



Nationaal Coördinator
Terrorismebestrijding

Jihadisten en het internet

Update 2009



Jihadisten en het internet

Update 2009

In Nederland hebben GOVCERT.NL, NCTb en KLPD/THTC namens de overheid een belangrijke rol in de strijd tegen cybercrime (inclusief terrorisme via het internet). Tussen deze organisaties vindt regelmatig overleg plaats inzake incidenten en ontwikkelingen rond dit thema, en zij trachten in hun rapportages een zo compleet mogelijk beeld te geven van de belangrijkste trends.

Woord vooraf

De grootste terroristische dreiging gaat in het laatste decennium uit van het zogeheten 'jihadistisch terrorisme'. Zeker sinds 11 september 2001 is sprake van vele bloedige terroristische aanslagen die worden uitgevoerd onder het mom van een religieuze gewapende strijd, de 'jihad'. Al begin 2007 stelde de NCTb vast dat jihadisten het internet in ruime mate gebruiken als middel voor bijvoorbeeld propaganda of om mensen te rekruteren. Ook verkende de NCTb de dreiging die uitgaat van terroristische aanslagen tegen het internet (internet als doelwit) of via het internet (internet als wapen).

Zowel het internet als het jihadisme is en blijft in ontwikkeling. Daarom ontstond de behoefte om de toenmalige beoordeling van de dreiging opnieuw te bezien in de vorm van deze 'update 2009'. De overheid en private partijen kunnen het zich immers niet permitteren achterover te leunen en de ontwikkelingen op zijn beloop te laten. Sinds het uitbrengen van de eerdere studie begin 2007 zijn daarom tal van maatregelen getroffen om de dreiging van het gebruik van het internet door jihadisten tegen te gaan. Hoewel uit deze studie blijkt dat de dreiging niet substantieel is gewijzigd, bieden de bevindingen in deze studie goede handvatten om blijvend op de dreiging te blijven inspelen.

Nationaal Coördinator Terrorismebestrijding
drs. E.S.M. Akerboom

INHOUD

Managementsamenvatting/conclusies	6		
1 Inleiding	14	3 Internet als middel	42
1.1 Aanleiding	15	3.1 Inleiding	43
1.2 Doel, onderzoeksvragen en afbakening	15	3.2 Gebruik van het internet als middel	43
1.3 Verantwoording werkwijze	16	3.2.1 Jihadistische beweging op het internet	43
1.4 Toelichting structuur	17	3.2.2 Gebruik van toepassingen	46
2 Internet als doelwit en als wapen	18	3.2.3 Verdwijning prominente internationale jihadistische sites 2008	48
2.1 Inleiding	19	3.2.4 Toenemende gerichtheid op een westers publiek	49
2.2 Achtergronden	19	3.2.5 Relatie virtuele en fysieke instituties, personen en activiteiten	50
2.2.1 Nieuwe vormen van/gegevens over internetgebruik	19	3.2.6 Beoordeling dreiging internet als middel: algemeen	51
2.2.2 Massale overbelastingsaanvallen en gerichte hacking: varianten	20	3.3 Gebruik van het internet als middel: specifiek	52
2.2.3 Ontwikkelingen rond cyberaanvallen bij jihadisten	21	3.3.1 Terugblik fenomeenstudie	52
2.2.4 Conclusie achtergronden	27	3.3.2 Propaganda: aanvullende of nieuwe inzichten	53
2.3 Het internet als doelwit	28	3.3.3 Invloed internet op radicalisering: aanvullende of nieuwe inzichten	57
2.3.1 Toelichting	28	3.3.4 Creatie van virtuele netwerken: aanvullende of nieuwe inzichten	60
2.3.2 Mogelijkheden cyberaanvallen, kwetsbaarheden en weerbaarheid	28	3.3.5 Rekrutering: aanvullende of nieuwe inzichten	61
2.3.3 Intentie van jihadisten bij cyberaanval	29	3.3.6 Informatie-inwinning: aanvullende of nieuwe inzichten	62
2.3.4 Capaciteiten cyberaanval bij jihadisten	30	3.3.7 Fondsenwerving	64
2.3.5 Gevolgen cyberaanval	30	3.3.8 Training: Aanvullende of nieuwe inzichten	65
2.3.6 Beoordeling dreiging cyberaanvallen door jihadisten	31	3.3.9 Onderlinge communicatie en planning: aanvullende of nieuwe inzichten	67
2.3.7 Andersoortige aanslagen en aanvallen tegen het internet	32	3.4 Slotbeschouwing	67
2.3.8 Beoordeling dreiging andersoortige aanslagen	35	4 Jihadisme op het Nederlandse internet	70
2.4 Het internet als wapen	36	4.1 Inleiding	71
2.4.1 Toelichting	36	4.2 Nederlandse jihadistische sites sinds 2006	72
2.4.2 Mogelijkheden internet als wapen, kwetsbaarheden en weerbaarheid	36	4.2.1 Groei jihadistische 'materiaalsites' sinds 2006 gestagneerd	72
2.4.3 Intentie jihadisten ten aanzien van internet als wapen	37	4.2.2 Weinig activiteiten op weblogsites	72
2.4.4 Capaciteiten jihadisten ten aanzien van internet als wapen	38	4.2.3 Thabaat.net (2007-2009): professionalisering, isolering en internationalisering van het jihadisme	72
2.4.5 Gevolgen	39	4.2.4 Nieuwe jihadistische website: centralisering van jihadistische informatie	73
2.5 Conclusie internet als wapen	40	4.3 Jihadisme op salafistische sites	73
2.6 Slotbeschouwing	41	4.4 Jihadisme op islamitische mainstreamsites sinds 2006	73
		4.4.1 Afname jihadistische uitingen op islamitische mainstreamsites	73
		4.4.2 Jihadisme op neutrale websites sinds 2006	74
		4.5 Conclusies en dreigingsimplicaties	75
		Bijlage	78
		Literatuur	82
		Begrippenlijst	90
		Colofon	96

Managementsamenvatting/ conclusies

Aanleiding en doel

Begin 2007 constateerde de NCTb in de fenomeenstudie 'Jihadisten en het internet' (hierna: fenomeenstudie) dat jihadisten op vele wijzen het internet gebruikten als middel voor bijvoorbeeld propaganda en rekrutering. In dezelfde studie concludeerde de NCTb dat het gebruik van het internet als doelwit of als wapen door jihadisten niet waarschijnlijk is. Zowel het internet als het jihadisme is en blijft in ontwikkeling. Daarom ontstond de behoefte om de toenmalige beoordeling van de dreiging opnieuw te bezien in de vorm van deze 'update 2009'. Het accent ligt op veranderingen sinds eind 2006 tot eind 2009.

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 verbindinglijnen 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 via een cyberaanval of op anderzortige wijze. 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. Voor de beoordeling van het gebruik door jihadisten van het internet als doelwit of wapen heeft de NCTb een literatuurstudie verricht en een expertmeeting georganiseerd. Hieraan hebben experts van inlichtingendiensten, wetenschap, politie, overige overheidsdiensten en de telecom- en internetsector deelgenomen. Het beeld is dat jihadisten niet in staat zijn om zonder hulp van buitenaf een succesvolle complexe aanval tegen of via het internet uit te voeren die een maatschappijontwrichtend effect heeft. Ook over intenties in die richting bestaan weinig aanwijzingen, noch dat hulp van buitenaf geboden wordt. Er zijn ook geen serieuze incidenten herleidbaar naar jihadisten. Dit beeld is vergelijkbaar met dat van eind 2006.

Bij dit beeld en de hierna volgende conclusies zijn drie kanttekeningen te plaatsen. De eerste heeft betrekking op de houdbaarheidsdatum. Ontwikkelingen gaan snel en niet alle jihadistische activiteiten, capaciteiten en intenties zullen worden onderkend. Niet bekend is of het ontbreken van aanvallen tegen of via het internet ligt aan een gebrek aan intentie bij jihadisten, gebrek aan capaciteiten bij jihadisten, een hoge weerbaarheid of de combinatie daarvan. Feit is dat er wel kwetsbaarheden bestaan, dat we ons intussen van veel kwetsbaarheden bewust zijn, maar ook dat deze kwetsbaarheden steeds breder bekend raken. Bovendien geven testen en incidenten aan dat die kwetsbaarheden uit te buiten zijn. Hoe dat in de toekomst uitpakt, laat zich moeilijk beoordelen. De tweede kanttekening betreft de focus op jihadisten. Vanuit NCTb-perspectief vormt de jihadistisch-terroristische dreiging momenteel de belangrijkste dreiging. Veel literatuur over het onderwerp maakt echter geen onderscheid naar wie een eventuele aanval onderneemt: staten, criminelen, vandalen of anderszortige individuen of terroristen. De geschetste kwetsbaarheden kunnen immers ook door anderen dan jihadisten worden benut. Omgekeerd geldt dit eveneens ten aanzien van de weerstand: de geschetste weerstand tegen aanvallen door jihadisten tegen of via het internet geldt ook voor alle andere potentiële bedreigers. Ten slotte is van belang te onderkennen dat de beoordeling dat een complexe aanval van terroristische aard tegen of via het internet en dus met echt maatschappijontwrichtende gevolgen niet te verwachten is, geen reden is voor minder waakzaamheid: ook een meer eenvoudige aanval, al dan niet van terroristische aard, kan bijvoorbeeld in vitale sectoren onverwachte effecten hebben. Een dergelijke verstoring is dan wellicht kleinschaliger of korter durend, de moedwilligheid ervan zal voor grotere onrust en media-aandacht zorgen dan wanneer sprake is van een technische storing of menselijke fout als oorzaak.

A1 Succesvolle cyberaanvallen door jihadisten tegen het internet zijn op beperkte schaal mogelijk, maar zeker op grote schaal niet waarschijnlijk

Via een cyberaanval is het op grotere schaal verstoren of uitschalen van het internet eigenlijk niet mogelijk: het internet is intussen te groot, te divers en de hele internet-industrie kent teveel weerstand. Toch zijn er wél kwetsbaarheden, waaronder in de standaard internetprotocollen. Deze zijn gelukkig niet eenvoudig uit te buiten en aanvallen zullen nooit alle delen van het internet in dezelfde mate treffen.

Er zijn geen aanwijzingen dat jihadisten beschikken over voldoende kennis om succesvol misbruik te maken van de kwetsbaarheden van het internet voor cyberaanvallen. Ook zijn er geen aanwijzingen dat intenties in die richting bestaan. Misbruik door jihadisten is ook niet zichtbaar geworden. Bovendien blijft het de vraag of de effecten van een aanval opwegen tegen de daarvoor benodigde inspanningen, gelet op de hierboven beschreven weerstand. Een succesvolle grootschalige cyberaanval tegen het internet door jihadisten wordt dan ook, net als eind 2006, niet waarschijnlijk geacht.

Andere bedreigers (criminelen en staten) hebben meer capaciteiten voor succesvolle cyberaanvallen en sommigen daarvan wellicht ook de intentie. Een onderzoek naar capaciteiten en intenties van hen vielen echter buiten de afbakening van de studie en zijn dus niet onderzocht. Wel geldt ook voor die bedreigers dat de weerstand van het internet groot is tegen cyberaanvallen, zeker tegen aanvallen op grote schaal.

A2 Succesvolle andersoortige aanslagen door jihadisten tegen het internet zijn op beperkte schaal mogelijk, maar zeker op grote schaal niet waarschijnlijk

Het succesvol uitschakelen van het internet via andersoortige aanslagen is niet mogelijk, tenzij terroristen de beschikking krijgen over nucleaire wapens die op grote hoogte tot ontploffing worden gebracht en een elektromagnetische puls veroorzaken. Indien zij over dergelijke wapens zouden beschikken, zal het internet echter niet het belangrijkste doelwit zijn.

Er zijn enige kwetsbare punten in het internet voor gerichte aanslagen zoals kabels en knooppunten als internet-exchanges. Echter, binnen het internet is grote redundantie, er zijn vele maatregelen getroffen om de kwetsbaarheden te beperken en het bewustzijn omtrent kwetsbaarheden is toegenomen. Wanneer het internet via bomaanslagen of door uitschakeling van elektriciteit of moedwillige overstrooming zou worden getroffen, dan zijn de gevolgen relatief kleinschalig, blijven deze lokaal of regionaal en zijn ze goed op te vangen. De hersteltijd van de aanslag is wel (aanzienlijk) langer dan in het geval van een cyberaanval.

In hoeverre zijn voorbeelden bekend waarbij jihadisten zich tegen het internet richten? Er is één plan voor een mogelijke bomaanslag op de belangrijkste Britse telecom-/internetlocatie bekend. Toch is het de vraag of dat plan zich echt heel specifiek richtte op het internet zelf. Infiltratie in de sector door jihadisten zou denkbaar zijn. De sector was en is zich echter van dit risico bewust en kent een vrij gesloten karakter. Daar staat wel tegenover dat de internet- en telecomsector snel groeit en dat het gesloten karakter mogelijk onder druk komt te staan. Hoewel terroristen gewend zijn te werken met explosieven, ligt het toch niet voor de hand dat jihadisten kiezen voor een aanval met explosieven tegen het internet: andere doelwitten zijn aantrekkelijker en de 'kosten' wegen waarschijnlijk niet op tegen de 'baten'.

Al met al moet worden geconcludeerd dat een succesvolle andersoortige aanval gericht tegen het internet, zeker één op grote schaal, niet waarschijnlijk is. Net als ten tijde van de fenomeenstudie lijkt een dergelijke aanslag het meest voorstelbaar in combinatie met (een) andere aanslag(en), met als doel de chaos na die

aanslag(en) te vergroten. De aanslagen in Mumbai eind november 2008 hebben aangetoond dat een mix van doelwitten (nog steeds) tot het speelveld van jihadisten behoort.

A3 Succesvolle cyberaanvallen van jihadisten via het internet zijn op beperkte schaal wel mogelijk, maar zeker op grote schaal niet waarschijnlijk

Geautomatiseerde systemen voor procescontrole in de vitale sectoren (vaak SCADA-systemen genoemd) zijn kwetsbaar voor verstoring of overname van buitenaf. Ook andere kritische, bijvoorbeeld financiële, online dienstverlening kan hiermee te maken krijgen. Er zijn op dit punt ontwikkelingen die wijzen op een toename van risicofactoren, zoals toenemende beschikbaarheid en kwaliteit van aanvalsmiddelen, online discussie over kwetsbaarheden, toename van outsourcing van serverbeheer en databewerking en toename van het gebruik van het internet, ook door de (vitale) bedrijfssectoren. Bovendien worden (jonge) hackers steeds slimmer. Ook tonen in de praktijk tests en incidenten aan dat vitale sectoren voorlopig nog kwetsbaar zijn voor, met name, insiders en toegewijde teams van hackers die over ten minste gevorderde capaciteiten beschikken. Maar er zijn tevens ontwikkelingen die wijzen op een risicodaling: zo is er meer aandacht voor cybersecurity, werken overheid en bedrijfsleven in verschillende landen (waaronder Nederland) samen aan *awareness* en daarmee aan weerstand, is er ook internationale samenwerking op dit terrein en zal de markt mogelijk hierop inspelen, waardoor de technische verdediging versterkt kan worden.

Ten aanzien van de dreiging geldt, dat, voor zover bij de NCTb bekend, jihadisten en hun supporters tot nu toe niet verder zijn gekomen dan (het aanzetten tot) eenvoudige cyberaanvallen zoals bekladding van websites (defacements). Intenties voor meer gevorderde of complexe cyberaanvallen zijn grotendeels afwezig en hun capaciteiten lijken beperkt. Mocht toch sprake zijn van dergelijke intenties, dan kan ter compensatie voor beperkte capaciteiten samenwerking worden gezocht met specialistische individuen, staten, of (criminele) groeperingen. Hiervoor bestaan geen aanwijzingen.

Indien jihadisten over capaciteiten gaan beschikken die het niveau van eenvoudige cyberaanvallen overstijgen, kunnen zij in ieder geval voor maatschappelijke onrust zorgen, ook al hebben dergelijke aanvallen niet zodanige rechtstreekse gevolgen dat zij het label terrorisme rechtvaardigen. Maatschappelijke ontwrichting is echter onwaarschijnlijk. Gezien hun intenties en capaciteiten in combinatie met de geschiedenis van jihadistische aanslagen, is de verwachting dat jihadisten toch meer heil blijven zien in het plegen van klassieke bomaanslagen en zelfmoordaanslagen. Daarmee hebben ze meer ervaring en dergelijke aanslagen hebben een directer en voorspelbaarder effect dan het digitaal verstoren van een vitale sector.

De conclusie luidt dan ook dat een succesvolle jihadistisch-terroristische aanslag via het internet gericht tegen de vitale infrastructuur of cruciale online-dienstverlening op de kortere termijn niet waarschijnlijk is, zeker niet een cyberaanval op grote schaal. Kwetsbaarheden en mogelijkheden zijn echter wel eerder toe- dan afgenomen, maar er zijn onvoldoende aanwijzingen dat jihadisten die willen of succesvol kunnen misbruiken. Eenvoudige verstoringen behoren echter wel degelijk tot de mogelijkheid, en kunnen voor maatschappelijke onrust zorgen.

De kans dat uit andere hoek dan die van jihadisten, zoals statelijke actoren of criminelen, een aanslag of cybergijzeling plaatsvindt, is groter. Een onderzoek naar intenties en capaciteiten van hen viel buiten de afbakening en deze zijn daarom niet expliciet onderzocht.

B Internet als middel

Jihadisten gebruikten en gebruiken het internet - net als gewone burgers - voor verschillende doeleinden en zij beschouwen het internet als een cruciaal middel voor de jihad. Drie mediaorganisaties, As-Sahab, GIMF en Al-Fajr, spelen nog meer dan eind 2006 mondiaal een cruciale rol voor de jihadistische beweging. Datzelfde geldt voor tussen de vijf en tien zogeheten moedersites van waaruit de eerste verspreiding plaatsvindt van jihadistische publicaties en de jihadistische boodschap en waar in fora over allerlei jihadistische onderwerpen informatie te vinden is en meningvorming kan plaatsvinden. Jihadisten verspreiden hun publicaties en boodschap daarentegen ook steeds meer via tal van niet-jihadistische sites en met behulp van sinds 2006 sterk opgekomen toepassingen zoals YouTube en sociale netwerksites. Dit is te bezien als een vorm van innesteling. Jihadisten hebben hier wel minder grip op, maar het bereik is vele malen groter dan op de eigen sites. Sinds eind 2006 zijn tweemaal op grote schaal jihadistische sites verdwenen, vermoedelijk in het kader van een contraterrorisme-operatie, namelijk aan de vooravond van de herdenking van de aanslagen in de VS in september 2008 en 2009. Daar waar jihadisten niet direct een antwoord konden vinden op de verdwijning in 2008, bleek in 2009 dat ze hun lessen hebben geleerd. Zij zijn minder kwetsbaar geworden voor het uit de lucht halen van hun prominente sites. Hieronder zijn de conclusies over het gebruik van het internet als middel verwoord.

B1 Propaganda via het internet draagt bij aan radicalisering

Op het internet zijn vele vormen van jihadistische propaganda te vinden. Vooral de drie mediaorganisaties Al-Fajr, GIMF en As-Sahab hebben een grote stroom propagandistische boodschappen (audio, video en tekst) uitgebracht. Propaganda via het internet is sinds eind 2006 verder geprofessionaliseerd, heeft een groot bereik en kent relatief weinig weerwoord. Jihadisten proberen nog meer de interactie aan te gaan met geïnteresseerden, op tal van manieren. Jihadisten reageren verder actief op nieuwsberichten vanuit westerse media voor propagandistische doeleinden en zijn alert op vermeende beledigingen van de islam en reageren op hun eigen fora op nieuwsberichten daaromtrent vanuit westerse media. De kans op bijvoorbeeld *defacements* als specifieke vorm van propaganda door jihadisten zal eerder toe- dan afnemen, ook in Nederland. Andere tendensen waarop gewezen kan worden zijn een nog verdere professionalisering en kwaliteitsverbetering van jihadistische publicaties en de jihadistische boodschap evenals een grotere gerichtheid op een westers publiek.

De combinatie van vooral grote groepen jongeren die toegang hebben tot het internet en dat intensief gebruiken in combinatie met de propaganda vanuit de jihadistische beweging creëert een voedingsbodemp voor (verdere) radicalisering.

B2 Internetgebruik ondersteunt het gehele proces van radicalisering

De inzichten over de invloed van het internet op radicalisering zijn niet wezenlijk veranderd. 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. Er gaat meer dreiging uit van interactieve sites, waaronder sociale netwerksites of fora, dan vanuit statische sites waar bijvoorbeeld alleen documenten kunnen worden gedownload. Juist de interactiviteit van het jihadistische internetgebruik is toegenomen en daardoor de invloed van het internet op radicalisering. Als gevolg van de toegenomen interactiviteit is het steeds lastiger een onderscheid te maken tussen propaganda, rekrutering, virtuele netwerkvorming en de invloed van het internetgebruik op radicalisering in het geheel. Het internet beïnvloedt radicalisering, maar de mate waarin het internet de enige of de doorslaggevende factor is, is nog niet duidelijk.

B3 Vorming van virtuele netwerken verhoogt de slagkracht van de jihadistische beweging

Het is nog steeds aannemelijk dat door de vorming van virtuele netwerken een informele pool van bereidwilligen voor de jihad kan ontstaan die in wisselende combinaties met elkaar of individueel geweldsactiviteiten kunnen ontplooiën. Lokale en internationale elementen kunnen daardoor meer met elkaar verweven raken.

B4 Rekrutering via het internet verloopt vooral op een interactieve wijze

Het is niet aannemelijk dat iemand vanuit Nederland zich via het internet rechtstreeks en één-op-één laat rekruteren door rekruteurs van internationale terroristische groeperingen. Wel bieden de interactieve jihadistische sites een uitgelezen plaats om te rekruteren. Daar bevinden zich immers personen die vergaand in de jihad zijn geïnteresseerd. Feit is ook dat jongeren zich aangetrokken voelen tot jihadistische strijdtoneelen en via het internet op zoek gaan naar een manier om daar te komen. Op het internet is een sterk interactieve vorm van rekrutering waarneembaar die sterk gekoppeld is aan de interactieve manieren van propaganda bedrijven. Er valt echter vanwege de diversiteit in casuïstiek geen algemeen patroon te benoemen, anders dan dat rekrutering via het internet op interactieve wijze verloopt en dat veelal eerder sprake is van 'zichzelf aanmelden' dan van 'rekrutering' in de klassieke zin van het woord.

B5 Toepassingen voor informatie-inwinning via het internet zijn potentieel ondersteunend bij het plegen van terroristische activiteiten

Internettoepassingen bieden vele mogelijkheden voor informatie-inwinning en terroristen 'spreken' over die mogelijkheden of maken daar al gebruik van. De mogelijkheden die die toepassingen bieden, maken de voorbereidingshandelingen van terroristen gemakkelijker. De toepassingen leveren op een gemakkelijke en anonieme manier informatie over een bepaald object, locatie, organisatie of persoon en zij verminderen de noodzaak om verkenningen ter plaatse uit te voeren. De informatie is toegankelijk doordat organisaties of personen onvoldoende veiligheidsbewust zijn en online veel informatie over zichzelf en hun omgeving prijsgeven. Toch is een deel van de informatie ook op een andere manier verkrijgbaar, bijvoorbeeld in het geval van luchtfoto's via commerciële partijen. Bovendien lijkt voor een echt goede voorbereiding een fysieke verkenning een vereiste. Naar verwachting zullen de mogelijkheden voor informatie-inwinning in de toekomst alleen nog maar verder toenemen. Bovendien zal het internet in de toekomst nog meer dan nu altijd en op iedere locatie beschikbaar zijn.

B6 Fondsenwerving via het internet door en voor jihadisten komt beperkt voor

In potentie bestaan nog steeds vele mogelijkheden voor fondsenwerving door en voor jihadisten. Er zijn enkele voorbeelden van deze varianten bekend, maar het komt in de praktijk nog weinig voor. De verwachte toename van het misbruik van bankieren via het internet en de verwachte verschuiving van meer openlijke naar meer heimelijke fondsenwerving, zijn niet uitgekomen.

B7 Training via het internet werkt drempelverlagend, maar gevaar fysieke training is groter

De verwachting dat het internet de rol van fysieke trainingskampen kan overnemen, is inmiddels gelogenstraft door de praktijk waarin tal van fysieke jihadistische trainingskampen bestaan en daar ook personen naar toe (proberen te) reizen. Het internet is eerder een bibliotheek van trainingsmateriaal en tot op zekere hoogte een virtueel klaslokaal voor beginnende jihadisten. Iemand moet de instructies of handleidingen nog altijd zélf goed kunnen begrijpen, daarmee oefenen, toepassen en (gedisciplineerd) uitvoeren. Ook kunnen bij bepaalde instructies ongetwijfeld vraagtekens geplaatst worden ten aanzien van 'gebruiks-

gemak' en veiligheid. Desondanks zijn het trainingsmateriaal en de sites waar ervaringen en inzichten worden gedeeld niet ongevaarlijk. Zij kunnen, zeker door terroristen van eigen bodem, wel worden gebruikt en daardoor de drempel tot het plegen van aanslagen verlagen.

B8 Jihadisten gebruiken het internet voor onderlinge communicatie en planning

Dat jihadisten het internet nog steeds gebruiken om onderling te communiceren, is zeer aannemelijk. Logischerwijze vindt dit grotendeels afgeschermd plaats. Strikt genomen maakt het voor de dreiging niet uit of jihadisten communiceren met de telefoon of via het internet. Inlichtingeninstanties en de politie kunnen, net als in het geval van andere communicatiemiddelen, ook het internetverkeer onderscheppen. Jihadisten zijn zich daar van bewust en waarschuwen elkaar daar ook voor.

B9 Het internet is voor de jihadistische beweging vooral een cruciaal middel als interactief communicatiemedium en bij (de voorbereiding van) terroristische activiteiten

Jihadisten gebruiken nog steeds volop het internet als middel. Het gebruik door jihadisten is interactiever geworden. Die toegenomen interactiviteit vereenvoudigt het voeren van propaganda, netwerkvorming en 'rekrutering' evenals communicatie en planning onderling. Daardoor is ook het effect op radicalisering groter. Verder speelt het internet een ondersteunende rol voor jihadisten bij (de voorbereiding van) terroristische activiteiten. Naast fondsenwerving en communicatie en planning onderling, komt die dreiging vooral voort uit het gebruik voor de creatie van virtuele netwerken, voor trainingsdoeleinden en voor informatie-inwinning.

C Jihadisme op het Nederlandse internet

C1 Omvang van jihadistische uitingen op het Nederlandse internet afgenomen

Uitingen van jihadisme zijn nog steeds op het Nederlandse internet te vinden, maar de omvang van deze manifestatie is sinds 2006 afgenomen. Dit is waarschijnlijk te verklaren door het actieve modereerbeleid door de beheerders op de mainstreamsites, de afname van de activiteiten van jihadistische lokaal autonome netwerken in Nederland zelf, en het toegenomen veiligheidsbewustzijn bij jihadisten dat door opsporingsinstanties en veiligheidsdiensten in Nederland wordt meegekeken. Verder bleken enkele sinds 2006 vormgegeven jihadistische websites veelvuldig te kampen met technische problemen en vaak offline te zijn.

Desalniettemin is er voor iemand die daadwerkelijk kennis wil opdoen over de gewelddadige jihad nog steeds genoeg materiaal op het Nederlandse web te traceren. Uiteraard kunnen voor het vergaren van jihadistische informatie eveneens Arabischstalige en/of Engelstalige jihadwebsites worden aangewend. Het feit dat in Nederland nog steeds diverse individuen, al dan niet in groepsverband, actief zijn met het online propageren van de gewelddadige jihad is evenmin positief. Hierin schuilt het gevaar dat personen (door)radicaliseren.

C2 Het Nederlandse online jihadisme richt zich bijna volledig op propagandavoering

Het Nederlandse online jihadisme richt zich bijna volledig op propagandavoering, zoals ook al werd geconstateerd in 2006. De propaganda loopt inhoudelijk en qua stijl sterk uiteen. Op statische websites wordt nog steeds (vertaalde) jihadistische literatuur aangeboden. Daarnaast doet zich ook modernere, op Web 2.0 gebaseerde, interactieve kennisuitwisseling over de jihad voor. Sinds eind 2008 zijn op

YouTube enkele Nederlandstalige filmpjes met daarop jihadistische nasheeds (islamitische liederen zonder instrumenten) gepost. Deze jihadistische liederen op YouTube trachten primair een gevoel van woede tegen het Westen bij moslims op te wekken en roepen op tot actie. Tevens wordt er in deze nasheeds een romantisch beeld van de gewelddadige jihad geschapen. Er zijn op het Nederlandse 'openbare' internet geen voorbeelden waargenomen van rechtstreekse rekrutering en/of het verspreiden van (Nederlandstalige) handleidingen over explosieven en het toepassen van wapens.

C3 Focus van Nederlandse jihadisten op het Nederlandse internet ligt op internationale aspecten van de jihad

De jihadistische focus op het Nederlandse internet ligt hoofdzakelijk op internationale aspecten van de jihad, te weten de traditionele strijdgebieden in Afghanistan, Pakistan maar ook - en dat is relatief nieuw - Somalië. Dit is in lijn met algemene bevindingen over jihadistische netwerken in Nederland.

D Overzicht belangrijkste veranderingen

De conclusies zijn op hoofdlijnen ongewijzigd ten opzichte van de oorspronkelijke fenomeenstudie. Dat is opmerkelijk in het licht van de snelle ontwikkelingen op het internet en binnen het jihadisme.

Voor wat betreft het internet als doelwit en wapen zijn de belangrijkste veranderingen dat de kwetsbaarheden voor cyberaanvallen tegen en via het internet zijn toegenomen en dat deze kwetsbaarheden steeds breder bekend raken. Positief is wel dat ook het bewustzijn over die kwetsbaarheden is gegroeid en er ook maatregelen daartegen getroffen worden of zijn. Als gevolg van de beoordeling dat jihadisten niet in staat zijn een complexe aanval uit te voeren en er ook weinig aanwijzingen bestaan over intenties hiertoe, zijn de conclusies over (cyber) aanvallen tegen en via het internet vrijwel gelijk gebleven.

Ook de conclusies over het gebruik door jihadisten van het internet als middel zijn grotendeels gelijk gebleven. Toch deden zich ook hier wel veranderingen voor. In lijn met ontwikkelingen op het internet zelf, is de belangrijkste verandering de toegenomen interactiviteit. Dit manifesteerde zich eind 2006 al op het 'Nederlandse jihadistische internet', maar is nu ook internationaal doorgedrongen. Die toegenomen interactiviteit vereenvoudigt het voeren van propaganda, netwerkvorming en 'rekrutering' evenals communicatie en planning onderling. Daardoor is ook het effect op radicalisering groter en is bovendien minder scherp af te bakenen waar bijvoorbeeld propaganda overgaat in rekrutering of netwerkvorming. Ook het misbruik door jihadisten van neutrale sites, dat zich eind 2006 al manifesteerde op het Nederlandse internet, doet zich internationaal voor. Tegenover deze bredere manifestatie van jihadistische uitingen staat de nog grotere rol van drie zogeheten jihadistische media-organisaties en tussen de vijf tot tien zogeheten moedersites. De eind 2006 verwachte toename van het misbruik van bankieren via het internet en de verwachte verschuiving van meer openlijke naar meer heimelijke fondsenwerving via het internet zijn niet uitgekomen. Inmiddels is ook duidelijk dat de toenmalige verwachting dat het internet de rol van fysieke trainingskampen kan overnemen, niet juist is gebleken. Dat het internet van invloed is op radicalisering is onomstreden, maar de mate waarin het internet daarbij de enige of de doorslaggevende factor is, is nog niet duidelijk. Onderzoek hiernaar is naar de aard lastig uitvoerbaar.

De belangrijkste verandering van het jihadisme op het Nederland internet is de afname sinds 2006 van jihadistische uitingen. Ook deze conclusies zijn in lijn met die van eind 2006.

1 Inleiding

1.1 Aanleiding

In januari 2007 verscheen de fenomeenstudie *Jihadisten en het Internet* van de NCTb, verder aangeduid als 'de fenomeenstudie'. De studie was bedoeld om inzicht te verschaffen in het gebruik van het internet door jihadisten. Voor beleidsvorming en -evaluatie ten behoeve van contraterorisme werd (en wordt) inzicht in het internetgebruik door jihadisten van groot belang geacht. In het onderzoek werd gekeken naar het gebruik van het internet als een wapen voor een aanslag op bijvoorbeeld de vitale infrastructuur in Nederland en naar het gebruik als een middel voor bijvoorbeeld propaganda en rekrutering. Ook werd gekeken naar de kwetsbaarheid van het internet zelf voor terrorisme: internet als doelwit. Ten aanzien van alle facetten werd een beoordeling van de dreiging gegeven. De onderzoeksperiode van de studie liep in feite van het ontstaan van het internet tot medio 2006. Literatuur uit de tweede helft van 2006 is toen slechts beperkt gebruikt bij het schrijven van de studie. In die periode werd tevens een expertmeeting gehouden waar enkele hypothesen en voorlopige conclusies konden worden getoetst. Ook werd een substantiële bijdrage van de AIVD in de teksten verwerkt. Het uiteindelijke resultaat heeft geresulteerd in uiteenlopende beleidsinitiatieven.

Zoals bekend mag worden verondersteld gaan de ontwikkelingen ten aanzien van ICT snel en ook het jihadisme is en blijft in ontwikkeling. Daarom ontstond de behoefte om de toenmalige beoordeling van de dreiging opnieuw te beoordelen in de vorm van deze 'update 2009'. Het accent ligt op veranderingen sinds het uitkomen van de fenomeenstudie van begin 2007. Wel is gestreefd naar een zelfstandig leesbare publicatie.

1.2 Doel, onderzoeksvragen en afbakening

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

Afgeleid van het doel luiden de onderzoeksvragen:

- In hoeverre hebben zich sinds eind 2006 belangrijke veranderingen voorgedaan in de wijze waarop jihadisten het internet gebruiken als doelwit, wapen en middel en welke veranderingen zijn dat?
- In hoeverre hebben zich belangrijke veranderingen voorgedaan in de wijze waarop het gebruik van het internet als middel door jihadisten invloed heeft op radicalisering en wat zijn die veranderingen?
- In hoeverre hebben zich sinds eind 2006 belangrijke veranderingen voorgedaan in de wijze waarop het jihadisme zich manifesteert op het Nederlandse internet?
- In hoeverre resulteren geïdentificeerde veranderingen in het gebruik van het internet door jihadisten in veranderingen in de dreiging door jihadisten tegen Nederland of Nederlandse belangen?

De afbakening is gelijk aan die van de fenomeenstudie. Deze update richt zich dus ook primair op het jihadistisch terrorisme en jihadistische radicalisering, in het verleden ook wel aangeduid als islamistisch terrorisme en islamistische radicalisering. In Nederland, maar ook in Europa, gaat de grootste dreiging uit van juist deze categorie terroristen. Tenzij anders aangegeven, hanteren we gemakshalve het begrip jihadisme of jihadisten (zie paragraaf 1.3). Voor een definitie van de begrippen wordt verwezen naar het begrippenkader.

Het criminele internetgebruik (cybercrime, zoals phishing) blijft buiten beschouwing. Het internetgebruik

voor economische en industriële spionage, voor politiek-militaire doeleinden (cyberwar) en het gebruik door activisten komen evenmin uitgebreid aan bod. Een uitzondering hierop vormt een casus in Estland. Deze wordt vaak genoemd als voorbeeld waarin een cyberaanval de internet-infrastructuur van een land ernstig heeft verstoord. Deze casus wordt ook vaak genoemd als voorbeeld van cyberterrorisme, een term die de NCTb liever niet hanteert, of cyberwar. Verder worden geen ICT-gerelateerde onderwerpen behandeld zoals het gebruik door jihadisten van satelliettelefoons en mobiele telefoons, alsmede het gebruik van satellietzenders.

Bij het schrijven en trekken van conclusies bleek de genoemde afbakening goed hanteerbaar voor het onderdeel 'Internet als middel' (hoofdstuk 3). De afbakening is echter lastiger hanteerbaar voor het onderdeel 'Internet als doelwit en wapen'. Veel literatuur over het onderwerp maakt geen onderscheid naar wie een eventuele aanval onderneemt: staten, criminelen, vandalen of anderssoortige terroristen. De geschetste kwetsbaarheden kunnen immers door anderen dan jihadisten worden benut en het weerstandvermogen beperkt zich niet alleen tot jihadisten. Alleen de beoordeling van de intentie en capaciteiten van jihadisten valt wel geheel binnen de afbakening te maken. De conclusies richten zich, overeenkomstig de afbakening van de update, wel specifiek op het gebruik van het internet als doelwit en wapen door jihadisten.

Ook een ander aspect van de afbakening, het terroristisch gebruik, was soms lastig hanteerbaar. Iedere cyberaanval is als ernstig te kwalificeren. Om echter te kunnen spreken van een terroristische aanslag, waar de NCTb zich vanuit de taakstelling specifiek op richt, moet die wel passen binnen de definitie van terrorisme (zie begrippenlijst). Het gaat dan om een specifieke intentie - maatschappelijke veranderingen bewerkstelligen, de bevolking ernstige vrees aanjagen of politieke besluitvorming beïnvloeden - en de gevolgen - op mensen gericht ernstig geweld, dan wel daden gericht op het aanrichten van maatschappij-ontwrichtende zaakschade.

1.3 Verantwoording werkwijze

Gekozen is voor een globale, maar wel brede oriëntatie op basis waarvan vervolgonderzoeken denkbaar zijn. Er is daarbij opnieuw gekozen voor vier onderzoeksmethoden, namelijk:

1. het houden van interviews,
2. een literatuurstudie,
3. een verkenning van het gebruik op enkele Nederlandstalige websites en -fora, en
4. een expertmeeting.

Interviews hebben plaatsgevonden met enkele deskundigen van instanties die zich in Nederland bezighouden met het verschijnsel internet of vitale sectoren. De interviews en achtergrondgesprekken zijn geanonimiseerd verwerkt. Ook hebben de auteurs deelgenomen aan congressen en zijn de bevindingen daarvan verwerkt.

De literatuurstudie heeft zich gericht op wetenschappelijke literatuur, open en gesloten bronnen. In de wetenschappelijke literatuur en open bronnen wordt uitvoerig ingegaan op het internetgebruik door terroristische groeperingen en jihadisten. Het gaat daarbij overwegend om buitenlandse literatuur en bronnen 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. Ook Nederlandse en buitenlandse inlichtingen- en opsporingsinstanties richten

zich op dit verschijnsel en publiceren daar ook over in vrijelijk beschikbare maar tevens in gerubriceerde documenten. Deze informatie is eveneens bestudeerd en, voor zover de rubricering dat toestaat, meegenomen in deze studie.

Op 11 juni 2009 organiseerde de NCTb in het kader van deze studie een expertmeeting (bijna exact drie jaar na de vorige), die opnieuw onderzoekers, overheidsdiensten en bedrijfsleven uit de terrorisme-, telecom- en internetsector bijeenbracht. Wederom stond het onderwerp 'internet als doelwit en wapen' centraal. De uitkomsten van die expertmeeting zijn verwerkt in hoofdstuk 2.

Bij het onderzoek ten behoeve van hoofdstuk 4 is het 'openbare gedeelte' van het Nederlandse internet geanalyseerd, dat wil zeggen het gedeelte van het internet dat niet afgeschermd is en wel doorzoekbaar is met behulp van zoekmachines zoals Google. Hierbij is gebruik gemaakt van zoektermen, in sommige gevallen Arabischstalige, die in verband zijn te brengen met het jihadisme. Indien jihadistische inhoud op de website werd geconstateerd, bleek vaak dat op dergelijke plekken *hyperlinks* of verwijzingen naar andere jihadistische weblocaties vermeld stonden. De bevindingen in hoofdstuk 4 zijn daarnaast gebaseerd op reguliere internetmonitoractiviteiten, openbare bronnen en interviews.

De periode waarop deze studie betrekking heeft, is afgesloten in december 2009. Ontwikkelingen na die tijd zijn niet meer meegenomen.

Met het begrip jihadisme wordt in deze publicatie het volgende bedoeld:

- Jihadisme is een stroming binnen de politieke islam die op basis van een specifieke invulling van de salafistische leer en op basis van het gedachtegoed van Sayyid Qutb door middel van een gewapende strijd (jihad) streeft naar een mondiale heerschappij van de islam en de heroprichting van de Islamitische Staat (Kalifaat).

Voor een uitgebreidere beschrijving zie Bijlage 1.

1.4 Toelichting structuur

Grotendeels wordt in deze actualisering de structuur van de oorspronkelijke fenomeenstudie gevolgd. Hoofdstuk 2 analyseert het internet als doelwit en wapen en hoofdstuk 3 het internet als middel. Hoofdstuk 4 behandelt de situatie op het Nederlandse internet. Geëindigd wordt met een literatuurlijst, begrippenlijst en een bijlage.

2 Internet als doelwit en als wapen

2.1 Inleiding

Dit hoofdstuk beschrijft in hoeverre jihadisten het internet zien als doelwit of gebruiken als wapen. Bij 'internet als doelwit' gaat het om terroristische activiteit gericht tegen (de infrastructuur van) het internet zélf, terwijl het bij 'internet als wapen' gaat om terroristische activiteit via het internet gericht tegen fysieke of online doelwitten, zoals de vitale infrastructuur of online diensten zoals internetbankieren, belangrijke zoekmachines, nieuwssites en internetwinkels. Staatsterreur of internetaanvallen uitgevoerd door of namens staten vallen niet binnen deze omschrijving. Dit is tevens van belang om verwarring te voorkomen met begrippen als cyberwar of hacktivisme in allerlei verschijningsvormen.

Van het begrip cyberterrorisme bestaan de nodige definities.¹ De NCTb hanteert bewust niet deze term. De term cyberterrorisme leent zich eenvoudig voor overdrijving. Daarbij wordt soms een overtreffende term gehanteerd in de vorm van 'electronic Pearl Harbor', 'digital Waterloo', of 'cybergeddon'.² Het belangrijkste argument om de term cyberterrorisme niet te gebruiken is echter de vraag of een bepaalde modus operandi (hetgeen het gebruik van het internet feitelijk is) een speciale definitie verdient.

In deze update wordt de brede term cyberterrorisme dus niet gebruikt. Wel is uit praktische overwegingen gekozen om een compacte term te hanteren voor een terroristische aanslag tegen het internet zelf of tegen de vitale infrastructuur of kritische online-dienstverlening waarbij het internet als vehikel wordt gebruikt. Net als in de fenomeenstudie is dit de term 'cyberaanval'.

2.2 Achtergronden

In deze paragraaf wordt aandacht besteed aan bepaalde begrippen en ontwikkelingen die zowel in de bespreking van het internet als doelwit (2.3), als wapen (2.4) en als middel (3) terugkomen. Tenslotte wordt in algemene zin gekeken naar indicatoren voor interesse bij jihadisten voor cyberaanvallen.

2.2.1 Nieuwe vormen van/gegevens over internetgebruik

De afgelopen periode heeft met name een snelle groei van mobiel internet plaatsgevonden. Zelfs in vliegtuigen wordt internetten mogelijk.³ Internetten via laptops, netbooks en mobiele telefoons, zonder afhankelijk te zijn van 'ouderwetse' hotspots, raakt volledig ingeburgerd.⁴ Daardoor wordt steeds meer, soms gevoelige, informatie - vaak draadloos - tussen personen en bedrijven (onderling) uitgewisseld. De bandbreedte neemt daarbij toe. Mede door die toegenomen bandbreedte werd de tijd rijp voor een andere belangrijke wijziging: de verschuiving van computertoepassingen van de laptop of desktopcomputer naar het internet. Daarmee wordt internet in feite het nieuwe besturingssysteem, en zijn behalve email ook tekstverwerking, foto- en videobewerking en relatiebeheer online beschikbaar. Dit wordt *cloud computing* genoemd en biedt veel voordelen. Zo hoeft de gebruiker niet zelf software te installeren en zijn de eigen gegevens overal benaderbaar. Deze gegevens staan echter niet langer op de eigen harde schijf, maar in de *cloud*. Daarnaast kunnen kwetsbaarheden in een onlinedienst door iedereen via het internet worden uitgebuit. Ook kunnen de gebruiksvoorwaarden eenzijdig worden gewijzigd, hetgeen vooral voor bedrijven een probleem kan vormen. Het feit dat meer mensen online zijn, vaker online zijn, vaker draadloos werken en te maken krijgen met nieuwe toepassingen biedt in principe ook aan terroristen meer mogelijkheden, voor phishing, informatievergaring, social engineering, propaganda en cyberaanvallen.

¹ Voor een Nederlandse definitie van cyberterrorisme zie: Luijff 2008.

² Stohl 2007.

³ Foxnews 2008.

⁴ Navolgende passage grotendeels gebaseerd op: GOVCERT 2009.

2.2.2 Massale overbelastingaanvallen en gerichte hacking: varianten

Nog steeds zijn massale overbelastingaanvallen en gerichte hacking de twee methodes om via het internet een daadwerkelijk terroristisch effect te bewerkstelligen.

Massale overbelastingaanvallen, doorgaans *Distributed Denial of Service* aanvallen (DDoS-aanvallen) genoemd, zijn met name geschikt voor pogingen om (delen van) het internet uit te schakelen. Gerichte hacking is voor terroristen toepasbaar voor aanslagen op bijvoorbeeld de vitale infrastructuur. Voor het aantasten van de beschikbaarheid van internetdiensten komen DDoS-aanvallen in aanmerking (gevolg: internetbankieren is niet mogelijk), voor het aantasten van de betrouwbaarheid is dat gerichte hacking (gevolg: gegevens zijn gecompromitteerd en/of valse transacties zijn gepleegd). DDoS- en virusaanvallen zijn echter ook in te zetten in de vitale sectoren vanwege het versturende effect. Daarbij zal dan echter geen sprake zijn van het gecontroleerd overnemen van een dergelijke sector.⁵

Meer en effectievere botnets: tevens steeds goedkoper

Het aantal DDoS-aanvallen neemt nog steeds toe, tot 6000 per dag wereldwijd. Voor een DDoS-aanval wordt doorgaans een botnet gebruikt. Een botnet is - kort gezegd - een netwerk van gehackte computers, dat zichzelf ook nog eens in omvang kan doen laten toenemen.⁶ Ten aanzien van botnets is sprake van een wedloop in technologieën. Een trend is dat men deskundigen of technieken inhuurt om eigen botnets te maken. Het is een grote markt, maar de winstmarges zijn kleiner aan het worden. Onder andere GOVCERT NL heeft over de ontwikkelingen rond botnets en malware (kwaadaardige software) gerapporteerd. Het aantal verschillende varianten van malware neemt snel toe.⁷

Ook worden technieken gebruikt waardoor botnets een andere structuur krijgen, zonder herleidbare eigenaar. Dergelijke botnets benutten de mogelijkheden van het internet beter en maakt het tegenhouden van aanvallen lastiger. Het vergroot niet de kans op een cyberaanval, maar wel de effectiviteit ervan.⁸

Ook andere technieken bemoeilijken het tegenhouden van cyberaanvallen of de opsporing, omdat ze als het ware het geheugen van het internet belemmeren. Een worm als Conficker waarover in 2009 veel werd bericht en waarover veel onduidelijkheid bestond, maakte gebruik van dergelijke technieken.⁹

Ondanks al deze technieken en mogelijkheden overstijgen de meeste incidenten met botnets, anders dan ten behoeve van cybercrime, het niveau van vandalisme niet.¹⁰

2.2.2.1 Niveau van cyberaanvallen

Het is en blijft van belang om onderscheid te maken naar uitvoerbaarheid en effecten van cyberaanvallen.¹¹ Sommige cyberaanvallen, defacements en kleine DDoS-aanvallen, zijn grotendeels geautomatiseerd en goedkoop uit te voeren, maar hebben ook, zowel qua duur als ernst, weinig effect. Ze vallen binnen de categorie 'eenvoudige aanvallen, 'scriptkiddie-aanvallen' of 'hacktivisme'. Dit geldt ook voor de defacements naar aanleiding van de film *Fitna*¹², die zich richtten op eenvoudige, oude kwetsbaarheden in server-software. Er was wel sprake van een zekere gerichtheid (alleen servers binnen het NL-domein waren

doelwit) maar deze was grofmazig en geautomatiseerd. De effecten waren gering en eenvoudig te verhelpen. Ook eenvoudige aanvallen kunnen de nodige publiciteit genereren, zoals in Nederland ten tijde van de defacements rond *Fitna* en in de VS ten tijde van de eenvoudige DDoS-aanvallen op Zuid-Korea en de VS in juli 2009. Bij laatstgenoemd incident werd zelfs al gesproken over elektronische oorlogsvoering (*cyberwarfare*), en het leidde tot de oproep van een Amerikaans congreslid tot 'a show of force or strength' tegen de vermoede dader (Noord-Korea).¹³ Langs deze weg belandt ook het onderwerp elektronische oorlogsvoering vaak onterecht in een discussie rond terrorisme op en via het internet. Dit wil niet zeggen dat het onderwerp elektronische oorlogsvoering en de rol van derde landen niet belangrijk is, aangezien de capaciteit van bepaalde landen voor dergelijke oorlogsvoering aanzienlijk lijkt.

Een hoger niveau van cyberaanvallen zijn gevorderde aanvallen, waarvoor men moet kunnen programmeren of andermans programma's moet kunnen aanpassen, waarvoor men goed thuis moet zijn in netwerken en besturingssystemen, en waarvoor men relatief onbekende kwetsbaarheden kan benutten of nieuwe kan vinden.¹⁴ Dit zijn serieuze aanvallen die echter gericht zullen zijn op één soort netwerk, dat in een bepaalde vitale- of overheidssector gebruikt wordt. Daarvoor is tenminste kennis nodig over de karakteristieken van het doelwit. Dergelijke aanvallen kunnen serieuze gevolgen hebben, maar zijn niet per sé (langdurig) effectief, laat staan maatschappijontwrichtend. Ook dit soort aanvallen kunnen doorgaans goedkoop worden uitgevoerd. In combinatie met de juiste publiciteit kan met name een sterk propagandistisch effect en maatschappelijke onrust worden bereikt.

Tenslotte zijn er complexe aanvallen die specifiek, van begin tot eind, op bijvoorbeeld één vitale sector gericht zijn. Dergelijke aanvallen kenmerken zich door een diepgaand vooronderzoek over het aan te vallen systeem, het bezit of de inhuur van de juiste kennis en vaardigheden op het gebied van programmeren en *social engineering*, het hebben van de beschikking over een team, apparatuur en zeer waarschijnlijk een testomgeving om te oefenen en (mogelijk ook keten-) effecten te voorspellen. Een dergelijke setting vergt tijd, discipline en fondsen. Lachow geeft als voorbeeld dat een dergelijke complexe cyberaanval bijvoorbeeld gericht zou kunnen zijn op een grote logistieke operatie, zoals de uitzending van troepen (waarbij logistieke planning, communicatie en transport samenkomen).

Zoals aan de bovenstaande beschrijvingen te zien is, zit er een groot verschil tussen hetgeen nodig is voor een eenvoudige of kortdurende cyberaanval en een langdurige, maatschappijontwrichtende aanval. Wel zijn op het internet meer en meer gekraakte procescontroleprogramma's, officiële handleidingen daarvoor en goedkope industriële hardware verkrijgbaar. Het opzetten van een testomgeving door kwaadwillenden is daardoor een mogelijkheid geworden. Ook zou de aandacht voor ICT-kwetsbaarheden in vitale sectoren sterk gestegen zijn sinds 2005. Gelet op de toegenomen aandacht voor dit onderwerp in algemene zin is zeker niet uit te sluiten dat, hoewel een beperkt aantal mensen daartoe in staat is én de intentie heeft, een cyberaanval van de derde categorie plaatsvindt. Of een dergelijke aanval van jihadisten te verwachten is, wordt vanaf 2.2.3 behandeld.

2.2.3 Ontwikkelingen rond cyberaanvallen bij jihadisten

Op 12 februari 2009 meldde de *Director of National Intelligence* voor een Amerikaanse Senaatscommissie dat onder andere al Qa'ida heeft aangegeven de wens te hebben om via cybermethoden de VS aan te vallen.¹⁵

⁵ Interviews.

⁶ Botnets worden, behalve voor DDoS, met name ingezet voor het versturen van spam.

⁷ GOVCERT 2008 en CRS 2008, p.5.

⁸ Expertmeeting 2009.

⁹ Expertmeeting 2009: het betreft hier bijvoorbeeld peer-to-peer botnets en de fastflux-techniek.

¹⁰ Expertmeeting 2009.

¹¹ Grotendeels gebaseerd op Lachow, p.443-445.

¹² Pers 2008 en Parool 2008.

¹³ Washington Times 2009.

¹⁴ Zero day exploits kunnen ook gekocht worden op de 'zwarte markt', zie Council of Europe 2007, p.26.

¹⁵ US Senate Select Committee 2009.

FBI *assistant-director* Henry zou gezegd hebben dat terroristische groepen bezig zijn met het creëren van een virtueel 9/11.¹⁶ Mark Oram, hoofd *Threat and Information Security knowledge department* van het *Center for the Protection of National Infrastructure* (CPNI) waarschuwde voor cyberspionage maar acht de kans klein dat er een cyberaanval van de kant van terroristen komt, gelet op hun beperkte capaciteiten en moeilijkheden met het begrijpen van kwetsbaarheden in de infrastructuur.¹⁷ Lord West of Spithead (*Home Office*, UK) daarentegen gaf aan dat de grootste dreiging komt van hackers die gesteund/gesponsord worden door terroristen die proberen in te breken in bijvoorbeeld het elektriciteitsnetwerk.¹⁸ Er is sprake van verdeeldheid over de werkelijke dreiging. Sommigen leggen sterk de nadruk op de mate van *dreiging*, anderen laten juist de mate waarin vitale sectoren verbonden zijn met het internet en het feit dat er *kwetsbaarheden* bestaan onderbelicht.

Om de dreiging van een jihadistische cyberaanval in te schatten wordt in de volgende paragrafen gekeken naar de volgende vragen.¹⁹ Hebben er aanslagen plaatsgevonden? Investeren jihadisten in cyberaanvallen? Huurt of koopt men wellicht kennis in? Doet men er (bepalende) uitspraken over en blijken er serieuze intenties uit? Is men geïnteresseerd in/ervaren met hacking? Is men ervaren met/bedreven in gebruik van computers en internet? Deze vragen worden in de volgende algemene paragrafen besproken en gebundeld onder de kernbegrippen intenties en capaciteiten. In sommige gevallen is een strikt onderscheid echter lastig te maken.

2.2.3.1 Intenties

Algemene intenties en uitspraken: wisselend van karakter en betrekkelijk vaag

In de fenomeenstudie werden de intenties van jihadisten om het internet te treffen op een rij gezet. In algemene zin was op strategisch niveau sprake van de intentie om de economie te treffen. De economische crisis die zich eind 2008 manifesteerde vormde eveneens een bron van inspiratie voor jihadisten en hun supporters, zo komt naar voren in een video-interview met Bin Laden en uit discussies op jihadistische webfora.²⁰ Het internet is onmisbaar voor de overheid, voor (vitale) bedrijven en daarmee voor de economie. Ondanks dat hierover regelmatig beweringen worden gedaan of naar wordt verwezen, hebben de auteurs het kader van al Qa'ida nimmer op rechtstreekse uitspraken ten aanzien van het treffen van het internet kunnen betrappen. Het dichtst bij een uitspraak met daadwerkelijk internetgerelateerde intenties die in het verlengde ligt van de bovenstaande theorie komt de tweede man van al Qa'ida, Al-Zawahiri, in zijn *Knights Under the Prophet's Banner uit 2002*.²¹ Dit document is niet beoordeeld ten tijde van de fenomeenstudie. In het document spreekt hij over doelen (zoals het verdrijven van westerse invloeden uit de islamitische wereld), vijanden (het Westen) en criteria voor doelwitselectie/middelen (het maken van veel slachtoffers/martelaarschap). Binnen deze indeling worden 'internationale netwerken voor informatie- en communicatietechnologie' in algemene zin onder 'de vijand' geschaard en op één lijn geplaatst met bijvoorbeeld internationale media. Hiermee is echter niet gezegd dat het internet een doelwit is: het maakt onderdeel uit van het vijandbeeld.

¹⁶ AFP 2009.

¹⁷ ZDNet 2008.

¹⁸ Times 2008.

¹⁹ Deels tevens ontleend aan Denning 2007, p.5-p.15.

²⁰ Weimann 2009.

²¹ Mansfield 2006.

Een andere uitspraak, eveneens niet beoordeeld in de fenomeenstudie, is toe te schrijven aan Bin Laden. Deze zou na '9/11' aan de editor van de krant *Ausaf* verteld hebben dat vele moslimwetenschappers aan zijn kant stonden die hun kennis zouden gebruiken "in chemistry, biology and [sic] ranging from computers to electronics against the infidels".²² Deze uitspraak is onvoldoende concreet om een strategie aan te ontlenen en lijkt met name een propagandistisch effect te beogen. Dat sinds 2001 geen succesvolle chemische, biologische of cyberaanvallen hebben plaatsgevonden lijkt deze duiding te ondersteunen. Wel is chemische kennis en kennis van elektronica benut voor de productie van IED's, is algemene computerkennis ingezet voor propaganda en is in Irak een korte periode geweest waarin vrachtwagens met chloor bij aanslagen werden ingezet.

Tenslotte is er de eveneens oudere theorie die al Qa'ida's 'zeven-fasen strijd' beschrijft. De vierde fase (*The healing stage and gathering strength for change*, van 2010-2013) zouden ook cyberaanvallen tegen de economie in de VS omvatten.²³ Een eerdere fase (van 2003-2007) omvatte mede de voorbereiding op de elektronische jihad via het internet. Of met deze elektronische jihad alleen propaganda-achtige activiteiten of ook cyberaanvallen werden bedoeld is niet duidelijk. In ieder geval breekt volgens de theorie van de zeven-fasen strijd in 2010 de fase van, onder andere, cyberaanvallen aan.

Al met al betreft het hier oudere uitspraken, die niet heel concreet zijn en waarvan tot op heden ook niet is gebleken dat ze uiterst serieus genomen moeten worden. Tijdens de expertmeeting werd aangegeven dat geen intenties bij jihadisten in de richting van een serieuze cyberaanval bekend zijn.

Ook de legitimiteit van cyberaanvallen kwam aan de orde in de fenomeenstudie. Gewezen werd op twee fatwa's dienaangaande. Sinds de fenomeenstudie heeft op het internet, in dit geval het Ansar Al-Haqq forum, in 2009 opnieuw een discussie plaatsgevonden over de vraag of cyberaanvallen zijn toegestaan. Dit gebeurde naar aanleiding van een kritisch stuk in een Tunesische krant over de legitimiteit van cyberjihad. Diverse forumleden zijn ervan overtuigd dat cyberjihad is toegestaan. Eén deelnemer plaatst de tekst "the Prophet recommended that we combat miscreants through all means... [and] fight jihad through all means." Deze krijgt de nodige bijval.²⁴ Andere discussies over de legitimiteit van cyberaanvallen zijn niet bekend. Dit kan betekenen dat de legitimiteit eigenlijk niet ter discussie staat, maar kan er ook op wijzen dat het onderwerp niet echt leeft.

In de wetenschap lopen de meningen over de intenties van jihadisten uiteen. Sommigen menen dat jihadisten een cyberaanval onvoldoende interessant (zullen blijven) vinden, dan wel dat zij onvoldoende capaciteiten (zullen blijven) hebben.²⁵ Anderen denken dat terroristen geïnteresseerd zullen blijven, maar dat deze interesse lastig valt af te zetten tegen andere opties, en dat de combinatie van een cyberaanval met een fysieke aanslag aantrekkelijker kan worden.²⁶ Wat hun intenties ten aanzien van een cyberaanval zou kunnen remmen is de kans dat een cyberaanval leidt tot een (verdere) toename van enerzijds beveiligingsmaatregelen in vitale- en overheidssectoren en anderzijds monitoring, controle en regulering door over-

²² Denning 2007, p.12.

²³ Spiegel 2005 en Denning 2007, p.13, verwijzend naar al-Zarqawi: al-Qaeda's Second Generation van de Jordanees reporter Fouad Hussein, op basis van interviews met Al-Zarqawi en verschillende leiders binnen het al Qa'ida netwerk.

²⁴ SITE 2009a.

²⁵ Stohl 2007.

²⁶ Lachow 2009.

heden van het internet en internetgebruik.²⁷ Een dergelijke ingreep zou ook de mogelijkheden van jihadisten voor hun kernactiviteit op het internet, propaganda, verder beperken.

Al met al zijn er aan de hand van algemene intenties weinig aanwijzingen dat cyberaanvallen zich snel tot een belangrijk aanslagmiddel van jihadisten zullen ontwikkelen.

Investeren in capaciteiten nauwelijks zichtbaar of effectief

'Investeren in capaciteiten' is een moeilijker te beschrijven onderdeel van intenties. Indien dit plaatsvindt, gebeurt het tenminste gedeeltelijk niet zichtbaar. Zo kan men formele ICT-opleidingen volgen die nodig zijn om een niveau van expertise te bereiken dat nodig is om complexe cyberaanvallen te kunnen uitvoeren. Anderzijds is niet gezegd dat wanneer men dergelijke opleidingen volgt, aanvallen in hetzelfde veld ook echt worden beoogd. Zo gebruikten de verschillende artsen die betrokken waren bij het bomcomplot in het Verenigd Koninkrijk in 2007 hun medische vaardigheden niet.

Er zijn enkele (oudere) voorbeelden van personen uit het ICT-veld die geassocieerd werden met terroristische groeperingen en in de VS met name op het gebied van fondsenwerving, rekrutering of facilitering actief zouden zijn geweest.²⁸ Nieuwere voorbeelden, laat staan voorbeelden waarbij dergelijke kennis daadwerkelijk met het oog op cyberaanvallen werd opgedaan, zijn niet bekend.

Behalve via formele ICT-opleidingen, kan ook kennis worden vergroot door onderzoek naar mogelijkheden, het opzetten van trainingsfaciliteiten en verspreiding van kennis. Sinds de fenomeenstudie is hierover weinig betekenisvol bekend geworden. Trainingsfaciliteiten zijn ondanks operaties in Irak en Afghanistan, voor zover bekend, niet aangetroffen en ten aanzien van onderzoek naar mogelijkheden lijken alleen enkele 'supporters' op jihadistische fora alert (zie hierna). Dit laatste zegt echter relatief weinig over de intenties van feitelijke jihadistische groeperingen.

Bundeling en verspreiding van kennis heeft wel aantoonbaar plaatsgevonden. Eind 2006, kort voor het verschijnen van de fenomeenstudie, heeft het Al-Fajr Information Center (zie paragraaf 3.2.1) het eerste exemplaar van 'The Technical Mujahid Magazine' gepresenteerd. Dit artikel is gericht op computer- en internetveiligheid, maar ook het gebruik van GPS komt aan bod. *Jihad in the information sector* wordt gezien als een belangrijke pijler in de strijd tegen de kruisvaarders. Het artikel is erg algemeen van aard. Oproepen worden gedaan om te participeren met bijdragen.²⁹ Het Al-Fajr Center is ingedeeld in verschillende brigades, waaronder de *Hacking Brigade* (voor het hacken van websites, DDoS-aanvallen en identificeren van kwetsbare websites) en de *Cybersecurity Brigade*, ten behoeve van de beveiliging van jihadistische websites. Iedere groep heeft eigen messageboards waartoe alleen leden van die brigade toegang hebben, en iedere brigade heeft leiders die coördineren met 'the jihadist leadership'.³⁰

Op Zuidoost-Aziatische websites zijn in de loop van 2007 hackinghandboeken verschenen, die afkomstig waren van Arabische websites. De plannen bleven echter beperkt tot hacktivism: de forumleden in Zuidoost-Azië (naar eigen zeggen propedeuse-studenten uit Indonesië en Maleisië) moedigden elkaar aan om websites aan te vallen die te liberale islamitische denkbeelden uitdroegen.³¹

²⁷ ITAC 2006.

²⁸ Denning 2007.

²⁹ SITE 2006a.

³⁰ Katz & Devon 2007a.

³¹ Agence 2009.

Op een Arabischtaalgig jihadistisch forum werd een uitgebreid (1000 pagina's) hacking- en cybersecurity-compendium geplaatst.³² Hierin is basale uitleg te vinden over de werking van het internet, netwerken en servers, maar wordt met name veel aandacht besteed aan beveiliging van websites en aan hacking via, bijvoorbeeld, *SQL-injection*, het vinden van kwetsbaarheden in servers, websites en webfora en DDoS-aanvallen. De, Arabischtalige, uitleg is gedetailleerd en de aandacht hiervoor op het forum zou aanzienlijk zijn geweest.

De voornoemde kennisgerichte activiteiten vormen mogelijk een investering in het ontwikkelen van een ideologie en strategie voor cyberaanvallen door jihadistische hackers, maar vormen geen directe reden tot zorg.

2.2.3.2 Capaciteiten

Ervaring met gebruik van computers en internet: prominent aanwezig

Over algemene ervaring bij jihadisten en hun aanhangers met gebruik van computers en internet bestaat geen twijfel. Jihadisten benutten het internet volop voor bijvoorbeeld propaganda. De fenomeenstudie en ook deze actualisering kent vele voorbeelden (zie Hoofdstuk 3). Dit zegt echter niets over capaciteiten om een cyberaanval uit te voeren. Wel kan het een basis vormen van waaruit enthousiasme voor dergelijke aanvallen wordt gecreëerd of rekrutering plaatsvindt.

Ervaring met cyberaanvallen en hacking blijft beperkt

In de fenomeenstudie werden enkele voorbeelden van hackingervaring besproken en werd een bekende in het Verenigd Koninkrijk gearresteerde jihadistische hacker *Irhabio07* genoemd. De reputatie die *Irhabio07* onder jihadisten opbouwde op het gebied van computervaardigheden is een indicatie voor de bescheiden staat van computervaardigheden onder jihadisten in het algemeen. Het werk van *Irhabio07* bestond voor een belangrijk deel uit het relatief eenvoudig 'kapen' van webruimte, het opzetten van websites voor publicatie van jihadistisch materiaal, en het hacken van websites met als doel eenvoudige DDoS-aanvallen uit te voeren. Hij gebruikte (en adviseerde) hiervoor standaard toolkits³³ en vormde geen bedreiging voor de veiligheid van het internet of diensten die (mede) afhankelijk zijn hiervan. Mogelijk heeft hij wel anderen geïnspireerd. Dat er sinds zijn arrestatie in 2005 geen succesvolle, naar jihadisten traceerbare cyberaanvallen zijn geweest, zegt mogelijk iets over zijn feitelijke kennis en het effect daarvan op anderen voor de kortere termijn.

In de periode sinds de fenomeenstudie zijn er ook anderszins weinig nieuwe aanwijzingen dat jihadisten meer- of sneller vaardigheden ontwikkelen. Op een jihadistisch forum zijn met name verwijzingen te vinden naar (gekraakte) software voor beveiliging van computers en data. Op het forum van een Arabischtalige, jihadistische website is een forumlid op zoek naar een instructiefilm om servers te hacken. Een ander forumlid geeft de gebruiker een verwijzing naar de internationale hackingwebsite *milworm*. Op deze laatste site kunnen goedwillende hackers hun methodes bekendmaken. Meestal worden deze lekken in software pas geopenbaard nadat producenten de kans hebben gekregen om iets aan de kwetsbaarheden te doen, maar soms al voor die tijd.³⁴ Er kunnen dus bruikbare exploits op staan. *Milworm* is een website voor kenners. Dat de website bekend is onder bepaalde jihadisten is op zich niet heel bijzonder.

³² SITE 2007a.

³³ Lachow 2009, p. 448-449.

³⁴ Techworld 2009.

Of degenen die hem kennen ook de intentie hebben om een ontwrichtende cyberaanval uit te voeren is de vraag. Het hacken van servers zal hoogstwaarschijnlijk als doel hebben om (propaganda)materiaal te hosten of om informatie te bemachtigen. Hiervan zijn in de fenomeenstudie (oudere) voorbeelden gegeven.

In algemene zin geldt echter, dat de vaardigheden van jonge ICT-specialisten, en dus van potentiële hackers, in hoog tempo blijven toenemen.³⁵ Jongeren zijn bovendien opgegroeid met ICT en zien soms onverwachte mogelijkheden, buiten de geijkte paden van bijvoorbeeld fraude. Demografisch gezien is de verwachting dat het bovenstaande ook geldt voor personen die gevoelig zijn voor jihadistische propaganda. Langs die weg zou kennis ook terecht kunnen komen bij terroristische organisaties. Voor jihadisten die willen strijden maar daartoe (fysiek) niet in de gelegenheid zijn blijft gelden dat de ‘cyberjihad’ een alternatief kan vormen. Vooral nog zijn er echter weinig aanwijzingen dat interesse of ervaring sinds de fenomeenstudie substantieel zijn toegenomen.

Geen serieuze cyberaanvallen bekend geworden

Binnen de categorieën ‘gevorderde’ en ‘complexe’ cyberaanvallen kan sprake zijn van verschillende gradaties. Een mislukte aanval gericht tegen een waterbedrijf zegt waarschijnlijk meer dan een geslaagde tegen een overheidswebsite, een enkelvoudige aanval zegt minder dan een meervoudige. Ten tijde van het onderzoek ten behoeve van de fenomeenstudie, noch in de periode daarna is een jihadistisch-terroristische cyberaanval, van welk type of gradatie dan ook, bekend geworden. Wel heeft hebben defacements uit de categorie ‘eenvoudige cyberaanvallen’ plaatsgevonden. (zie 3.3.2.2).

Inhuren capaciteiten blijft een mogelijkheid, maar geen aanwijzingen

Ten aanzien van de kennis geldt dat de leercurve voor een aanval uit de eerste twee categorieën naar een aanval uit de derde categorie exponentieel is (zie 2.2.2.1). Die exponentiële curve is te overbruggen door inhuur van kennis. Het is echter nog maar de vraag of de inhuur van kennis voldoende zou zijn: waarschijnlijk is ook inhuur van personeel voor de uitvoering nodig. Een van de conclusies in de fenomeenstudie was, dat het de vraag is of de gemiddelde hacker daadwerkelijk wil bijdragen aan terroristische activiteiten. Bezien vanuit onder andere persoonlijkheid en groeps cultuur is dit niet waarschijnlijk. Aanvullend kan worden opgevoerd dat er voor terroristische organisaties ook een risico kleeft aan het feit dat hackers op bepaalde websites graag opscheppen over hun prestaties: de kans op ontdekking wordt daarmee groter.³⁶

Op het moment van schrijven van deze actualisering is echter sprake van een wereldwijde economische crisis. Deze treft ook de ICT-sector. Nu zullen maar weinig hoogopgeleide ICT-specialisten zich voor duistere zaken laten inhuren, zeker wanneer terrorisme aan de orde is. Voorstelbaar is echter, dat zich onder dergelijke specialisten personen bevinden waar een combinatie van geldgebrek en rancune richting hun ex-werkgever en/of de maatschappij hen aanzet tot een poging om hun ‘vijanden’ te treffen met behulp van jihadisten. Ook zouden specialisten gedwongen kunnen worden tot medewerking. Gecombineerd met het gegeven dat de meeste serieuze ICT-incidenten zijn veroorzaakt door ‘insiders’, is er ten aanzien van samenwerking met individuele specialisten reden voor voorzichtigheid (zie 2.4.2).

³⁵ Achtergrondgesprek.

³⁶ Lachow 2009, p. 451.

Ook zou criminele kennis kunnen worden ingehuurd. Dit leidt echter tot een kans op vroegtijdige ontdekking bijvoorbeeld doordat de criminele groep geïnfiltrerd is. Ook is de vraag of criminele groepen willen meewerken aan een dergelijke operatie. Hoewel het hun reputatie als succesvolle onderneming kan versterken³⁷ en zij mogelijk de capaciteiten hebben om een vitale infrastructuur via het internet te gijzelen, zijn criminelen doorgaans niet opofferingsbereid. De opsporingscapaciteit die na een succesvolle terroristische cyberaanval wordt ingezet zal groot zijn. En hoewel er geen garanties op succes zijn, geldt dat ondanks alle ICT-vaardigheden van criminele groeperingen de kans op ontdekking achteraf aanzienlijk kan zijn. Zo worden professionele botnets en cybercrime-activiteiten geregeld ontmanteld. Ook zou de politie van Mumbai (India) de IP-adressen van betrokkenen bij de voorbereiding van de aanslagen aldaar eind 2008 hebben getraceerd naar individuen.³⁸ Welke succesvolle cybercrimineel zal zijn carrière in de waagschaal stellen om terroristen te helpen?

Eenzelfde redenering kan worden gevolgd voor staatssteun aan terroristen. Zelfs bij kleinschalige incidenten als kortdurende DDoS-aanvallen wordt al snel argwanend gekeken naar staten, zoals in het geval van Estland in april 2007 en de aanvallen in juli 2009 op websites van organisaties in Zuid-Korea en de VS. In beide gevallen was voor zover nu bekend geen sprake van actieve staatsbemoediging.

2.2.4 Conclusie achtergonden

Nog steeds geldt dat een cyberaanval met name past binnen de algemene strategie van al Qa’ida, aangezien een dergelijke aanval kan resulteren in grote economische schade. Specifieke uitspraken zijn echter niet gezien. Intenties bij jihadisten in de richting van een serieuze, complexe cyberaanval zijn niet bekend.

De algemene computerkennis van jihadisten en hun supporters is weliswaar groot, maar dergelijke kennis levert niet de capaciteiten op voor een serieuze cyberaanval. Ook is geen informatie bekend geworden die duidt op het inhuren van externe kennis of vaardigheden door jihadisten. Jihadisten zelf doen aan kennisverspreiding over hacking, waarbij de nadruk vooral nog lijkt te liggen bij cybersecurity. Het aantal DDoS-aanvallen en het gebruik van hacking en botnets voor cybercrime neemt toe. De drempel voor aanvallen ligt lager, terwijl de kennis erover is toegenomen. Er is enige belangstelling hiervoor onder jihadisten en er zijn acties aangekondigd, maar deze hebben geen merkbaar effect gehad. Indien jihadisten DDoS-aanvallen uitvoeren zijn het waarschijnlijk aanvallen uit de eenvoudige categorie, maar een cyberaanval uit de gevorderde categorie valt niet uit te sluiten. Een belangrijk gegeven blijft dat er sinds de fenomeenstudie (opnieuw) geen serieuze cyberaanvallen uitgevoerd door jihadisten bekend zijn geworden, terwijl andersoortige aanslagen door hen juist veelvuldig zijn gepleegd of voorbereid. Ook is geen informatie bekend geworden die duidt op het inhuren van externe kennis of vaardigheden door jihadisten, hoewel ook hiervoor geldt dat de kans dat dit gebeurt natuurlijk niet geheel valt uit te sluiten.

Wat verder opvalt is, dat vermenging van dreiging en kwetsbaarheden plaatsvindt. Concepten als *cyberwar* en hacktivisme zoals defacements worden geregeld met terrorisme verward. Hacktivisme lijkt geen opstap naar terrorisme, vooral vanwege de aanzienlijk grotere complexiteit van een serieuze cyberaanval. De angst die met

³⁷ Lachow 2009, p. 452.

³⁸ United News of India 2009.

verwarring van dreiging en kwetsbaarheden wordt gegenereerd dient vooral het doel van de terroristen. Er lijkt geen reden voor angst, maar zeker ook niet voor laksheid. Wél is er reden voor waakzaamheid, het wegnemen van kwetsbaarheden, en een blijvende voorbereiding op cyberaanvallen. Dat jihadisten zich niet of nauwelijks op deze modus operandi lijken te richten sluit niet uit dat anderen (cybercriminelen en staten) dat wel doen. Door weerstand op te bouwen groeit de weerstand tegen alle bedreigers.

2.3 Het internet als doelwit

2.3.1 Toelichting

Onze samenleving wordt steeds afhankelijker van het internet. Deze toegenomen afhankelijkheid vormt een kwetsbaarheid die jihadisten op het idee zou kunnen brengen om het internet zelf als doelwit te kiezen. Net als in de fenomeenstudie beschrijven we hier vier verschillende vormen van aanvallen op het internet: een cyberaanval via het internet, dan wel een fysieke-, elektromagnetische- of indirecte aanslag, gericht tegen (kern)knooppunten, kernfunctionaliteiten, verbindingslijnen, de elektriciteitsvoorziening, koelvoorzieningen of apparatuur om de interne klok te ijken (via bijvoorbeeld verstoring van het GPS-signaal) waardoor (de infrastructuur van) het internet niet (optimaal) kan functioneren.³⁹

2.3.2 Mogelijkheden cyberaanvallen, kwetsbaarheden en weerbaarheid

Eén van de belangrijkste conclusies van de fenomeenstudie was, dat het internet intussen zo robuust is, dat het eigenlijk ondoenlijk is om het in zijn geheel plat te leggen. In deze update wordt getoetst of die conclusie nog overeind blijft.

2.3.2.1 Cyberaanval op rootservers van 6 februari 2007 goed opgevangen

Kort na het verschijnen van de fenomeenstudie vond een grootscheepse, zeven uur durende cyberaanval plaats op de dertien DNS-rootservers plaats, die een essentiële functie hebben in het 'adresboek' van het internet. Er is geen enkele aanwijzing dat terroristen achter de aanval zaten. Een wel heel cynische mogelijke verklaring van de aanval is, dat het een reclamestunt voor de kwaliteit van een te huren botnet zou zijn geweest.⁴⁰

Deze aanval op 6 februari 2007 betrof de grootste aanval sinds 2002, toen een deel van de belangrijkste rootservers bezweek onder een aanval. Afhankelijk van waar wordt gemeten, kunnen de effecten van een verstoring of een aanval als die van februari 2007 sterk verschillen. Volgens berichtgeving in de pers werden zes rootservers getroffen, waarvan twee ernstig. Volgens experts was de techniek van de aanval van 6 februari 2007 in de basis eenvoudig. Het versterkende effect van de aanval was wel zorgelijk. Een vergelijking is te maken met een succesvolle kettingbriefactie, waarbij de brieven niet alleen doorgestuurd worden, maar ook nog eens beantwoord. Doordat rootservers verschillende technieken gebruiken (anycast, maar ook andere) is de weerstand echter groot.⁴¹

³⁹ Zie fenomeenstudie.

⁴⁰ ICANN 2007, p.5.

⁴¹ Deze twee zouden de enige servers zijn die niet van een relatief nieuwe techniek genaamd Anycast gebruik maakten. Dit is een routingsschema voor netwerken waarbij datapakketjes gericht op een bepaald adres naar fysiek verschillende locaties gestuurd kunnen worden. Op deze manier kan een grote hoeveelheid verkeer over verschillende geografisch verspreide servers worden verdeeld. Een bijkomend voordeel is dat als een server in het geval van bijvoorbeeld een aardbeving uitvalt, de dienstverlening niet in gevaar komt. Door de anycast-technologie is het moeilijker geworden om rootservers plat te leggen, waarbij moet worden opgemerkt dat daarmee de

Ten aanzien van de weerstand tegen cyberaanvallen geldt ook dat het internet een netwerk van netwerken is. De diversiteit daarbinnen neemt nog steeds verder toe, en niet alleen ten aanzien van rootservers, waardoor aanvallen nooit alle delen van het internet in dezelfde mate kunnen treffen.⁴² Anderzijds waarschuwt Verisign, de beheerder van de .com sites, dat criminele netwerken steeds professioneler worden, dat zij hiermee de infrastructuur van het internet bedreigen en dat aanvallen tot nu toe door het vergroten van de bandbreedte konden worden opgevangen, maar dat daar ooit een eind aan komt.⁴³

2.3.2.2 Cyberaanval op Estland succesvol door beperkte infrastructuur

In mei 2007 kreeg Estland te maken met een cyberaanval. Deze aanval was primair lokaal gericht en was een reactie op het verplaatsen van een oorlogsmonument. Rusland werd ervan verdacht achter de aanval te zitten en er zou sprake zijn van 'cyberwar'. Volgens de deelnemers aan de expertmeeting was hier sprake van een hype. Estland is een zeer sterk op internet gericht land, maar het ontbreekt aan de bijbehorende infrastructuur met redundantie en voldoende datatransportcapaciteit.⁴⁴ Daardoor konden de effecten van de gebruikte botnets zo groot en langdurig zijn. Een vergelijkbare aanval zou in Nederland waarschijnlijk weinig effect hebben. Wel is het mogelijk om voor kortere tijd overheidswebsites onbereikbaar te maken.

2.3.2.3 Infrastructuur internet kwetsbaar

De infrastructuur van het internet blijkt kwetsbaar. GOVCERT.NL spreekt daarbij van 'barsten in het fundament van het internet'.⁴⁵ In enkele communicatieprotocollen (zoals TCP, DNS en BGP: de 'talen' die computers en netwerken gebruiken)⁴⁶ blijken kwetsbaarheden te zitten die ervoor zorgen dat de fundamente van het internet niet aansluiten bij de eisen die het moderne gebruik eraan stelt. Volgens GOVCERT.NL is onderhoud of reparatie aan het internet dringend nodig, maar niet eenvoudig vanwege de omvang van het internet en de versnipperde verantwoordelijkheden.⁴⁷ De kwetsbaarheid van DNS kan worden aangepakt door de invoering van DNSSEC (secure DNS).⁴⁸

2.3.3 Intentie van jihadisten bij cyberaanval

De fenomeenstudie beschreef de intenties van jihadisten alsmede de voor- en nadelen voor hen om het internet te treffen. Deze lijken nog steeds valide. Een cyberaanval gericht tegen de infrastructuur van het internet past binnen de algemene strategie van al Qa'ida. Een cyberaanval kan in potentie resulteren in grote economische schade. Een cyberaanval sluit goed aan bij een asymmetrische strijd. De combinatie van het onbekende van cyberspace en terrorisme vergroot de psychologische angst. Er is geen sprake van eigen

problemen wat verlegd zijn naar andere lagen van het internet. De rootservers die andere technieken gebruiken dragen echter niet aan dit verplaatsingseffect bij. Bij serieuze problemen kan verkeer blijven doorgaan door ip-adressen zélf in te geven in de browser. Daarmee wordt de DNS-server omzeild. In de praktijk is dat voor de gemiddelde gebruiker geen serieuze optie. Bronnen: Tweakers 2007 en Expertmeeting 2009.

⁴² Expertmeeting 2009.

⁴³ Automatiseringsgids 2007.

⁴⁴ Expertmeeting 2009.

⁴⁵ GOVCERT 2009.

⁴⁶ Alle computers hebben een uniek IP-adres. DNS koppelt namen aan IP-adressen. Daardoor kun je www.nctb.nl intoetsen, waarna DNS het vertaalt naar het IP-adres. Met behulp van BGP wordt de route bepaald via welke netwerken je van computer A naar computer B reist. TCP verzorgt de daadwerkelijke verbinding tussen twee computers (bron GOVCERT.NL).

⁴⁷ GOVCERT 2009.

⁴⁸ Automatiseringsgids 2009a.

verliezen, zoals bij een zelfmoordaanslag. Computers, internettoegang en hacking-tools zijn 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 (relatief) anonieme karakter bemoeilijkt de ontdekking en arrestatie van de aanslagpleger. Een cyberaanval is laagdrempeliger dan een gewone aanslag en zeker laagdrempeliger dan een zelfmoordaanslag.

Anderzijds is de werkelijke schade slecht voorspelbaar. Een cyberaanval tegen het internet levert waarschijnlijk geen spectaculaire beelden op van rokende puinhopen, doden en gewonden. Een succesvolle 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. Anonimiteit op het internet is verder relatief. Een cyberaanval past niet bij het streven naar het martelaarschap van jihadisten. De hoge weerstand maakt het geen aantrekkelijk domein.

Ook een ander in de fenomeenstudie benoemd argument tegen een jihadistische cyberaanval is nog steeds valide, maar verdient nuancering. Jihadisten gebruiken het internet volop voor andere doeleinden (zie Hoofdstuk 3). Met het verstoren van het internet als geheel schiet men zich in de eigen voet: of dit nu is vanwege het feit dat zij in een dergelijke situatie ook zelf geen gebruik van het internet kunnen maken, laat staan de cyberaanval via het internet claimen, dan wel omdat een terroristische cyberaanval hoogstwaarschijnlijk zou leiden tot monitoring, controle en regulering door overheden van het internet en internetgebruik. Mogelijk trekken zij zich van het tweede gedeelte van de bovenstaande argumentatie meer aan dan van het eerste.

2.3.4 Capaciteiten cyberaanval bij jihadisten

In paragraaf 2.2.2 zijn twee methoden voor een cyberaanval beschreven, namelijk massale overbelastingaanvallen en gerichte hacking. Voor een aanval tegen het internet is de eerste methode de meest voor de hand liggende, zeker wanneer men daarbij gebruikmaakt van de kwetsbaarheden in de structuur van het internet (zie 2.3.2.3). Een dergelijke aanval op het internet zelf vergt de nodige voorbereiding, maar geen overdreven diepgaande kennis: met voldoende geld en inspanning kan een enorm botnet voor dit doel worden ingezet. De slagingskans is echter gering, gelet op de weerstand van het internet. Wanneer jihadisten zouden (kunnen) infiltreren binnen de internetbranche, dan zou dat de mogelijkheden voor een cyberaanval doen toenemen. Deze optie is beschreven in de fenomeenstudie. Daar werd aangegeven dat zij - om echt effect te sorteren - bij de grote partijen moeten infiltreren. Net als in 2006 wordt aangegeven dat dit weinig kans van slagen lijkt te hebben, omdat de technici die over de juiste kennis beschikken erg close zijn en elkaar goed kennen. Natuurlijk is het wel van belang dat verdacht gedrag vroegtijdig wordt ontdekt. Weliswaar zal vrij snel traceerbaar zijn wie iets op zijn geweten heeft, maar het kwaad is dan al geschied. Ook is de telecommarkt een groeimarkt waardoor de kwetsbaarheid ten aanzien van infiltratie toeneemt. Meer medewerkers betekent tevens meer kans op succesvolle *social engineering*.⁴⁹

2.3.5 Gevolgen cyberaanval

In de fenomeenstudie zijn de gevolgen beschreven van een succesvolle cyberaanval gericht tegen het internet. Daarbij werd aangegeven dat de gevolgen van het wegvallen van het internet groot zouden zijn in economische zin, maar dat de kans op menselijke slachtoffers klein is, behalve wellicht bij de uitval van

⁴⁹ Expertmeeting 2006 en 2009.

telecommunicatie indien noodnummers niet kunnen worden bereikt. Intussen is het gebruik van het internet verder toegenomen en blijft de afhankelijkheid van het internet stijgen. Stond internettelefonie enige jaren geleden nog in de kinderschoenen, nu is het aantal abonnementen groot.⁵⁰ Daarnaast zijn er 'slimme energiemeters' beschikbaar, komt er een elektronisch patiëntendossier en neemt benutting van het internet door vitale sectoren wereldwijd steeds verder toe. Dit creëert allerlei koppelingen tussen systemen of infrastructuren. Daardoor ontstaan nieuwe kwetsbaarheden die nu nog niet onderkend zijn. De toegenomen afhankelijkheid van internet maakt het waarschijnlijk dat uitval (ook relatief kortdurende) meer maatschappelijke impact zal hebben. Net zoals bij een plotselinge uitval van elektriciteit zal blijken dat in het moderne leven veel aan internet gekoppeld is. Een recente inschatting van de wereldwijde kosten van een grootschalige uitval van de *critical information infrastructure* is 250 miljard dollar.⁵¹ Beschikbaarheid is daarmee van groot belang, en uitval kan vertrouwen schaden. Consumenten vertrouwen echter nog steeds het digitale betalingsverkeer ondanks de nodige incidenten en het risico slachtoffer te worden van cybercrime. Dit vertrouwen lijkt stand te houden zolang bijvoorbeeld banken de ontstane schade vergoeden. Daarnaast blijkt uit diverse sociologische studies dat consumenten erop vertrouwen dat de instituties de problemen wel weer oplossen.⁵²

De verwachting was en is nog steeds dat eventuele uitval van het internet door een cyberaanval van relatief korte duur zal zijn.⁵³ Technische storingen komen met enige regelmaat voor en veroorzaken wel overlast maar geen paniek. Een logische redenering is dan, dat de effecten al met al niet opwegen tegen de inspanningen die ervoor nodig zijn om een dergelijke aanval te laten slagen. Wél is voorstelbaar dat een moedwillige verstoring, ook al is die beperkt in omvang en tijd, die door jihadisten wordt veroorzaakt, verhoudingsgewijs meer onrust zal veroorzaken dan een reguliere technische storing: een dergelijk incident zal waarschijnlijk anders worden beleefd bij burgers, media en politiek. Ook een beperkte verstoring zal dus als 'succes' op het conto van jihadisten geschreven kunnen worden.

2.3.6 Beoordeling dreiging cyberaanvallen door jihadisten

Enorme botnets zijn nodig om het internet zelf aan te vallen. Botnets nemen in aantal en omvang toe, terwijl de prijs ervan daalt. Daarnaast is de kwetsbaarheid van het internet sinds de fenomeenstudie toegenomen. Dit neemt niet weg dat de weerstand groot blijft. Dat een aanval op de rootservers van 6 februari 2007 zonder veel problemen is opgevangen en dat daarna geen andere (merkbare) pogingen lijken te zijn ondernomen, bevestigt de capaciteit en mate van redundantie van het internet. Daarnaast geldt ten aanzien van de weerstand dat het internet een netwerk van netwerken is. De diversiteit daarbinnen neemt nog steeds verder toe, waardoor aanvallen nooit alle delen van het internet in dezelfde mate kunnen treffen. Het feit dat in 2007, weliswaar niet door terroristen, toch weer geprobeerd is het internet ernstig te verstoren, geeft aan dat een dergelijke actie nooit helemaal valt uit te sluiten.

Er zijn bij de NCTb geen intenties van jihadisten bekend met betrekking tot cyberaanvallen op het internet, ondanks dat de kwetsbaarheid van het internet is toegenomen en onze maatschappij er steeds afhankelijker van wordt. Er zijn ook geen aanwijzingen dat jihadisten beschikken over voldoende kennis en capaciteiten om succesvol misbruik te maken van de (toegenomen) kwetsbaarheid van het internet voor cyberaanvallen,

⁵⁰ Televisie via het internet wordt echter nog steeds betrekkelijk kleinschalig gebruikt.

⁵¹ Global Risks 2008.

⁵² Expertmeeting 2009.

⁵³ Expertmeeting 2009.

hoewel kennis natuurlijk wel valt op te bouwen. Insiderkennis lijkt echter nog steeds noodzakelijk voor een echt effectieve aanval.

Een grootschalige, succesvolle jihadistische cyberaanval gericht tegen het internet is al met al niet waarschijnlijk. Wel moet er rekening mee worden gehouden dat ook een kleinschalige, moedwillige verstoring door jihadisten, hetgeen niet geheel valt uit te sluiten, voor verhoudingsgewijs veel consternatie zal zorgen.

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 aanslag met een elektromagnetische puls, en indirecte aanvallen - zoals aanslagen gericht tegen de elektriciteitssector of telecomsector - waardoor (de infrastructuur van) het internet niet kan functioneren.

2.3.7.1 Mogelijkheden, kwetsbaarheden en weerbaarheid

In de fenomeenstudie zijn enkele kwetsbare plekken en onderdelen in Nederland voor dit type aanslagen beschreven, zoals kernknooppunten, kernfunctionaliteiten en verbindinglijnen die van belang zijn voor het internet in Nederland, maar soms ook voor het Europese of zelfs het mondiale internet. SIBN beheert het ‘.nl-domein’ in Nederland via servers waarvan een aantal zich in Nederland bevindt en de Amsterdam Internet Exchange (AMS-IX), die een mondiale functie vervult, vormt een belangrijk knooppunt. De AMS-IX is een soort rotonde waar vele wegen op uitkomen en die onderlinge verbinding tussen netwerken mogelijk maakt. Er is echter geen sprake van een verkeersleiding en de AMS-IX beheert zelf geen gegevens. Providers en andere partijen die gebruik maken van de rotonde zijn zelf verantwoordelijk voor de routing van hun data. Deze kunnen dus ook buiten de rotonde om verzonden worden. Het onderling tussen netwerken uitgewisselde verkeer zal aanzienlijke hinder kunnen ondervinden indien de AMS-IX uitvalt, maar al snel zal automatisch een omleiding van het dataverkeer plaatsvinden. Dit zal mogelijk wel ten koste gaan van de snelheid. Als meer exchanges uitvallen ontstaan capaciteitsproblemen, hoewel veel netwerkverkeer via andere verbindingen⁵⁴ afgehandeld zal blijven worden. Als ook dergelijke verbindingen uitvallen zal sprake zijn van een ingrijpende storing.

De weerstand is echter groot. Dit blijkt onder andere uit een artikel over het in Amsterdam gevestigde *Reken- en netwerkcentrum SARA*.⁵⁵

De apparatuur die wordt gebruikt op de (kern-)knooppunten ten behoeve van de kernfunctionaliteiten is sterk afhankelijk van stroom, is gevoelig voor water en elektromagnetische straling en vereist veel koeling. Daarbij is sprake van een concentratie in het Westen van het land. Gezien de geografische ligging van Nederland komen veel transatlantische kabelverbindingen binnen in Nederland en verbindt Nederland met kabels Europese landen met elkaar. Dat dergelijke verbindingen kwetsbaar zijn bleek uit een aantal incidenten in de Middellandse Zee en de Perzische Golf die in januari 2008 kort op elkaar volgden, en die voor specifieke regio's aanzienlijke gevolgen hadden. Hierdoor leek kwade opzet in het spel. Twee incidenten

⁵⁴ De bij een IX aangesloten partijen besluiten zelf om via hun ip-netwerken onderling bilateraal en op vrijwillige basis verkeer met elkaar uit te wisselen. Deze vrijwilligheid vertaalt zich dan ook in het feit dat de uitwisseling van het verkeer niet alleen via een IX plaatsvindt maar ook via private verbindingen (private interconnects) en door middel van het inkopen van transit bij zogenaamde carriers. De keuzeafweging voor deze alternatieven en de verdeling daarbinnen (redundantie) ligt bij de individuele partij die haar netwerk wil koppelen aan andere netwerken.

⁵⁵ Spangers 2007.

werden waarschijnlijk veroorzaakt door een combinatie van corrosie en beweging van de zeebodem (hetgeen niet ongebruikelijk schijnt te zijn), een andere kabel werd beschadigd door een anker van een verlaten schip en tenslotte moest een verbindinglijn worden afgesloten door problemen met de energievoorziening in een station waar de kabel aan land kwam.⁵⁶ De effecten waren beperkt, zeker mondiaal, en hebben het vertrouwen niet beperkt. Soms worden moedwillig kabels vernield uit economische motieven of worden kabels gestolen voor verkoop van materiaal.⁵⁷

Bedrijven, al dan niet in de vitale sectoren, hebben te maken met bestaande en nieuwe risicofactoren. Outsourcing van taken levert kwetsbaarheden op. Outsourcing is ‘extending the layer of trust’. Een bedrijf dat voor verschillende klanten werkt, heeft al snel veel kennis en een sterke positie, en is aantrekkelijk voor infiltranten. *Supply chain security*, mede in verband met het gevaar van namaak-hardware, is eveneens een punt van aandacht voor bedrijven. De opbouw van afweermechanismen neemt echter ook steeds toe. Zo is er een betere screening van medewerkers en begeleiding van medewerkers die met ontslag gaan.⁵⁸ Overheden beseffen ook steeds meer het belang van internetexchanges en ICT-centers.

2.3.7.2 Intentie andersoortige aanslagen

Het enige voorbeeld van een hierboven beschreven type aanslag - in dit geval aanslagplan of mogelijk slechts een intentie - is afkomstig uit het Verenigd Koninkrijk. Door een groot telecomknooppunt in Londen (Telehouse) van binnenuit, na infiltratie, op te blazen, zouden jihadisten het Britse internet hebben willen treffen. Dit complot zou volgens Britse media door Scotland Yard zijn ontdekt in aangetroffen bestanden tijdens aanhoudingen eind 2006.⁵⁹

Hoewel het nieuw is dat er mogelijk serieuze plannen bestaan voor een dergelijke aanval, blijft de vraag gerechtvaardigd of jihadisten hun capaciteit en materialen aan een dergelijk doelwit willen spenderen. Wel geeft dit voorbeeld opnieuw aan dat jihadisten nieuwe werkwijzen en doelwitten overwegen, zich ook richten op economische doelwitten, en zich kennelijk bewust zijn van het nut of zelfs de noodzaak van infiltratie.

Online-jihadisten speelden in op de incidenten rond de kabelbreuken genoemd onder 2.3.7.1. Via een webforum attendeerden zij hun broeders op deze kwetsbaarheden, inclusief een beschrijving van glasvezelkabels, FLAG (Fiberoptic Link Around the Globe) kabelroutes, gevolgen, de wijze waarop reparatie zal plaatsvinden en de modus operandi voor de aanslag: duikers die de kabels handmatig doorknippen.⁶⁰ Voor dergelijke berichten van ‘supporters’ op jihadistische fora geldt echter, dat dit weinig tot niets zegt over de intenties en capaciteiten van feitelijke jihadistische groeperingen. Wel kan het personen inspireren.

Over intenties voor het gebruik van elektromagnetische aanvallen richting de internetinfrastructuur is niets bekend geworden.⁶¹ Wel speelde in augustus 2009 in de VS de angst voor EMP-/stralingswapens op. Het Amerikaanse leger zou intussen een wapen hebben dat zo krachtig is, dat het op drie kilometer afstand

⁵⁶ Wolfe 2008.

⁵⁷ Expertmeeting 2009.

⁵⁸ Expertmeeting 2009.

⁵⁹ Leppard 2007.

⁶⁰ SITE 2008a.

⁶¹ Dit neemt niet weg dat de NCTb een dergelijke dreiging wel verwerkt heeft in het scenario voor een oefening met één van de sectoren binnen het Alerteringssysteem Terrorisbestrijding.

een computer kan uitschakelen. Voor het transport is een vrachtwagen nodig, maar, vermoedelijk een minder krachtige versie, zou ook door een soldaat kunnen worden vervoerd. Het Amerikaanse *Department of Energy* schat echter in dat de kans op een EMP-aanval vele malen kleiner is dan een aanval in cyberspace.⁶² Daarbij wordt met een EMP-aanval overigens bedoeld op een grootschalige aanval met *high altitude detonation* van nucleaire wapens. Dat is ten aanzien van terrorisme niet aan de orde, en indien zij al over dergelijke wapens zouden gaan beschikken dan zal uitschakeling van het internet niet het eerste of belangrijkste doel zijn. In het kader van terrorisme zal - in de sfeer van voorstelbaarheid - eerder sprake zijn van een kleine, gerichte aanslag met een compacter (non-nucleair) NNEMP-wapen. De benodigde technieken worden steeds breder bekend en raken steeds toegankelijker, hetgeen een risico inhoudt.⁶³

Ook ten aanzien van overige manieren om het internet uit te schakelen zijn geen intenties bekend.

In de fenomeenstudie werd aangegeven dat andersoortige aanvallen - zoals in de voorgaande alinea's genoemd - niet zo goedkoop of laagdrempelig zijn als cyberaanvallen, en dat fysieke voorbereidingshandelingen nodig zijn, hetgeen sporen achterlaat en de terrorist kwetsbaar maakt. Deze beschrijving is ook in 2009 valide. Daarnaast gold, en geldt, dat het zelfs voor een groep wel heel veel inspanning zou vergen om bijvoorbeeld op vele kritieke plaatsen kabelbreuken te veroorzaken, verschillende internet-exchanges op te blazen of anderszins onklaar te maken.

Wel is het nog steeds zo, dat dit type aanslagen tot spectaculaire beelden kan leiden, die dan mogelijk wel via andere mediakanalen dan het internet getoond moeten worden. De (zichtbare) gevolgen van een dergelijke aanslag kunnen onrust veroorzaken en indirect (tijdelijk) de economie treffen. Vanwege de afhankelijkheid van de economie van het internet sluit een dergelijke aanslag zeker aan op de strategie van jihadisten.⁶⁴ Het is echter onverminderd de vraag of terroristen dat een voldoende terroristisch effect vinden. Vanuit die optiek ligt het voor de hand om een strategie te veronderstellen waarbij er meervoudige aanslagen of een mix van aanslagen zouden worden uitgevoerd, waaronder één of meer tegen het internet. Een aanslag zoals in Mumbai eind november 2008 leent zich voor een dergelijk scenario en is daarmee niet onvoorstelbaar. Wel vergroot een complexere aanslag de kans op vroegtijdige ontdekking.

2.3.7.3 Capaciteiten

Informatie over belangrijke knooppunten zijn betrekkelijk eenvoudig toegankelijk. De benodigde kennis en materialen voor de inzet van (zelfgemaakte) explosieven zijn eveneens redelijk toegankelijk. Zoals in de fenomeenstudie aangegeven is er op het internet voldoende trainingsmateriaal voor zelfgemaakte explosieven aanwezig. Voor handboeken over zelfgemaakte explosieven geldt dat deze het ook voor mensen zonder de juiste ervaring of het benodigde opleidingsniveau eenvoudiger maken om te experimenteren en explosieven te maken.

Ook voor elektromagnetische aanslagen en apparatuur zijn handleidingen en studiemateriaal aanwezig en de beschikbaarheid en toegankelijkheid ervan zou toenemen.⁶⁵ Het bereiken van voldoende vermogen

⁶² EETimes 2009.

⁶³ Graham 2004. Uit dit onderzoeksrapport blijkt, dat hardening van apparatuur tegen EMP overzichtelijke (1-3%) extra kosten met zich meebrengt, wanneer dit meegenomen wordt in het ontwerp en de productie van nieuwe apparatuur.

⁶⁴ Mede gebaseerd op expertmeeting 2006.

⁶⁵ Automatiseringsgids 2009b.

voor een aanslageffect lijkt echter nog steeds niet eenvoudig. Het is voor zover bekend dan ook nog niet door terroristen toegepast. Voor een gerichte en grote elektromagnetische aanval is meer kennis en zijn meer middelen nodig dan nu beschikbaar is.

De mate waarin de telecomsector afhankelijk is van elektriciteit moet algemeen bekend worden verondersteld. Of een aanslag op de energiesector, zo die al plaatsvindt, onderkend kan worden als feitelijk gericht op telecommunicatie lijkt niet waarschijnlijk, tenzij jihadisten achteraf expliciete claims hieromtrent publiceren. Een gerichte aanslag op de energievoorziening van een belangrijk knooppunt zal wel als zodanig gezien kunnen worden. Een dergelijke aanslag is wel weer eenvoudiger lokaal op te vangen.

2.3.7.4 Gevolgen

De gevolgen van andersoortige aanslagen op de infrastructuur van het internet zijn soortgelijk aan die van cyberaanvallen. Indien explosieven worden gebruikt kunnen echter wel degelijk rechtstreeks doden en gewonden vallen, zoals medewerkers van het betreffende bedrijf en eventuele omstanders. Een belangrijk verschil met cyberaanvallen is tevens dat schade veroorzaakt door dit type aanvallen een grotere hersteltijd vergt.⁶⁶ Vooral het veroorzaken van fysieke schade op kernpunten (tijdens het conflict in Georgië (medio 2008) zijn bij ISP's routers opgeblazen) kan daarom effectief zijn. Een kapot gebouw en serverapparatuur laat zich niet zo snel vervangen of 'resetten', zoals bij een cyberaanval. Anderzijds heeft de casus rond de brand in de Universiteit Twente eind 2002 uitgewezen dat partijen elkaar snel voorzien van apparatuur. Uit concurrentieoverwegingen zal dit mogelijk niet in alle gevallen gebeuren.⁶⁷ Een inschatting van gevolgen van sabotage van kabels is te geven aan de hand van een incident in de VS, waar een tiental vernielde glasvezelkabels op vier verschillende locaties tot een zeventien uur durende storing leidde.⁶⁸ Zoals ook in de fenomeenstudie aangegeven geldt nog steeds dat dienstverleners zoals de AMS-IX veelal vanuit diverse co-locaties werken, waardoor zelfs bij uitval de effecten betrekkelijk zullen zijn voor die specifieke dienstverlener. De redundantie neemt toe en de zichtbaarheid neemt af. Dit beschermt niet alleen tegen DDoS-aanvallen, maar ook tegen fysieke aanvallen.

2.3.8 Beoordeling dreiging andersoortige aanslagen

Het internet uitschakelen via andersoortige aanslagen is niet mogelijk, tenzij terroristen de beschikking krijgen over nucleaire wapens die op grote hoogte tot ontploffing worden gebracht en een EMP veroorzaken. Indien zij al over dergelijke wapens zouden gaan beschikken dan zal uitschakeling van het internet niet hun eerste of belangrijkste doel zijn.

Er zijn enige kwetsbare punten in het internet voor gerichte aanslagen zoals exchanges en kabels. Echter, binnen het internet is grote redundantie, er zijn vele maatregelen getroffen om de kwetsbaarheden te beperken en het bewustzijn omtrent kwetsbaarheden is toegenomen. Wanneer het internet via bom-aanslagen of door uitschakeling van elektriciteit zou worden getroffen, dan zijn de gevolgen relatief kleinschalig, blijven deze lokaal of regionaal (tenzij het een landelijke stroomuitval betreft) en zijn ze goed op te vangen. De hersteltijd na een bomaanslag is wel (aanzienlijk) langer dan in het geval van een cyberaanval.

⁶⁶ Expertmeeting 2009.

⁶⁷ Expertmeeting 2009.

⁶⁸ Webwereld 2009. De eerste doorgehakte kabel verzorgde het AT&T-netwerk van vaste telefoonlijnen en het achterliggende netwerk voor mobiele telefoons. Daarna werd een andere glasvezelkabel vernield waardoor een telecom-provider (Sprint) en een datacenter werden getroffen. Aanbieders van mobiele telecom zoals Verizon en Nextel kregen ook last van de sabotage aangezien zij de lijnen van AT&T en Sprint benutten.

Ook kunnen er doden en gewonden vallen. Hoewel terroristen gewend zijn te werken met explosieven, ligt het toch niet voor de hand dat jihadisten kiezen voor een aanval met explosieven tegen het internet: andere doelwitten zijn aantrekkelijker en de kosten wegen waarschijnlijk niet op tegen de baten.

In het kader van deze afweging is het bericht over een mogelijke bomaanslag op de belangrijkste Britse telecom-/internetlocatie van belang. Het past weliswaar in het beeld van de vele complotten en netwerken, al dan niet door (kern) al Qa'ida geïnspireerd, waarmee het Verenigd Koninkrijk in ieder geval op dat moment geconfronteerd werd, en mogelijk zou het idee voor de aanslag nooit gematerialiseerd zijn, maar in ieder geval geeft die zaak een indicatie van mogelijke intenties bij jihadisten, alsmede onderkenning van het risico van infiltratie. Zoals gezegd in 2.3.4 is de sector zich van dit risico bewust.

Al met al moet worden geconcludeerd dat een andersoortige jihadistische aanslag gericht tegen het internet niet waarschijnlijk is, maar wel waarschijnlijker dan een succesvolle cyberaanval gericht tegen het internet. Net als ten tijde van de fenomeenstudie geldt ook nu dat een dergelijke aanslag het meest voorstelbaar is in combinatie met andere aanslagen, met als doel de chaos te vergroten. De aanslagen in Mumbai eind november 2008 hebben aangetoond dat een mix van doelwitten (nog steeds) tot het speelveld van jihadisten behoort.

2.4 Het internet als wapen

2.4.1 Toelichting

In de fenomeenstudie zijn met name de digitale kwetsbaarheden van vitale bedrijven aan de orde geweest. Daarbij werd bedoeld op een vijandelijke overname of manipulatie via het internet van de besturing van bijvoorbeeld een kerncentrale, dan wel het voor langere duur onbruikbaar (en daarmee onbetrouwbaar) maken van essentiële (bijvoorbeeld financiële) diensten: internet als wapen.⁶⁹

2.4.2 Mogelijkheden internet als wapen, kwetsbaarheden en weerbaarheid

De fenomeenstudie ging in op de rol van procescontrolesystemen als SCADA in vitale sectoren. SCADA⁷⁰ (*Supervisory Control And Data Acquisition*) is een generieke term voor procescontrolesystemen die worden gebruikt door veel bedrijfssectoren, waaronder de transportsector, de chemische industrie, water- en energiebedrijven. Een SCADA-systeem monitort (*view*) en beheert (*control*) complete installaties, waarbij sturing of uitlezen van gegevens vaak op afstand plaatsvindt. Eenvoudig gezegd: het controleert of alle kleppen goed staan, krijgt signalen binnen van meetpunten en kan aan de hand daarvan bijsturen. Daardoor is SCADA aantrekkelijk voor gerichte hacking: de eigenlijke beheerder krijgt dan te maken met een *loss of view*, waardoor hij niet langer ziet wat het systeem doet. Ook kan een *loss of control* optreden, waardoor de operator de controle over het systeem kwijt is, hetgeen kan betekenen dat een ongeautoriseerde derde de installatie bestuurt. Voor de aanval kan dat een doel op zich zijn, maar het zou ook

⁶⁹ Ook hierbij geldt dat cyberaanvallen die dienen om een politiek statement te maken (het zogeheten hacktivism) niet worden meegenomen omdat noch de intentie, noch de gevolgen binnen de definitie van terrorisme vallen. Verder is van belang om een scherp onderscheid te (blijven) maken met het gebruik van het internet als middel. Het verspreiden van informatie via het internet over de locaties van kerncentrales of het dreigen met een aanslag als vorm van angst aanjagen vallen onder internet als middel, niet als wapen.

⁷⁰ Eerdere publicaties onder verantwoordelijkheid van bijvoorbeeld het ministerie van Economische Zaken waren hier eveneens op ingegaan.

gebruikt kunnen worden als drukmiddel voor afpersing. Over een dergelijk geval, waarschijnlijk met hulp van binnenuit, richting enkele vitale sectoren buiten de VS heeft de CIA een bericht laten uitgaan.⁷¹ Hiermee zou dergelijke afpersing zich verbreden, omdat tot nu toe met name online gok- en pornobedrijven hiermee te maken hadden.⁷² Zoals altijd is bij dergelijke berichten de vraag of daadwerkelijk het procescontrole netwerk gegijzeld is of alleen het administratieve gedeelte van bijvoorbeeld een gasbedrijf. Dit laatste is eveneens vervelend, maar van een andere orde en zou geen terroristisch effect hebben. Ten aanzien van het op afstand bedienen van procescontrolesystemen geldt dat de kwetsbaarheid van draadloze verbindingen verder is toegenomen vanwege het gedeeltelijk breken van de WPA-versleuteling.⁷³

Er zijn tal van incidenten en kwetsbaarheden sinds eind 2006 bekend geworden. Zo werd in de VS - weliswaar in een testomgeving - brand veroorzaakt door een cyberaanval op het elektriciteitsnetwerk: een turbine raakte hierdoor dusdanig overbelast dat hij uiteindelijk afsloeg.⁷⁴ Opvallend is dat de incidenten vaak aan *insiders* gerelateerd zijn. In de fenomeenstudie werd in dit kader al het bekende incident in Australië in 2001 genoemd, waar een boze ex-medewerker van een waterzuiveringsbedrijf ervoor zorgde dat miljoenen liters ongezuiverd water vrijkwam.⁷⁵ De kwetsbaarheid van procescontrolesystemen zoals SCADA is deels te verklaren uit de verschillen met reguliere ICT. Zo dient een SCADA-systeem 24/7 operationeel te zijn. De voor de hand liggende standaardoplossing bij problemen in ICT-kantooromgevingen, een zogeheten reboot (herstart) is bijvoorbeeld geen optie.⁷⁶ Verder zou sprake zijn van 'active and sophisticated chatter' in de (algemene) hacker community, waar kennis, ervaring en exploits worden uitgewisseld.⁷⁷ Wel verkleint de heterogeniteit van systemen de kans op breed ingezette, succesvolle aanslagen.⁷⁸ Daar staat echter weer tegenover dat steeds meer procescontrolesystemen op standaard besturingssystemen werken en er een beperkt aantal leveranciers van procescontrolesoftware is.

Voor de Nederlandse situatie geldt, dat veel vitale sectoren zich bewust zijn van kwetsbaarheden en mogelijke gevolgen, en daar ook naar handelen. De overheid brengt op dat punt organisaties en kennis bij elkaar. Mogelijk speelt de markt in op deze ontwikkeling en biedt dat instrumenten voor versterking van de verdediging. Anderzijds zijn er bepaalde incidenten en penetratietests die aangeven dat het kwaadwillenden soms wel erg makkelijk wordt gemaakt, en dat beveiligingsmaatregelen zich op drie verschillende aspecten dienen te richten: technische (bijvoorbeeld firewalls en logging), procesgeïntendeerde (bijvoorbeeld autorisaties), en medewerkergeïntendeerde (bijvoorbeeld het verhogen van de weerstand tegen *social engineering*).⁷⁹

2.4.3 Intentie jihadisten ten aanzien van 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. Voordelen zijn: in potentie grote economische schade, aansluiting bij het concept van een

⁷¹ Computerworld 2008 en SANS 2008. Latere berichten spreken over Brazilië als mogelijk slachtoffer.

⁷² Buxbaum 2008.

⁷³ ZDNet 2009.

⁷⁴ Nationalterroralert 2007.

⁷⁵ Kravets 2009.

⁷⁶ Cheong 2008.

⁷⁷ Forbes 2007.

⁷⁸ Expertmeeting 2009 en Lachow 2009, p.453.

⁷⁹ Zie ook: Lachow 2009, p.445.

asymmetrische strijd, veroorzaken van cyberfear, benutting van aanwezige kwetsbaarheden, computers, internettoegang en hacking-tools zijn voor iedereen bereikbaar, de mogelijkheid om op afstand opereren, (relatieve) anonimiteit en (relatief) lage pakkans, laagdrempeligheid (in vergelijking met een (zelfmoord-) aanslag, en geen eigen verliezen. Met een aanval tegen de vitale infrastructuur snijden jihadisten zichzelf bovendien niet in de vingers, zoals bij een aanval tegen het internet. Nadelen zijn de complexiteit van een serieuze cyberaanval en onzekerheid over zowel de slagingskans als de gevolgen van een aanval. Ook de zichtbaarheid van de gevolgen is mogelijk minder direct dan bij een reguliere bomaanslag.

In de fenomeenstudie werd aangegeven dat discussie (*chatter*) in jihadistische webfora over SCADA zou toenemen. In de algemene paragraaf 2.2.3 zijn belangstelling en vaardigheden van terroristen beschreven. Van een toename van belangstelling of 'chatter' is de afgelopen drie jaar weinig te merken geweest.⁸⁰ Wel verscheen eind 2009 een bericht dat de FBI personen onderzoekt die mogelijk banden hebben met al Qa'ida, dan wel het gedachtegoed van deze organisatie aanhangen, en zich bewust zouden zijn van de kwetsbaarheid van de vitale infrastructuur in de VS voor cyberaanvallen en deze ook hebben besproken.⁸¹ Dit lijkt echter een uitzondering te zijn.

Veel jihadistische websites hebben subfora over 'techniek' en 'internet'. Deze bestaan in veel gevallen grotendeels uit topics waar gekraakte besturingssystemen, softwarepakketten, andere programma's/tools (waaronder security- en encryptiegerelateerde tools) en serienummers worden aangeboden en besproken. Illegale software is wat dat betreft net zo bekend bij (supporters van) jihadisten als bij anderen, maar dit vormt nauwelijks een indicatie voor andersoortige intenties of capaciteiten. Wellicht zijn er andere lokaties op het internet of daarbuiten waar het onderwerp sterk leeft. Hierover is echter weinig bekend geworden. Een uitzondering hierop vormde een bericht dat verscheen op het, sinds september 2008 niet meer beschikbare, jihadistische al-Ekhlaas forum, waar veel suggesties voor aanslagen werden gedaan (zoals de eerder genoemde mogelijkheden voor aanslagen op kabels, zie 2.3.7.1). Daar werd door een forumlid uitgebreid verslag gedaan van een openbaar gemaakte penetratietest en werden de 'technische' forum-collega's aangespoord om zich met dergelijke zaken bezig te gaan houden.⁸² Voor deskundigen staat in een dergelijk bericht echter geen nieuws. Voor wie het wel nieuws is geldt vrijwel zeker dat zij de kennis niet hebben om het uit te voeren. Het kan mogelijk inspiratie opleveren, maar geen risico op korte of middel-lange termijn.⁸³ Dat jihadisten zich bewust zijn van kwetsbaarheden, wil nog niet zeggen dat ze iets met die kennis kunnen of willen doen. Veel van die kennis komt door discussies in het Westen over kwetsbaarheden. Zo zou Al-Zawahiri geen belangstelling voor CBRN-aanslagen hebben gehad totdat hij las hoe eenvoudig je aan bepaalde materialen kon komen en hoe bedreigend men dat in het Westen vond.⁸⁴

2.4.4 Capaciteiten jihadisten ten aanzien van internet als wapen

Al eerder was bekend dat op in Afghanistan buitgemaakte laptops informatie over bepaalde vitale objecten was aangetroffen. In een interview uit 2003, dat niet aan de orde is geweest in de fenomeenstudie, geeft een Amerikaanse oud-overheidsfunctionaris aan dat op dergelijke laptops informatie verzameld was over

⁸⁰ In algemene zin is deze belangstelling overigens wel degelijk gegroeid sinds 2005.

⁸¹ Wall Street Journal 2009.

⁸² SITE 2008b.

⁸³ Expertmeeting 2009.

⁸⁴ Stenersen 2008, p.41.

SCADA-systemen in de elektriciteitssector. Anderen rapporteerden over aanwezigheid van informatie over SCADA in de drinkwatersector.⁸⁵ Zonder zelf toegang te hebben tot dergelijk materiaal is de informatie moeilijk te beoordelen. Betreft het informatie over het feit dat SCADA-systemen gebruikt worden in bepaalde sectoren, dat SCADA-systemen kwetsbaar zijn voor manipulatie via het internet of betrof het uitgebreide instructies en tools om daadwerkelijk actie te ondernemen? Was de SCADA-informatie 'bijvangst' in een zoektocht naar fysieke kwetsbaarheden? Was sprake van rudimentaire ideeëvorming of doelwitselectie dan wel voorbereiding op actie? Waren de eigenaren of gebruikers van de laptops geïnspireerd door berichten over de kwetsbaarheid van SCADA-systemen en zijn ze enkel op zoek gegaan naar informatie? Dat maakt hen nog geen experts en daarmee is nog geen sprake van een dreiging. Zoals aangegeven in 2.2.2.1 is het mogelijk om een testomgeving op te zetten op basis van gekraakte procescontroleprogrammatuur, handleidingen en via het internet aan te schaffen onderdelen/apparatuur. Dat sinds het interview uit 2003 niets bekend is geworden over een dergelijke testomgeving en geen relevante incidenten als aanslagen door terroristen geclaimd zijn, is mogelijk een begin van een antwoord op de voorgaande vragen.

Voor aanvallen via het internet is gerichte hacking de meest voor de hand liggende methode, hoewel ook gerichte DDoS-aanvallen tot verstoringen in vitale sectoren kunnen leiden. Zoals in de fenomeenstudie aangegeven kan een serieuze hackpoging niet op een achternamiddag worden uitgevoerd. Berichtgeving over geslaagde penetratietests doen wellicht anders vermoeden, maar de verwachting is toch dat terroristen een lange voorbereidingstijd in acht moeten nemen en geld moeten investeren. In de fenomeenstudie en in paragraaf 2.2.3 werden het huidige niveau van computer- en internetvaardigheden en interesses van jihadisten aangegeven. Dit niveau en de belangstelling, alsmede het feit dat er geen voorbeelden bekend zijn van het gebruik van het internet als wapen door jihadisten, doen niet vermoeden dat in Nederland een aanslag op kortere termijn te verwachten is. Eenvoudigere cyberaanvallen die leiden tot verstoring van processen zijn echter niet uit te sluiten: daarvoor zijn geen vergevorderde capaciteiten noodzakelijk. Het risico zit daarnaast in andere dan technische middelen, zoals social engineering en infiltratie. Daarnaast zijn er de nodige voorbeelden van serieuze cybercrime uit winstbejag bekend: criminelen die virtuele diensten misbruiken, afpersen of onbetrouwbaar maken. Kennis daarover is wellicht eerder bij jihadisten aanwezig dan kennis over manipulatie van een procescontrolesysteem in een Nederlandse sector.

2.4.5 Gevolgen

In de fenomeenstudie werd aangegeven dat er ontelbare scenario's denkbaar zijn, maar dat het lastig voorstelbaar is dat er als gevolg van een cyberaanval grote aantallen doden en gewonden zullen vallen. Ziekenhuizen en personenvervoer vormen hier wellicht een uitzondering op. Een grote stroomstoring kan mogelijk paniek onder een deel van de bevolking veroorzaken, waardoor er hamstergedrag vertoond zal worden, de beurshandel beïnvloed kan worden en uiteindelijk sprake zou kunnen zijn van maatschappij-ontwrichtende schade. Het uitvallen van virtuele diensten zoals internetbankieren, waarvan de maatschappelijke afhankelijkheid toeneemt, zal voor enorme overlast zorgen. Terroristen zullen echter meer doelen tegelijk voor een langere periode moeten aanvallen om een maatschappijontwrichtend effect te bereiken.⁸⁶ Het verstoren van de procescontrole van één elektriciteitscentrale zal eerder propagandistisch uitgebuit kunnen worden, dan dat de stroomlevering serieus in gevaar komt.

⁸⁵ Luijff 2008.

⁸⁶ Lachow 2009, p446 en Expertmeeting 2009.

Net als bij 'internet als doelwit' - waar de dienstensector evengoed een slachtoffer kan zijn - geldt dat het vertrouwen lang standhoudt en de consument erop vertrouwt dat de instituties de problemen oplossen.⁰ Niet iedere verstoring zal ook echt als een aanslag gevoeld worden. Zoals hiervoor aangegeven zijn mensen gewend aan storingen met bijvoorbeeld elektriciteit en computers. En tenslotte is er nog altijd de factor mens die storingen en veranderingen in een vroeg stadium kan opmerken en daarmee de gevolgen kan beperken. Net als bij 'internet als doelwit' moet ook hier echter rekening worden gehouden met de verwachting dat moedwillige verstoring een grotere impact zal hebben dan een louter technische storing.

2.5 Conclusie internet als wapen

Er zijn ontwikkelingen die wijzen op een toename van risicofactoren, zoals demografische gegevens, toenemende beschikbaarheid en kwaliteit van aanvalsmiddelen, 'chatter' over kwetsbaarheden, het risico van outsourcing, en de toename van het gebruik en van de afhankelijkheid van het internet, ook door de (vitale) bedrijfssectoren. Maar er wordt ook gewerkt aan weerstand: zo is er meer aandacht voor cybersecurity, werken overheid en bedrijfsleven in verschillende landen (waaronder Nederland) samen aan *awareness* en daarmee aan weerstand, is er ook internationale samenwerking op dit terrein en zal de markt mogelijk hierop inspelen, waardoor de technische verdediging versterkt kan worden.

In de praktijk tonen tests en incidenten echter aan dat vitale sectoren voorlopig nog kwetsbaar zijn voor insiders en toegewijde teams van hackers. Steeds is bij dergelijke voorbeelden de vraag hoe ver men daadwerkelijk is gekomen: voldoende om de besturing daadwerkelijk over te nemen en dan ook nog te weten wat men met het systeem doet, of slechts voldoende om een lokale verstoring te veroorzaken? Voor zover bij de NCTb bekend, zijn jihadisten en hun supporters tot nu toe niet verder gekomen dan (het aanzetten tot) eenvoudige cyberaanvallen zoals defacements, hetgeen een belangrijke graadmeter is voor hun intenties en capaciteiten. Dit neemt niet weg, dat indien jihadisten erin slagen om een ander effect te bereiken, waarbij nog geen sprake hoeft te zijn van rechtstreekse gevolgen die het label terrorisme rechtvaardigen, wel degelijk het spook van *cyberfear* om de hoek kan komen zetten. Daardoor hebben jihadisten met het veroorzaken van ongemak en onrust toch succes. Als we echter kijken naar hun intenties en capaciteiten in combinatie met de geschiedenis van jihadistische aanslagen, is de verwachting dat jihadisten toch meer heil blijven zien in het plegen van klassieke bomaanslagen en zelfmoordaanslagen. Daarmee hebben ze meer ervaring, en dergelijke aanslagen hebben een directer en voorspelbaarder effect, dan het digitaal verstoren van een vitale sector.

De conclusie luidt dan ook dat een succesvolle jihadistisch-terroristische aanslag via het internet gericht tegen de vitale infrastructuur of cruciale online-dienstverlening op de kortere termijn nog steeds niet waarschijnlijk is: kwetsbaarheden en mogelijkheden zijn eerder toe- dan afgenomen, maar er zijn onvoldoende aanwijzingen dat jihadisten die willen of succesvol kunnen misbruiken. Eenvoudige verstoringen behoren echter wel degelijk tot de mogelijkheid. De weerstand van de vitale sectoren en cruciale online-dienstverlening moet (verder) omhoog, om te voorkomen dat het kwaadwillenden, waaronder uiteindelijk wellicht ook jihadisten, te gemakkelijk wordt gemaakt om serieuzere schade aan te richten.

2.6 Slotbeschouwing

Dit onderzoek heeft zich tot jihadisten beperkt, aangezien jihadistisch terrorisme vanuit NCTb-perspectief de belangrijkste dreiging vormt. Ten aanzien van het gedeelte 'internet als doelwit en als wapen' zijn, voor zover nu bij de NCTb bekend, jihadisten niet in staat om zonder hulp van buitenaf een succesvolle complexe cyberaanval uit te voeren, die een maatschappijontwrichtend effect heeft. Ook over intenties in die richting bestaan weinig aanwijzingen, noch dat hulp van buitenaf gezocht of geboden wordt. Er zijn geen serieuze cyberincidenten herleidbaar naar jihadisten.

Bij de bovenstaande redenering zijn twee kanttekeningen te plaatsen.

De eerste heeft betrekking op de houdbaarheidsdatum van de conclusies. Ontwikkelingen gaan snel en niet alle intenties en activiteiten zullen worden onderkend. Een houvast vormt, dat de conclusies die de NCTb in 2006, trok tot nu toe stand hebben gehouden. Bovendien zijn we ons intussen van veel kwetsbaarheden bewust. Deze kwetsbaarheden worden echter wel steeds breder bekend en bovendien geven tests en incidenten aan dat ze, zeker in combinatie met social engineering, daadwerkelijk uit te buiten zijn. Hoe dat in de toekomst uitpakt, laat zich moeilijk beoordelen. Om te voorkomen dat de weerbaarheid achteruit gaat, is het in ieder geval dat dergelijke kwetsbaarheden worden weggenomen.

De tweede kanttekening betreft de focus op jihadisten. Zoals aangegeven in de inleiding maakt veel literatuur over het onderwerp geen onderscheid naar wie een eventuele aanval onderneemt: staten, criminelen, vandalen of andersoortige terroristen. De geschetste kwetsbaarheden kunnen immers door anderen dan jihadisten worden benut. Daar staat tegenover dat het verhogen van de weerstand tegen cyberaanvallen door jihadisten, effect heeft op de effectiviteit van *alle* bedreigers.

3 Internet als middel

3.1 Inleiding

Het is van groot belang te beseffen dat het internetgebruik door jihadisten niet geïsoleerd kan worden bestudeerd van algemene ontwikkelingen in de samenleving, op het internet en binnen het jihadisme. Ontwikkelingen op het internet gaan snel, er verschijnen voortdurend nieuwe toepassingen en het gebruik van het internet raakt steeds meer vervlochten in ons dagelijks leven. In deze context is het niet vreemd dat het jihadistische internetgebruik zich blijft ontwikkelen.

In paragraaf 1.2 staan de onderzoeksvragen geformuleerd. Dit hoofdstuk start met een algemene beschrijving van het gebruik van het internet als middel (paragraaf 3.2). Geconcludeerd wordt dat het internet een cruciaal middel is voor de jihadistische beweging en voor vele doeleinden wordt gebruikt. Het eind 2006 in de fenomeenstudie gehanteerde analytische onderscheid in soorten gebruik is als zodanig nog steeds bruikbaar, maar een strak onderscheid is lang niet altijd te maken. Zo kan propaganda bijdragen aan radicalisering, rekrutering en fondsenwerving en binnen virtuele netwerken kan rekrutering plaatsvinden. Ook in de literatuur worden radicalisering via het internet, propaganda, rekrutering en virtuele netwerkvorming soms in één keer behandeld.⁸⁸ Omwille van helderheid en vanwege de samenhang tussen bepaalde vormen van gebruik, is gekozen om voor de vormen van internetgebruik een andere volgorde te hanteren dan in de fenomeenstudie. Achtereenvolgens komen in de paragrafen 3.3 tot en met 3.10 de verschillende vormen van internetgebruik aan bod. Iedere paragraaf eindigt met een beoordeling van de dreiging van deze vorm van internetgebruik voor Nederland of Nederlandse belangen, maar wel bezien in de internationale context. Het hoofdstuk eindigt met een slotbeschouwing.

3.2 Gebruik van het internet als middel

Deze paragraaf schetst enkele algemene noties over het jihadistische internetgebruik. Aan de orde komen:

- a. de jihadistische beweging op het internet,
- b. het gebruik van toepassingen,
- c. de verdwijning van prominente internationale jihadistische sites,
- d. de toenemende gerichtheid op een westers publiek, en
- e. de relatie tussen virtuele en fysieke activiteiten.

3.2.1 Jihadistische beweging op het internet

Jihadistische concepten, theoretische inzichten, opvattingen en denkbelden worden op tal van manieren ge(re)produceerd en verspreid via jihadistische moskeeën, opleidings- en vormingsinstellingen, via reguliere media, maar zeker ook of wellicht zelfs vooral via het internet. Volgens Sageman is de grote rol van het internet binnen de jihadistische beweging niet gepland, maar het gevolg van een spontane evolutie. Dit als gevolg van de groei van het internet en de aandacht van de overheid voor ontmoetingsplaatsen en moskeeën.⁸⁹

Productie, reproductie en verspreiding vinden plaats door diverse leiders van de jihadistische beweging. Allereerst zijn er de spreekbuizen van kern al-Qa'ida, vooral Osama Bin Laden en Ayman al-Zawahiri, A. Y. al-Libi en M. Abu al-Yazeed. In de tweede plaats zijn er de leiders van de zelf uitgeroepen 'islamitische staten' in Afghanistan, Irak en Tsjetsjenië. Als derde zijn de lokale of regionale leiders van diverse jihadistische groepen te onderscheiden. Verder worden de jihadistische ideologie en strategie ge(re)produceerd

⁸⁸ Voorbeelden zijn Sageman 2008a, ICSR 2007 en ICSR 2009.

⁸⁹ Sageman 2008a, p. 110, 121.

en verspreid door geestelijke (aspirant) geleerden, predikers, strategen en analisten, vertalers en jihadstrijders in het veld. De strategen en analisten zijn personen die visies en evaluaties over de voortgang van de jihadstrijd produceren. In diverse jihadistische fora duiken van tijd tot tijd namen of pseudoniemen op van gezaghebbende analisten die de koers van al Qa'ida en de jihadistische beweging verwoorden. De vertalers vormen een belangrijke schakel tussen de veelal Arabische producenten en de leden van de tweede en derde generatie moslimjongeren in het Westen. Individuen nemen vaak op vrijwillige basis dit vertaalwerk op zich. Voorbeelden van producties van jihadstrijders zijn 'verhalen van Arabische strijders' en teksten van individuele jihadstrijders die gestorven zijn als martelaar. Deze uit het leven gegrepen verhalen lijken primair bedoeld als hulpmiddel bij rekrutering. Daarnaast nemen tal van sympathisanten deel aan tal van discussies. Op deze wijze ontstaat niet alleen een mondiale verspreiding van het gedachtegoed en materialen, maar ook een mondiale brainstorm over de wijze waarop de jihad kan worden gediend.⁹⁰

De manifestatie van het virtuele jihadisme leunt vooral op drie virtuele mediaorganisaties. Deze spelen een cruciale rol bij het maken van jihadistische publicaties en audiovisuele producties en nemen de tijdige en simultane verspreiding onder aangewezen websites en fora voor hun rekening. Het betreft:

1. As-Sahab ('Al Sahab Institute for Media Production'),
2. Global Islamic Media Front (GIMF), en
3. Al-Fajr (Media Center).

Deze mediaorganisaties zijn relatief autonoom en hun organisatorische link met jihadistische groepen varieert. Zij opereren in virtuele netwerken en kennen een zekere mate van taakverdeling. De aard en kwaliteit van producties, de werkwijze en het aandachtsgebied lopen uiteen. As-Sahab, dat staat voor 'De Wolken', fungeert als mediaorganisatie van kern al Qa'ida. De boodschappen worden in verschillende talen en versies geproduceerd en zijn gericht op een uiteenlopend publiek. Het is de enige en exclusieve organisatie die fysiek contact onderhoudt met de leiding van al Qa'ida. Het GIMF is één van de grote en tot nu toe duurzaamste mediaorganisaties. Het GIMF heeft tot op heden geen directe link met de leiding van al Qa'ida. Het GIMF opereert min of meer openlijk op het internet. Haar producties richten zich eerder op de strijd in het veld, dan op de leiding van de jihadistische beweging. Vermoedelijk bestaat het GIMF uit amateurs die diverse mediaprojecten ontwikkelen, zoals internet-TV. Het GIMF fungeert echter ook als uitgeverij van digitale boeken en tijdschriften. Daarnaast heeft het GIMF videotrainingen gemaakt voor het omgaan met wapens, munitie en explosieven. Al-Fajr tenslotte vormt één van de distributiecentra, die zich toelegt op de ondersteuning van diverse jihadistische groepen binnen Irak, maar ook in Noord-Afrika en het Arabische Schiereiland. Al-Fajr, wat staat voor 'De Dageraad' en de titel is van soera 89 in de Koran, werd begin 2006 opgericht en voorzorg een aantal websites van al Qa'ida, zoals de websites al-Falluja en Shumukh al-Islam, van nieuwe publicaties en mediaproducties. Dit centrum ondersteunt de 'al-Malahem Foundation', de mediaorganisatie van al Qa'ida in het Arabisch Schiereiland. Het reproduceert de mediaproducties van as-Sahab en Labbayk, de mediaorganisatie van de Taliban. Een zelfstandig product van het al-Fajr centrum is het tijdschrift 'The Technical Mujahid', dat aandacht besteedt aan ICT-methoden en technieken.

Naast deze 'grote' mediaorganisaties bestaat nog een aantal kleinschalige virtuele mediaorganisaties die zich richten op specifieke taken zoals de mediadekking van jihadistische acties van sommige groepen.

⁹⁰ Voor dat laatste: Hegghammer 2006.

Een prominent voorbeeld van een kleinschalige mediaorganisatie is de 'Al-Furqan Foundation for Media Production', een organisatie die sterk in opkomst is.

Naast mediaorganisaties zijn ook vele terroristische groeperingen en sympathisanten aanwezig op het internet. Zij gebruiken statische websites en interactieve fora, chatrooms, blogs et cetera. Er bestaan internationaal honderden zo niet duizenden jihadistische sites, -fora et cetera.⁹¹ Daardoor komt het jihadisme op het internet ogenschijnlijk heel chaotisch over. Toch is er wel degelijk een zekere structuur te onderkennen. Die structuur ontstaat aan de ene kant als gevolg van de drie genoemde virtuele mediaorganisaties en aan de andere kant door de aanwezigheid van een beperkt aantal zogeheten moedersites, een eerste laag van primaire bronnen van waaruit verdere verspreiding plaatsvindt. Bijvoorbeeld Al-Fajr controleerde en runde enkele (voormalige) moedersites zoals al-Ekhlaas, al-Boraq, al-Firdaws en al-Hesbah.⁹² Het aantal moedersites varieert tussen de vijf en tien.

Ondanks het beperkte aantal is het bereik van de moedersites groot. Enerzijds is dat het gevolg van het grote aantal geregistreerde leden, anderzijds van het feit dat de boodschap snel wordt gedistribueerd naar of wordt overgenomen door een tweede laag van sites en vervolgens door een derde laag. Op deze wijze worden zowel de voordelen van meer centrale communicatie als die van decentrale communicatie optimaal gecombineerd: authenticiteit van de berichtgeving en brede verspreiding. Wanneer deze eenmaal is geplaatst op één van de moedersites, verdwijnt de boodschap niet snel van het internet.⁹³ Bovendien nemen de oude massamedia regelmatig berichten over van de mediaorganisaties, wat de verspreiding van de boodschap nog groter maakt. Deze snelle en brede verspreiding kan bijdragen aan het beeld van een sterke en gemeenschappelijke jihadistische beweging.

Toch zijn ook nadelen verbonden aan deze werkwijze. Naarmate verdere verspreiding plaatsvindt in de periferie of berichten worden overgenomen door de oude massamedia, is het mogelijk dat de boodschap verdraaid raakt of wordt becommentarieerd door tegenstanders.⁹⁴ Nog een nadeel is dat er weliswaar veel jihadistische sites zijn, maar dat deze sites alleen in de jihadstrijd geïnteresseerde personen trekt. Hierdoor bereiken ze niet een bredere groep van zoekenden.

Jihadisten gebruiken niet alleen specifieke jihadistische sites, maar acteren ook op meer algemene sites die zich richten op de islam of moslims in de breedte. Daarnaast plaatsen jihadisten in toenemende mate oproepen gebruik te maken van meer westerse en algemene media zoals YouTube. Zo is op een jihadistische site een uitgebreide oproep geplaatst om populaire Amerikaanse webfora te gebruiken voor de distributie van jihadfilms en voor het verspreiden van desinformatie over de oorlog. Bij die oproep worden tips geplaatst hoe je te presenteren, welke forumonderdelen te gebruiken, welk type discussies op te zoeken of op te starten en welke topics juist te vermijden. Gesuggereerd wordt om bijvoorbeeld een topic te starten over een gefingeerde Amerikaanse militair, die je goed zou hebben gekend en die in Irak zelfmoord zou hebben gepleegd.⁹⁵ Het grote voordeel hiervan is een breder bereik van de boodschap. Het nadeel is dat

⁹¹ Als overkoepelende term wordt in het vervolg gesproken over 'sites'.

⁹² Voor dat laatste inSITE 2008.

⁹³ Katz & Devon 2007a, p. 4-5.

⁹⁴ Zie hiervoor bijvoorbeeld Rogan & Stenersen 2008.

⁹⁵ De volgende bronnen memoreren de oproep: Special 2007, Australian Financial Review 2007.

de boodschap kan worden verdraaid, becommentarieerd of verwijderd door moderatoren en dat de waarschijnlijkheid dat inlichtingeninstanties en opsporingsinstanties meelesen toeneemt.

Vermeldenswaardig is ook het bestaan van mailing-groepen. De mailing Group 'Ansar al-Jihad' is bijvoorbeeld actief sinds 2007 en verzendt jihadistische publicaties en videofilms naar leden die zich hebben ingeschreven op de gelijkgenaamde website. Een andere groep, al-Ansar, verspreidt via e-mail boodschappen van de leiding van de islamitische staat Irak. Een andere groep is 'Jihadistische Brigades voor Expedities op het Internet'.

Alles overziend valt te concluderen dat de moedersites als eerste laag een cruciale rol spelen in de propaganda van de jihadistische beweging, de verspreiding van ander jihadistisch materiaal, waarschijnlijk ook in de onderlinge communicatie tussen sleutelfiguren van terroristische netwerken en de vorming van virtuele netwerken. Sageman gaat zelfs zo ver om te stellen dat het discours op de ongeveer zes invloedrijke moedersites de echte leider van de jihadistische beweging vormt en niet de leider van kern al Qa'ida, Osama bin Laden. Zelfs hij kan geen invloed uitoefenen op de veelheid aan jihadistische fora en deelnemers.⁹⁶ Des te verder een site komt af te staan van de moedersite, des te minder grip de jihadistische beweging heeft op het gebruik, de gebruikers en dus des te minder de sites zich lenen voor directe rekrutering, communicatie, planning van operaties en creatie van virtuele netwerken. Bovendien bestaat de kans dat jihadistische bijdragen snel worden verwijderd, zeker nu vele van de meer neutrale sites werken met moderatoren en de faciliteit bieden om onwelgevallige content aan te melden voor verwijdering. Het bereik wordt daarentegen wel groter. Dat geldt zeker voor het grote aantal sites dat is gericht op verspreiding van kennis over de diverse algemene aspecten van de islam en andere neutrale sites waarin jihadisten zich kunnen 'nestelen'. Op deze wijze verspreidt het jihadistische gedachtegoed zich steeds verder op het internet, maar wordt de grip op de inhoud steeds beperkter.

Sageman beschouwt het internet als cruciaal voor de jihadistische beweging, beschrijft het als de 'onzichtbare hand die het wereldwijde Salafistische terrorisme organiseert' en geeft aan dat 'jihadistische sites het zwaartepunt vormen van deze *leaderless organization*'.^{97, 98} Europol stelt dat het internet een factor blijft die in grote mate de activiteiten van terroristische groeperingen, waaronder jihadistische, faciliteert.⁹⁹

3.2.2 Gebruik van toepassingen

De afgelopen jaren is het gebruik van sociale netwerksites in de gehele wereld, ook in Nederland, uiterst populair geworden. Een persoonlijk aangemaakt profiel kan worden gekoppeld aan andere profielen waardoor als het ware een sociaal netwerk wordt opgebouwd. Gezien het interactieve karakter zijn dergelijke sociale netwerksites exemplarisch voor Web 2.0. Hoewel er door Nederlanders diverse (internationale) sociale netwerksites worden gebruikt (onder andere Facebook, Myspace en Netlog) is het Nederlandse Hyves de populairste sociale netwerksite. In juli 2009 had de website, opgericht in november 2004, meer

⁹⁶ Sageman 2008a, p. 118.

⁹⁷ Sageman 2008a, p. 121.

⁹⁸ In dit kader kan de term 'islamistisch' en 'Salafi terrorisme' worden beschouwd als synoniemen voor jihadistisch en jihadistisch terrorisme.

⁹⁹ Europol 2009, p. 40.

dan negen miljoen leden, waarvan er vijf-en-een-half miljoen maandelijks inloggen.¹⁰⁰ In navolging van de algehele populariteit zijn sociale netwerksites ook populair bij jihadisten. Zo ontdekte de FBI in maart 2009 dat Somalische Amerikanen actief zijn op Facebook om jihadistisch geweld te prediken.¹⁰¹ In februari 2009 hebben jihadisten - verenigd in de groep 'Facebook invasion' - opgeroepen om propaganda te plaatsen op de sociale netwerksites.¹⁰² Overigens lijken de bovengenoemde ontwikkelingen gelijk op te gaan met tegenmaatregelen. Sociale netwerksites worden namelijk steeds beter gemodereerd. Van Facebook worden bijvoorbeeld pagina's verwijderd die foto's of berichten bevatten die bedreigend, beledigend of haatdragend zijn.

Een toepassing die in algemene zin sterk aan populariteit heeft gewonnen, hoewel het hoogtepunt alweer voorbij is, is de driedimensionale virtuele wereld Second Life (SL). In SL kan iemand een karakter (avatar) creëren en zo een tweede leven leiden. Zij kunnen allerhande activiteiten verrichten die mensen in het echt ook verrichten, waaronder het kopen van grond, onroerend goed en goederen en het aanbieden van allerlei soorten diensten, al dan niet tegen betaling. Jihadisten zouden in potentie SL kunnen gebruiken voor: a) propaganda en communicatie met anderen of onderling, bijvoorbeeld in de vorm van huiskamerbijeenkomsten, b) creatie van radicale groepen of gebieden, c) constructie en oefening van scenario's en d) als financieel transactiemedium of voor het witwassen van gelden. Wat iemand namelijk schept, is het eigendom van die persoon en de waarde van virtuele grond, onroerend goed, goederen en diensten zijn niet reëel te bepalen en de Linden-dollars zijn inwisselbaar tegen echt geld. Dit alles maakt SL of andere virtuele werelden in potentie aantrekkelijk voor witwassen.¹⁰³

Onderzoekers van de Universiteit van Arizona hebben een verkennende studie uitgevoerd naar het gebruik door internationale jihadistische extremistische groepen van enkele Web 2.0 media, namelijk blogs, YouTube en SL. Aan de hand van enkele zoekcriteria vonden de onderzoekers zes belangrijke zogeheten blog hosting sites en achtentwintig grote blogs die van belang zijn voor de internationale jihadistische beweging. Zij vonden 265 video's op YouTube op basis van de geselecteerde jihadistische termen, waarvan 34% (90) echt jihadistisch van aard waren. Deze gingen veelal over explosieven, aanslagen, bombardementen, gijzeling en dergelijke. Weliswaar verwijderd YouTube dergelijke video's, maar verspreiding heeft dan al plaatsgevonden of de video's duiken opnieuw op. In SL vonden de onderzoekers veel groepen die zelf aangaven terroristisch te zijn, hoewel de indruk van de onderzoekers was dat het hier vooral ging om jihadistische sympathisanten of verspreiders. Die groepen bouwden succesvol aan hun virtuele infrastructuur en gemeenschap. Sommige van die groepen hadden al honderden ingeschreven leden.¹⁰⁴ Anderen betwijfelen of SL wel echt aantrekkelijk is voor jihadisten.¹⁰⁵ De genoemde onderzoekers concluderen dat deze nieuwe, interactieve, multimediarijke vormen van communicatie effectieve middelen zijn voor extremisten om hun ideeën te verkondigen, bronnen te delen en te communiceren onder elkaar.¹⁰⁶

Rogan en Stenersen, twee Noorse onderzoeksters, hebben een verschuiving waargenomen van zogeheten statische sites naar interactieve. In discussiefora participeren leden en sympathisanten en zij verspreiden

¹⁰⁰ Hyves 2009.

¹⁰¹ Elsevier 2009.

¹⁰² SITE 2009b.

¹⁰³ Cochran 2007a en Cochran 2007b, Nood & Attema 2006.

¹⁰⁴ Chen e.a. 2008.

¹⁰⁵ Cochran 2007a en Cochran 2007b.

¹⁰⁶ Chen e.a. 2008.

materiaal, geven nieuwe informatie over bijvoorbeeld verdwenen sites en nemen deel aan de discussies die veelal worden geagendeerd door de mediaorganisaties.¹⁰⁷ Sageman stelt dat het gevaar veel meer uitgaat van deze interactieve sites dan van de meer statische, in zijn terminologie passieve sites¹⁰⁸ (zie verder paragraaf 3.3.3).

3.2.3 Verdwijning prominente internationale jihadistische sites 2008

De jihadistische (moeder)sites verdwijnen regelmatig, maar duiken veelal elders weer op. Dat kan het gevolg zijn van bijvoorbeeld gerichte acties van inlichtingeninstanties, van providers, al dan niet onder druk van bepaalde groeperingen of doordat de eigenaren niet langer aan hun verplichtingen kunnen voldoen. Ook de eigenaren van de jihadistische sites zelf kunnen regelmatig van ip-adres wisselen, bijvoorbeeld uit oogpunt van veiligheid.

De prominente internationale jihadistische site al-Ekhlaas is aan de vooravond van 11 september 2008 verdwenen van het internet. Ook andere prominente jihadistische sites waren toen niet meer actief of verdwenen keer op keer. Het gaat om bijvoorbeeld al-Firdaws, al-Boraq en al-Hesbah en websites van gezaghebbende geestelijke leiders en ideologen van de jihadistische beweging, zoals die van Abu Mohammed Al-Maqdissi en Abu Qatada Al-Filistini. De verdwijning was tot dan toe de grootste in zijn soort.

In de eerste dagen, weken en maanden na de verdwijning zochten jihadisten hun toevlucht in andere nog operationele jihadistische sites. Toen deze ook getroffen werden, ontstonden geleidelijk nieuwe websites en gingen reeds bestaande, oorspronkelijk kleinere, jihadistische sites, verder aangeduid als niet getroffen sites, de rol en inhoud van de verdwenen sites min of meer overnemen. Op diverse fora werd verwezen naar de werkende links hiervan.

Het veiligheidsbewustzijn is vergeleken met de periode vóór september 2008 toegenomen. Zo wijzigden de toegangsprocedures van de nieuwe prominente sites ten opzichte van voor de verdwijning. In de eerste plaats werd de toegang tot de nieuw opgerichte site onderworpen aan een inschrijvingsprocedure. In de tweede plaats werden de gegevens van de aanmelders, zoals IP-adres, opgegeven identiteit, omvang en aard van bijdragen, gecheckt. In de derde plaats werd de toegang tot bepaalde onderdelen of fora van de site voorbehouden aan bekenden van de webmasters. Het ging dan bijvoorbeeld om fora over de 'Voorbereiding op de jihadstrijd', waar technische en operationele aspecten van de jihad in het omgaan met wapens, munitie en explosieven werden besproken. In de vierde plaats werden de bijdragen van leden kritisch onder de loep genomen ter voorkoming van desinformatie en valse berichtgeving. Tenslotte waarschuwden de sites en deelnemers elkaar op tijd over vermeende infiltratie of desinformatiepogingen en kregen bezoekers adviezen over de persoonlijke beveiliging ter afscherming van hun identiteit.

De sites kregen, ten opzichte van de verdwenen sites ook een nieuwe vormgeving en andere manieren van interactie met het publiek. Verder kregen zij een uniforme structurering en rubricering: discussiefora over de politieke actualiteit in de moslimlanden, rubrieken met communiqués over uitgevoerde jihadistische acties alsmede wekelijkse of maandelijkse bulletins met een balans van de 'oogst' van de jihadstrijd in diverse

¹⁰⁷ Rogan & Stenersen 2008.

¹⁰⁸ Sageman 2008a, p. 114-115.

gebieden. Opmerkelijk is dat de informatie over de jihadstrijd en jihadistische beweging in verschillende talen wordt aangeboden. Naast Arabisch wordt ook informatie gegeven in ondermeer het Engels, Duits, Turks, Urdu, Somalisch, Albanees, Indonesisch, Filipijns en Russisch. Andere rubrieken zijn onderverdeeld in de 'islamitische emiraten' van dat moment, namelijk Afghanistan, Irak en Tsjetsjenië en voor jihadisten relevante conflicthaarden, zoals Palestina, Somalië, Algerije, Oezbekistan en Kasjmir. Via deze websites worden publicaties van ideologische, strategische en tactische aard verspreid. Daarnaast wordt met berichten, oproepen en andere wervende teksten getracht bezoekers van de sites bij de jihadstrijd te laten aansluiten. De websites verschillen in hun regionale en lokale accenten.

Kort voor 11 september 2009 gingen opnieuw enkele prominente jihadistische sites offline, zoals al-Shura, al-Falluja en Shumukh al-Islam.¹⁰⁹ Enkele keerden kort daarna weer terug, terwijl andere dat nog steeds niet gelukt is, waaronder al-Shura en Shumukh al-Islam. De beide genoemde websites waren sinds het voorjaar van 2009 opgekomen als vervangers van de verdwenen gezaghebbende al-Ekhlaas en al-Hesbah.

Uit diverse jihadistische postings blijkt dat jihadisten er van uitgaan dat de verdwijning van de site al-Ekhlaas in september 2008 gepaard is gegaan met infiltratieacties van inlichtingendiensten. Dat is ook het geval bij de verschijning van een nieuwe versie van al-Ekhlaas in september 2009. De bezoekers van de jihadistische sites reageerden zeer argwanend en wantrouwig op deze nieuwe al-Ekhlaas. Later werden uitvoerige artikelen gepubliceerd waarin de 'terugkeer' van al-Ekhlaas werd uitgelegd als een inlichtingenoperatie bedoeld om de jihadstrijders te traceren met het oog op de ontmanteling van hun virtuele en fysieke organisatie.¹¹⁰ De bezoekers van deze jihadistische sites werd gewaarschuwd op hun hoede te zijn voor deze manipulaties en ze kregen praktische hints en tips daarvoor.

In algemene zin blijkt uit de verdwijning en terugkeer van de sites in de periode september 2008 tot en met september 2009 een grote mate van veerkracht en veiligheidsbewustzijn. Daar waar jihadisten na de verdwijning in september 2008 niet snel een antwoord hadden gevonden op de verdwijning en in twijfel verkeerden, hadden zij wel snel een antwoord gevonden op de verdwijning van de jihadistische sites in september 2009. Veel sites blijven namelijk toch actief, nemen de rol van de verdwenen sites over en er verschijnen nieuwe met een ander webadres. Jihadisten wijzen elkaar op nieuwe sites en webadressen en waarschuwen ook voor mogelijke infiltratie of betrokkenheid van inlichtingeninstanties bij sites. De in paragraaf 3.2.1 genoemde jihadistische mediaorganisaties zorgen daarbij voor de continuïteit en blijven de ruggengraat van het jihadistische internet vormen. Zij beschikken over een groot jihadistisch archief en stellen die beschikbaar en zorgen voor de aanlevering van mediaproducties. Wel blijkt uit de ervaringen van de afgelopen jaren dat jihadistische sites tijd nodig hebben om zich volledig en krachtig te herstellen. Bovendien lijken jihadisten onderling argwanend te worden. Zij waarschuwen elkaar voor mogelijk gehackte sites en stellen soms openlijk de betrouwbaarheid van een site ter discussie.

3.2.4 Toenemende gerichtheid op een westers publiek

De internationale, veelal van origine Arabischtalige jihadistische sites en media richten zich in toenemende mate op een westers publiek. Dit manifesteert zich in een drietal ontwikkelingen. In de eerste plaats krijgen toespraken van de leiders van al-Qa'ida en videoproducties over de uitgevoerde terroristische acties

¹⁰⁹ Site 2009c.

¹¹⁰ Communiqué over 'Shabakat Shumukh al-Islam', 22 september 2009.

nog vaker een verzorgde ondertiteling in westerse talen, met name in het Engels.¹¹¹ In de tweede plaats manifesteert zich ook een merkbare kwaliteitsverbetering in de vertalingen en het taalgebruik. Sommige publicaties zoals ‘Jihad Recollections’ zijn in perfect Amerikaans Engels geschreven of gesproken.¹¹² Dit draagt bij aan de begrijpelijkheid en overtuigingskracht van de jihadistische boodschap. Voor de vergroting van de ontvankelijkheid van de jihadistische boodschap wordt verder een gefingeerde figuur ingezet om te laten zien dat ook fysieke personen uit het Westen en Amerika zich aansluiten bij al Qa’ida. Het gaat hier om bijvoorbeeld ‘Rakan Bin William’. Deze virtuele persoon wordt voorgesteld als een Amerikaan die zich tot de islam heeft bekeerd en zich heeft aangesloten bij al Qa’ida.¹¹³ In de derde plaats worden de invloedrijke jihadistische sites voorzien van Engelstalige, Franstalige en Duitstalige onderdelen. Deze bevatten nieuws, communiqués, bulletins en videofilms over de jihadstrijd.

3.2.5 Relatie virtuele en fysieke instituties, personen en activiteiten

De link van de jihadistische mediaorganisaties en sites naar diverse organisatorische takken van de jihadistische beweging lijkt moeilijk vast te stellen. De sites vormen veelal geen officiële organen, noch een weerspiegeling van organisatorische verbanden van diverse jihadistische groepen. Maar er zijn aanwijzingen dat de jihadistische virtuele actoren, zoals webmasters en deelnemers aan fora, over een goede informatiepositie beschikken over de diverse takken van de jihadistische beweging. Zo hebben de jihadistische mediaorganisaties het monopolie op interviews en nieuwsprimeurs van de leiding van kern al Qa’ida. As-Sahab beschikt over het alleenrecht om de leiding van al Qa’ida te interviewen en die interviews te distribueren. Hetzelfde geldt voor Al-Fajr ten aanzien van de leiding van de ‘Islamitische Staat Irak’.¹¹⁴ Een andere indicatie is dat sommige deelnemers aan jihadistische fora zodanig goed onderlegd en ingelicht zijn in vraagstukken aangaande de jihadstrijd, dat aangenomen mag worden dat hun kennis en informatiepositie voortkomen uit ervaringen in het veld. Enkelen lijken te zijn vertrokken naar het strijdgebied. Te denken hierbij valt aan het forumlid ‘asdasd99’ alias ‘al-Miskin al-Muhajir’ van de websites al-Firdaws en al-Ekhlaas, die zich heeft aangesloten bij de jihadstrijders in Afghanistan in juni 2008.¹¹⁵ Of de ‘Mujahid 1988,’ die veel postings heeft geplaatst op de site al-Ekhlaas in de loop van het jaar 2007 en in een ‘afscheidsbrief’ in mei 2007 zijn afscheid en vertrek naar het slagveld van de jihadstrijd aankondigde.¹¹⁶ In de videoboodschap van al Qa’ida waarin de achtste ‘verjaardag’ van de aanvallen in de VS werd gevierd, kwamen clips voor van twee zelfmoordterroristen die betrokken waren bij de zelfmoordaanlagen in Pakistan in mei 2009. Eén daarvan, Ali Jaleel, was een bekende van Engelstalige jihadistische fora, waaronder die op Tibyan en Firdaws. Hij was een belangrijke vertaler van dat forum.¹¹⁷

Volgens open bronnen bestonden er relaties tussen virtuele activiteiten en fysieke activiteiten van de betrokkenen bij de jihadistische site Minbar SOS. In december 2008 zijn in België leden van een vermeende Belgische cel van al Qa’ida gearresteerd, waaronder Malika El Aroud. Malika El Aroud was volgens open bronnen tot haar arrestatie in december 2008 de beheerder van de Franstalige jihadistische website

111 Lia 2009, p. 4, Europol 2009, p. 14, SITE 2009h, p. 1.

112 Hegghammer 2007.

113 Moss & Mekhennet 2007.

114 Reals 2007.

115 NEFA 2008.

116 Kohlmann 2008.

117 SITE 2009h, p. 23-24.

“Minbar-SOS”^{118 119} en zou diverse jihadistische postings op haar naam hebben staan. Tevens zou zij diverse interviews en pamfletten van prominente jihadisten hebben vertaald vanuit het Arabisch naar het Frans.¹²⁰ Zij was volgens open bronnen in augustus 2007 ook actief op de site in een discussie over het voorgestelde niqaab-verbod in Nederland.¹²¹ Eerder was zij getrouwd met de Tunesiër Abdessatar Dahmane, die in 2001 een zelfmoordaanslag pleegde in Afghanistan. In juni 2007 is zij samen met haar huidige man in Zwitserland veroordeeld voor het beheren van sites met pro al Qa’ida content.^{122 123}

Inmiddels wordt op grond van open bronnen steeds duidelijker dat Minbar-SOS een prominente rol speelde binnen de ‘Belgische cel van al Qa’ida’. Malika El-Aroud zou samen met haar huidige man onder andere via de site mensen hebben geronseld voor de jihad. Haar man is begin 2008 met zes rekruten naar het Pakistaans-Afghaanse grensgebied getrokken. Hij had via het forum nog tot eind mei 2009 contact met zijn volgelingen in België. Tevens postte hij eind september 2008 een oproep om aanslagen in Europa te plegen. Hij zou op 24 mei 2009 voor de laatste keer hebben ingelogd op het forum.¹²⁴ Sinds begin juni 2009 is Minbar-SOS niet langer beschikbaar,¹²⁵ wellicht doordat de individuen achter de website gedetineerd zijn.

3.2.6 Beoordeling dreiging internet als middel: algemeen

De drie genoemde mediaorganisaties, As-Sahab GIMF en Al-Fajr spelen nog meer dan eind 2006 mondiaal een cruciale rol voor de jihadistische beweging. Datzelfde geldt voor tussen de vijf en tien zogeheten moedersites van waaruit de eerste verspreiding plaatsvindt van jihadistische publicaties en de jihadistische boodschap en waar in fora over allerlei jihadistische onderwerpen informatie te vinden is en meningvorming kan plaatsvinden. Jihadisten verspreiden hun publicaties en boodschap daarentegen ook steeds meer via tal van niet-jihadistische sites en met behulp van sinds 2006 sterk opgekomen ‘toepassingen’ zoals YouTube en sociale netwerksites. Dit is te bezien als een vorm van innesteling. Jihadisten hebben hier wel minder grip op, maar het bereik is vele malen groter dan op de eigen sites. Sinds eind 2006 zijn tweemaal op grote schaal jihadistische sites verdwenen, vermoedelijk in het kader van een contraterrorismeoperatie, namelijk aan de vooravond van de herdenking van de aanslagen in de VS in september 2008 en 2009. Daar waar jihadisten niet direct een antwoord konden vinden op de verdwijning in 2008, bleek in 2009 dat ze hun lessen hebben geleerd. Zij zijn minder kwetsbaar geworden voor het uit de lucht halen van hun prominente sites. Andere tendensen waarop gewezen kan worden zijn een nog verdere professionalisering en kwaliteitsverbetering van jihadistische publicaties en de jihadistische boodschap evenals een grotere gerichtheid op een westers publiek.

Duidelijk is dat het internet een factor is die, zoals ook Sageman en Europol aangeven, in grote mate de activiteiten van jihadisten faciliteert.

118 Cruickshank 2009a, Vlierden 2009.

119 Minbar: spreekgestoelte binnen de moskee van waaraf gepreikt wordt.

120 SITE 2007b, Cruickshank 2009c, Israel Military.net 2008.

121 SITE 2007b.

122 SITE 2007b, Cruickshank 2009c, Israel Military.net 2008.

123 De leden van de Belgische cel waren ten tijde van het schrijven eind oktober 2009 nog niet veroordeeld door een Rechtbank. In formele zin zijn zij dus slechts verdachte voor wat betreft hun betrokkenheid bij Minbar SOS en de relatie met fysieke activiteiten.

124 Site 2009d, Cruickshank 2009a, Vlierden 2009, Cruickshank 2009b.

125 Vlierden 2009 en eigen waarneming op 2 juli 2009.

3.3 Gebruik van het internet als middel: specifiek

In de onderstaande paragrafen wordt ingegaan op de specifieke vormen van benutting van het internet als middel, zoals die ook in de fenomeenstudie aan de orde kwamen. Eerst wordt in een paragraaf teruggeblikt naar de conclusies van de fenomeenstudie, waarna nieuwe of aanvullende inzichten per onderwerp worden behandeld.

3.3.1 Terugblik fenomeenstudie

Propaganda

De conclusie van de fenomeenstudie luidde: 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: 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 voedingsbodempodem 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.

Invloed op radicalisering

De conclusie luidde: internetgebruik ondersteunt het gehele proces van radicalisering. Voor iedere fase van radicalisering is aanbod van jihadistisch materiaal beschikbaar. Met behulp van het internet kan een potentiële jihadist processen doorlopen van ideologievorming, ideologieversterking en ideologische indoctrinatie. Het draagt bovendien bij aan groepsvorming en tot netwerkvorming van gelijkgestemden. Individuen en groepen kunnen zich daardoor gaan keren tegen de samenleving, eerst ideologisch en mogelijk op termijn activistisch-gewelddadig. Wel werd de vraag gesteld in hoeverre en op welke wijze het internet daadwerkelijk een rol speelt bij radicalisering en uiteindelijk leidt tot terrorisme.

Creatie van virtuele netwerken

De conclusie luidde: virtuele netwerken verhogen de slagkracht van de jihadistische beweging. Door de vorming van virtuele netwerken kan een informele pool van bereidwilligen voor de jihad ontstaan die in wisselende combinaties met elkaar of individueel geweldsactiviteiten kunnen ontplooien. Lokale en internationale elementen kunnen daardoor meer met elkaar verweven raken. Aan virtuele netwerken kleven voor jihadisten zowel voor- als nadelen, waarvan de vertrouwenskwestie één van de belangrijkste nadelen is.

Rekrutering

De conclusie luidde: internetgebruik resulteert in meer interactieve vormen van rekrutering die nog niet goed te duiden zijn, evenals in conscriptie en zelfontbranding. Kenmerkend voor het internet is vooral dat potentiële strijders zich zelf willen aanmelden voor deelname aan de gewelddadige jihad (conscriptie). In relatie tot het internet wordt ook wel gesproken van zelfontbranding, waarvan sprake is als iemand op 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, voor het internet dat geldt zeker.

Infomatie-inwinning

De conclusie luidde: informatie-inwinning via het internet draagt potentieel bij aan het plegen van terroris-

tische activiteiten. Informatie-inwinning kan uiteenlopende doelen dienen. Net als voor iedereen vormt het internet voor jihadisten een onuitputtelijke, laagdrempelige bron van informatie die met behulp van professionele hulpmiddelen zoals datamining kunnen worden gecombineerd. De inwinning kan zowel op legale als illegale wijze plaatsvinden, bijvoorbeeld door hacking.

Fondsenwerving

De conclusie luidde: fondsenwerving via het internet door en voor jihadisten komt nog beperkt voor, Verschuiving naar meer heimelijke fondsenwerving is te verwachten.

Training

De conclusie luidde: gebruik van het internet voor trainingsdoeleinden werkt drempelverlagend voor het plegen van aanslagen.

Onderlinge communicatie en planning

De conclusie luidde: jihadisten gebruiken het internet voor onderlinge communicatie en planning.

3.3.2 Propaganda: aanvullende of nieuwe inzichten

3.3.2.1 Propaganda heel divers van aard

Analytisch zijn enkele vormen van propaganda te onderscheiden, namelijk:

- het verwerven of behouden van de directe aanhang en (de grotere) achterban;
- het beïnvloeden van de internationale publieke opinie;
- het beïnvloeden van de vijand en het publiek van de vijand;
- het aanjagen van angst;
- hacktivisme.

Dit onderscheid is niet altijd scherp doordat één boodschap uiteenlopende doelen kan dienen en gericht kan zijn op diverse doelgroepen.

Op het internet zijn vele vormen van jihadistische propaganda te vinden. Er is een continue stroom van edities en herdrukken van jihadistische publicaties, productie van audiovisuele media et cetera. Deze kunnen handelen over de jihadstrijd, maar ook over vele andere onderwerpen vanuit een jihadistisch perspectief. Voorbeelden zijn democratie, liberalisme, secularisme en verhoudingen tussen de islam en het Westen. Naast drie prominente mediaorganisaties en enkele prominente moedersites, bestaan er ook grote hoeveelheden jihadistische sites en maakt de jihadistische beweging ook gebruik van sites die zich richten op de islam of moslims in het algemeen en neutrale sites zoals YouTube. Het is dan ook logisch dat de jihadistische propaganda vele gezichten kent.

Voor de drie eerder genoemde prominente mediaorganisaties hebben een grote stroom propagandistische boodschappen (audio, video en tekst) uitgebracht. Zeker de eerste en tweede man van kern al Qa'ida, Osama Bin Laden en Ayman al-Zawahiri, doen veelvuldig van zich horen. Zij behandelen zowel actuele thema's, bijvoorbeeld het binnenvallen van Israël in de Gazastrook eind 2008 en de toespraak van president Obama aan de Universiteit van Cairo in juni 2009, als ook de voortgang van de jihadistische strijd en de situatie op de jihadistische strijdtoneel. Conflicten zoals die in de Gazastrook kunnen aanleiding zijn om bedreigingen te uiten aan landen. Zo heeft een lid van kern al Qa'ida, Abu Yahya al-Libi, de oorlog in Gaza aangegrepen om in

een video in januari 2009 op te roepen tot wraakacties tegen het Verenigd Koninkrijk.¹²⁶ In de video wordt dit land, vanwege de historische rol die het Verenigd Koninkrijk heeft gespeeld bij de stichting van Israël, verantwoordelijk gehouden voor het lot van de Palestijnen. Ook individuele posters kunnen propaganda plaatsen van uiteenlopende aard op bijvoorbeeld de moedersites.

Het is lastig een beeld te vormen van de kant die het discours opgaat op de jihadistische fora en welke waarde daar aan gehecht moet worden. Is het de mening of oproep van één individu, is het de mening van een terroristische groepering of geeft het een beeld van de mening binnen de jihadistische beweging? Sageman vergelijkt dit met de discussies van de deelnemers aan één en hetzelfde diner. Zij hebben verschillende discussies onderling, op uiteenlopende momenten en in andere contexten. De discussie is afhankelijk van tal van factoren, waaronder de actualiteiten van die dag. Het is lastig om te bepalen welke kant de discussie opgaat. Datzelfde geldt voor fora. Ook hier nemen vele deelnemers aan deel, die op uiteenlopende fora actief kunnen zijn. Een deelnemer aan een forum heeft een invloed die proportioneel is aan het aantal postings dat hij plaatst, de mate van consistentie daarvan met het algemene discours op het forum en de toegevoegde waarde daarvan voor de andere deelnemers.¹²⁷ Bepalend bij de waarde van een posting is verder het forum waar deze is geplaatst, de hoeveelheid postings van een plaatser, de onderbouwing, het aantal reacties en dergelijke.

Een duidelijk voorbeeld waarbij propaganda zich richt op het aanjagen van angst en het beïnvloeden van het publiek zijn dreigvideo's richting Duitsland. Jihadisten plaatsten sinds eind 2008 diverse videoboodschappen op het internet waarin de aanwezigheid van Duitse troepen in Afghanistan wordt bekritiseerd en tegelijkertijd het Duitse volk wordt gewaarschuwd voor de gevolgen daarvan. Redenen hiervoor kunnen zijn gelegen in de toenmalige combinatie van discussies in Duitsland over opname van gevangenen uit Guantanamo Bay, de verlenging van de inzet van Duitse troepen in Afghanistan en de verkiezingen die in 2009 werden gehouden in Duitsland. Mogelijk zouden jihadistische verkiezingen in Duitsland hebben proberen te beïnvloeden door angst te zaaien.¹²⁸ Eerder, in november 2007, was ook al een videoboodschap verschenen waarin Duitsland en Oostenrijk onder druk werden gezet om hun troepen uit Afghanistan terug te trekken. Hoewel twijfels zijn te plaatsen bij de feitelijke dreiging die uitgaat van de videoboodschappen, dragen ze wel bij aan angst. De pijlen van de jihadistische beweging richtten zich soms ook op Nederland. Zowel vóór als ná verschijning van de film *Fitna* zijn op vooraanstaande jihadistische sites dreigementen geuit tegen de PVV-fractievoorzitter, tegen Nederland in het algemeen en tegen de Nederlandse troepen in Afghanistan.

In een specifiek geval bleef het niet bij het plaatsen van videoboodschappen alleen. Eén van de dreigende videoboodschappen die was gericht aan Duitsland is volgens de 'Jihadist Brigades to Invade the Internet' actief verzonden naar ruim 40.000 Duitse e-mailadressen. Deze actie flankeerde de verspreiding op zoveel mogelijk Duitstalige (neutrale) sites door het Global Islamic Media Front (GIMF).¹²⁹ Door de verzending van jihadistisch materiaal naar burgers kunnen jihadistische angst zaaien, doordat burgers nu veel directer worden aangesproken. Overigens zullen spamfilters veel van dergelijke berichten onderscheppen.

¹²⁶ Voor dat laatste SITE 2009e.

¹²⁷ Sageman 2008a, p. 118-120.

¹²⁸ Onder andere gebaseerd op Hamburger Abendblatt 2009, Welt 2009 en NRC Handelsblad 2009.

¹²⁹ SITE 2009f.

Iets dat de afgelopen jaren opviel is dat jihadistische acties reageren op nieuwsberichten vanuit westerse media voor propagandistische doeleinden. Nieuws dat jihadistische acties kan helpen bij hun propaganda, of hun moreel kan versterken, verspreiden zij vervolgens via het internet.¹³⁰ Zo probeerden jihadistische acties te trekken uit bijvoorbeeld interviews met Amerikaanse soldaten in Irak en uit de reacties naar aanleiding van het via het internet verspreide ultimatum aan Duitsland en Oostenrijk in maart 2007 om hun troepen uit Afghanistan terug te trekken. Zij houden ook de contra-initiatieven van regeringen, organisaties en vooraanstaande intellectuelen en opinieleiders, die zijn gericht op de bestrijding van de ideologie, in de gaten. De jihadistische strategen, opinieleiders en commentatoren volgden bijvoorbeeld de plannen van de Amerikaanse regering om de gematigde islam te bevorderen en de initiatieven van moslimlanden zoals Saoedi-Arabië om extremistische vormen van de islam te bestrijden. Tegelijkertijd vielen ze nieuwe publicaties van liberale en kritische intellectuelen en opinieleiders aan. Zij brengen de nieuwe plannen, initiatieven en publicaties in verband met de 'complotten tegen de islam en moslims' en waarschuwen hiervoor.

Jihadisten zijn alert op vermeende beledigingen van de islam en reageren op hun eigen fora op nieuwsberichten daarover vanuit westerse media. Ook proberen ze berichtgeving op neutrale sites te beïnvloeden. Zo werd op een forum van de jihadistische al-Ekhlaas website in de periode juli tot en met begin december 2007 zes keer door verschillende deelnemers in het Arabisch een oproep geplaatst om mee te doen aan een stemming over een stelling op de website van het Nederlandse Radio 1-programma 'Stand.nl'. Onderwerpen waarover gestemd moest worden door jihadistische acties waren: het verbod op de hoofddoek in Nederland (twee keer), verbod op de niqab, het verbieden van de Koran (twee keer) en een klacht van moslims over het verbod op de Koran. In die periode bestond in Nederland op basis van uiteenlopende gebeurtenissen een discussie over aan de islam gerelateerde onderwerpen. Wellicht is de indruk ontstaan dat de Nederlandse overheid haar oordeel laat hangen van de uitkomst van dergelijke stemmingen. Waarschijnlijk beseffen de plaatsers van de oproep onvoldoende dat het gaat om dagelijks wisselende stellingen en dat het tijdsverschil met Nederland tot gevolg kan hebben dat wordt gestemd op een andere stelling dan beoogd. De oproep komt dus amateuristisch over. Toch schetsen dergelijke oproepen op een Arabisch-talige jihadistische website wel een beeld van Nederland als moslimvijandig en geeft het aan dat jihadistische acties westerse berichtgeving goed volgen. Overigens blijkt uit deze casuïstiek ook dat tal van andere sites de oproep op een prominente site overnemen en dat de oorspronkelijke oproep een heel andere lading kan krijgen. Op tal van sites werd namelijk de onjuiste informatie verspreid dat de Koran in Nederland werd verboden en dat de Nederlandse regering een referendum daarover had georganiseerd. Een nieuwsfeit is daarmee gecreëerd, namelijk het vermeende verbod op de Koran in Nederland.

Volgens het Israëlische instituut Memri zou blijken dat de indoctrinatie van vrouwen via vele websites aanzienlijk is, zowel ten aanzien van het leveren van een financiële bijdrage, het steunen van tot jihad bereide echtgenoten of kinderen alsook tot het zelf plegen van zelfmoordaanslagen.¹³¹ Via het internet kan zo een grotere groep worden bereikt met de oproep deel te nemen aan de jihad, een groep die op andere wijze voor mannelijke jihadistische acties moeilijk bereikbaar is. Sageman wijst op de groeiende rol van vrouwen op het internet in chatrooms.¹³²

¹³⁰ Memri 2007.

¹³¹ Memri 2008.

¹³² Sageman 2008a, p. 111-112.

Een bijzondere vorm van interactieve propaganda deed zich eind 2007 en begin 2008 voor. As Sahab (zie paragraaf 3.2.1) kondigde in december 2007 aan dat Al Zawahiri, de tweede man van kern al Qa'ida, vragen zou beantwoorden van aanhangers van al Qa'ida, journalisten en critici. In twee videoboodschappen, waarvan de eerste op 2 april en de tweede op 21 april 2008 verscheen, gaf hij honderden antwoorden op ruim meer dan duizend van de gestelde vragen. Controversiële vragen ging hij daarbij niet uit de weg.¹³³ Ook werd een game gelanceerd waarin onder andere president Bush en de Britse premier Blair propagandistisch op de korrel werden genomen. Het betrof het een zogeheten *first person shooter* met de titel 'night of Bush capturing', gericht op 'terrorist children', met zogeheten nasheeds (zie ook 4.4.2.2) als achtergrondmuziek.¹³⁴

De propaganda via het internet is, zoals eerder is vermeld, verder geprofessionaliseerd, maakt gebruik van nieuwe toepassingen, richt zich ook op een westers publiek en heeft nog steeds een groot bereik (zie paragraaf 3.2). Hoewel verschillende vormen van propaganda zijn te onderscheiden, is zeker het 'winnen van zieltjes' een belangrijk doel daarachter. Deze propaganda creëert een voedingsbodem voor (verdere) radicalisering van individuen en groepen (zie verder paragraaf 3.3.3).

3.3.2.2 Jihadistisch/islamitisch hacktivisme in opkomst

Hacktivisme heeft sinds eind 2006 een grotere vlucht genomen.¹³⁵ Begin november 2007 werd bijvoorbeeld een actie aangekondigd om vanaf 11 november 2007 westerse, joodse, Israëlische en 'afvallige' islamitische en shi'itische nieuws-, overheidswebsites als ook websites van belang voor de vitale infrastructuur te verstoren en te defacen.¹³⁶ De aangekondigde actie is, voorzover bekend, niet uitgevoerd, maar trok wel de nodige (media-)belangstelling. In oktober en november 2007 was daadwerkelijk sprake van hacktivisme, in dit geval door Turkstalige hackers. Eenmaal zijn meer dan vijfduizend Zweedse websites aangevallen, mogelijk in verband met de plaatsing van een omstreden Mohammed-cartoon in een Zweedse krant.¹³⁷

Islamitisch of jihadistisch hacktivisme deed zich ook enkele malen voor in Nederland om ongenoegen kenbaar te maken over situaties van (vermeende) anti-islam-uitingen en -houdingen. Vanaf begin februari 2008 hebben hackers defacements uitgevoerd richting diverse Nederlandse websites als protest rondom en tegen de (aangekondigde) film *Fitna* en Wilders.¹³⁸ Over langere tijd gemeten werden naar schatting 20.000 Nederlandse websites getroffen. De gewijzigde webpagina bevat een duidelijke boodschap van de hacker in kwestie, vaak inclusief een filmpje of links naar andere webpagina's of bestanden. Het is dus niet zo dat gegevens gestolen worden, dat de controle over een website wordt overgenomen of dat de website volledig ontoegankelijk wordt gemaakt. Een defacement is door de eigenaar van de pagina ook eenvoudig te herstellen. Gelet op de grotere aantallen werden de genoemde defacements zeer waarschijnlijk geautomatiseerd uitgevoerd.¹³⁹ De websites die het doelwit werden, zijn dan ook niet gekozen vanwege hun specifieke

¹³³ Algemeen Dagblad 2008, International Herald Tribune 2008, Whitlock 2008. Het aantal antwoorden en vragen is afkomstig uit de laatste bron.

¹³⁴ Jihadwatch 2006.

¹³⁵ Zie ook: Rogan & Stenersen 2008.

¹³⁶ Debka 2007.

¹³⁷ Nu.nl 2007. De Zweedse krant *Nerikes Allehanda* drukte 19 augustus een tekening af van de kunstenaar Lars Vilks, die het hoofd van Mohammed had getekend op een hondenvlijf.

¹³⁸ ANP 2008 en Pers 2008.

¹³⁹ In hackerkringen staat het defacen van onvoldoende beveiligde, kwetsbare websites door middel van geautomatiseerde scripts zeer laag in de pikorde.

inhoud, maar omdat ze draaiden op kwetsbare servers en omdat ze tot het Nederlandse internetdomein (.nl) behoorden. De boodschappen bestonden uit een mix van Nederlandse, Engelse, Turkse en Arabische teksten en kenden verschillende verschijningsvormen. Dit wijst erop dat meerdere hackers(groepen) actief zijn en dat de daders waarschijnlijk verschillende achtergronden hebben. Dit neemt niet weg dat de meeste defacements door hackers met een Turkse achtergrond lijken te zijn uitgevoerd.

De vraag is in hoeverre de hacker(s) puur vanuit ideologisch standpunt te werk is/zijn gegaan. 'Prestaties' van hackers worden op specifieke websites in statistiekvorm bijgehouden en de onderlinge wedijver speelt daarbij zeker een rol.

3.3.2.3 Beoordeling dreiging

Op het internet zijn nog steeds vele vormen van jihadistische propaganda te vinden. Vooral drie prominente mediaorganisaties, Al-Fajr, GIMF en As-Sahab hebben een grote stroom propagandistische boodschappen (audio, video en tekst) uitgebracht. Propaganda via het internet is verder geprofessionaliseerd, heeft nog steeds een groot bereik en kent nog steeds relatief weinig weerwoord. Jihadisten proberen actief de interactie aan te gaan met geïnteresseerden op tal van manieren. Jihadisten reageren actief op nieuwsberichten vanuit westerse media voor propagandistische doeleinden, zijn alert op vermeende beledigingen van de islam en reageren op hun eigen fora op nieuwsberichten daaromtrent vanuit westerse media. De kans op 'hacktivisme' door jihadisten zal eerder toe- dan afnemen, ook in Nederland.

Nog steeds geldt dat de combinatie van de vooral grote groepen jongeren die toegang hebben tot het internet en dat intensief gebruiken in combinatie met de propaganda vanuit de jihadistische beweging een voedingsbodem creëert voor (verdere) radicalisering. De conclusie luidt dan ook dat propaganda via het internet (nog steeds) bijdraagt aan radicalisering.

3.3.3 Invloed internet op radicalisering: aanvullende of nieuwe inzichten

Hoewel deze paragraaf primair gaat over radicalisering en in andere paragrafen virtuele netwerkvorming en rekrutering expliciet aan bod komen, staat deze paragraaf toch ook stil bij die onderwerpen. In de literatuur wordt niet altijd het onderscheid gemaakt en de analytische onderverdeling is in de praktijk niet altijd te maken.

Sageman gaat in op de invloed van het internet op radicalisering. Volgens hem moet in dat kader wel een onderscheid worden gemaakt tussen het worldwide web, dat de verzameling van alle websites is en gebruikers van informatie voorziet, en interactieve sites. Het worldwide web is in de kern passief en is vergelijkbaar met de traditionele media, zoals kranten en tijdschriften. Gebruikers absorberen de informatie die wordt aangeboden. Het instructiemateriaal dat op deze passieve websites te vinden is, speelde bijvoorbeeld een rol bij enkele (verijdelde) aanslagen. Voorbeelden daarvan zijn de aanslagen in Madrid in 2004, de poging tot aanslagen in treinen in Duitsland via kofferbommen en de verijdelde aanslagen in Londen en de mislukte aanslag in Glasgow in juni 2007. Volgens Sageman zijn deze 'passieve' websites echter niet de motor van radicalisering, aangezien ze alleen gezichtspunten bevestigen en versterken.¹⁴⁰ Bovendien zijn veel jihadistische teksten intellectueel van aard en vereist het het nodige geduld en doorzettingsvermogen om de inhoud tot zich te nemen.

Naast passieve sites omvat het internet ook vele mogelijkheden voor communicatie tussen individuen en tussen individuen en groepen in de vorm van bijvoorbeeld e-mail, forums en chatrooms. Deze inter-

¹⁴⁰ Sageman 2008a, p. 114.

activiteit is revolutionair en verandert menselijke relaties op een manier die we nog niet goed begrijpen. Vanwege de anonimiteit geven mensen zich snel bloot op het internet. Via het internet kunnen sterke banden tussen mensen ontstaan, zonder dat ze elkaar in eerste instantie in het echt kennen. Zo komen via het internet huwelijken tot stand, en er zijn gevallen bekend waarin jongeren via het internet afspraken collectief zelfmoord te plegen. De tegenhanger daarvan is natuurlijk dat de interactie van het ene op het andere moment kan worden opgezegd. Verder is de tegenhanger van een grotere intimiteit een gebrek aan beschaving. Dit als gevolg van het gevoel van anonimiteit.¹⁴¹ In de fenomeenstudie is naast de vluchtigheid van contacten en identiteiten ook het punt van vertrouwen benoemd. Kun je virtuele contacten wel vertrouwen als het gaat om illegale activiteiten?¹⁴²

Uit een Nederlands promotieonderzoek blijkt dat via het internet eenvoudig nieuwe contacten kunnen worden gelegd en dat online communicatie positieve effecten heeft op vriendschapsvorming. Online onthullen mensen meer persoonlijke informatie en stellen meer vragen aan de gesprekspartner. Daarbij is het volgens de onderzoekster niet belangrijk of mensen elkaar kunnen zien (via een webcam). Daaruit concludeert ze dat het bovenstaande effect niet tot stand komt doordat mensen anoniemer zijn. Het maakt voor de kwaliteit van bestaande vriendschappen ook niet uit hoe je elkaar hebt leren kennen. De vriendschappen die online zijn ontstaan en later ook offline werden, zijn van dezelfde kwaliteit als vriendschappen die offline zijn ontstaan.¹⁴³

De interactiviteit van het internet is een belangrijke factor bij radicalisering¹⁴⁴ en de interactiviteit van jihadistische sites is toegenomen (zie paragraaf 3.2.2). Volgens Sageman spelen de fora op het internet de rol die voorheen radicale moskeeën speelden. Door de interactie met gelijkgestemden of vrienden op interactieve sites veranderen mensen hun gedachten. De discussie en het uitwisselen van gedachten en meningen via deze interactieve voorzieningen inspireren en leiden tot radicalisering.¹⁴⁵ De deelnemers krijgen het gevoel onderdeel uit te maken van een grotere gemeenschap, de moslimgemeenschap of umma.¹⁴⁶ In beginsel kan iedereen, leider, deskundige of niet, op gelijke voet met anderen communiceren. Personen kunnen zelf op zoek gaan naar fora waar ze gelijkgestemden ontmoeten. Tevens kunnen zij fora waar meningen worden geventileerd die hen niet aanstaan, vermijden. De interactie met gelijkgestemden geeft het gevoel niet alleen te staan. Andere geluiden komen nauwelijks voor het voetlicht, waardoor de eigen gedachten worden versterkt. De interactie kan bovendien beginnen met een algemene vraag, zoals “waar kan je als moslim ‘veilig’ op vakantie?” en uiteindelijk uitmonden in uitwisseling of vorming van radicale standpunten. Dit interactieve proces kan leiden tot verdere radicalisering.

- “[...] the internet can form an environment in which individuals’ commitment to the ‘cause’ and their concept of what means are justified in defending the ummah are exaggerated”.

Het internet biedt dus de mogelijkheid tot netwerken tussen gelijkgestemden. Hierdoor komen zij in contact met anderen die ze anders niet zouden ontmoeten. Op deze wijze kunnen interactieve sites fungeren als een soort rekruteringsmagneet waarbij ‘zoekers’ toegang krijgen tot delen van de jihadistische

beweging.¹⁴⁷ De interactieve sites beïnvloeden dus niet alleen radicalisering, maar fungeren ook als middel voor rekrutering en virtuele netwerkvorming.

Nog steeds is niet volledig duidelijk in hoeverre en op welke wijze het internet een rol speelt bij radicalisering en eigenlijk ook niet bij rekrutering en virtuele netwerkvorming. Dat het internet een belangrijke factor is, is onomstreden. Over de mate waarin bestaan wel meningsverschillen, zeker in relatie tot andere factoren. Illustratief in dat kader is een rapport van The International Centre for the Study of Radicalisation and Political Violence (ICSR). Dit rapport stelt dat het internet een rol kan spelen in radicalisering en rekrutering, maar dat het niet de voornaamste factor is. Radicalisering en rekrutering zijn tevens geworteld in de ‘echte wereld’.¹⁴⁸ De argumentatie in het rapport dat de invloed van het internet niet dominant is, is vooral gestoeld op het ontbreken van menselijk contact op het internet en de noodzaak van ‘echte’ sociale netwerken en groepsprocessen. Toch sluit het ICSR in een eerder rapport niet uit dat sprake kan zijn van virtuele zelf-rekrutering waarin het internet wel de dominante of zelfs enige factor is geweest van radicalisering en rekrutering. Zij noemen in dat kader ook twee voorbeelden, namelijk de in de fenomeenstudie en in deze update Irhabio07 en Irfan Raja uit Ilford in Engeland.¹⁴⁹

Het ICSR benoemt in het eerdere rapport drie functies waarin het internet rekrutering kan ondersteunen. Als eerste illustreert en versterkt het internet de ideologische boodschap die rekruten ontvangen tijdens studiesessies. Zij zien zo ook dat ze niet alleen staan, maar onderdeel uitmaken van een virtuele jihadistische beweging. Als tweede biedt het de mogelijkheid tot netwerken, zoals hierboven aangegeven, en als derde kan het internet de betrokkenheid bij de jihad versterken en drempels wegnemen. Wel geven de onderzoekers aan dat ‘*armchair jihadis*’ toch radicale standpunten kunnen innemen zonder dat zij ooit tot actie zouden overgaan. Zij geloven op basis van hun onderzoek dat de internetondersteuning van rekrutering zal toenemen.¹⁵⁰

Dat radicalisering en/of rekrutering niet exclusief via het internet plaatsvinden, blijkt bijvoorbeeld uit de casus van een Duitse bekeerling die ervan verdacht wordt leider te zijn van de zogeheten Sauerlandgroep. Deze groep bereidde in 2007 aanslagen voor in Duitsland, stond half 2009 terecht en is in maart 2010 door de rechter veroordeeld. Voor de rechter verklaarde hij dat zijn keuze om moslim te worden een rationele keuze was. Na de aanslagen van 11 september 2001 in de VS radicaliseerde hij. Hij ging op het internet op zoek naar informatie over de islam.¹⁵¹ In de casus van de zogeheten Belgische cel van al Qa’ida zou de jihadistische site Minbar SOS een rol hebben gespeeld om individuen te identificeren die bereid zijn tot de gewapende strijd om ze na verloop van tijd, fysiek te rekruteren (zie paragraaf 3.2.5). Eén van de in de zomer van 2008 door de Turkse politie opgepakte personen zou hebben verklaard dat er voortdurend oproepen waren tot jihad op Minbar SOS. De propagandavideo’s die hij daar zag, waren voor hem reden om zich aan te melden.¹⁵²

Europol geeft aan dat de rol van het internet op radicalisering zelden helder is, maar dat het buiten twijfel is dat het internet een rol heeft gespeeld in de radicalisering van verdachten uit opsporingsonderzoeken

141 Sageman 2008a, p. 114-115.

142 NCTb 2007, p. 90.

143 Antheunis 2009, UvA 2009.

144 Sageman 2008a, p. 116-117.

145 Sageman 2008a, p. 116-117.

146 Sageman 2008a, p. 116-117, ICSR 2007, p. 51.

147 ICSR 2007, p. 50-52.

148 ICSR 2009.

149 ICSR 2007, p. 50-54.

150 ICSR 2007, p. 50-54.

151 Haegens 2009.

152 Cruickshank 2009a.

in het Verenigd Koninkrijk. Europol spreekt verder uit dat rekrutering via het internet een bron van zorg is, maar stelt wel dat het internet nooit de persoonlijke interactie tussen potentiële rekruten en rekruteur kan vervangen. Aan de andere kant geeft Europol aan dat een bekeerling in het Verenigd Koninkrijk die in 2008 een bom had geplaatst in een restaurant in Zuidwest-Engeland zelf was geradicaliseerd en was aangemoedigd door literatuur en ander materiaal op het internet. Doordat de bom te vroeg was afgegaan, raakte alleen hij zelf gewond.¹⁵³

Volgens Sageman heeft het internet de aard van de terroristische interacties gewijzigd. Tot 2004 kwamen netwerken merendeels voort uit fysieke interactie tussen vrienden. Daarna wijzigde dat in interactie via het internet.¹⁵⁴ Toch stelt hij ook dat terroristische netwerken een mengsel zijn van online en offline elementen en de virtuele en fysieke netwerken en contacten onderling.¹⁵⁵

3.3.3.1 Beoordeling dreiging

De inzichten over de invloed van het internet op radicalisering zijn niet wezenlijk veranderd. 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. Er gaat meer dreiging uit van interactieve sites, waaronder sociale netwerksites of fora, dan vanuit statische sites waar bijvoorbeeld alleen documenten kunnen worden gedownload. Juist de interactiviteit van het jihadistische internetgebruik is toegenomen en daardoor de invloed van het internet op radicalisering. Als gevolg van de toegenomen interactiviteit is het steeds lastiger een onderscheid te maken tussen propaganda, rekrutering, virtuele netwerkvorming en de invloed van het internetgebruik op radicalisering in het geheel. Het internet beïnvloedt radicalisering, maar de in de literatuur lopen de meningen uiteen over de mate waarin het internet de enige of de doorslaggevende factor is. De conclusie luidt nog steeds: internetgebruik ondersteunt het gehele proces van radicalisering.

3.3.4 Creatie van virtuele netwerken: aanvullende of nieuwe inzichten

Sociale netwerksites zoals Facebook en Hyves zijn populair. Ook jihadisten maken gebruik van de mogelijkheden van sociale netwerksites voor het vormen en/of onderhouden van netwerken. Volgens Sageman zijn terroristische netwerken een mengsel van online en offline elementen en de virtuele en fysieke netwerken en contacten onderling.¹⁵⁶ Zoals eerder aangegeven bestaat een debat in hoeverre radicalisering en rekrutering alleen via het internet kunnen optreden. Ook bij de netwerkvorming doet zich die vraag voor. Dat interactie via het internet bij kan dragen aan netwerkvorming, kan worden afgeleid uit het feit dat in het algemeen via het internet eenvoudig nieuwe contacten kunnen worden gelegd, vriendschappen kunnen ontstaan of mensen kunnen besluiten collectief zelfmoord te plegen (zie paragraaf 3.3.3).

3.3.4.1 Beoordeling dreiging

Het is nog steeds aannemelijk dat door de vorming van virtuele netwerken een informele pool van bereidwilligen voor de jihad kan ontstaan die in wisselende combinaties met elkaar of individueel geweldsactiviteiten kunnen ontplooiën. Lokale en internationale elementen kunnen daardoor meer met elkaar

¹⁵³ Europol 2009, p. 17-21.

¹⁵⁴ Sageman 2008a, p. 109-110.

¹⁵⁵ Sageman 2008a, p. 121.

¹⁵⁶ Sageman 2008a, p. 121.

verweven raken. De conclusie luidt: het internet biedt mogelijkheden voor vorming van virtuele netwerken; deze verhogen de slagkracht van de jihadistische beweging.

3.3.5 Rekrutering: aanvullende of nieuwe inzichten

Als het gaat om rekrutering via het internet is het beeld bestendigd van een permanente en interactieve mix van top-down en bottom-up informatieverschaffing en -inwinning, vermengd met online aanmoediging, -sturing of -netwerkvorming. Hierdoor is het onderscheid tussen propaganda, radicalisering en rekrutering niet altijd goed te maken. Ook het onderscheid tussen rekrutering in de strikte zin van het woord, conscriptie of zelf-rekrutering is niet altijd goed te maken (zie ook paragraaf 3.3.3).

Het ICSR stelt omtrent internet en rekrutering:

- *The internet has come to play an increasingly important role. The main function is to support 'real-world' recruitment (by reinforcing religious and political themes; by facilitating networking; and by creating a climate of exaggeration). In recent years, however, new forms of Islamist militant online activism have emerged, which rely less on human contact and can be described as 'virtual self-recruitment'.*¹⁵⁷

Een tweetal voorbeelden kan de wijze waarop rekrutering plaatsvindt illustreren. Ten tijde van de herpublicatie van de Deense cartoons in september 2007 was een oproep te lezen op een forum van het eerdergenoemde al-Ekhlaas voor een zelfmoordbrigade.

- *"We are registering a suicide brigade here, which is on the way to Denmark (...) I ask you to register your names in order to spread fear among the Danish people and show them how much we love Allah's messenger (...) For me it would be an honour to be the first suicide bomber."*¹⁵⁸

Hoewel al-Ekhlaas een prominente jihadistische website was, is het, zoals eerder aangegeven, lang niet altijd helder welke waarde aan een posting op een dergelijke website moet worden gehecht. Het toenmalige hoofd van de Deense inlichtingendienst (PET) heeft destijds geweigerd commentaar te leveren.¹⁵⁹ Bovendien oogt deze oproep ook niet echt als een professionele manier van rekrutering, eerder als een spontaan initiatief. Rekruteurs kunnen uiteraard hier wel op inspelen door juist deze personen te benaderen. Een tweede voorbeeld van 'rekrutering' is de ondersteunende rol die de Franstalige jihadistische site Minbar-SOS (zie paragraaf 3.2.5) speelde.

Voorbeelden van zelfrekrutering of zelfontbranders, ook wel aangeduid als 'lone wolves' blijven schaars, maar zijn er wel.¹⁶⁰

De onderzoekers van het ICSR geven aan dat het internet een strijdgebied zal worden voor Europese beleidsmakers om de groei van militante jihadistische rekrutering tegen te gaan.¹⁶¹

3.3.5.1 Beoordeling dreiging

Het is niet aannemelijk dat iemand zich vanuit Nederland via het internet rechtstreeks en één-op-één laat rekruteren door rekruteurs van internationale terroristische groeperingen. Wel bieden de interactieve jihadistische sites een uitgelezen plaats om te rekruteren. Daar bevinden zich immers personen die

¹⁵⁷ ICSR 2007, p. 55.

¹⁵⁸ BBC Monitoring 2007.

¹⁵⁹ Voor dat laatste: BBC Monitoring 2007.

¹⁶⁰ Zie bijvoorbeeld voorbeelden genoemd in US Senate Committee 2008, p. 12-15, 52, ICSR 2007, p. 52-54 en Europol 2009, p. 17-21.

¹⁶¹ ICSR 2007, p. 55.

vergaand in de jihad zijn geïnteresseerd. Feit is ook dat jongeren zich aangetrokken voelen tot jihadistische strijdtoneelen en via het internet op zoek gaan naar een manier om daar te komen. Op het internet is een sterk interactieve vorm van rekrutering waarneembaar die sterk gekoppeld is aan de interactieve manieren van propaganda bedrijven. Er valt echter vanwege de diversiteit in casuïstiek geen algemeen patroon te benoemen, anders dan dat rekrutering via het internet op interactieve wijze verloopt en dat veelal eerder sprake is van zichzelf aanmelden dan van rekrutering in de klassieke zin van het woord. De conclusie luidt derhalve: rekrutering via het internet verloopt vooral op een interactieve wijze.

3.3.6 Informatie-inwinning: aanvullende of nieuwe inzichten

Op het internet verschijnen veel toepassingen die gedetailleerde informatie bieden. Het kan hierbij bijvoorbeeld gaan om informatie over mogelijke doelwitten, kwetsbare plekken, personen, organisaties en beveiligingsmaatregelen. Deze paragraaf staat stil bij enkele toepassingen en het (mogelijke) gebruik daarvan door jihadisten.

Het internet biedt steeds meer mogelijkheden om satellietbeelden en luchtfoto's van alle mogelijke plekken op aarde vanachter de computer te bekijken. In navolging van Google Earth, heeft ook Microsoft een kaarttoepassing uitgebracht: Microsoft Live Maps (Microsoft Virtual Earth), dat nu onderdeel is van Bing. Deze toepassing biedt min of meer dezelfde kwaliteit foto's als Google Earth en biedt ook een faciliteit waar enkele steden en landschappen in driedimensionale vorm kunnen worden bekeken. Er komen steeds meer aanbieders van gedetailleerde satelliet- en luchtfoto's. Ook wordt de resolutie van satellietbeelden steeds hoger en worden de beelden vaker ververst, mogelijk zelfs tot (maximaal) vier maal per jaar.

Afgezien van satelliet- en luchtfoto's, zijn ook veel beelden op straatniveau beschikbaar via het internet. Met een street view-applicatie die gekoppeld is aan Google Maps is het mogelijk op een plattegrond een plaats aan te klikken, waar je wilt gaan 'staan'. Vervolgens wordt van die plaats een panoramisch (360 graden) uitzicht gegeven. De satellietbeelden en luchtfoto's zijn veelal ook verbonden met andere informatie, zoals straatnamen, foto's en bedrijven of bezienswaardigheden. Via de site Panoramio zijn per locatie op een digitale kaart foto's van de omgeving te downloaden, die internetgebruikers zelf kunnen uploaden. Ook andersoortige fotosites als Flickr, waar mensen hun gewone foto's op kunnen zetten, krijgen steeds meer mogelijkheden. Zo kan Flickr inmiddels ingezonden foto's via de labels die mensen aan de foto's koppelen aan elkaar plakken. Hierdoor kunnen driedimensionale wandelingen worden gemaakt over bijvoorbeeld het San Marcoplein in Venetië en andere beroemde plaatsen op aarde. Het is dan ook te verwachten dat er in de toekomst steeds meer en steeds recenter beeldmateriaal (foto's en video's) op straatniveau op het internet beschikbaar zal zijn, gekoppeld aan een bepaalde gps-locatie op een digitale kaart. Dit betekent dat van gevoelige objecten zowel van de bovenkant als van de buitenkant een nauwkeurig en recent beeld kan worden verkregen via het internet. Ook komen vele andere details van gebouwen beschikbaar via het internet, bijvoorbeeld in de vorm van livebeelden van de ontbijtzaal van een hotel of in de vorm van informatie van de overheid, zoals bouwvergunningen. Ook dit soort informatie kan behulpzaam zijn bij het plannen van aanslagen.

Op het internet is ook veel informatie over personen te vinden. Veel mensen hebben een profiel van zichzelf op een sociale netwerksite zoals Hyves, LinkedIn, Facebook of MySpace. Daarnaast houden sommige mensen ook blogs bij of gebruiken real time communicatiesites als twitter. Er zijn ook internettoepassingen

die informatie bieden over de locatie van personen, zelfs de actuele. Een voorbeeld daarvan is Google Latitude, een toepassing waarmee het via internet mogelijk is om iemands gangen na te gaan.

Naar verwachting zal de informatie die over personen op het internet te vinden is in de toekomst alleen nog maar toenemen, alsmede de toegankelijkheid van deze informatie. Zo zijn onlangs Hyves-pagina's geïndexeerd via Google. Door combinatie van verschillende gegevens ontstaat een veel scherper beeld van personen en van waar zij zich bevinden. Mensen geven veel informatie over zichzelf vrij, maar ook via slecht beveiligde computers kan onbewust en ongewild veel informatie over iemand beschikbaar komen. Persoonlijke informatie op het internet kan in de voorbereiding van aanslagen worden gebruikt om specifieke informatie te vergaren over bijvoorbeeld de beveiliging van objecten en personen en wie daarbij betrokken zijn.

Google Earth is een onderwerp dat onder jihadisten werd besproken. Zo werd op 8 maart 2007 een bericht op een jihadistisch forum geplaatst met een gedetailleerde kaart van de Abu Graib gevangenis in Irak. In het bericht worden lezers gestuurd naar een website waar ze 'hacks' voor Google Earth kunnen downloaden om zo de satellietkaarten te kunnen voorzien van bijvoorbeeld operationeel getinte opmerkingen en symbolen.¹⁶² Al eerder werd op jihadistische fora gewezen op het gebruik van Google Earth voor de selectie van westerse en Israëliëse doelwitten en voor voorbereidingen voor het reizen naar gebieden voor de jihad.¹⁶³ In video's van de Nood-Afrikaanse tak van al Qaeda (AQIM), liet de groep zien hoe Google Earth was gebruikt bij de voorbereiding van aanslagen in Algerije.¹⁶⁴ Leden van het Iraakse verzet maakten gebruik van Google Earth om aanvallen te doen op militaire bases van het Britse leger.¹⁶⁵ Ook de daders van de terroristische acties in Mumbai eind 2008 zouden Google Earth-beelden hebben gebruikt om de omgeving vooraf te verkennen.¹⁶⁶ Op een extremistische website werd in januari 2007 een bericht geplaatst met een link naar een webcam op een luchthaven in Alaska, die op afstand kon worden bediend. Gebruikers konden inzoomen op de terminals en de vrachtruimtes.¹⁶⁷ Er is nog geen informatie bekend dat terroristen van foto's en video's op straatniveau gebruik hebben gemaakt bij de voorbereiding van een terroristische aanslag. Een bijzondere vorm van informatie-inwinning is het gebruik van Twitter tijdens aanslagen. De Indiase politie waarschuwde ten tijde van de aanslagen in Mumbai eind november 2008 dat ook de aanslagplegers mee konden lezen en zo voorzien konden worden van voor hen belangrijke informatie over politiesterke, eventueel nog in het gebouw aanwezig zijnde personen en dergelijke.¹⁶⁸

De beschikbaarheid van satellietbeelden, luchtfoto's en ander beeldmateriaal evenals (of gecombineerd met) persoonsinformatie via het internet, maakt de voorbereidingshandelingen van terroristen gemakkelijker. Toch lijkt voor een echt goede voorbereiding een fysieke verkenning een vereiste. Immers, beelden zijn verouderd waardoor bijvoorbeeld recente wijzigingen of wegopbrekingen niet te zien zijn, zaken als de mate van beveiliging zijn veelal alleen plaatselijk te zien en de beelden zijn onvoldoende scherp.

¹⁶² Site 2007c.

¹⁶³ Site 2007d.

¹⁶⁴ Burton 2007b.

¹⁶⁵ Daily Telegraph 2007.

¹⁶⁶ Blakely 2008, Weizhen & Singh 2008.

¹⁶⁷ Canadian Press 2007.

¹⁶⁸ Nu.nl 2008, Friesch Dagblad 2008.

Bovendien is kijken naar beelden via het internet nog wat anders dan opereren in een vijandige en fysieke omgeving zonder op te vallen.¹⁶⁹

3.3.6.1 Beoordeling dreiging

Internettoepassingen bieden vele mogelijkheden voor informatie-inwinning en terroristen bespreken die mogelijkheden of maken daar al gebruik van. De mogelijkheden die deze toepassingen bieden, maken de voorbereidingshandelingen van terroristen eenvoudiger. De toepassingen leveren op een gemakkelijke en anonieme manier informatie over een bepaald object, locatie, organisatie of persoon en zij verminderen de noodzaak om verkenningen ter plaatse uit te voeren. De informatie is toegankelijk doordat organisaties of personen onvoldoende veiligheidsbewust zijn en online veel informatie over zichzelf en hun omgeving prijsgeven. Toch is een deel van de informatie ook op andere wijze verkrijgbaar, bijvoorbeeld met luchtfoto's via commerciële partijen. Bovendien lijkt voor een echt goede voorbereiding een fysieke verkenning een vereiste. Naar verwachting zullen de mogelijkheden voor informatie-inwinning in de toekomst alleen nog maar verder toenemen. Bovendien zal het internet in de toekomst nog meer dan nu altijd en op iedere locatie beschikbaar zijn. Meer dan voorheen zijn toepassingen voor informatie-inwinning via het internet potentieel ondersteunend bij het plegen van terroristische activiteiten.

3.3.7 Fondsenwerving

In potentie bestaan vele mogelijkheden voor fondsenwerving door en voor jihadisten. Een eerste variant betreft rechtstreekse en openlijke fondsenwerving via sites. Een tweede variant is de benutting van profiling, e-commerce tools en het plegen van (online) fraude. Een derde variant is die van exploitatie en misbruik van liefdadigheidsinstellingen. In veel zo niet vrijwel alle literatuur die handelt over het gebruik van het internet door terroristen of jihadisten noemen de auteurs fondsenwerving. Toch levert dat weinig nieuwe voorbeelden op van fondsenwerving via het internet. In Duitsland zou een site hebben opgeroepen geld te doneren voor de jihad door de Taliban. Ieder bedrag, hoe laag ook, was welkom. Op de primitieve site werden twee emailadressen gegeven voor verdere informatie: één voor mannen en één voor vrouwen. De site was gelieerd aan de eerder genoemde GIMF.¹⁷⁰ Hoewel Second Life zou kunnen worden misbruikt als financieel transactiemedium of voor het witwassen van gelden (zie paragraaf 3.2.2), zijn er geen voorbeelden bekend bij de NCTb. Het internet biedt voor fondsenwerving door jihadisten weliswaar voordelen, maar ook nadelen. Dat jihadisten de drie genoemde mogelijkheden voor fondsenwerving via het internet gebruiken, is nog steeds aannemelijk. De in de fenomeenstudie genoemde mogelijke verschuiving van meer openlijke naar meer heimelijke fondsenwerving heeft zich voor zover bekend niet voorgedaan.

Verder is de verwachting uitgesproken dat fondsenwerving via het internet kan gaan toenemen als gevolg van nieuwe digitale en anonieme betalingsmiddelen. De SITE Intelligence Group meldde eind 2006 dat de maanden daarvoor het gebruik van CashU toenemende aandacht had gekregen in jihadistische fora op het internet en dat er aanwijzingen waren dat Iraakse verzetsgroepen dit middel ook daadwerkelijk gebruiken. Ten opzichte van andere meer klassieke betalings- en overschrijvingsmethoden zijn er extra mogelijkheden om min of meer anoniem goederen via het internet te bestellen of de huur van webruimte te betalen.

¹⁶⁹ De kanttekeningen bij nut virtuele toepassingen bij de voorbereiding van aanslagen zijn afkomstig van Burton 2007a, Burton 2007b en Stratfor 2007.

¹⁷⁰ Voorbeeld afkomstig van BBC Monitoring 2008.

Verzending van goederen naar een fysiek adres levert echter toch weer sporen op. Er zijn daarnaast extra handelingen nodig als de ontvangers het geld, anders dan via internet, willen besteden en dergelijke handelingen kunnen resulteren in ongewenste sporen. In dat geval is immers een overgang naar baar of giraal geld noodzakelijk. Bovendien verlangt bijvoorbeeld CashU enkele persoonsgegevens, wat eveneens afbreuk doet aan de anonimiteit.¹⁷¹ Er is dus wel wat af te dingen op het gemak voor fondsenwerving en de anonimiteit. Bovendien zijn de nieuwe betalingsmogelijkheden op enige wijze veelal gekoppeld aan het reguliere betalingsverkeer. Er zijn geen voorbeelden bekend van het gebruik van digitale en anonieme betalingsmiddelen. De verwachte toename van het gebruik daarvan is dus niet uitgekomen en er is op dit moment geen aanleiding om aan te nemen dat dit wel zal toenemen.

3.3.7.1 Beoordeling dreiging

In potentie bestaan nog steeds vele mogelijkheden voor fondsenwerving door en voor jihadisten. Er zijn enkele voorbeelden van deze varianten bekend, maar het komt in de praktijk nog weinig voor. De verwachte toename van het misbruik van bankieren via het internet en de verwachte verschuiving van meer openlijke naar meer heimelijke fondsenwerving zijn niet uitgekomen. De conclusie luidt: fondsenwerving via het internet door en voor jihadisten komt (nog steeds) beperkt voor.

3.3.8 Training: Aanvullende of nieuwe inzichten

Velen hebben aangegeven dat het internet de rol van fysieke trainingskampen had overgenomen of kon overnemen. Inmiddels is wel duidelijk dat de jihadistische beweging nog steeds hecht aan fysieke trainingskampen en dat deze bestaan in vooral het grensgebied van Afghanistan en Pakistan en in Somalië. Onder andere vanuit Europa, de VS en Australië vertrekken ook daadwerkelijk personen naar die trainingskampen.

Rogan en Stenersen stellen dat er een overvloed is aan militaire en tactische trainingshandleidingen op jihadistische webpagina's. Over vrijwel alle onderwerpen die relevant kunnen zijn voor training en voorbereiding zijn handleidingen te vinden. De bronnen variëren van Engelstalige open bronnen tot materiaal afkomstig van ervaren jihadistische commandanten of trainers. Er circuleren ook rond de vijftig Arabischstalige instructievideo's op allerlei jihadistische sites. Ongeveer twintig daarvan zijn van hogere kwaliteit. Deze video's zijn gemaakt door het Libanese Hezbollah, dat strikt genomen niet behoort tot de jihadistische beweging (zie Bijlage 1). Temidden van de grote hoeveelheid aan materiaal is het lastig om het materiaal van hoge kwaliteit te vinden. Het trainingsaanbod is eerder afkomstig van onderop dan van bovenaf. Met andere woorden, het materiaal is niet echt afkomstig van kern al Qa'ida.¹⁷²

Naast trainingsmateriaal fungeert het internet ook als een soort klaslokaal. Geïnteresseerden kunnen discussiëren over trainingsgerelateerde vraagstukken, persoonlijke ervaringen uitwisselen en communiceren met virtuele trainers die problematische onderwerpen kunnen uitleggen en verduidelijken. De jihadistische fora zijn echter een arena voor beginners en aspirant-jihadisten. Het is niet een instrument voor ervaren jihadistische groepen om de nieuwste inzichten op grote schaal te verspreiden. Zij zijn zich bewust van het meekijken door tal van inlichtingenorganisaties wereldwijd. Het internet is daarom eerder een bibliotheek of klaslokaal van de jihad dan de vaak genoemde universiteit voor de jihad. Dit laat onverlet

¹⁷¹ Voor dat laatste, zie Katz & Devon 2006, Holahan 2006.

¹⁷² Rogan & Stenersen 2008.

dat actueler en geavanceerder trainingsmateriaal kan worden uitgewisseld buiten het openbare deel van het internet om, bijvoorbeeld met behulp van e-mail.¹⁷³

Dat het openbaar verkrijgbare trainingsmateriaal niet altijd van hoge kwaliteit is, geen succes garandeert of kan leiden tot gevaarlijke situaties, blijkt uit de volgende casus. Op 31 juli 2006 hebben twee Libanese mannen geprobeerd twee regionale treinen op te blazen in Duitsland met behulp van explosieven die zij aan de hand van een online handleiding hadden gemaakt. De kofferbommen gingen echter niet af, doordat de aanslagplegers op een bepaald punt waren afgeweken van de handleiding.¹⁷⁴ Net als dat online informatie-inwinning niet de plaats kan innemen van een fysieke verkenning, geldt dat een online training niet een fysieke training volledig kan vervangen. Lezen hoe te opereren in een vijandige omgeving is nog wat anders dan het werkelijk doen. Ook de ervaring van docenten is van belang.

Toch kan het materiaal wel bijdragen aan een proces van radicalisering en terroristische acties laag-drempeliger maken, zeker als echte training in een kamp niet haalbaar is. Het materiaal draagt verder bij aan de jihadistische machocultuur die aantrekkelijk kan zijn voor jongeren. Het kan ook helpen bij de voorbereiding voordat aspirant jihadisten naar trainingskampen of strijdtonelen trekken.¹⁷⁵ Er is echter geen bevestigde casus bekend waarbij een succesvolle aanslag is gepleegd met behulp van online trainingsmateriaal alleen,¹⁷⁶ hoewel in het geval van de mislukte aanslag in Duitsland het materiaal van het internet is gebruikt en dit in een geval van het Verenigd Koninkrijk uit 2008 mag worden aangenomen.

Hier en daar duiken berichten op dat online games gebruikt kunnen worden voor trainingsdoeleinden door jihadisten. Er is echter geen voorbeeld bekend waarbij terroristen of jihadisten daadwerkelijk aanslagen hebben uitgebreed in virtuele 'gamewerelden'.¹⁷⁷ Games kunnen tot op zekere hoogte natuurlijk wel inzage geven in bepaalde tactieken die in de game tot succes leiden. De realiteitswaarde daarvan voor echte aanslagen is echter betwistbaar. Feit is wel dat in juli 2009 een forumlid van een Engelstalige jihadistische website het gebruik van realistische videogames, zoals Battlefield 2, bepleitte als een goede methode van voorbereiding voor de jihad. Anderen reageerden daarop met aanvullende suggesties of vragen. Er was echter ook een tegengeluid te horen, namelijk dat fysieke activiteiten een betere voorbereiding vormen.¹⁷⁸

3.3.8.1 Beoordeling dreiging

Dat het internet de rol van fysieke trainingskampen kan overnemen, is inmiddels gelogenstraft door de praktijk waarin tal van fysieke jihadistisch trainingskampen bestaan en daar ook personen naar toe (proberen te) reizen. Het internet is eerder een bibliotheek van trainingsmateriaal en tot op zekere hoogte een virtueel klaslokaal voor beginnende jihadisten. De instructies of handleiding moet iemand nog altijd zélf goed kunnen begrijpen, daarmee oefenen, toepassen en uitvoeren. Verder kan de discipline die benodigd is voor het uitvoeren van een grootschalige aanslag in een feitelijk trainingskamp vele malen beter worden ontwikkeld. Ook kunnen bij bepaalde instructies ongetwijfeld vraagtekens geplaatst worden

¹⁷³ Rogan & Stenersen 2008 en Europol 2009, p. 21.

¹⁷⁴ ANP 2006 en Schofield 2007.

¹⁷⁵ Jane's Terrorism and Security Monitor 2008, Europol 2009, p. 21.

¹⁷⁶ Jane's Terrorism and Security Monitor 2008, Rogan & Stenersen 2008.

¹⁷⁷ Shachtman 2008.

¹⁷⁸ SITE 2009g.

ten aanzien van 'gebruiksgemak' en veiligheid. Desondanks zijn het trainingsmateriaal en de sites waar ervaringen en inzichten worden gedeeld niet ongevaarlijk. Zij kunnen, zeker door terroristen van eigen bodem, wel worden gebruikt en daardoor de drempel tot het plegen van aanslagen verlagen. De conclusie luidt: gebruik van het internet voor trainingsdoeleinden werkt (nog steeds) drempelverlagend voor het plegen van aanslagen, maar het gevaar van fysieke training en trainingskampen is groter.

3.3.9 Onderlinge communicatie en planning: aanvullende of nieuwe inzichten

Een aanwijzing dat het internet kan worden gebruikt voor operationele communicatie, blijkt bijvoorbeeld uit het feit dat in Casablanca een terrorist zichzelf met een bomgordel heeft opgeblazen in een internet-café. Volgens berichten zou hij daar instructies hebben willen ontvangen via het internet voor een serie van (zelfmoord)aanslagen. Toen dat niet lukte en de eigenaar van het café de politie had gebeld, heeft hij zich opgeblazen.¹⁷⁹ Ook de man van Malika el-Aroud zou volgens open bronnen vanuit het grensgebied van Afghanistan en Pakistan contact onderhouden met zijn vrouw via e-mail en via Skype, een vorm van telefonie via het internet. Ook plaatste hij postings op de jihadistische site Minbar SOS (zie ook paragraaf 3.2.5). Via de jihadistische website al-Ekhlaas werd in 2008 de encryptiesoftware 'Mujahideen Secrets 2' beschikbaar gesteld, die ook chatgesprekken versleutelt.¹⁸⁰ Chatgesprekken zijn uiteraard beter geschikt voor operationele communicatie dan websites.

Volgens mediaberichten zouden de aanslagplegers in Mumbai eind november 2008 VoIP (voice over IP-telefonie via het internet) hebben gebruikt om met hun leiders in Pakistan te communiceren en specifieke instructies te ontvangen. Als zodanig is er natuurlijk geen verschil met bijvoorbeeld communicatie via mobiele telefoons, maar VoIP is lastiger of voor sommige landen niet af luisterbaar.¹⁸¹ Overigens zou de Indiase politie met behulp van de FBI wel degelijk tien IP-adressen hebben kunnen traceren. Vijf daarvan waren afkomstig van een zogeheten Proxy, waardoor het IP-adres naar een dood spoor leidde. Vijf zouden wel volgbaar zijn geweest.¹⁸² Toch is het verre van aannemelijk dat leden van kern al Qa'ida communiceren via het internet. Voor hen is het risico te groot.

3.3.9.1 Beoordeling dreiging

Dat jihadisten het internet nog steeds gebruiken om onderling te communiceren, is zeer aannemelijk. Logischerwijze vindt dit grotendeels afgeschermd plaats. Strikt genomen maakt het voor de dreiging niet uit of jihadisten communiceren met de telefoon of via het internet. Inlichtingeninstanties en de politie kunnen, net als in het geval van andere communicatiemiddelen, ook het internetverkeer onderscheppen. Jihadisten zijn zich daar van bewust en waarschuwen elkaar daar ook voor. De conclusie luidt: jihadisten gebruiken (nog steeds) het internet voor onderlinge communicatie en planning.

3.4 Slotbeschouwing

Jihadisten gebruiken het internet onverminderd als middel. In lijn met het algemene gebruik van het internet en de opkomst van web 2.0 geldt dat het gebruik door jihadisten interactiever is geworden. Die toegenomen interactiviteit vereenvoudigt het voeren van propaganda, netwerkvorming en 'rekrutering'

¹⁷⁹ AFP 2007.

¹⁸⁰ Webwereld 2008a.

¹⁸¹ Business Line 2009.

¹⁸² United News of India 2009, Times of India 2009.

evenals communicatie en planning onderling. Als gevolg van de interactiviteit is het effect van het gebruik van het internet door jihadisten op radicalisering groter, zeker voor wat betreft propaganda. Toch is de mate waarin het internet van invloed is, nog niet helder. Is het één factor of dé factor? Geconcludeerd kan worden dat er een dreiging uitgaat van het gebruik van het internet als interactief communicatiemedium. Verder gaat een dreiging uit van de ondersteunende rol die het internet speelt voor jihadisten bij (de voorbereiding van) terroristische activiteiten. Naast fondsenwerving en communicatie en planning onderling, komt die dreiging vooral voort uit het aanwenden van het internet voor de creatie van virtuele netwerken, voor trainingsdoeleinden en voor informatie-inwinning. Het internet kan echter de rol van trainingskampen niet overnemen waardoor van die kampen een groter gevaar uitgaat. Evenmin kan het internet de rol van fysieke verkenningen volledig overnemen.

Geconcludeerd kan worden dat het internet voor de jihadistische beweging een cruciaal middel is en zal blijven.

4 Jihadisme op het Nederlandse internet

4.1 Inleiding

De fenomeenstudie bevatte een inventarisatie van de manifestatie van jihadistische uitingen op het Nederlandse internet. Ten aanzien van Nederlandse jihadistische websites bleken drie, deels overlappende, categorieën te onderkennen, die ook te bezien zijn als perioden:

- op het buitenland georiënteerde jihadistische sites in Nederland (2000-2001);
- Nederlandse jihadistische sites met een buitenlandse oriëntatie (2002);
- Nederlandse jihadistische sites gericht op Nederland (2003-2006).

Nederlandse jihadisten richtten zich primair op het ordenen, aanbieden en verspreiden van jihadistische informatie en materiaal, vaak via gratis websites, zoals tk.domeinen, geocities en freewebs. Deze informatie betrof onder andere in het Nederlands vertaalde literatuur over het voeren van de gewelddadige jihadistische strijd, verklaringen van al Qa'ida en de voorgeschreven omgang met 'ongelovigen' (niet-moslims). Deze websites werden gekenschetst als jihadistische 'materiaalwebsites'. Het gebruikmaken van gratis webruimte bleek aantrekkelijk omdat het nauwelijks registratie en administratie vereiste en anonimiteit bood. In de periode 2003 tot en met 2005 bleken Microsoft Network (MSN) groepen zeer populair onder jihadisten. 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. Voorbeelden hiervan waren onder andere groups.msn.com/zustersinrotterdam en groups.msn.com/supportersOfTheSjariah. De jihadistische MSN-groepen waren vooral populair onder jongeren, onder wie enkele leden van de Hofstadgroep. De MSN-groepen, met veelal expliciet jihadistische namen, verdwenen gedurende een korte periode om weer elders op te duiken met een nieuwe naam en met een nieuw uiterlijk. Nadat er onder andere in de media bekend werd dat er veel jihadistische uitingen op MSN stonden, besloten de beheerders van MSN-communities de betreffende jihadistische MSN-groepen te sluiten.¹⁸³ Hierna was het jihadistisch materiaal nagenoeg van MSN verdwenen.

De jihadistische informatie die via de verschillende sites werd aangeboden, diende primair propaganda-doeleinden. Deze uitingen van virtueel jihadisme en discussie hierover bleken zowel te traceren op jihadistische websites als op sommige webfora van neutrale signatuur. Daarnaast bleek dat vooral moslima's een belangrijk aandeel hadden bij het vertalen en verspreiden van jihadistisch materiaal op het internet.

De online-activiteiten leken destijds ook aan te sluiten bij een actieve periode van lokaal autonome jihadistische netwerken in Nederland. Uit de recente edities van het Dreigingsbeeld Terrorisme Nederland (DTN) blijkt dat de lokaal autonome jihadistische netwerken in Nederland de laatste jaren aan kracht en activiteit hebben ingeboet.¹⁸⁴ Daarnaast geldt dat bij deze personen de aandacht vooral uitgaat naar de strijd in klassieke jihadistische strijdgebieden en niet naar Nederland. In dit hoofdstuk wordt onderzocht of deze veranderingen binnen het jihadisme in Nederland zich ook na 2006 voordeden bij de manifestatie van het jihadisme op het Nederlandstalige internet. Het is hierbij wel van belang te benadrukken dat Nederlandse jihadisten uiteraard eveneens van Arabischstalige en/of Engelstalige jihadwebsites gebruik kunnen maken, maar die vallen buiten het bestek van dit hoofdstuk. Ook wordt in dit hoofdstuk geanalyseerd of eventuele wijzigingen wat betreft het jihadisme op het Nederlandse internet consequenties hebben voor de jihadistische dreiging tegen Nederland of Nederlandse belangen.

¹⁸³ Novatv.nl.

¹⁸⁴ NCTb 2009.

4.2 Nederlandse jihadistische sites sinds 2006

4.2.1 Groei jihadistische 'materiaalsites' sinds 2006 gestagneerd

Veel van de onder 4.2 genoemde jihadistische materiaalsites zijn nu verdwenen of zijn niet of nauwelijks aangevuld met nieuw (jihadistisch) materiaal. De websites die in de lucht bleven, zien er daarom in grote lijnen nog net zo uit als drie jaar geleden. Er is sprake van enkele nieuwe jihadistische materiaalsites. Het aangeboden materiaal is een gemêleerde verzameling van enerzijds vertaalde literatuur van radicale ideologen en anderzijds materiaal van eigen, Nederlandse makelij. De meeste jihadistische teksten op de jihadistische materiaalsites hebben een weinig toegankelijk karakter dat behoorlijke voorkennis van de lezer over de jihadistische ideologie veronderstelt. Het is daarom moeilijk om precieze uitspraken te doen over het bereik van de jihadistische materiaalsites, mede omdat er op deze sites geen sprake is van communicatiefuncties (zoals een forum) waar uit op te maken valt wat de reacties zijn. Het op statische, eenzijdige wijze aanbieden van jihadistisch materiaal lijkt echter niet goed meer te passen bij het huidige internettijdsgewricht van Web 2.0, waarbij juist de nadruk ligt op de interactiviteit tussen content-aanbieder en -afnemer.

4.2.2 Weinig activiteiten op weblogsites

Het gebruikmaken door jihadisten van (gratis) weblogsites, waarop een auteur een bericht (blog) kan plaatsen en waar vervolgens lezers op kunnen reageren, is de laatste jaren in beperkte mate voortgezet. De blogbijdrages zijn veelal korter en hebben vaker een persoonlijke boodschap in vergelijking met de lange jihadistische artikelen die op de bovengenoemde materiaalsites staan. Ondanks dat het technisch mogelijk is te reageren op de geplaatste jihadistische boodschappen, gebeurt dit zelden. Er staan op de jihadistisch-georiënteerde blogsites vaak diverse hyperlinks naar soortgelijke websites, waardoor een substantieel gedeelte van het Nederlandstalige jihadistische materiaal door de gebruiker snel online kan worden geraadpleegd. Hierdoor wordt een zogenaamde 'sneeuwbalmethode' voor de jihadistische geïnteresseerde mogelijk. Niettemin blijft het aantal van dergelijke Nederlandse 'jihadblogs' beperkt tot ongeveer vijf.

4.2.3 Thabaat.net (2007-2009): professionalisering, isolering en internationalisering van het jihadisme

Naast de bovengenoemde gratis jihadistische websites waren er sinds 2006 ook twee nieuwe jihadistische websites met een eigen domeinnaam in de lucht, waaronder Thabaat.net die reeds enige tijd offline is. De servers van de twee websites bevonden zich in het buitenland, die van Thabaat in de Verenigde Staten, mogelijk vanwege minder strikte wet- en regelgeving betreffende uitlatingen op het internet.

In juni 2007 werd de professioneel vormgegeven website www.thabaat.net opgezet en geregistreerd vanuit Brussel, waarop veelvuldig video's van de grote jihadistische mediaorganisaties (zie 3.2.1) werden geplaatst. In april 2009 had de website in totaal 286 geregistreerde forumleden, inclusief gebruikersnaam en wachtwoord, die op het webforum diverse discussies voerden over de wenselijkheid van de gewelddadige jihad en aanverwante politiek-religieuze zaken. In de rubriek 'Ummah Nieuws' kwamen eveneens actuele kwesties aan de orde. Thabaat.net was hiermee het enige grootschalige interactieve webforum waar Nederlandstalige jihadisten elkaar virtueel ontmoetten. De website werd volgens de internettool Statbrain.com tot die tijd gemiddeld door 1.300 bezoekers per dag bezocht. De website bleek, ondanks de professionele vormgeving, echter opvallend vaak offline te zijn, zoals periodes in zowel in 2007 als 2008. Vanaf mei 2009 is de website, al dan niet definitief, offline. Een beheerder van Thabaat.net

verklaarde in het voorjaar van 2009 op het forum dat 'joden en kuffaar de website [digitaal] aanvallen.' Hoe dan ook zorgt deze langdurige offline status voor een abrupte onderbreking van het jihadistische discours op het Nederlandse internet.

Een opvallend gegeven is dat vanaf hetzelfde ip-adres de Engelstalige website Revolution.thabaat.net met als ondertitel 'The ignored puzzle pieces of knowledge' werd onderhouden. De website in blog-formaat werd vanaf december 2007 bijna dagelijks aangevuld met jihadistische onderwerpen, met onder andere berichten over de bewondering van mujahideenstrijders in Pakistan, al Qa'ida en de invoering van de sharia. Deze internationale versie van Thabaat sloot qua vormgeving en inhoud erg aan op andere Engelstalige jihadistische websites, waaruit blijkt dat die laatste mogelijk als inspiratiebron hebben gegolden. Dat [Revolution.thabaat](http://Revolution.thabaat.net) ook de aandacht trok van andere toonaangevende Engelstalige jihad-sites, bleek uit de diverse hyperlinks die op deze sites naar [Revolution.thabaat](http://Revolution.thabaat.net) verwezen. [Revolution.thabaat](http://Revolution.thabaat.net) deelde hetzelfde ip-adres met Thabaat.net en is dus eveneens sinds mei 2009 offline.

4.2.4 Nieuwe jihadistische website: centralisering van jihadistische informatie

Enkele maanden nadat Thabaat.net van het web verdween, werd een nieuwe Nederlandstalige jihad-website opgericht. De nadruk bij de nieuwe website ligt voornamelijk op het aanbieden van in het Nederlands vertaalde jihadistische literatuur en video's, die deels dateren uit de periode 2004-2007. Communicatiefaciliteiten voor de websitebezoekers, zoals destijds op [Thabaat](http://Thabaat.net), worden op de website in zeer beperkte mate aangeboden. Het doel van de websitebeheerders lijkt primair om alle Nederlandstalige jihadistische informatie te bundelen en die op een centrale plaats aan te bieden. De informatie richt zich, net als [Thabaat](http://Thabaat.net) destijds, vooral op de buitenlandse jihadistische strijdgebieden.

4.3 Jihadisme op salafistische sites

In tegenstelling tot het beperkte aantal jihadistische websites op het Nederlandse internet, nam het aantal salafistische websites op het Nederlandse internet in de periode 2006-2009 toe. Als kritisch wordt gekeken naar de aanwezige salafistische websites in Nederland, blijkt dat de websites op de eerste plaats een ultra-orthodoxe religieuze oriëntatie hebben, waarbij kennisvergaring over de salafistische aqiedah (geloofsleer) en manhadj (geloofsmethodologie) centraal staat. Op de waargenomen salafistische websites zijn geen secties over de (gewelddadige) jihad aangetroffen. Ook door vooraanstaande salafistische geleerden en imams wordt via online preken stellinggenomen tegen de jihadistische ideologie. Op het belangrijkste salafistisch-georiënteerde webforum Ansaar.nl blijken echter wel enkele jihadistische forumleden actief te zijn, hoewel ze veruit in de minderheid zijn. Zij plaatsen daarbij in sommige gevallen vertaalde jihadistische artikelen zoals het artikel '44 manieren om de jihad te voeren' van de radicale Amerikaans-Jemenitische geestelijke Anwar al-Awlaki of uiten doodsverwensingen en bedreigingen aan het adres van vermeende beledigers van de islam. Over het algemeen leiden dergelijke opmerkingen tot verhitte interne salafistische discussies over de verschillende betekenissen van de jihad, waar ook geweldloze interpretaties van bestaan.

4.4 Jihadisme op salafistische sites

4.4.1 Afname jihadistische uitingen op islamitische mainstreamsites

In de periode 2004-2007 was een groot aantal jihadisten actief op Marokko.nl, de grootste islamitische jongerenwebsite van Nederland. Zowel binnen de actualiteitensectie als het subforum 'Islam en ik' werd door forumleden met jihadistische online pseudoniemen opgeroepen tot de gewelddadige jihad en werd

veelvuldig (vertaalde) jihadpropaganda verspreid. Hierdoor kwamen veel argeloze bezoekers in aanraking met de ideologie van het jihadisme. Sinds 2007 is het aantal jihadistische uitingen echter sterk afgenomen. Dit is heeft waarschijnlijk meerdere oorzaken. Ten eerste is het modereerbeleid op de website toegenomen en verbeterd. Radicale uitingen worden indien gesignaleerd sneller dan voorheen verwijderd. Ten tweede is het aantal islamcritici op Marokko.nl gegroeid. Dit heeft tot gevolg gehad dat de islam in veel discussies wordt aangevallen, hetgeen waarschijnlijk voor jihadisten aanleiding is geweest om zich niet meer actief in discussies te mengen. Ten derde heeft het besef bij jihadisten dat opsporingsdiensten meekijken er voor gezorgd dat er minder openlijk over jihadistische intenties wordt gecommuniceerd. Dit betekent overigens niet dat jihadisten totaal niet meer trachten hun gedachtegoed via Marokko.nl te verspreiden. Zo werd op Marokko.nl in juni 2008 de lancering kenbaar gemaakt van de Nederlandse tak van een jihadistisch radiostation, Sana-Al-Islam geheten, die via Profilepitstop.com in het Nederlands te beluisteren was. Er werd bij de posting vermeld dat de zender behoorde tot de organisatie 'Qaidat al-Tawheed en Al-Jihaad'.¹⁸⁵ Bij deze forumbijdrage werd de lezers opgeroepen de hyperlink op andere webfora te verspreiden. De Nederlandstalige online jihadistische radiozender Sana bleek overigens een kortstondig fenomeen: midden 2009 bleek de zender niet meer traceerbaar.

Ook Maroc.nl heeft niet of nauwelijks te kampen met jihadistische uitingen door forumleden. Islamitische forumleden op deze website spreken zich expliciet uit tegen gewelddadige interpretaties van de islam: er is sprake van een weerwoord tegen bijvoorbeeld terroristische aanslagen uit naam van de islam door al Qa'ida.

4.4.2 Jihadisme op neutrale websites sinds 2006

4.4.2.1 Hyves.nl lijkt onder jihadisten in Nederland niet populair

Het is voorstelbaar dat Hyves.nl in het kader van propagandavoering of onderlinge jihadistische communicatie een geschikt middel voor jihadisten kan zijn. Toch is er op Hyves nauwelijks materiaal over de jihad te traceren. Voor communicatie tussen jihadisten lijkt Hyves.nl geen geschikt middel te zijn. Dit ligt vermoedelijk aan het uiterst openbare karakter van Hyves.nl waardoor anoniem communiceren moeilijk is. Opsporingsdiensten en veiligheidsdiensten kunnen vrij eenvoudig meekijken. Tevens wordt er op Hyves.nl actief gemodereerd waardoor onwettig materiaal spoedig van de website kan worden verwijderd.

4.4.2.2 YouTube door Nederlandse jihadisten soms benut als propagandamiddel

Er blijkt zich ook Nederlandstalig of in het Nederlands ondertiteld jihadistisch beeld- en geluidsmateriaal op YouTube te bevinden. Enkele Nederlands ondertitelde jihadistische video's waren oorspronkelijk te vinden op internationale jihadistische websites, waaronder vertaalde propagandafilmpjes van Al Shabaab, de radicaal-islamitische beweging uit Somalië.

Een bijzonder fenomeen, zichtbaar vanaf het einde van 2008, is dat er op YouTube enkele Nederlandstalige filmpjes met daarop jihadistische nasheeds (islamitische liederen zonder instrumenten) worden gepost. In deze nasheeds worden de ideologisch-politieke stellingen van al Qa'ida, onder andere betreffende de 'bezetting door de Amerikanen van het heilige Saoedi-Arabië', integraal overgenomen. Gepercipieerde

¹⁸⁵ 'Qaidat al-Tawheed en Al-Jihaad' (ook bekend als Al Qa'ida in Irak) was een jihadistische terroristische organisatie in Irak die onder leiding stond van Al Zarqawi. De organisatie maakt thans onderdeel uit van de overkoepelende organisatie 'Islamitische Staat Irak'.

misstanden worden verder aangevuld met beelden en getallen van moslimdoden in Afghanistan, Irak, Tsjetsjenië en Palestina door toedoen van het Westen. De strekking van de liederen is dat het voor de moslims noodzakelijk is om in verzet te komen tegen de onderdrukking door het Westen (benoemd als 'apen en zwijnen' en de 'joden en kruisvaarders'). Tegelijkertijd zou het merendeel van de umma geperverteerd zijn door wereldse (dounia) zaken. Jihadisten worden geportretteerd als een voorhoedebeweging die ter meerdere eer en glorie van de islam actief strijdt tegen de 'ongelovige invasielegers' in het jihadistische strijdtheater van Afghanistan. Deze elementen worden op technisch vakkundige wijze gelardeerd met dramatische video-beelden van mujahideenstrijders in onherbergzame gebieden, vermoedelijk in Afghanistan.

Het blijkt dat dergelijke jihadistische nasheeds op YouTube duizenden keren worden bekeken en veelal positief worden becommentarieerd. Onder de reagerende lezers zijn er op deze weblocaties weinig die een kritisch weerwoord formuleren tegen het gewelddadige, jihadistische vertoog. De muzikale bewieroking van de jihad in het Nederlands lijkt een tactiek van jihadisten om te appelleren aan de islamitische jeugd in Nederland die niet allemaal het standaard-Arabisch machtig is. Jihadistisch gezang en video's lijken een groter bereik te bewerkstelligen dan de bovengenoemde, 'droge' ideologisch-religieuze artikelen op de jihadistische materiaalsites. De traditioneel islamitische achtergrond van de nasheed is daarnaast vanuit de jihadistische ideologie te beschouwen als een legitiem communicatiemiddel. Daarnaast blijkt uit de video's dat de interesse van de videomakers in de eerste plaats uitgaat naar de klassieke jihadistische strijdtonelen in de wereld en niet Nederland. Deze 'internationale outlook' in de virtuele wereld komt overeen met de conclusies over de primair internationale gerichtheid van de Nederlandse jihadisten in de fysieke wereld.¹⁸⁶ Het materiaal betreft in de eerste plaats jihadistische propaganda. Aanwijzingen voor rekrutering of handleidingen voor het maken van wapens zijn op YouTube niet gevonden. Voorts moet de kwantitatieve omvang van deze Nederlandstalige, jihadistische propagandafilms niet worden overdreven: het blijft beperkt tot onder de tien.

4.4.2.3 MSN-groepen sinds 2006 door jihadisten niet meer gebruikt

Per februari 2009 zijn de diensten van MSN overgenomen door MultiPLY (geschikt voor grote groepen) en Windows Live Groups (geschikt voor groepen tot duizend personen). Hierop blijken geen expliciete jihadistische activiteiten met een Nederlands karakter te worden ontplooid. Ook in andere discussiegroepen op bijvoorbeeld Yahoo en Google blijken niet of nauwelijks te worden gesproken over de wenselijkheid en/of noodzaak van de gewelddadige jihadstrijd.

4.5 Conclusies en dreigingsimplicaties

Uitingen van jihadisme zijn nog steeds op het Nederlandse internet te vinden, maar de omvang van deze manifestatie is sinds 2006 afgenomen. Dit is waarschijnlijk te verklaren door het actieve modereerbeleid door de beheerders op de mainstreamsites, de afname van de activiteiten van jihadistische lokaal autonome netwerken in Nederland zelf en het toegenomen veiligheidsbewustzijn bij jihadisten dat door opsporingsinstanties en veiligheidsdiensten in Nederland wordt meegekeken. Niettemin is er nog steeds Nederlandstalig jihadistisch materiaal op het Nederlandse web voorradig. Wel bleken enkele sinds 2006 vormgegeven jihadistische websites veelvuldig te kampen met technische problemen en vaak offline te zijn.

¹⁸⁶ NCTb 2009.

Het Nederlandse online jihadisme richt zich bijna volledig op propagandavoering, zoals dat ook al werd geconstateerd in 2006. De propaganda loopt inhoudelijk en qua stijl op het Nederlandse internet sterk uiteen. Op statische websites wordt nog steeds (vertaalde) jihadistische literatuur aangeboden, soms nog daterend uit de tijd van de Hofstadgroep. Deze literatuur legitimeert aan de hand van vooraanstaande internationale jihadisten de gewelddadige jihad. Daarnaast is er ook meer moderne, op Web 2.0 gebaseerde, interactieve kennisuitwisseling over de jihad voorradig. De interactieve kennisuitwisseling vindt in vergelijking met de situatie in 2006 in toenemende mate geïsoleerd plaats op al dan niet afgeschermd websites (inclusief gebruikersnamen en wachtwoorden) en in mindere mate op neutrale webfora. De jihadistische liederen op YouTube trachten juist primair bij moslims een gevoel van woede tegen het Westen op te wekken en roepen op tot actie. Tevens wordt er in deze nasheeds een romantisch beeld van de gewelddadige jihad geschapen.

De jihadistische focus op het Nederlandse internet ligt hoofdzakelijk bij internationale aspecten van de jihad, te weten de traditionele strijdgebieden in Afghanistan, Pakistan maar ook - en dat is relatief nieuw - Somalië. Er zijn op het Nederlandse internet geen voorbeelden waargenomen van rechtstreekse rekrutering en/of het verspreiden van (Nederlandstalige) handleidingen over explosieven en het toepassen van wapens. Uiteraard is het zeer wel mogelijk dat rechtstreekse rekrutering buiten het zichtveld van het openbare internet wel degelijk plaatsvindt.

De constatering dat de jihadistische propaganda op islamitische (mainstream) webfora in omvang is afgenomen, betekent in theorie dat anno 2009 minder personen online in aanraking komen met de jihadistische ideologie dan in 2006. De kans op radicalisering met behulp van jihadistische websites lijkt daarom afgenomen. Ook het kritische weerwoord dat op salafistische websites veelal wordt geformuleerd tegen de gewelddadige jihad kan op de middellange termijn positieve effecten hebben.

Uiteraard kunnen voor het vergaren van jihadistische informatie, zoals al gesteld in de inleiding, Arabisch-talige en/of Engelstalige jihadwebsites worden aangewend. Een individu dat daadwerkelijk kennis wil opdoen over de gewelddadige jihad kan echter nog steeds genoeg materiaal op het Nederlandse web vinden. Zorgelijk zijn tevens de diverse positieve reacties die zijn waar te nemen bij de Nederlandstalige nasheeds op YouTube. Er blijkt nog steeds een voedingsbodem onder delen van de Nederlandse bevolking te bestaan voor de gewelddadige jihadistische boodschap.

Het feit dat in Nederland nog steeds diverse individuen, al dan niet in groepsverband, actief zijn met het online propageren van de gewelddadige jihad, maakt het niet onvoorstelbaar dat bepaalde personen (door)radicaliseren.

Bijlage

Jihadisme, jihadistische beweging, jihadistisch terrorisme en online jihadisme

In veel moslimlanden is de islam de afgelopen decennia een steeds belangrijkere politieke factor geworden. Tal van politieke partijen en bewegingen ontleen hun doelen en activiteiten aan de islam. In dat kader wordt wel gesproken van 'politieke islam' of 'islamisme'. Het islamisme kan zowel soennitisch als sji'itisch van aard zijn. Het salafisme en het jihadisme, twee stromingen binnen het islamisme, zijn soennitisch evenals de Moslimbroeders, de Hizb-u Tahrir (HuT)¹⁸⁷ en Hamas. Hezbollah is sji'itisch.

Binnen het islamisme is (onder andere) een onderscheid aan te brengen in de wijze waarop veranderingen worden nagestreefd: gewelddadig of niet-gewelddadig. Kenmerkend voor de niet-gewelddadige stroming is dat deze geen geweld praktiseert of bepleit voor realisatie van de beoogde veranderingen. Het jihadisme valt onder 'gewelddadig islamisme'.

Het jihadisme is samengesteld uit extremistische en gewelddadige elementen van vooral de salafistische leer (zie begrippenlijst) en het gedachtegoed van Sayyid Qutb, de belangrijkste ideoloog van de Moslimbroeders. Het jihadisme beschouwt de gewapende strijd, die wordt gedefinieerd als jihad, als hét middel voor het realiseren van een mondiale heerschappij van de islam en een heroprichting van de Islamitische Staat. Het uitgangspunt daarvoor is de jihadistische interpretatie van het model van de geloofsgemeenschap van de Profeet. 'Jihadisme', evenals 'jihadistisch' is dus afgeleid van het begrip 'jihad'. Het begrip 'jihad' in de islam is echter een complex en veelomvattend begrip dat nadrukkelijk ook een spirituele en 'vreedzame' betekenis heeft (zie begrippenlijst). Wanneer gesproken wordt over jihadisme of jihadistisch gaat het altijd om jihad in de betekenis van een gewapende strijd, ook wel aangeduid als 'kleine jihad' of door sommigen als 'heilige oorlog'. Het gaat hierbij om jihad door individuen, groepen en vrijheidsstrijders en niet door landen.

Ligt bij het begrip 'jihadisten' het accent op de actoren die deel uitmaken van de jihadistische beweging, bij het gebruik van het begrip 'jihadistische beweging' ligt het accent op de collectiviteit van die actoren.

Het element 'beweging' is te preciseren als: het geheel van netwerken, groepen, cellen en individuen met gelijksoortige opvattingen en doelen. Als kanttekening geldt dat geen sprake is van een homogeen geheel. Binnen de jihadistische beweging bestaan meningsverschillen over bepaalde onderwerpen en andere verschillen. Er is evenmin sprake van een centrale aansturing of gezag. Toch kan wel worden gesproken van een beweging met de ideologie als bindmiddel. Men kan het vergelijken met de communistische beweging, waarbinnen eveneens verschillen van mening, stromingen (en dergelijke) bestonden en waar geen sprake was van één mondiale aansturing en gezag. Al Qa'ida vervult een sleutelrol binnen de jihadistische beweging. Daarbij wordt onderscheid gemaakt tussen 'kern al Qa'ida', 'al Qa'ida gelieerd' en 'al Qa'ida geïnspireerd' (zie begrippenlijst).

'Jihadisme' is te omschrijven als een stroming binnen de politieke islam die op basis van een specifieke invulling van de salafistische leer en op basis van het gedachtegoed van Sayyid Qutb door middel van een gewapende strijd (jihad) streeft naar een mondiale heerschappij van de islam en de heroprichting van de Islamitische Staat (Kalifaat).

¹⁸⁷ De HuT is een wereldwijd opererende politiek-activistische groepering. De ideologie is gericht op de (her-) oprichting van een kalifaatstaat, geleid volgens de regels van de shari'a.

Op basis van de combinatie met de definitie van jihadisme luidt de definitie van jihadistisch terrorisme dan als volgt:

- Jihadistisch terrorisme is terrorisme vanuit jihadistische doeleinden. Kenmerkend voor deze categorie van terrorisme is:
- het bestempelen als jihad van het dreigen met, voorbereiden of plegen van op mensen gericht ernstig geweld, dan wel daden gericht op het aanrichten van maatschappij-ontwrichtende zaakschade;
- het plegen van activiteiten die passen in het streven naar een mondiale heerschappij van de islam en de heroprichting van de Islamitische Staat.

Criteria voor online jihadisme

Een site is als jihadistisch te bestempelen wanneer die door middel van artikelen, audiovisuele documenten, postings en andere internetfunctionaliteiten (mailinglist, chat of Paltalkroom) het jihadisme verkondigt en verspreidt.

De jihadistische ideologie bestaat uit een mix van theologische, dogmatische, liturgische, ethische, juridische en politieke begrippen of leerstukken die nauw met elkaar samenhangen. Zij kunnen als volgt worden gerangschikt:

1. De enigheid van God [Tawhied];
2. Geloof en ongelooft [Imaan en Kufr];
3. Aanbidding van God [Ibada];
4. De plicht om de goddelijke wet- en regelgeving toe te passen [al-Hukm bi-ma Anzala Allah];
5. Loyaliteit en afkeer [al-Walaa wa al-Baraa];
6. De gemeenschap der moslims [Jamaat al-Muslimin];
7. De prediking en missiewerk [ad-Da'wa];
8. De gewapende strijd [al-Jihad];
9. Heroprichting van de Islamitische Staat (Kalifaat).

De eerste acht begrippen komen overeen met de centrale begrippen van het salafisme. Jihad in de betekenis van gewapende strijd vloeit zowel in het salafisme als in het jihadisme voort uit alle centrale begrippen/leerstukken. Wel geeft het jihadisme aan die begrippen een radicale en activistische uitleg en heeft daar activistische consequenties aan verbonden. Bovendien heeft het jihadisme de omstandigheden waaronder jihad mag of moet worden gevoerd opgerekt en beperkingen terzijde geschoven.

Het jihadisme kent vier hoofdthema's: de eindtijd, de mondiale heerschappij van de islam, de heroprichting van de Islamitische Staat en als laatste dawa en jihad door de voorhoede als middel om deze doelen te bereiken. De eindtijd, waarmee bedoeld wordt het einde van de wereld en de daarop volgende 'dag des oordeels', vormt het ultieme doel. Daaraan voorafgaand streeft het jihadisme naar een mondiale heerschappij van de islam en de heroprichting van de Islamitische Staat. Dawa en jihad door de voorhoede, lees jihadisten, vormen daartoe de enige en geëigende middelen. Dawa moet in het teken staan van jihad en Hijra, naar analogie van het vertrek van de profeet Mohammed van Mekka naar Medina, vormt een tussenschakel tussen dawa en jihad. Jihadisten wijzen alles af wat met die idealen in strijd is.

¹⁸⁷ Hijra betekent emigratie of vertrek uit een land en uitwijking naar een ander land wegens religieuze en politieke redenen, maar ook een tijdelijke of permanente vestiging in het land waar moslims naar zijn uitgeweken.

Voor verdere achtergronden van het jihadisme wordt verwezen naar: Ideologie en strategie van het jihadisme, Nationaal Coördinator Terrorismebestrijding, december 2009.

Literatuur

AFP 2007

'Suicide attack in Casablanca kills bomber, wounds three', AFP, 11 maart 2007.

AFP 2009

'US security braced for 'cybergeddon'', AFP, 7 januari 2009.

Agence 2009

'Singapore - Backroom cyber warriors trawl web for extremist threats', Agence France Press, 16 augustus 2009.

Algemeen Dagblad 2008

'Al-Qaeda houdt 'spreekuur' en beantwoordt 100 vragen', Algemeen Dagblad, 24 april 2008.

ANP 2006

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

ANP 2008

'Website Willem II gekraakt tegen Wilders', ANP, 1 februari 2008.

Antheunis 2009

M.L. Antheunis, *Online Communication, Interpersonal Attraction, and Friendship Formation*, Amsterdam 2009 (<http://dare.uva.nl/document/129138>).

Australian Financial Review 2007

'Media proves a powerful vehicle for terrorists', Australian Financial Review, 22 maart 2007.

Automatiseringsgids 2007

'DoS-aanvallen gevaar voor internet', Automatiseringsgids, 26 september 2007.

Automatiseringsgids 2009a

'Beveiliging kern internet vertraagd', Thijs Doorenbosch, Automatiseringsgids, 12 oktober 2009.

Automatiseringsgids 2009b

'Angst in VS voor stralingswapens', Automatiseringsgids, 19 augustus 2009.

BBC Monitoring 2007

'Website linked to al-Qa'idah reported seeking suicide bombers to attack Denmark', BBC Monitoring, 22 september 2007.

BBC Monitoring 2008

'German paper says Islamists collecting Internet donations', BBC Monitoring, 11 april 2008.

Blakely 2008

R. Blakely, 'Google Earth accused of aiding terrorists', Times Online, 9 december 2008 (http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article5311241.ece).

Burton 2007a

F. Burton, 'The Secrets of Countersurveillance', Stratfor, 6 juni 2007.

Burton 2007b

F. Burton, 'Surveillance in the Information Age', Stratfor, 14 juni 2007.

Business Line 2009

'E-World falling short on security', Business Line, 12 januari 2009.

Buxbaum 2008

Peter Buxbaum, 'Cyberterrorism, Inc.', ISN Security Watch, 11 februari 2008.

Canadian Press 2007

'Terrorists eyeing webcams as means to assess vulnerabilities, says FBI', Canadian Press, 11 januari 2007.

Chen e.a. 2008

Hsinchun Chen, Sven Thoms, T. J. Fu, 'Cyber Extremism in Web 2.0: An Exploratory Study of International Jihadist Groups (Forthcoming, IEEE International Conference on Intelligence and Security Informatics)', 2008.

Cheong 2008

Lee Kwok Cheong, 'Must we wait for crisis to strike?', Business Times Singapore, 14 juli 2008.

Cochran 2007a

A. Cochran, *MetaTerror: The Potential use of MMORPGs by Terrorists*, Counterterrorism Blog (http://counterterrorismblog.org/2007/03/print/metaterror_the_potential_urse_o.php)

Cochran 2007b

A. Cochran, Part II of “*MetaTerror: The Potential use of MMORPGs by Terrorists*”, Counterterrorism Blog (http://counterterrorismblog.org/2007/03/print/part_ii_of_metaterror_the_pote.php)

Computerworld 2008

‘CIA says hackers pulled plug on power grid’, Computer-World/ IDG News Service, 18 januari 2008.

Council of Europe 2007

Council of Europe, ‘*Cyberterrorism - the use of the internet for terrorist purposes*’, Council of Europe Publishing, december 2007.

CRS2008

CRS Report for Congress, ‘*Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress (update)*’, 29 januari 2008.

Cruickshank 2009a

P. Cruickshank, ‘*The Belgium Cell and FATA’s Terrorist Pipeline*’, CTC Sentinel, volume 2, issue 4, april 2009.

Cruickshank 2009b

P. Cruickshank, ‘*Italy arrests linked to Brussels ‘al Qaeda’ recruiting network*’, CNN, 15 mei 2009.

Cruickshank 2009c

P. Cruickshank, ‘*Love in the Time of Terror*’, Marie Claire (updated 18 mei 2009) (www.marieclaire.com/print-this/world-reports/news/international/malika-el-aroud...)

Daily Telegraph 2007

‘*Terrorists ‘use Google maps to hit UK troops*’’, Daily Telegraph, 13 januari 2007.

Debka 2007

‘*Al Qaeda declares Cyber Jihad on the West*’, Debka.com, 7 november 2007.

Denning 2007

Dorothy E. Denning, *A View of Cyberterrorism Five Years Later*, in *Internet Security: Hacking, Counterhacking and Society*, K. Himma ed., Jones and Bartlett Publishers, 2007.

District Court 2009

Indictment ‘Unauthorized Impairment Of a Protected Computer’, US District Court for the Central District of California, februari 2009.

EETimes 2009

Rick Merrit, ‘*Congress debates how to holster RF weapons, Electromagnetic pulse attacks: impact high, probability low*’, EETimes.com, 25 augustus 2009.

Elsevier 2009

‘*Terroristen prediken terreur op Facebook*’, Elsevier.nl, 17 maart 2009.

Europol 2009

TE-SAT 2009, EU terrorism situation and trend report, Europol, 2009.

Forbes 2007

Andy Greenberg, ‘*America’s Hackable Backbone*’, http://www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_o822hack.html, 22 augustus 2007.

Foxnews 2008

‘*How to Hack Into a Boeing 787*’, Foxnews.com, 18 februari 2008.

Friesch Dagblad 2008

‘*Twitter eerste bron bij terreur*’, Friesch Dagblad, 1 december 2008.

Global Risks 2008

Global Risks 2008, A Global Risk Network Report, World Economic Forum, januari 2008.

GOVCERT 2008

Trendrapport 2008, GOVCERT.NL, juni 2008.

GOVCERT 2009

Trendrapport 2009, GOVCERT.NL, juni 2009.

Graham 2004

Dr. William R. Graham et al, ‘*Report of the Commission to Assess the Threat to the United States from Electromagnetic pulse (EMP) Attack*’, Volume 1, Executive Report, 2004.

Haegens 2009

K. Haegens, ‘*Hoe Fritzi Abdullah werd*’, De Groene Amsterdammer, 19 augustus 2009.

Hamburger Abendblatt 2009

‘*Videos: Terroristen starten eine Propagandaoffensive*’, Hamburger Abendblatt, 29 januari 2009.

Hegghammer 2006

T. Hegghammer, ‘*Global Jihadism After the Iraq War*’, Middle East Journal, Vol.60, No.1 (Winter 2006): pp.11-32.

Hegghammer 2007

T. Hegghammer, *Jihad Recollections*, 07 april 2007 (www.jihadica.com/jihad-recollections/).

Holahan 2006

C. Holahan, ‘*Policing Online Money Laundering*’, BusinessWeek.com, 6 november 2006.

Hyves 2009

Raymond Spanjer over de echte statistieken van Hyves, Hyves.nl, persbericht, 22 juli 2009.

ICANN 2007

ICANN Factsheet root server attack on 6 February 2007, ICANN, 1 maart 2007.

ICSR 2007

Recruitment and Mobilisation for the Islamist Militant Movement in Europe, ICSR, 2007 (www.icsr.info).

ICSR 2009

Countering Online Radicalisation. A Strategy for Action, ICSR, 2009 (www.icsr.info).

inSITE 2008

‘*Inside the Online Jihadist Network*’, inSITE, september 2008.

International Herald Tribune 2008

‘*Al-Qaida deputy Al-Zawahri says group is still targeting Western countries*’, International Herald Tribune, 22 april 2008.

Israel Military.net 2008

‘*Something about Malika*’, Israel Military.net, 16 december 2008, (<http://www.israelmilitary.net/showthread.php?t=7978>).

ITAC 2006

‘*A Framework for Understanding Terrorist Use of the Internet*’, Trends in Terrorism Series, ITAC, Canada, 2006.

ITworld 2008

‘*Sorting out the facts in the Terry Childs case*’, ITworld.com, 30 juli 2008.

Jane’s Terrorism and Security Monitor 2008

‘*Finding Nemo*’, Jane’s Terrorism and Security Monitor, 4 juli 2008.

Jihadwatch 2006

‘*New “jihad” videogame targets Bush, US Forces, Shi’ite leaders*’, Jihad Watch, 19 september 2006.

Katz & Devon 2006

R. Katz, J. Devon, ‘*Jihadist Use Online Remittance System to Fundraise and Transfer Money*’, SITE Intelligence Group, 26 oktober 2006.

Katz & Devon 2007a

R. Katz, J. Devon, 'The Online Jihadist Threat', (Testimony before the House Armed Services Committee Terrorism, Unconventional Threats and Capabilities Subcommittee, United States House of Representatives), Washington: SITE Intelligence Group, 14 februari 2007.

Katz & Devon 2007b

R. Katz, J. Devon, 'Web Of Terror; Al Qaeda and its allies are exploiting the Internet to recruit and plot havoc. Here's how we can stop them', Forbes, 7 mei 2007.

Kohlmann 2008

E.F. Kohlmann, 'Al-Qa'ida's "MySpace": Terrorist Recruitment on the Internet', CTC Sentinel, januari 2008 http://counterterrorismblog.org/2008/01/alqaidas_myspace_how_suicide_b.php

Kravets 2009

David Kravets, 'Feds: Hacker Disabled Offshore Oil Platforms' Leak-Detection System', <http://blog.wired.com/27bstroke6/2009/03/feds-hacker-dis.html>, 18 maart 2009.

Lachow 2009

Irving Lachow, 'Cyberterrorism: Menace or Myth', in: Cyberpower and National Security, Franklin D. Kramer e.a, National Defense University Press en Potomac Books, 2009.

Leppard 2007

D. Leppard, 'Al-Qaeda plot to bring down UK internet', The Sunday Times, 11 maart 2007.

Lia 2009

B. Lia, 'Does al-Qaida Articulate a Consistent Strategy? A Study of al-Qa'ida Leadership Statements, 2001-2009', Paper to be presented at the International Studies Association's 50th Annual Convention, New York City, februari 2009.

Luijff 2008

H.A.M. Luijff, 'Cyberterrorisme' in: Terrorisme, Studies over terrorisme en terrorismebestrijding, Muller e.a., Kluwer, 2008.

Mansfield 2006

Laura Mansfield, 'His Own Words. A translation of the writings of Dr. Ayman al-Zawahiri', TLG Publications, 2006.

Memri 2007

'How Islamist Internet Forums Are Used to Inform Mujahideen of News from Western Media', Memri Special Dispatch Series - No. 1615, 8 juni 2007.

Memri 2008

'Women's forums on islamist websites; tools for preparing women to carry out jihad and suicide operations', memri.org, 1 februari 2008.

Moss & Mekhennet 2007

M. Moss, S. Mekhennet, 'An Internet Jihad Aims at U.S. Viewers', New York Times, 15 oktober 2007.

Nationalterroralert 2007

Video Shows Simulated Hacker Attack of Power Grid, <http://www.nationalterroralert.com/updates/2007/09/26/video-shows-simulated-hacker-attack-of-power-grid/>, 26 september 2007.

NCTb 2007

'Jihadisten en het Internet', Nationaal Coördinator Terrorismebestrijding, januari 2007.

NCTb 2009

'Aanbieding Samenvatting Dreigingsbeeld Terrorisme Nederland 18', http://www.nctb.nl/Images/Samenvatting%20DTN_tcm91-216361.pdf, 11 september 2009.

NEFA 2008

'Report: "Supervisor of Al-Firdaws Forum Joins Jihad in Afghanistan"', NEFA Foundation, 29 juni 2008 (www.nefafoundation.org).

Nood & Attema 2006

D. de Nood, J. Attema, *Second Life. Het Tweede Leven van Virtual Reality*, EPN: Den Haag, 1 oktober 2006.

Novatv.nl

<http://www.novatv.nl/page/detail/uitzendingen/3213/MSN-groepen+staan+vol+met+radicale+uitingen>, Novatv.nl, 8 februari 2005.

NRC Handelsblad 2009

'Duitsland vreest grotere kans op terreuraanslag', NRC Handelsblad, 2 februari 2009.

Nu.nl 2007

'Zweedse sites doelwit van Turkse hackers', Nu.nl, 8 oktober 2007.

Nu.nl 2008a

'Indiase politie waarschuwt Twitteraars', Nu.nl, 28 november 2008.

Parool 2008

'Link hackers tegen Fitna', Het Parool, 13 september 2008.

Pers 2008

'Duizenden sites kraken als reactie op Fitna', Dagblad De Pers, 29 augustus 2008.

UvA 2009

'Communicatie via internet heeft positief effect op vriendschap', Persbericht, Universiteit van Amsterdam, 2009 (<http://www.uva.nl/actueel/agenda.cfm/24764780-1321-BoBE-6840CC1036F6BC54>).

Reals 2007

T. Reals, 'Was London Bomb Plot Heralded On Web', CBSNEWS, 29-06-2007 (<http://www.cbsnews.com/stories/2007/06/29/terror/main2997517.shtml>).

Rogan & Stenersen 2008

H Rogan, A. Stenersen, 'Jihadism online. Al-Qaida's use of the internet', Norwegian Defence Research Establishment, mei 2008.

Sageman 2008a

M. Sageman, 'Leaderless Jihad. Terror Networks in the Twenty-First Century', Philadelphia: University of Pennsylvania Press, 2008.

Sageman 2008b

M. Sageman, 'Radical web of Islam's Terror', National Post, 8 juli 2008.

SANS 2008

'CIA Confirms Cyber Attack Caused Multi-city power outage', SANS NewsBites - Volume: X, Issue: 5, 18 januari 2008.

Schofield 2007

M. Schofield, 'New generation of terrorists cyber-inspired, -trained', McClatchy Newspapers, 7 februari 2007.

Shachtman 2008

N. Shachtman, 'Pentagon researcher unveils warcraft terror plot', Wired.com, 15 september, 2008.

SITE 2006a

'First Issue of Technical Mujahid by al-Fajr', SITE Intelligence Group, 28 november 2006.

SITE 2007a

'Large Arabic Compendium of Hacking and Cybersecurity Documents Distributed through Al-Firdaws Jihadist Forum', SITE Intelligence Group, 14 november 2007.

SITE 2007b

'SITE Monitoring Service on European Jihadist Websites Malika El Aroud: Internet Jihadist', SITE Intelligence Group, 31 augustus 2007.

SITE 2007c

'Detailed Google Earth map of Abu Graib prison provided to jihadists, in addition to available hacks for the Google Earth software', SITE Intelligence Group, 8 maart 2007.

SITE 2007d

'Jihadist forum member suggests method of joining al-Qaeda and striking western and Israeli interests', SITE Intelligence Group, 11 januari 2007.

SITE 2008a

'Jihadist Forum Member Suggests Mujahideen Sever Underwater Fiber-Optic Cables Providing Internet to European Countries and America', SITE Intelligence Group, 6 februari 2008.

SITE 2008b

'Jihadist Informs of Possibility to Attack a Nuclear Reactor Via the Internet', SITE Intelligence Group, 10 april 2008.

SITE 2009a

'Permissibility of Cyber Jihad' in: Western Jihadist Forums', SITE Intelligence Group, juni 2009.

SITE 2009b

'Facebook Invasion Jihadists continue campaign', SITE Intelligence Group, 5 februari 2009.

SITE 2009c

'Jihadist Forums Go offline, Online Community Frustrated and Confused', SITE Intelligence Group, 11 september 2009.

SITE 2009d

SITE Intelligence Group, 'SITE Monitoring Service on European Jihadist Websites Covering the Period of April to May 2009', juni 2009.

SITE 2009e

'Al Qa'ida Urges Gaza Reprisals in Western, Arab Capitals', SITE Intelligence Group, 22 januari 2009.

SITE 2009f

'Internet Invasion Brigades Spreads German al-Qaeda Video', SITE Intelligence Group, 17 april 2009.

SITE 2009g

SITE Intelligence Group, 'SITE Monitoring Service on European Jihadist Websites. Covering the Period of Early Summer 2009', september 2009.

SITE 2009h

SITE Intelligence Group, 'INSITE', The official Newsletter of Site Intelligence Group, Volume 2, No. 9, november 2009.

Spangers 2007

Chris Spangers, 'Het onkwetsbare net: Kunnen terroristen het internet platleggen?', Intermediair, 11 mei 2007.

Special 2007

'Islamist Website Instructs Mujahideen in Using Popular U.S. Web Forums to Foster Anti-War Sentiment among Americans', Special Dispatch-Jihad & Terrorism Studies Project, nr.1508, 20 maart 2007.

Spiegel 2005

Yassin Musharbash, 'What al-Qa'ida Really Wants, The Future of Terrorism', Spiegel Online, 12 augustus 2005.

Stenersen 2008

Anne Stenersen, 'Al-Qaida's Quest for Weapons of Mass Destruction, The History behind the Hype', VDM Verlag Dr. Müller, 2008.

Stohl 2007

'Cyber Terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?', Michael Stohl, Springer Science + Business Media BV, 30 maart 2007.

Stratfor 2007

'U.S.: The Role and Limitations of the 'Dark Web' In Jihadist Training', Stratfor, 11 december 2007.

Techworld 2009

Michel van Blommenstein, 'Hackersite Milworm is dood! Leve Milworm?', www.techworld.nl, 9 juli 2009.

Times 2008

'Thousands of cyber attacks each day on key utilities', The Times, 23 augustus 2008.

Tweakers 2007

'ICANN verklaart falen ddos-aanval rootservers', Tweakers.net, 12 maart 2007.

United News of India 2009

'Mumbai Cyber cell traced IP addresses of 26/11 terrorists', United News of India, 2009.

US Senate Committee 2008

'Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat', United States Senate Committee on Homeland Security and Governmental Affairs, 8 mei 2008.

US Senate Select Committee 2009

'Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence', Dennis C. Blair, Director of National Intelligence, 12 februari 2009.

Vlierden 2009

G. van Vlierden, 'Terreurforum van internet gegooid', Het Laatste Nieuws, 11 juni 2009.

Wall Street Journal 2009

'FBI Suspects Terrorists Are Exploring Cyber Attacks', The Wall Street Journal, 18 november 2009.

Washington Times 2009

'Hoekstra: 'Stand up to N. Korea'', The Washington Times, 9 juli 2009.

Webwereld 2008a

Martin Gijzemijter, 'Al-Qaida verbeterd encryptiesoftware', Webwereld.nl, 3 februari 2008.

Webwereld 2009

Jasper Bakker, 'Vandalen saboteren glasvezelnetwerk Silicon Valley', Webwereld.nl, 10 april 2009.

Weimann 2008

Gabriel Weimann, 'Al-Qa'ida's Extensive Use of the Internet', CTC Sentinel, Volume 1, issue 2, januari 2008.

Weimann 2009

Gabriel Weimann, 'Econo-Jihad, a new Al-Qaeda priority', Daily Star, 10 augustus 2009.

Weizhen & Singh 2008

Tan Weizhen & Khushwant Singh, 'Concerns over use of Google Earth by terrorists', Straits Times, 8 december 2008.

Welt 2009

'BKA: Terroristen wollen Bundestagswahl beeinflussen', Die Welt, 2 februari 2009.

Whitlock 2008

C. Whitlock, 'Al-Qaeda's Growing Online Offensive', Washington Post, 24 juni 2008.

Wolfe 2008

'The internet's vulnerability', Adam Wolfe, ISN Security Watch, 19 februari 2008.

ZDNet 2008

'Cyberattacks target UK national infrastructure', ZDNet News, 30 oktober 2008.

ZDNet 2009

Merijn Gelens, 'WPA in zestig seconden gekraakt', ZDNet Nederland, 28 augustus 2009.

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.

Anycast: Dit is een routingsschema voor netwerken waarbij datapakketjes gericht op een bepaald adres naar fysiek verschillende locaties gestuurd kunnen worden. Op deze manier kan een grote hoeveelheid verkeer over verschillende geografisch verspreide servers worden verdeeld.

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 computer-inbraak 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 alarm-centrales 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.

Jihad (in dit kader in de betekenis van gewapende strijd): het ontplooiën 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.

Jihadisme: een stroming binnen de politieke islam die op basis van een specifieke invulling van de salafistische leer en op basis van het gedachtegoed van Sayyid Qutb door middel van een gewapende strijd (jihad) streeft naar een mondiale heerschappij van de islam en de heroprichting van de Islamitische Staat (Kalifaat).

Jihadisten: samentrekking van jihadistische terroristen en jihadistische radicalen.

Jihadistische beweging: de jihadistische beweging is het geheel van netwerken, groepen, cellen en individuen dat op basis van een specifieke invulling van de salafistische leer en op basis van het gedachtegoed van Sayyid Qutb door middel van een gewapende strijd (jihad) streeft naar een mondiale heerschappij van de islam en de heroprichting van de Islamitische Staat (Kalifaat).

Jihadistisch terrorisme: terrorisme vanuit jihadistische doeleinden. Kenmerkend voor deze categorie van terrorisme is:

- het bestempelen als jihad van het dreigen met, voorbereiden of plegen van op mensen gericht ernstig geweld, dan wel daden gericht op het aanrichten van maatschappij-ontwrichtende zaakschade;
- het plegen van activiteiten die passen in het streven naar een mondiale heerschappij van de islam en de heroprichting van de Islamitische Staat.

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

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, sofnummer 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: 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.

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.

Salafisme/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: een procescontrolesysteem dat het geheel omvat 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.

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 uit ideologische motieven dreigen met, voorbereiden of plegen van op mensen gericht ernstig geweld, dan wel daden gericht op het aanrichten van maatschappij-ontwrichtende zaakschade, met als doel maatschappelijke veranderingen te bewerkstelligen, de bevolking ernstige vrees aan te jagen of politieke besluitvorming te beïnvloeden.

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/>.

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).

COLOFON

Uitgave

Nationaal Coördinator Terrorismebestrijding (NCTb), april 2010

Ontwerp & omslagfoto

Richard Sluijs, Den Haag

Druk

Koninklijke De Swart, Den Haag

Oplage

400 exemplaren

Nationaal Coördinator Terrorismebestrijding (NCTb)

Postbus 16950

2500 BZ Den Haag

Telefoon 070-315 0315

E-mail info@nctb.nl

Website www.nctb.nl



De NCTb werkt aan een veiliger samenleving

De Nationaal Coördinator Terrorismebestrijding heeft als taak het risico van en de vrees voor 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 niveau komt en blijft.