit van het web uitgebreid met dynamische inhoud en uitgebreidere grafische opmaak (Java, ActiveX, flash et cetera), dataobject-georiënteerde presentatie en uitwisseling (XML).

BIJLAGEN

BIJLAGE 1 Indelingen terroristisch/ jihadistisch internetgebruik *

Conway	Weimann	Benschop
1. Information provision	1. Communicatief gebruik	1. Publiciteit en propaganda
2. Financing	2. Instrumenteel gebruik • datamining • networking • recruitment and mobilisation • instructions and online manuals • planning and coordination • fundraising and attacking other terrorists	2. Interne communicatie
3. Networking		3. Socialisatie en disciplinering
4. Recruitment		4. Psychologische oorlogsvoering
5. Information gathering	3. Het gebruik van internet als wapen	5. Verwerving van inlichtingen
		6. Fondsenwerving
		7. Rekrutering
		8. Trainingskamp
		9. Mobilisatie en actie-coördinatie
		10. Massadisruptie (cyberterrorisme)
		11. Virtuele islamitische staat

* Conway 2005, Weimann 2006, Benschop 2006a.

BIJLAGE 2 Criteria om te bepalen of een site jihadistisch is

Een site is jihadistisch wanneer deze door middel van artikelen, audiovisuele documenten en andere internetfunctionaliteiten (zoals een mailinglist, chat of Paltalkroom) de jihadistische leer verkondigt en verspreidt. Jihadisme, en daarmee een jihadistische site, is te herkennen aan de volgende thema's:

- Het godsbegrip dat zich kenmerkt door de verabsolutering van de enigheid van God (Tawhied).
- De geloofsleer van het salafisme die uitgaat van het geloof (Iemaan)in de leer van enigheid van God (Tawhied) en het concreet belijden daarvan in de praktijk. Dit leerstuk vormt de grondslag van de overige leerstukken.
- De erediensten (Ibadaat): dit zijn de gangbare pijlers van de islam (geloofsbelijdenis, gebed, vasten, afdracht van de godsdienstige belasting en de pelgrimstocht). De salafisten leggen bepaalde accenten in het verrichten van deze rituele plichten.
- De toepassing van de goddelijke wet- en regelgeving (al-Hukm bima Anzala Allah, Shari'a). Het gaat hierbij om thema's als het alleenrecht van God om wetten te maken en de ongeldigheid van de 'door de mens gemaakte wetten'. Dit leerstuk vormt de grondslag voor de salafistische theorie over de oprichting van een islamitische staat en de inrichting van een islamitische samenleving.
- De ethiek van loyaliteit en afkeer. Deze houdt in dat een moslim verplicht is om uitsluitend loyaliteit te betuigen aan geloofsgenoten en afkeer te tonen aan ongelovigen.
- De leer van de 'uitverkoren groep' (at-Ta'ifat al-Mansoera): als zuiver in de leer menen zij deze groep te vormen.
- De leer van de jihadstrijd omwille van God (al-Jihad fi Sabili Allah) oftewel de gewapende strijd als zijnde een verplichting voor individuele moslims om de ongelovigen en de afvalligen te bestrijden en de islamitische staat (het kalifaat) op te richten.

De jihadistische internetsites in Nederland onderscheiden zich van de salafistische door het expliciet politiseren van deze theologische, dogmatische, liturgische en ethische grondslagen en het oproepen tot de (gewapende) jihadstrijd.

Colofon

Uitgave
December 2006,
Nationaal Coördinator Terrorismebestrijding

Ontwerp & omslagfoto
Richard Sluijs, Den Haag

Druk
DeltaHage, Den Haag

De NCTb werkt aan een veiliger samenleving

De Nationaal Coördinator Terrorisme-bestrijding heeft als taak het risico van terroristische aanslagen in Nederland zoveel mogelijk te verkleinen, alsmede het op voorhand beperken van schade als gevolg van een mogelijke aanslag. De NCTb heeft de centrale regie rond terrorismebestrijding en zorgt dat de samenwerking tussen alle betrokken partijen op een structureel hoog peil komt en blijft.