Kabinetsreactie op het AIV/CAVV-advies Digitale Oorlogvoering

Op 17 januari heeft een gezamenlijke commissie van de Adviesraad voor Internationale Vraagstukken (AIV) en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken (CAVV) het advies 'Digitale oorlogvoering' gepresenteerd. Het kabinet is de commissie erkentelijk voor het gedegen advies. Het levert een waardevolle bijdrage aan de discussie over digitale veiligheid en helpt het kabinet het beleid op dit terrein te verhelderen en te versterken. Het advies vormt een aanvulling op de Nationale Cyber Security Strategie, waarin de bescherming van de nationale veiligheid en de bestrijding van cybercrime centraal staan (Kamerstuk 26643, nr. 174). Het vormt tevens een aanvulling op het juridisch kader *cyber security* zoals dat op 23 december aan de Tweede Kamer is gezonden (Kamerstuk 26643, nr. 220).

1. Samenvatting

De hoofdpunten van de kabinetsreactie zijn als volgt:

- De digitale dreiging vereist een integrale aanpak. Het advies betreft een aanvulling op de nationale aanpak. De huidige crisisbeheersingsstructuur zal hiertoe tegen het licht worden gehouden;
- Het digitale domein is een nieuw operationeel domein voor de krijgsmacht. Defensie investeert om bestaande capaciteiten aanzienlijk te versterken en nieuwe (waaronder offensieve) te ontwikkelen;
- Het recht op zelfverdediging is ook van toepassing op cyberaanvallen.
- Het kabinet ziet geen noodzaak tot een nieuw wereldwijd cyberverdrag. Wel zal het kabinet inzetten op praktische uitwerking van de toepassing van internationaalrechtelijke bepalingen in het digitale domein;
- Het NAVO cyberbeleid is defensief, maar op termijn is een discussie over het gebruik van offensieve capaciteiten nodig. Artikel 5 is ook van toepassing op cyberaanvallen.
- Een integrale EU-aanpak is noodzakelijk.

2. De digitale dreiging

De toenemende dreiging tegen nationale belangen in het digitale domein en de stijging van het aantal (complexe) digitale aanvallen baren het kabinet zorgen. Spionage, sabotage, misdaad en terrorisme langs digitale weg vormen een directe bedreiging voor de nationale veiligheid. Dit werd onder meer geconstateerd in het eerste Cyber Security Beeld Nederland (CSBN) van december 2011 (Kamerstuk 26 643, nr. 220). Zonder af te doen aan de ernst van de dreiging, onderschrijft het kabinet de constatering van de commissie dat nader onderzoek naar de digitale dreiging wenselijk is. Het CSBN is hiervoor een belangrijk instrument, dat onder coördinatie van het Nationaal Cyber Security Centrum wordt opgesteld. Het CSBN zal de komende jaren verder worden ontwikkeld, waarbij nadrukkelijk wordt ingezet op een kwantitatieve en kwalitatieve verbetering van dit instrument.

Voor Nederland, met een open en internationaal georiënteerde economie en een sterke dienstensector, is een veilige en goed functionerende digitale infrastructuur essentieel. Uitgangspunt voor het kabinetsbeleid blijft de integrale benadering zoals vastgelegd in de Nationale Cyber Security Strategie. Op grond hiervan is onder andere het Nationaal Cyber Security Centrum opgericht, waarbinnen publieke en private partijen samenwerken. Een gezamenlijke, publiek-private en civiel-militaire aanpak is noodzakelijk aangezien niet altijd duidelijk zal zijn wat de aard van een digitale aanval is, hoe uitgebreid en geraffineerd deze is en wat het uiteindelijke doel van de aanvaller is (crimineel, ideologisch, militair of politiek). Dit maakt het moeilijk te bepalen op welke (juridische) grond en met welke middelen moet worden gereageerd. Bij het organiseren van een gezamenlijke aanpak is het van belang dat rollen, taken en verantwoordelijkheden helder zijn. In dit kader zal, op initiatief van de NCTV, worden bezien of de huidige crisisbeheersingsstructuur afdoende is voor het snel en effectief beheersbaar maken van een grootschalige digitale verstoring. Zoals de commissie terecht stelt, is het daarnaast van belang te investeren in een samenhangende cyberdiplomatie.

3. Operationeel domein voor de krijgsmacht

Het grootschalig gebruik van ICT stelt Defensie in staat haar taken effectiever en efficiënter uit te voeren maar zorgt ook voor een grotere kwetsbaarheid. Het digitale domein is derhalve van fundamenteel belang voor de krijgsmacht. Zonder goed functionerende ICT-infrastructuur kan de krijgsmacht haar taken eenvoudigweg niet meer uitvoeren. Vrijwel alle wapen- en sensorsystemen functioneren dankzij het gebruik van ICT-componenten en ook de commandovoering en de logistieke ondersteuning zijn afhankelijk van digitale systemen. Een verstoring van de ICT-infrastructuur van de krijgsmacht zal de slagkracht en het voorzettingsvermogen dan ook in gevaar brengen. In het digitale domein moet Defensie daarom de betrouwbaarheid van eigen netwerken, (wapen- en regel)systemen en informatie waarborgen en ontvreemding van informatie voorkomen.

Het digitale domein vormt tegelijkertijd een nieuw operationeel domein voor de krijgsmacht dat, zoals de commissie terecht constateert, “naar verwachting in elk toekomstig conflict een belangrijke rol zal spelen.” Aangezien niet alleen onze eigen netwerken kwetsbaar zijn maar ook die van potentiële tegenstanders kan het digitale domein ook worden gebruikt voor het versterken van de eigen inlichtingenpositie en het uitvoeren van militaire operaties. De opkomst van *cyber space* als operationeel domein versterkt de ontwikkeling waarbij klassieke oorlogvoering plaatsmaakt voor een meer hybride en veelvormig conflictmodel waar de inzet van ICT-middelen een steeds grotere rol speelt. Het beeld wordt verder gecompliceerd doordat bij digitale aanvallen moeilijk vast te stellen is waar deze vandaan komen en wie er achter zit. Daarnaast constateert de commissie terecht dat de kans op een zuivere ‘cyberoorlog’, die uitsluitend in het digitale domein wordt

uitgevochten, momenteel gering is. Het is echter wel waarschijnlijk dat operationele cybercapaciteiten in de nabije toekomst veelvuldig zullen worden ingezet. Deze kunnen zowel zelfstandig als ter ondersteuning van het regulier optreden van krijgsmachten worden ingezet. Hiermee is het noodzakelijk dat operationele (offensieve) cybercapaciteiten onderdeel worden van het totale militaire vermogen van de Nederlandse krijgsmacht. De krijgsmacht moet daarbij over de capaciteiten beschikken om onder alle omstandigheden en tegen elke tegenstander doeltreffend en afdoende te kunnen reageren.

Inlichtingenpositie
Een uitstekende inlichtingenpositie is een randvoorwaarde voor het functioneren en opereren van Defensie in het digitale domein. Ten aanzien van het adresseren van de attributieproblematiek constateert de commissie terecht dat hier een belangrijke rol is weggelegd voor de inlichtingen- en veiligheidsdiensten. Het vergaren van inlichtingen en het uitvoeren van contra-inlichtingen activiteiten door de MIVD is geen offensieve activiteit. Het gaat hier om het, binnen de kaders van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002), vergaren van inlichtingen uit gesloten bronnen.
De commissie is van mening dat de technologische ontwikkelingen het wenselijk maken dat wordt bezien of het onderscheid tussen kabelgebonden en niet-kabelgebonden interceptie gehandhaafd moet blijven. Deze constatering wordt onderschreven door de conclusie van de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) in het recente toezichtsrapport nr. 28 over SIGINT. Het kabinet is van mening dat dit onderscheid niet gehandhaafd kan blijven. Daartoe wordt een wijziging van de Wiv 2002 voorbereid, waarbij ook een zorgvuldige afweging gemaakt moet worden met betrekking tot de privacybescherming en rekening wordt gehouden met de effecten op de aanbieders van elektronische communicatienetwerken. In de loop van 2012 zal uw Kamer hieromtrent worden geïnformeerd.
Versterken digitale capaciteiten van Defensie
Naar aanleiding van het WGO-Materieel van 7 november 2011 is aan het lid Hernandez toegezegd in deze reactie in te gaan op de activiteiten van Defensie. Deze toezegging wordt hierbij gestand gedaan. De mate waarin invulling kan worden gegeven aan de beschreven activiteiten is afhankelijk van de beschikbare financiële ruimte. Teneinde richting te geven aan de beleidsontwikkeling wordt, in nauw overleg met nationale en internationale partners, een defensiestrategie voor *cyber operations* opgesteld. Deze wordt nog voor de zomer vastgesteld en aan de Kamer aangeboden.
Onder verantwoordelijkheid van de CDS is een programmamanager Cyber aangetreden en is de Taskforce Cyber opgericht. De programmamanager is verantwoordelijk voor de coördinatie van alle cybergerelateerde activiteiten binnen Defensie. Op korte termijn ligt de prioriteit van Defensie bij het versterken van de defensieve en inlichtingenvermogens. Op de middellange

termijn gaat de aandacht uit naar het oprichten van een Defensie Cyber Expertise Centrum (DCEC) eind 2013 en een Defensie Cyber Commando (DCC) eind 2014. Het DCC coördineert *cyber operations* binnen Defensie en zorgt voor de verbinding tussen de verschillende cybervermogens van de defensieonderdelen. In het operationele domein is een belangrijke, uitvoerende rol weggelegd voor het Commando Landstrijdkrachten (CLAS).
Zoals ook de commissie constateert wordt het vinden en vasthouden van voldoende gekwalificeerd personeel een grote uitdaging voor Defensie. Gezien de algemene behoefte aan gekwalificeerde specialisten moet ook hier intensief worden samengewerkt met andere publieke en private partijen om gezamenlijk te komen tot een zo effectief mogelijke benutting van schaarse capaciteiten. Daartoe vindt overleg plaats tussen departementen en met bedrijfsleven en universiteiten. Ook wordt onderzocht welke mogelijkheden er zijn om een pool van cyberreservisten te creëren.
De defensieve maatregelen richten zich op het versterken van de bescherming van netwerken en wapen- en regelsystemen. Het Defensie *Computer Emergency Response Team* (DefCERT) is mede verantwoordelijk voor de beveiliging van deze netwerken en systemen en moet medio 2013 volledig operationeel zijn om 24 uur per dag, zeven dagen per week de meest kritieke defensienetwerken te beschermen. De capaciteit wordt in de periode tot 2016 verder uitgebreid naar de overige netwerken en wapen- en regelsystemen. DefCERT zal binnenkort een convenant afsluiten met het NCSC waarin de kaders voor intensieve samenwerking worden vastgelegd voor informatie-uitwisseling en ondersteuning bij calamiteiten.
Vanuit de Taskforce *Cyber* zal tevens vorm worden gegeven aan een offensieve capaciteit en wordt een Defensie cyberdoctrine opgesteld. De commissie constateert dat voor offensief optreden vaak dezelfde technieken worden gebruikt als voor inlichtingendoeleinden. Voor de realisatie van een offensieve capaciteit is een efficiënte inzet van alle schaarse cybercapaciteiten (waaronder inlichtingencapaciteiten) binnen Defensie dan ook noodzakelijk. Bij de vormgeving van offensieve capaciteit wordt rekening gehouden met de aanbeveling van de commissie over de functiescheiding tussen de CDS en de directeur van de MIVD.
De MIVD zal in de periode 2012-2015 de *cyber* inlichtingencapaciteit versterken. Een eerste stap is gezet door de uitbreiding van de capaciteit met negen vte'n per 1 januari 2012. Verder intensiveren de MIVD en de AIVD de samenwerking op het gebied van *cyber* en *signals intelligence* (SIGINT) wat moet leiden tot een gezamenlijke eenheid voor de verwerving van SIGINT en cyberinlichtingen.
Binnen Defensie zal de kennisontwikkeling en –borging primair vorm worden gegeven door het DCEC. In eerste instantie heeft het vergroten van de bewustwording bij het personeel over de cyberdreiging prioriteit. Een interactieve oefenomgeving bestaande uit *e-learning* modules, een simulatie en een kennisbank wordt binnenkort opgeleverd.
Ook wordt in onderzoek geïnvesteerd. In 2012 wordt aan de NLDA een Universitair Hoofddocent Cyber aangesteld en een onderzoeksgroep ingericht. Per 1 januari 2014 wordt een leerstoel *cyber defence* ingesteld. Bij

TNO is in januari 2012 een breed cyber onderzoeksprogramma gestart. Het onderzoeksprogramma van Defensie is onderdeel van een nationale onderzoeksagenda *cyber security* die tot doel heeft de beschikbare onderzoeksbudgetten zo effectief mogelijk te besteden.

4. Het internationaalrechtelijk kader

Gebruik van geweld en recht op zelfverdediging (jus ad bellum)
De bevindingen van de commissie ten aanzien van het gebruik van geweld en het recht op zelfverdediging komen in grote lijnen overeen met het standpunt van het kabinet (*jus ad bellum*). De constatering van de commissie dat ten aanzien van digitale aanvallen geen ander regime geldt dan voor het gebruik van geweld in het fysieke domein, acht het kabinet van belang. In het advies worden de bestaande volkenrechtelijke regels inzake het gebruik van geweld strikt toegepast op digitale aanvallen, dit strookt met opvattingen van het kabinet. De commissie oordeelt dat, behalve Staten, ook niet-statelijke actoren een gewapende aanval in de zin van het VN Handvest kunnen plegen, waartegen geweld ter zelfverdediging mag worden aangewend. Het kabinet onderschrijft dit en benadrukt dat dit een belangrijke rechtsontwikkeling vormt.
Het kabinet onderschrijft tevens de constatering van de commissie dat attributie een belangrijke uitdaging vormt bij aanvallen in het digitale domein. Met de commissie is het kabinet van mening dat alleen gebruik mag worden gemaakt van geweld ter zelfverdediging indien de herkomst van de aanval en de identiteit van de aanvallers met een voldoende mate van zekerheid kan worden vastgesteld. Het kabinet onderschrijft tevens de bevinding van de commissie dat, bij gebruik van geweld in reactie op een gewapende digitale aanval, moet worden voldaan aan de volkenrechtelijke eisen van ‘noodzakelijkheid’ en ‘proportionaliteit’.
Humanitair oorlogsrecht (jus in bello)
Het kabinet deelt de conclusie van de commissie dat toepassing van de regels van het humanitair oorlogsrecht (*jus in bello*) op vijandelijkheden in het digitale domein “technisch gezien haalbaar en juridisch gezien ook een vereiste” is. Echter, met de commissie is het kabinet van mening dat digitale daden van geweld alleen onder het oorlogsrecht vallen wanneer ze worden gepleegd in de context van een gewapend conflict, door de partijen bij dat conflict. Dit vormt een belangrijke afbakening ten opzichte van andere daden van digitaal geweld. Het advies geeft nadere invulling aan het ontstaan van een ‘gewapend conflict’ door een digitale aanval, als ook een aantal nuttige voorbeelden van de praktische toepassing van de basisprincipes van het oorlogsrecht op digitale oorlogvoering.
Neutraliteit
Het kabinet beschouwt de uitwerking van de commissie van het begrip neutraliteit in relatie tot de inzet van digitale wapens als een nuttig startpunt voor nadere gedachtevorming op dit gebied. Nederland kan bij een gewapend conflict van andere partijen zijn neutraliteit beschermen door het verhinderen van het gebruik door deze partijen van infrastructuur en systemen (bijv. botnets) op Nederlands grondgebied. Hierbij is permanente waakzaamheid

geboden. Een goede inlichtingenpositie en een permanente scanfunctie zijn hierbij noodzakelijk.

Cyberverdrag

Met de commissie ziet het kabinet op dit moment geen noodzaak tot een nieuw wereldwijd cyberverdrag. Het kabinet is van mening dat bestaande regels van internationaal en Europees recht voldoen ten aanzien van het gebruik van digitaal geweld. Het kabinet ondersteunt wel de aanbeveling van de commissie om door middel van een c*ode of conduct* meer politiek gewicht en praktische uitwerking te geven aan de toepassing van internationaal rechtelijke bepalingen in het digitale domein.

5. Internationale samenwerking

Door de wereldwijd verregaande onderlinge verbondenheid en wederzijdse afhankelijkheid van ICT-systemen, is internationale civiel-militaire en publiek-private samenwerking essentieel. Bilateraal vindt hiertoe intensief contact plaats met de Verenigde Staten, het Verenigd Koninkrijk, Duitsland, Australië en de Benelux-landen. Tevens worden mogelijkheden bezien voor geïntensiveerde samenwerking met o.a. de Scandinavische landen, Canada en Frankrijk.

Zoals de commissie opmerkt, neemt Nederland actief deel aan de discussie over gedragsnormen in het digitale domein, allereerst om een open en vrij internet te behouden en tegenwicht te bieden aan landen die het vrije gebruik van internet en media aan banden willen leggen in naam van veiligheid en bestrijden van cybercriminaliteit. Tegelijkertijd onderkent het kabinet het belang om potentiële conflicten tussen landen als gevolg van cyberincidenten te voorkomen. Nederland zal zich hiervoor via geëigende fora inzetten.

Nederland acht het daarnaast van groot belang dat bedrijven hun verantwoordelijkheid nemen voor de uitvoer van technologie die zowel goed als kwaadschiks kan worden gebruikt door overheden. Omdat Nederland er ter bescherming van mensenrechten belang aan hecht dat bedrijven naast zelfrestrictie ook een kader hebben om besluiten te nemen over export van hun producten, zet Nederland zich er voor in om de *dual-use* verordening van de EU uit te breiden. Hierdoor zou het mogelijk worden een ad-hoc vergunningplicht op te leggen voor individuele gevallen indien er aanwijzingen zijn dat de goederen geheel of gedeeltelijk zullen worden gebruikt voor mensenrechtenschendingen.

NAVO

Het nieuwe strategisch concept van de NAVO heeft navolging gekregen in een in juni 2011 vastgesteld beleidsplan voor *cyber defence*. Zoals de commissie constateert, richt de NAVO zich vooral op het versterken van het defensieve vermogen ten aanzien van cyberdreigingen. Mede op aandringen van Nederland is de noodzaak van intensievere informatie-uitwisseling, het ontwikkelen van een gezamenlijke dreigingsanalyse en het belang van EU-NAVO samenwerking in het NAVO-beleid opgenomen. Het kabinet is daarnaast van mening dat de NAVO op termijn een doctrine voor de inzet van offensieve cybercapaciteiten zou moeten ontwikkelen. Ten aanzien van een

eventuele collectieve reactie op een aanval geldt dat een beslissing hierover via de bestaande procedures genomen zal worden. Ook in het digitale domein is niet altijd eenduidig vast te stellen wanneer artikel 5 in werking treedt. Dit is altijd onderwerp van politieke besluitvorming.

Europese Unie

Het kabinet deelt de visie van de commissie dat de EU gebaat is bij een integrale, gecoördineerde aanpak van digitale veiligheid. Vorig jaar heeft de Europese Commissie haar interne veiligheidsstrategie gelanceerd, waarin het verhogen van het niveau van veiligheid voor burgers en bedrijfsleven in *cyber space* geïdentificeerd is als een van de vijf strategische doelen. Uw Kamer is hierover op 19 januari 2011 geïnformeerd (Kamerstuk 32317 nr. 32). Begin dit jaar heeft Eurocommissaris Kroes aangekondigd een voorstel te doen voor een Europese internetveiligheidsstrategie. Nederland steunt deze ontwikkelingen en zal haar expertise inbrengen, bijvoorbeeld op het gebied van dreigingsanalyse en publiek-private samenwerking. Daarnaast bepleit Nederland bij de Europese Commissie dat externe, geopolitieke aspecten een duidelijke plek krijgen bij de EU-aanpak van digitale veiligheid.

DIGITALE OORLOGVOERING

No 77, AIV/No 22, CAVV December 2011

ADVIESRAAD INTERNATIONALE VRAAGSTUKKEN
ADVISORY COUNCIL ON INTERNATIONAL AFFAIRS

AIV

COMMISSIE VAN ADVIES INZAKE VOLKENRECHTELIJKE VRAAGSTUKKEN
ADVISORY COMMITTEE ON ISSUES OF PUBLIC INTERNATIONAL LAW

CAVV

Leden Adviesraad Internationale Vraagstukken

Voorzitter	Mr. F. Korthals Altes
Vicevoorzitter	Prof.dr. W.J.M. van Genugten
Leden	Mw. mr. L.Y. Gonçalves-Ho Kang You
	Mw. prof.dr. J. Gupta
	Mw. dr. P.C. Plooij-van Gorsel
	Prof.dr. A. de Ruijter
	Mw. drs. M. Sie Dhian Ho
	Prof.dr. A. van Staden
	Lt-gen. b.d. M.L.M. Urlings
	Mw. mr. H.M. Verrijn Stuart
	Prof.dr.ir. J.J.C. Voorhoeve
Secretaris	Drs. T.D.J. Oostenbrink

Postbus 20061
2500 EB DEN HAAG
telefoon 070 - 348 5108/6060
fax 070 - 348 6256
e-mail aiv@minbuza.nl
www.AIV-Advies.nl

Commissie van Advies inzake Volkenrechtelijke Vraagstukken

Voorzitter	Prof.dr. M.T. Kamminga
Leden	Prof.dr. K.C.J.M. Arts
	Dr. A. Bos
	Dr. C.M. Brölmann
	Prof.dr. M.M.T.A. Brus
	Dr. A.G. Oude Elferink
	Prof.dr. T.D. Gill
	Prof.dr. L.J. van den Herik
	Dr. N.M.C.P. Jägers
	Prof.dr. J.G. Lammers
	Prof.dr. W.G. Werner
	Prof.dr. R.A. Wessel
Ambtelijk adviseur	Prof.dr. E. Lijnzaad
Secretariaat	Mr.drs. W.E.M. van Bladel
	Mr. M.A.J. Hector

Leden Commissie Digitale Veiligheid

Voorzitter	Lt-gen. b.d. M.L.M. Urlings
Leden vanuit de AIV	Drs. D.J. Barth Mw. dr. I. Duyvesteyn Dr. P. van Ham Gen-maj. b.d. mr.drs. C. Homan Mw. dr. P.C. Plooij-van Gorsel Drs. J. Ramaker Mw. mr. H.M. Verrijn Stuart
Leden vanuit de CAVV	Prof.dr. T.D. Gill Mw. prof.dr. L.J. van den Herik Prof.dr. M.T. Kamminga
Extern deskundige	Prof.dr. M.J.G. van Eeten
Secretaris	Drs. A.D. Uilenreef

Inhoudsopgave

Woord vooraf

Bij brief van 30 augustus 2011 hebben de ministers van Buitenlandse zaken en Defensie, mede namens de minister van Veiligheid en Justitie, zich tot de Adviesraad Internationale Vraagstukken (AIV) en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken (CAVV) gewend met het verzoek een advies uit te brengen over digitale veiligheid. Met als centraal thema de betekenis van ontwikkelingen op cybergebied voor het Nederlandse buitenlands-, veiligheids- en defensiebeleid, zijn de volgende twaalf concrete vragen gesteld:

1. Op grond van welke politieke en militaire doelstellingen moeten operationele cybercapaciteiten worden ontwikkeld en kunnen worden ingezet?

2. Wat is de aard en rol van operationele cybercapaciteiten bij militaire operaties?

3. Onder welke omstandigheden kan een cyberdreiging worden beschouwd als het gebruik van geweld of een dreiging hiermee, in de zin van artikel 2 lid 4 van het VN-Handvest?

4. Onder welke omstandigheden kan een cyberaanval worden beschouwd als een gewapende aanval waartegen geweld mag worden gebruikt ter zelfverdediging op basis van artikel 51 van het VN Handvest?

5. Wanneer is er sprake van toepasselijkheid van het humanitair oorlogsrecht op gedragingen in het digitale domein?

6. Moeten deze samenhangen met kinetisch geweldsgebruik?

7. Hoe zou bij een dergelijke toepassing gestalte moeten worden gegeven aan de oorlogsrechtelijke principes van onderscheid en proportionaliteit, en aan de verplichting tot het nemen van voorzorgsmaatregelen?

8. Hoe zou in het cyberdomein gestalte moeten worden gegeven aan de volkenrechtelijke begrippen soevereiniteit, neutraliteit?

9. In hoeverre kunnen internationale gedragsnormen over het gebruik van het digitale domein een effectieve bijdrage leveren aan het vergroten van cyber security?

10. Kunnen we lering trekken uit ervaringen met bestaande gedragscodes, bijvoorbeeld op het gebied van non-proliferatie?

11. Hoe kunnen de NAVO en de EU concreet inhoud geven aan de principes van *common defence, deterrence* en de solidariteitsclausule ten aanzien van cyberdreigingen?

12. Hoe kunnen de NAVO en de EU de informatie-uitwisseling ten behoeve van dreigingsanalyses verbeteren?

Het eerste deel van het advies gaat in op de aard van digitale conflicten en het ontwikkelen van hiermee verband houdende operationele capaciteiten door de

Nederlandse krijgsmacht. Het tweede deel behandelt vraagstukken rondom het internationaal recht op dit gebied, in het bijzonder de voorwaarden voor het gebruik van geweld en de toepassing van het humanitair oorlogsrecht. In het derde deel komt de internationale samenwerking aan bod, zoals afspraken over gedragsnormen die kunnen bijdragen aan de vermindering van digitale conflicten evenals de samenwerking in het kader van de NAVO en de EU. Tot slot volgt een overzicht met de belangrijkste conclusies en aanbevelingen, dat tevens als samenvatting kan worden gelezen.

Het advies is opgesteld door een gecombineerde commissie van leden van de AIV en CAVV bestaande uit lt-gen. b.d. M.L.M. Urlings (voorzitter), drs. D.J. Barth, mw. dr. I. Duyvesteyn, prof.dr. T.D. Gill, mw. prof. L.J. van den Herik, dr. P. van Ham, gen-maj. b.d. mr.drs. C. Homan, prof.dr. M. Kamminga, mw. dr. P.C. Plooij-van Gorsel, drs. J. Ramaker en mw. mr. H.M. Verrijn Stuart. Prof.dr. M.J.G. van Eeten van de TU Delft was toegevoegd aan de commissie als extern deskundige. De commissie werd bijgestaan door de ambtelijke contactpersonen mw. drs. L.C. den Breems (Ministerie van Buitenlandse Zaken, DVB/VD), drs. M.A. Veenendaal (Ministerie van Defensie, DAB), mw. drs. E. van Beurden (Ministerie van Veiligheid en Justitie) en de secretaris van de CAVV, mw. mr. M.A.J. Hector. Het secretariaat van de commissie werd gevoerd door drs. A.D. Uilenreef (AIV), bijgestaan door de stagiaires mw. S. de Jong en dhr. A.P. Smit.

Voor dit advies heeft de commissie gesproken met een aantal deskundigen. In bijlage IV is een overzicht van geraadpleegde personen opgenomen. De AIV/CAVV is hen zeer erkentelijk voor hun inbreng.

Het advies is vastgesteld tijdens de vergadering van de CAVV op 6 december en de vergadering van de AIV op 16 december 2011.

Inleiding

'Cyber' en de noodzaak tot demystificatie

Digitale veiligheid of 'cyber security' is een relatief nieuw fenomeen dat in korte tijd op veel aandacht van politici, beleidsmakers, wetenschappers en media heeft mogen rekenen. De digitale ruimte wordt soms echter ook gezien als *terra nullius* waarover een echt politiek debat nog moet plaatsvinden.[1] De AIV en de CAVV beogen daar in de Nederlandse context een bijdrage toe te leveren. De betrokkenheid bij digitale conflicten dient te worden getoetst aan politieke uitgangspunten en internationaalrechtelijke beginselen. Het debat mag niet worden overheerst door militaire en technologische antwoorden op deze nieuwe dreiging. Het digitale domein, of *cyberspace,* is per definitie grensoverschrijdend. Het vergroten van de veiligheid op dit terrein dient daarom voor een belangrijk deel via internationale samenwerking tot stand te komen. De AIV en de CAVV hebben in dit gezamenlijk advies geprobeerd zich te laten leiden door een nuchtere blik op deze problematiek, zoveel mogelijk technisch jargon te vermijden en zich niet te laten meeslepen door veelgebruikte *sciencefiction*-achtige parallellen. De leidende gedachte is daarbij geweest dat het fenomeen wellicht nieuw is, maar dat de samenleving niet voor het eerst in de geschiedenis met technologische vernieuwing wordt geconfronteerd en dat bestaande principes en beginselen behulpzaam kunnen zijn bij het formuleren van een antwoord hierop.

Gebruikte definities en het risico van begripsverwarring

Aangezien 'cyber security', hierna voornamelijk aangeduid als digitale veiligheid, een relatief nieuw fenomeen is, wordt hieronder allereerst een omschrijving gegeven van de in dit advies gehanteerde terminologie. Onder *digitale veiligheid* wordt verstaan: '*het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van informatie- en communicatietechnologie (ICT) of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie'*.[2]

De bedreiging van de digitale veiligheid kan - afgezien van uitval vanwege technische gebreken of natuurverschijnselen - voortkomen uit digitale oorlogvoering, digitale spionage, digitaal terrorisme, digitaal activisme en digitale criminaliteit. Definiëring van deze verschijningsvormen is niet alleen nodig voor een juist begrip van de adviestekst, het dient eveneens om te voorkomen dat verschillende vormen van dreiging in politiek en beleid conceptueel met elkaar worden vermengd. Dit betekent niet dat deze dreigingsvormen geen samenhang kunnen vertonen, integendeel, zo kunnen bijvoorbeeld staten voor spionageactiviteiten gebruik maken van criminele organisaties of 'hacktivisten'. Vaak komen de gebruikte technieken overeen en verschilt alleen het beoogde doel. Het onderscheiden van de doelstelling is vooral van belang voor het bepalen van de juiste nationale respons op specifieke dreigingen, bijvoorbeeld om het risico van een overreactie te beperken. Het is daarom wenselijk dat de overheid gebruik maakt van duidelijke en uniforme begripsomschrijvingen. Op internationaal niveau is het eveneens noodzakelijk dat overheden en organisaties tot eensluidende interpretaties komen, wil men in staat zijn om internationale afspraken te maken over de aanpak van digitale dreigingen.

1 Chatham House, *On Cyber Warfare*, November 2010.

2 Nationale Cyber Security Strategie, 22 februari 2011.

In dit advies wordt *digitale oorlogvoering* gedefinieerd als: *het uitvoeren van militaire operaties die erop zijn gericht om met digitale middelen computersystemen of netwerken van een tegenstander te verstoren, misleiden, veranderen of vernietigen*. Belangrijke criteria die bepalen of er sprake is van digitale oorlogvoering zijn: 1) het betreft een militaire operatie met als doelstelling het behalen van politiek en militair voordeel, 2) het gaat om het berokkenen van schade aan de digitale infrastructuur van de tegenstander en 3) door middel van de inzet van digitale middelen (aangezien immers ook met kinetische middelen computersystemen kunnen worden vernietigd).

Onder *digitale spionage* moet worden verstaan: *het heimelijk verwerven van gegevens op netwerken of informatiesystemen door overheden of bedrijven ten bate van hun diplomatieke, militaire of economische belangen.*

In dit advies wordt *digitaal terrorisme* omschreven als: *via de inzet van digitale middelen pogen een samenleving of delen daarvan ernstig te ontwrichten om een politiek doel te bereiken*.

Digitaal activisme (ook wel *hacktivisme*) wordt beschouwd als: *het inbreken op netwerken of informatiesystemen door een individu of groepering met als doel deze te verstoren of te veranderen om zodoende een politieke ideologie of sociale overtuiging onder de aandacht te brengen.*

Digitale criminaliteit wordt hier gedefinieerd als: *een strafbare gedraging waarbij wordt getracht door middel van gebruikmaking van netwerken of informatiesystemen financieel of andersoortig voordeel te behalen*.

Dit advies behandelt, conform de adviesaanvraag, digitale veiligheid gerelateerd aan het Nederlands buitenlands-, veiligheids- en defensiebeleid. Digitale criminaliteit krijgt om deze reden minder nadruk in dit advies. Wanneer nodig zal uiteraard aandacht worden besteed aan dwarsverbanden met digitale criminaliteit. In praktijk is immers niet altijd direct vast te stellen om welke vorm van dreiging het precies gaat.

I De digitale dreiging en capaciteiten voor de krijgsmacht

I.1 Aard en intensiteit van digitale conflicten

De digitale dreiging
De regering constateert in de adviesaanvraag dat de afhankelijkheid van het functioneren van digitale netwerken nieuwe veiligheidsrisico's met zich meebrengt. In het bestaande dreigingsbeeld wordt erop gewezen dat burgers, overheid en bedrijven kwetsbaar zijn voor digitaal misbruik, dat cybercriminaliteit geavanceerder wordt en dat er diverse voorbeelden zijn van digitale spionage vanuit het buitenland.[3] Daarbij wordt gebruik gemaakt van verschillende technieken, zoals *botnet*s en het versturen van kwaadaardige software (*malware*). Soortgelijke aanvallen worden eveneens toegepast bij militaire operaties. Voorbeelden zijn de verstoring van het internetverkeer en militaire communicatiesystemen in Georgië (2008) en de Stuxnet-aanval op de procesbesturing van een Iraanse verrijkingscentrale voor nucleair materiaal (2010). Het betreft dus geen virtuele, maar een reële dreiging. Zelfs het in opdracht van de OESO opgestelde rapport 'Reducing Systematic Cybersecurity Risk', dat kritisch van toonzetting is waar het gaat om de invloed van de dreiging, concludeert dat 'het gebruik van cyberwapens wijdverbreid is' en dat het 'een veilige veronderstelling is dat cyberwapens binnenkort alomtegenwoordig zullen zijn'.[4]

Waar het bestaan van digitale dreigingen als zodanig niet ter discussie staat, is er wel onduidelijkheid over de omvang en invloed hiervan. De regering erkent in de beschikbare trendanalyses dat het onderzoek hiernaar 'nog in de kinderschoenen' staat.[5] De bestaande kwantitatieve onderzoeken zijn over het algemeen statistisch dermate onbetrouwbaar en subjectief van aard dat hieruit geen bruikbare conclusies kunnen worden getrokken.[6] De Nederlandse organisatie *Bits of Freedom* vraagt om deze reden om een onafhankelijke en wetenschappelijk verantwoorde nulmeting naar de aard en omvang van aan cybersecurity gerelateerde vraagstukken.[7] De AIV/CAVV onderschrijft het belang van meer systematisch en kwantitatief onderzoek naar de omvang van de dreiging. Aangezien het bij uitstek grensoverschrijdende problematiek betreft en omdat de aanwezige capaciteiten zo het best gebundeld kunnen worden, beveelt de AIV/CAVV de regering aan een dergelijk onafhankelijk onderzoek in EU- en NAVO-verband te initiëren.

Op basis van openbare en gerubriceerde informatie, onder meer afkomstig van de politie, inlichtingendiensten en bedrijfsleven, geeft het Cyber Security en Incident Response Team van de Nederlandse overheid (GOVCERT.NL) een schatting van de bedreiging van de digitale

3 Het Nationale Trendrapport Digitale Veiligheid en Cybercrime 2010. Cybersecuritybeeld Nederland, December 2011.

4 P. Sommer and I. Brown, *Reducing Systematic Cybersecurity Risk*, OECD/IFP Project on Future Global Shocks, 14 January 2011.

5 Cybersecuritybeeld Nederland, December 2011. GOVCERT.NL, p. 12.

6 D. Florêncio en C. Herley, *Sex, Lies and Cyber-crime Surveys*, Microsoft Research, <http://www.research.microsoft.com/pubs/149886/SexliesandCybercrimeSurveys.pdf>.

7 Bits of Freedom, *Kamerbriefing Nationale Cybersecurity Strategie*, 27 mei 2011.

veiligheid. De overheid constateert dat digitale criminaliteit gerichter en geavanceerder wordt en de meerderheid van alle cyberincidenten omvat. Voorts wordt aangegeven dat overheden en bedrijven regelmatig slachtoffer zijn van digitale spionage en dat recente incidenten wereldwijd duiden op een toenemende dreiging hiervan. Terroristen zouden nog nauwelijks digitale aanvallen initiëren en het internet alleen instrumenteel gebruiken, zoals voor propaganda- en rekruteringsdoeleinden. Ten aanzien van digitale oorlogvoering wordt in de beschikbare trendanalyses volstaan met de opmerking dat deze dreigingsvorm zich op het moment het minst manifesteert, maar het 'potentiële effect waarschijnlijk het grootst' is.[8] In vrij sensationele publicaties van sommige buitenlandse toekomstvoorspellers valt te beluisteren dat toekomstige oorlog in het digitale domein zal worden uitgevochten en beslecht.[9] De AIV/CAVV is van mening – zoals hieronder wordt toegelicht – dat de kans op een dergelijke 'cyberoorlog', die uitsluitend in het digitale domein wordt uitgevochten, gering is. Het gebruik van dit soort terminologie draagt bovendien niet bij tot een goed begrip van de problematiek.

Een vijfde dimensie voor militair optreden

Wanneer wordt gesproken over 'cyberspace' of het digitale domein, wordt soms gesuggereerd dat het een losgekoppelde 'ruimte' betreft, die geen verband houdt met tijd, plaats en menselijk handelen. Onder het digitale domein moet echter niets meer of minder worden verstaan dan het geheel van ICT-middelen en -diensten. Hiermee wordt dus niet alleen het internet bedoeld, maar ook alle niet met internet verbonden netwerken of andere digitale apparaten.[10] Wanneer we dit vertalen in termen van militaire activiteiten, dan kunnen we het digitale domein gewoonweg beschouwen als een vijfde operatiegebied – zij het met specifieke kenmerken – dat interacteert met de andere vier dimensies voor militaire operaties: land, zee, lucht en ruimte. Dit betekent dat operaties in de vijfde dimensie ook kunnen fungeren als *force multiplier* van activiteiten in de overige dimensies. Het optreden in andere dimensies is overigens nauwelijks meer mogelijk zonder het gebruik van digitale middelen. Oorlogen werden aanvankelijk alleen te land en ter zee uitgevochten. Aan het begin van de Eerste Wereldoorlog kwam hier, met de strijd in de lucht, een derde dimensie bij. Vanaf de jaren '80 kreeg de vierde dimensie, met de ontwikkeling van antisatellietraketten en het *Space Defence Initiative*, operationele betekenis. De ontwikkeling en verspreiding van internet alsmede de algehele digitalisering van de samenleving maakt dat nu wordt gesproken over een vijfde dimensie, de enige door de mens gecreëerde dimensie.

Bij het uitvoeren van militaire operaties kan er voor worden gekozen ook gebruik te maken van digitale aanvallen. In essentie gaat het om de inzet van een middel – digitale capaciteit – uit de *toolbox* van militaire middelen die een bijdrage kunnen leveren aan het bereiken van een politiek doel. In een aantal van de meest bekende voorbeelden, zoals eerder in dit advies genoemd, zijn digitale aanvallen gecombineerd met conventionele operaties. In het geval van Stuxnet was het noodzakelijk om het geïnfecteerde programma via een fysieke *human intelligence*operatie de Iraanse verrijkingscentrale in te smokkelen. Uiteraard is het mogelijk om een militaire operatie te beperken tot het uitvoeren van digitale aanvallen. Op deze wijze zou het technisch uitvoerbaar kunnen zijn om delen van de kritieke infrastructuur van een land – in ieder geval tijdelijk – te ontregelen. Het digitale domein zal naar verwachting in elk toekomstig conflict een belangrijke rol spelen. Een 'cyberoorlog', die uitsluitend in het

8 Het Nationale Trendrapport 2010, p. 37.

9 R.A. Clarke, R.K. Knake, *Cyber War: The next threat to national security and what to do about it*, Harper Collins Publishers Inc, 2010.

10 Het Nationale Trendrapport 2010.

digitale domein wordt uitgevochten, met verwoestende gevolgen, is echter niet aannemelijk. Daarom wordt in dit advies de meer afgebakende term 'digitale oorlogvoering' gebruikt, te beschouwen als onderdeel van een militaire operatie die ook andere (niet digitale) dimensies kan omvatten.

I.2 Operationele cybercapaciteiten

Politieke en militaire doelstellingen
Op grond van welke politieke en militaire doelstellingen moeten operationele cybercapaciteiten worden ontwikkeld? Politieke doelstellingen dienen vooraf te gaan aan militaire doelstellingen, of om met de militair theoreticus Von Clausewitz te spreken: oorlog is de voortzetting van politiek met andere middelen. Als vertrekpunt wordt daarom aangesloten bij de doelstellingen van het buitenlands beleid, waarbij de Nederlandse regering inzet op de versteviging van drie pijlers: veiligheid, welvaart en vrijheid. Hieraan wordt invulling gegeven door het bevorderen van de internationale stabiliteit en veiligheid, de energie- en grondstofzekerheid, de internationale rechtsorde, inclusief mensenrechten, en handels- en economische belangen.[11] Daarbij realiseert de regering zich dat – aangezien de open Nederlandse samenleving sterk verbonden is met het buitenland – interne en externe veiligheid nauw met elkaar samenhangen. Deze verbondenheid levert een grote bijdrage aan de welvaart van ons land, maar maakt ook kwetsbaar. De dreigingen van de 21e eeuw kennen een sterk grensoverschrijdend karakter en zijn niet alleen van staten maar ook van niet-statelijke actoren afkomstig.

Voor de krijgsmacht heeft de regering drie hoofdtaken geformuleerd: bescherming van het eigen en bondgenootschappelijk grondgebied; bevordering van de internationale rechtsorde en stabiliteit; en ondersteuning van civiele autoriteiten.[12] In praktijk betekent dit dat voor de bescherming van het eigen en bondgenootschappelijk grondgebied alle ons ter beschikking staande middelen zullen worden ingezet. Aan de tweede hoofdtaak van de krijgsmacht, de bevordering van de internationale rechtsorde, wordt bijgedragen door de deelname aan interventie- en stabilisatieoperaties in EU- en NAVO-verband of door deelname aan ad-hoc-coalities. Ook kan worden deelgenomen aan politiemissies. De derde hoofdtaak krijgt vorm door het verlenen van incidentele bijstand aan civiele autoriteiten (rampenbestrijding, handhaving openbare orde en veiligheid) en reguliere taken zoals grensbewaking door de marechaussee, het beheer van de kustwacht door de marine en de ruiming van explosieven.

De inzet van operationele cybercapaciteiten dient ten dienste te staan van bovenstaande doelstellingen. Voor de welvaart van Nederland, met een sterk internationaal georiënteerde logistieke en dienstensector, is een veilig en goed functionerend digitaal netwerk essentieel. Nederland kent een van de hoogste internetdichtheden ter wereld. De vrijheid om overal ter wereld op internet op vreedzame wijze van gedachten te wisselen, sluit aan bij het belang dat Nederland hecht aan de eerbiediging van de mensenrechten en fundamentele vrijheden. Voor het vertrouwen van de burger in de overheid is een veilige digitale dienstverlening essentieel. Het tegengaan van digitale dreigingen dient voorts de nationale veiligheid. De AIV/CAVV hecht eraan te benadrukken dat dergelijke dreigingen, waarvan zoals eerder geconstateerd de omvang niet bekend is, vooraleerst met niet-militaire middelen dienen

11 Regeerakkoord en de Memorie van Toelichting van het ministerie van Buitenlandse Zaken 2012. De bevordering van de internationale rechtsorde is tevens vastgelegd in de Grondwet (artikel 90).

12 De Grondwet (artikel 97) bepaalt dat er een krijgsmacht is ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde. Dit is verder uitgewerkt in de Defensienota 2000 en opvolgende regeringsstukken.

te worden ingeperkt. Hierbij is – naast de belangrijke bijdrage die private partijen kunnen leveren – ook een rol weggelegd voor diplomatieke inspanningen, zoals het overeenkomen van internationale gedragsnormen ten behoeve van de beheersing van potentiële digitale conflicten. Dit komt aan de orde in hoofdstuk III.1. Naast de ontwikkeling van operationele cybercapaciteiten is het tevens van belang te investeren in een samenhangende 'cyberdiplomatie', waarbij als reactie op concrete dreigingen met kennis van zaken een breed palet aan maatregelen wordt overwogen, variërend van politieke druk, de inzet van economische sancties, het aandringen op strafrechtelijke maatregelen tot – in laatste instantie – het gebruik van gesanctioneerd geweld.

Operationele cybercapaciteiten – deel uitmakend van militair vermogen – kunnen een bijdrage leveren aan het bereiken van een politiek doel. Voor de inzet van deze capaciteiten is een helder politiek kader essentieel. Vanwege het grensoverschrijdende karakter van de meeste dreigingsvormen, en dit geldt zeker voor digitale dreigingen, is er sprake van een sterke verwevenheid tussen externe en interne veiligheid. Nederland kent evenwel geen geïntegreerde strategie voor het buitenlands en binnenlands veiligheidsbeleid. De bestaande nationale veiligheidsstrategie is nationaal gericht en het bevorderen en handhaven van de internationale rechtsorde ontbreekt hierin als vitaal belang.[13] De AIV/CAVV is van mening dat operationele cybercapaciteiten en ontwikkelingen op dit gebied een plaats moeten krijgen in een geïntegreerde strategie voor het binnenlands en buitenlands veiligheidsbeleid. Een dergelijke strategie moet inzicht geven in de te bereiken doelen (*ends*), de wijze waarop we deze doelen willen bereiken (*ways*) en de middelen die we daar voor willen inzetten (*means*).

Aard van operationele cybercapaciteiten

Er is een aantal specifieke kenmerken verbonden aan het gebruik van 'digitale wapens'.[14] De aard hiervan heeft gevolgen voor de operationele inzet in het digitale domein. Allereerst kennen digitale aanvallen veelal *indirecte effecten*. Op internet is alles nauw met elkaar verbonden, waardoor een aanval op een militair systeem gevolgen kan hebben voor civiele netwerken zonder dat van te voren is vast te stellen wat de omvang en ernst van die gevolgen is. Het is lastig om een onderscheid te maken tussen strijders en niet-strijders. Ook is sprake van relatief *geringe materiële instapkosten*: het vereiste materiaal is eenvoudiger en goedkoper aan te schaffen dan vliegtuigen of gevechtstanks. Dit betekent niet dat elke digitale aanval met eenvoudig te verkrijgen middelen kan worden uitgevoerd. Voor het plannen en uitvoeren van een gerichte *technisch complexe aanval* is gespecialiseerde kennis noodzakelijk. Dit wordt in veel beschouwingen onderschat, maar geldt zeker ook voor activiteiten als inlichtingenoperaties die aan een inzet voorafgaan. Voorts kennen digitale wapens een *beperkte houdbaarheidsduur.* Ontwikkelde digitale aanvallen die feitelijk uit programmeertaal bestaan, kunnen, anders dan traditionele wapens, op elk moment achterhaald zijn en dienen geheim te worden gehouden.[15] Op het moment dat digitale middelen worden ingezet, of op andere wijze openbaar worden, kunnen anderen kennisnemen van de gebruikte kwetsbaarheden en deze verhelpen. In die zin is er geen sprake van een klassieke wapenwedloop, maar een nieuwe wedloop in digitale expertise en vaardigheden. Tot slot zijn aan-

13 P.A.L. Ducheine en J.E.D. Voetelink, 'Cyberoperaties: naar een juridisch raamwerk', *Militaire Spectator,* 180(6).

14 Deze wapenanalogie behoeft wel nuancering. Het gaat immers vooral om technologische kennis en vaardigheden.

15 The New York Times, *U.S. Debated Cyberwarfare in Attack Plan on Libya*, 17 oktober 2011. Het artikel noemt dit als een van de overwegingen om geen cybercapaciteiten in Libië in te zetten.

vallen *moeilijk toerekenbaar* aan een staat, groepering of individu. Op dit probleem van 'attributie', dat in de discussie over het gebruik digitale wapens een centrale rol speelt, wordt hieronder uitgebreider in gegaan.

De genoemde kenmerken hebben tot gevolg dat de inzet van digitale wapens *asymmetrisch* van aard kan zijn. Het benodigde materiaal kan immers door landen die op kinetisch terrein militair achterlopen, 'hackers' en andere niet-statelijke actoren worden verworven en – indien men niet zwaar tilt aan mogelijke indirecte effecten – met relatief beperkte kosten en zonder een omvangrijk militair apparaat worden ingezet. Dit wordt nog versterkt door het feit dat een aanvaller moeilijk is te identificeren. Er is in het digitale domein tevens sprake van *offensieve dominantie*: het is makkelijker, sneller en goedkoper om een systeem aan te vallen dan om het te beschermen. Dit hangt ook samen met de anonimiteit waarin een aanvaller zich kan voorbereiden en het element verrassing kan uitbuiten. Wel is het zo dat er naar alle waarschijnlijkheid geen daadwerkelijke 'first strike'-capaciteit bestaat waarmee de verdediging van de tegenstander en de mogelijkheid om digitaal of kinetisch terug te slaan kan worden uitgeschakeld. Tot slot is het toezicht op het gebruik van digitale wapens *lastig reguleerbaar*. Dit komt doordat deze gemakkelijk te verbergen zijn en – anders dan bij kernwapens – offensieve capaciteiten heimelijk kunnen worden ontwikkeld en getest. Over de mogelijkheden van non-proliferatie en normstelling op dit terrein, wordt ingegaan in hoofdstuk III.1.

Zoals gezegd speelt de attributieproblematiek een centrale rol in de discussie over het beleid rond digitale wapens. Het is moeilijk om in het geval van spionage of kleinschalige aanvallen te herleiden wie daar achter schuil gaat. Zo kan een aanvaller gebruik maken van een keten van andere – gehackte – computers om te spioneren of van een *botnet* van geïnfecteerde computers om schade aan te richten. Een overheid kan bij een aanval gebruik maken van niet-statelijke actoren, zoals zogenoemde *patriotic hackers*. Andersom kunnen hackers zich verbonden verklaren met staten, zonder dat dit zo is. Dit alles heeft consequenties voor het gebruik van offensieve acties gericht tegen een aanvaller. Indien het lastig is te bepalen wie achter een aanval zit, maakt dit het doen van een tegenaanval gecompliceerd. Het is technisch gezien mogelijk om de bron (IP-adres van een computer) van waaruit een aanval afkomstig is te identificeren en een tegenaanval te doen tegen die computer. Hiervoor bestaan zogeheten 'terugtraceer-applicaties' *(traceback).* Maar het blijft altijd mogelijk dat wat men als de bron identificeert, ook slechts een schakel in de aanval is geweest. Hoe dan ook, de systemen die bij de aanval zijn betrokken kunnen worden gecompromitteerd. Men weet dan nog niet wie de verantwoordelijkheid draagt voor de aanvankelijk ingezette aanval. Het is echter zeker niet onmogelijk om de identiteit van een aanvaller vast te stellen. Hierbij hoeft niet altijd het internet zelf te worden gebruikt, maar kunnen ook andere bronnen worden aangewend (niet-technische attributie), zoals die van inlichtingendiensten, politieke uitlatingen – opeisen aanval of eerdere publieke dreigingen – en andere zaken die op een potentiële dader wijzen. Indien er op basis hiervan een voldoende mate van zekerheid bestaat over de oorsprong van de aanval zou onder bepaalde voorwaarden, die worden uiteengezet in hoofdstuk II, uitoefening van het recht op zelfverdediging gerechtvaardigd kunnen zijn.

Rol cybercapaciteiten bij militaire operaties

De minister van Defensie heeft de ambitie uitgesproken dat de krijgsmacht – naast defensieve cybercapaciteiten – ook offensieve capaciteiten ontwikkelt. In de motie Knops (december 2009) wordt geconstateerd dat defensieve capaciteiten niet volstaan.[16] Om de vraag welke de rol dient te zijn van operationele cybercapaciteiten bij militaire operaties

16 Motie van de Tweede Kamerleden Knops, Voordewind en Eijsink: Tweede Kamer, vergaderjaar 2009–2010, 32 123 X, nr. 66.

goed te beantwoorden, is het noodzakelijk duidelijk aan te geven wat onder defensieve en offensieve capaciteiten moet worden verstaan, hetgeen in het publieke debat niet altijd gebeurt. Dit heeft tevens gevolgen voor het toepasselijke rechtsregime. Zo is op het via digitale weg vergaren van inlichtingen de Wet op de inlichtingen en veiligheidsdiensten 2002 (WIV 2002) van toepassing, terwijl het digitaal uitschakelen van de luchtverdediging van een tegenstander onder het *ius in bello* valt. De juridische implicaties hiervan worden verder uitgewerkt in hoofdstuk II.

In het onderstaande schema worden de verschillende typen operationele cyberactiviteiten gegroepeerd in defensieve-, inlichtingen- en offensieve activiteiten. De verschillende interventies zijn aangeduid als netwerkverdediging, netwerkexploitatie en netwerkaanval.

Defensieve activiteiten	- Beveiliging/monitoring eigen netwerken (inclusief wapensystemen) **netwerkverdediging (passieve verdediging)** - Beveiliging netwerkverbinding defensie-industrie **netwerkverdediging (passieve verdediging)** - Neutraliserende tegenaanval ter bescherming eigen systemen *(bijvoorbeeld ontregelen command&control van botnets of via malware een systeem van de aanvaller overnemen/saboteren*) **netwerkaanval (actieve verdediging)**
Inlichtingen activiteiten	- Aftappen/toegang tot internetverkeer *(interceptie IP-data of onderliggende protocollen)* **netwerkexploitatie** - Monitoring omvang en patronen dataverkeer buitenlandse netwerken **netwerkexploitatie** - Heimelijk inbreken op systemen en data downloaden (*bijvoorbeeld door middel van exploits*) **netwerkexploitatie** - Contra-inlichtingen activiteiten *(bijvoorbeeld het manipuleren of verstoren van cyberinlichtingenactiviteiten van derden)* **netwerkexploitatie**
Offensieve activiteiten	- Psychologische operaties *(bijvoorbeeld versturen berichten aan bevolking of overheden via gehackt netwerk)* **netwerkaanval** - Uitschakelen/storen van commando-, controle- en communicatiefuncties en andere defensiesystemen tegenstander *(DDoS-aanvallen)* **netwerkaanval** - Vernietiging kritieke infrastructuur *(beïnvloeden procesbesturing van bijvoorbeeld nutsbedrijven)* **netwerkaanval**

Operationele cyberactiviteiten

Het ministerie van Defensie en de krijgsmacht maken gebruik van digitale toepassingen, variërend van commando- tot bedrijfsvoering. Deze functies dienen adequaat beveiligd te zijn. De *beveiliging van defensiesystemen* kan bestaan uit statische verdediging, zoals het

installeren van een 'firewall' of andere middelen die het moeilijk maken om een systeem binnen te dringen, en dynamische verdediging die erop is gericht om 'achter de eigen voordeur' te kijken naar verdachte activiteiten binnen de eigen netwerken. Tevens kan worden overwogen het eigen netwerk te beschermen door een tegenaanval uit te voeren op de systemen van de aanvaller.

Bij het vergaren van *inlichtingen* wordt het gebruik van het digitale domein steeds belangrijker. Digitale capaciteiten bij de inlichtingendiensten dragen bij aan de informatiepositie over aard en herkomst van (potentiële) digitale dreigingen evenals het vermogen zelf netwerken binnen te dringen en te exploiteren ten behoeve van inlichtingenoperaties. Het digitaal afluisteren van een persoon of organisatie kan door middel van de interceptie van IP-data of door het technisch monitoren van de activiteiten van netwerken van derden. Het langs digitale weg kopiëren van data op andere computers of netwerken is eveneens mogelijk. Bij het vergaren van inlichtingen kan een onderscheid worden gemaakt tussen het onderscheppen van dataverkeer en het binnendringen van systemen. In het eerste geval gaat het om analyseren van datapatronen (omvang en richting dataverkeer) of het afluisteren van dataverkeer, eventueel met behulp van onderschepte encryptiecodes. In het tweede geval gaat het om het toegang verschaffen tot het netwerk zelf via het plaatsen van *malware*, het benutten van systeemkwetsbaarheden of het gebruik van *social engineering*technieken.

Bij militaire operaties kunnen *offensieve digitale capaciteiten* worden ingezet. Het is de ambitie van de krijgsmacht om niet alleen te verdedigen, maar ook te kunnen aanvallen in het digitale domein. Digitale aanvallen betreffen operaties gericht op verstoren, beschadigen of vernietigen van computers en netwerken, of van de hierop aanwezige informatie.[17] Er zijn velerlei vormen van digitale aanvallen mogelijk, zoals het verstoren van de commandofuncties van de tegenstander door kwetsbaarheden hierin te benutten. Andere aanvallen, die bijvoorbeeld gericht zijn op de kritieke infrastructuur, kunnen fysieke schade en menselijk letsel tot gevolg hebben. Vaak worden overigens voor exploitatie en aanvallen dezelfde technieken gebruikt en wijkt alleen de doelstelling af. Zo kan een 'Trojaans paard' dat is geplaatst voor het ongezien downloaden van data op een binnengedrongen netwerk, een inlichtingenactiviteit, op een later moment ook worden gebruikt om de data op dit netwerk te vernietigen.

Naast de daadwerkelijke inzet van operationele capaciteiten, is een belangrijke functie van militair vermogen *afschrikking*. De vraag rijst welke rol offensieve cybercapaciteit kan spelen in het kader van *afschrikking*, zowel tegen statelijke- als niet-statelijke actoren. Geloofwaardige *afschrikking* moet zijn gebaseerd op de overtuiging bij een potentiële tegenstander dat men beschikt over de capaciteit en de bereidheid om die capaciteit in te zetten teneinde een aanval te vergelden of een dreigende aanval te voorkomen.[18] Bij de toepassing van dit principe in het digitale domein doen zich echter de nodige problemen voor. Adequate digitale *afschrikking* vereist in de eerste plaats middelen voor vroegtijdige detectie. Bij conventionele en nucleaire middelen zijn de capaciteiten van de verschillende landen meestal bekend, digitale wapens kunnen echter volstrekt heimelijk worden ontwikkeld en getest. De aanval zelf kan plaatsvinden 'met de snelheid van het licht'. Menselijke besluitvorming voor tegenmaatregelen loopt hier altijd achter. De inzet van defensieve middelen met *automatische* vergeldingscapaciteit brengt echter het risico met zich mee dat verkeerde doelen worden getroffen

17 Gebaseerd op de definitie van de National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 2009, pp. 10-11.

18 *'UK warns it will strike first against cyber-attackers'*. Interview met Britse minister van Buitenlandse Zaken William Hague, The Sun, 18 oktober 2011.

of dat de reactie buitenproportioneel is. Ook kan het moeilijk zijn om het motief van de aanval te onderkennen, met het oog op een proportionele reactie. Gaat het om digitale spionage of om meer?[19] Tot slot is er, zoals hiervoor besproken, het probleem van attributie.

Gevolgen voor de operationele inzet van de krijgsmacht
Juridische randvoorwaarden: Net zoals bij elk wapensysteem, is ook de inzet van digitale wapens gebonden aan internationaalrechtelijke beperkingen. Deze komen aan de orde in het volgende hoofdstuk. Er zijn ook beperkingen ten aanzien van het gebruik van digitale middelen bij het inlichtingenwerk, die volgen uit de WIV 2002. Ten eerste is het zo dat waar voorheen berichten – met de benodigde ministeriële toestemming – konden worden onderschept door het 'afluisteren' van satellietverkeer, via deze methode nog slechts een deel van de benodigde data waaruit een bericht bestaat, kan worden getraceerd. Berichten worden namelijk opgeknipt in datapakketjes en via verschillende kanalen verstuurd, onder andere via glasvezelkabels. Volgens artikel 27 van de huidige WIV mogen alleen niet-kabelgebonden data ongericht worden onderschept.[20] De AIV/CAVV is van mening dat de technologische ontwikkelingen het wenselijk maken dat wordt bezien of het huidige onderscheid tussen kabelgebonden en niet-kabelgebonden gehandhaafd moet blijven. Ten tweede merkt de AIV/CAVV op dat artikel 24 van de WIV de mogelijkheid biedt tot netwerkexploitatie, waarbij door het plaatsen van een *exploit* (bijvoorbeeld een Trojaans paard of virus), data van een ander netwerk wordt gehaald.[21] Het is echter om goede redenen op basis van de WIV niet toegestaan dat een inlichtingendienst een geplaatste *exploit* gebruikt voor een netwerkaanval met een militair oogmerk, die het wijzigen of beschadigen van een systeem tot doel heeft. Een dergelijke aanval dient onder verantwoordelijkheid van de Commandant der Strijdkrachten (CDS) plaats te vinden, na verkregen politieke toestemming. Het is noodzakelijk binnen de krijgsmacht ook op digitaal terrein duidelijke procedurele afspraken te maken, die volgen uit deze functiescheiding.

Technische beperkingen: De specifieke kenmerken van 'digitale wapens' – zoals eerder in de hoofdstuk beschreven – leggen eveneens beperkingen op aan een verantwoorde operationele inzet hiervan. Aan de inzet zijn immers indirecte effecten verbonden, waarbij niet altijd voorspelbaar is op welke wijze en in welke omvang civiele systemen worden geraakt. Voorts is het technisch complex en kan het een lange voorbereidingstijd vergen om digitale capaciteiten in te zetten bij een militaire operatie, zoals bijvoorbeeld het digitaal uitschakelen van een luchtverdedigingssysteem. Wanneer snel ingrijpen noodzakelijk is en er geen noodzaak bestaat om een dergelijke operatie geheim te houden, dan kan ook het gebruik van kinetische middelen overwogen worden. Bij het inzetten van digitale wapens is het probleem van attributie een complicerende factor.

Personele en financiële capaciteit: het ministerie van Defensie heeft, ondanks de grootschalige bezuinigingen op de krijgsmacht een intensivering op het terrein van vergroting van de

19 Digitale spionage kan – binnen de regels van het internationale recht – slechts leiden tot diplomatieke vergeldingsmaatregelen, hoe schadelijk het verlies van informatie ook is.

20 WIV 2002, Artikel 27, lid 1: 'De diensten zijn bevoegd tot het met een technisch hulpmiddel ongericht ontvangen en opnemen van niet-kabelgebonden telecommunicatie. Tot de bevoegdheid, bedoeld in de eerste volzin, behoort tevens de bevoegdheid om versleuteling van de telecommunicatie ongedaan te maken'.

21 Dit artikel bepaalt dat de inlichtingendiensten bevoegd zijn om met gebruikmaking van technische hulpmiddelen binnen te dringen in een geautomatiseerd netwerk, inclusief de bevoegdheid de hierin opgeslagen gegevens over te nemen.

digitale weerbaarheid en de ontwikkeling van een operationele cybercapaciteit aangekondigd. Per 1 januari 2012 is er een operationele *taskforce cyber* opgericht. Voor de periode tot en met 2015 wordt 50 miljoen euro vrijgemaakt. Dit bedrag zal in deze periode vooral worden besteed aan het verbeteren van de bescherming van de netwerken, systemen en informatie van Defensie en de uitbreiding van de inlichtingencapaciteit in het digitale domein. Dit is een relatief bescheiden bedrag wanneer dit wordt afgezet tegen de totale defensiebegroting en de middelen die een aantal andere landen (vooral VS, VK) investeert in cybercapaciteiten. Defensie zal tevens voldoende expertise moeten opbouwen om operationele cybercapaciteiten te kunnen inzetten. Dit krijgt onder meer vorm door de versterking van DefCERT en de oprichting van het Defensie Cyber Expertise Centrum. Voor een deel zal deze gespecialiseerde kennis extern moeten worden geworven. De arbeidsvoorwaarden in de publieke sector maken het echter lastig om hoogwaardige IT-specialisten en vaardige hackers aan te trekken. Daarbij lijkt de bedrijfscultuur – die slecht aansluit bij hackers – een grotere hindernis te vormen dan de financiële arbeidsvoorwaarden. Het inzetten van cybervrijwilligers en cyberreservisten, zoals sommigen landen doen, is geen panacee. Mogelijk bestaat er in Nederland onvoldoende animo om zich als gekwalificeerde vrijwilliger te melden en zijn er grenzen aan de inzet gezien de vertrouwelijkheid van informatie. Cyberreservisten zouden een rol kunnen vervullen, bijvoorbeeld bij het trainen en opleiden van defensiepersoneel. Tevens zou op beperkte schaal gebruik van reservisten kunnen worden gemaakt bij geplande operaties. In het geval van een (dreigende) aanval op Nederlandse netwerken waarbij de krijgsmacht behoefte heeft aan extra capaciteit, bestaat echter het risico dat de bedrijven waar dergelijke IT-specialisten werkzaam zijn deze capaciteit zelf hard nodig hebben.

Civiel-militaire samenwerking ten behoeve van de digitale veiligheid

Civiel-militaire samenwerking ten behoeve van de digitale veiligheid raakt aan de derde hoofdtaak van de krijgsmacht. Aangezien militaire en civiele netwerken nauw met elkaar zijn verknoopt op internet, en vanwege de taak die defensie is toebedeeld bij de assistentie van de civiele autoriteiten, ligt het voor de hand dat ook op het terrein van digitale veiligheid wordt samengewerkt. Aan het begin van dit advies werd geconstateerd dat het lastig is een strikte afbakening te hanteren voor de verschillende vormen van digitale dreiging. Het is bij een inbreuk op een systeem niet direct duidelijk welke actoren hiervoor verantwoordelijk zijn (hacktivisten, criminelen, staten) en welk oogmerk men daarbij had. De gebruikte technieken komen grotendeels overeen. Voor het adequaat reageren op deze problematiek is een geïntegreerde overheidsbenadering nodig. De recente gebeurtenissen rondom DigiNotar hebben het belang hiervan nog eens onderstreept. De regering heeft een belangrijke eerste stap gezet met het opstellen van een Nationale Cyber Security Strategie en de oprichting van het *Nationaal Cyber Security Centrum* (NCSC) in januari 2012 onder verantwoordelijkheid van de minister van Veiligheid en Justitie. Het exacte ambitieniveau van het centrum is nog niet uitgekristalliseerd. Het centrum zal volgens een groeimodel toewerken naar verbreding en verdieping van het takenpakket. Vooralsnog ziet het er naar uit dat het centrum vooral gericht zal zijn op informatie-uitwisseling en crisisbesluitvorming. GOVCERT.NL gaat op in het centrum en Defensie zal net als andere betrokken overheidsorganisaties, een liaison (waarschijnlijk van de MIVD) bij het centrum plaatsen. De AIV/CAVV bepleit – mede gezien de schaarse technische kennis en capaciteiten – een nog meer ontkokerde aanpak. Het centrum zou zich op termijn kunnen ontwikkelen tot een soort nationale CERT die de geaggregeerde monitoring van vitale netwerken voor zijn rekening neemt, meer gebruikmakend van capaciteit die nu aanwezig is bij GOVCERT.NL, MIVD, AIVD, KLPD en soms wordt aangevuld door commerciële en wetenschappelijke organisaties. Het *poolen* van dit soort kennis en vaardigheden moet niets af doen aan de formele verantwoordelijkheden van de verschillende opdrachtgevers binnen de rijksoverheid en mag de wettelijke bevoegdheden van de organisaties en hun relatie met buitenlandse partners niet in de weg staan. Zo is Defensie primair verantwoordelijk voor de bescherming van de eigen netwerken evenals de netwerken

waarmee vertrouwelijke informatie met bondgenoten en de defensie-industrie wordt uitgewisseld. Het eventueel uitvoeren van tegen staten gerichte (tegen)aanvallen in het digitale domein dient eveneens door de krijgsmacht plaats te vinden. Tot slot wordt opgemerkt dat ten aanzien van de inlichtingentaak verdergaande samenwerking tussen de AIVD en de MIVD mogelijk is. Het verdient aanbeveling om de beschikbare kapitaal- en kennisintensieve *signals intelligence* (SIGINT) en cybercapaciteiten in een gezamenlijke eenheid onder te brengen.

II Het internationaalrechtelijk kader

II.1 Digitale aanvallen en het *ius ad bellum*

Het geweldsverbod
Artikel 2 lid 4 van het Handvest van de Verenigde Naties verbiedt het gebruik of dreigen met het gebruik van geweld in internationale betrekkingen. Dit verbod wordt vaak beschouwd als een regel van dwingend internationaal recht, waarop geen uitzonderingen zijn toegestaan, behalve in de erkende uitzonderingsgevallen. De gebruikelijke uitleg van deze bepaling is dat alle vormen van gewapend geweld onder het verbod vallen, maar dat puur economische, diplomatieke en politieke druk of dwang niet vallen onder wat in artikel 2 lid 4 wordt verstaan onder geweld. Het beëindigen van de handelsrelaties of het bevriezen van tegoeden kan bijvoorbeeld zeer nadelig zijn voor de staat die het betreft, maar wordt tot nu toe niet beschouwd als vorm van geweld in de zin van het verbod uit het Handvest. Gewapend geweld met een feitelijk of mogelijk fysiek effect op de staat die het doelwit is, valt wel onder het verbod. Dit geweld is echter niet beperkt tot het kinetisch effect van conventionele wapensystemen. De scheidslijn tussen gewapend geweld en andere vormen van geweld hangt af van de vraag of het geweld heeft geleid of had kunnen leiden tot dood, letsel of schade aan goederen of infrastructuur. Dit gebruik van geweld valt onder het verbod indien dit het niveau van een geïsoleerd kleinschalig incident overschrijdt en een vergelijkbaar effect heeft als een gewapende aanval met kinetische wapens. Een en ander wordt hieronder nader uiteengezet.

Het recht op zelfverdediging
Artikel 51 van het Handvest van de Verenigde Naties bevestigt het recht op zelfverdediging tegen een gewapende aanval. Dit is een tijdelijk recht dat mag worden uitgeoefend totdat de Veiligheidsraad geëigende maatregelen heeft getroffen. In het Nicaragua-vonnis van het Internationaal Gerechtshof (hierna te noemen het IGH) werd vastgesteld dat het recht van zelfverdediging voortvloeit uit het Handvest en het gewoonterecht. Het Handvest geeft niet aan uit welke vormen van geweld een gewapende aanval kan bestaan of hoe vastgesteld kan worden wanneer een dergelijke aanval begonnen is. Daarvoor moet gekeken worden naar het gewoonterecht betreffende de uitoefening van zelfverdediging, dat aan artikel 51 ten grondslag ligt. De algemene opvatting luidt dat een gewapende aanval een aanmerkelijke inzet van gewapend geweld vergt die het niveau van een kleinschalig gewapend incident of criminele activiteit te boven gaat. Wat betreft het tijdstip van de aanvang van een gewapende aanval wordt het gewoonterecht doorgaans geacht een reactie te billijken in het geval van een onmiddellijke en onmiskenbare dreiging van een gewapende aanval (*imminent threat)*.[22] Algemeen wordt aanvaard dat een gewapende aanval rechtstreeks kan worden uitgevoerd door de strijdkrachten van een staat of indirect via gewapende groepen die opereren onder het gezag of controle van een staat. Om het laatste geval uit te leggen als gewapende aanval bepaalde het IGH in de Nicaragua-zaak dat de schaal en gevolgen van een indirecte aanval vergelijkbaar moeten zijn met die van een direct door een staat uitgevoerde conventionele gewapende aanval.

Minder overeenstemming is er over de mate van controle die een staat bij een dergelijke indirecte gewapende aanval moet uitoefenen. Het IGH hanteert ‘effectieve controle’ als norm, maar het Joegoslavië-tribunaal (hierna te noemen ICTY) kwam bij zijn vonnis inzake

22 Zie hierover AIV/CAVV-advies nummer 36, *Preëmptief Optreden*, juli 2004.

Tadic met de iets ruimere 'algehele controle'-norm, zij het in een iets andere – namelijk strafrechtelijke – context. Beide vormen van gewapende aanval hebben betrekking op aanvallen uitgevoerd door of onder de controle van een staat. Inmiddels is er sinds de aanslagen van 11 september 2001 een derde mogelijkheid die in het Nicaragua-vonnis niet aan de orde kwam, namelijk dat ook een georganiseerde gewapende groep eigener beweging, dus zonder noodzakelijke controle of aanmerkelijke betrokkenheid van een staat, een gewapende aanval uitvoert. Het IGH heeft in deze kwestie nog niet duidelijk stelling genomen. In de praktijk van staten en die van de VN-Veiligheidsraad is na de aanslagen van 11 september de mogelijkheid geopend dat ook een georganiseerde groep in principe wordt aangemerkt als het brein achter een gewapende aanval en dat zelfverdediging bijgevolg in aanmerking kan komen als reactie erop. Het lijkt redelijk te veronderstellen dat de aanval dan ook vergelijkbaar dient te zijn met een aanval die ofwel rechtstreeks door een staat dan wel door een gewapende groep onder de controle of substantiële invloed van een staat wordt gepleegd. Wordt deze derde mogelijkheid aanvaard, dan rijst de vraag tegen wie of wat de zelfverdediging gericht moet zijn en of deze kan plaatsvinden op het grondgebied van een staat die niet direct betrokken is bij de aanval. Deze vragen komen hieronder afzonderlijk aan de orde aan de hand van de criteria van noodzakelijkheid en proportionaliteit bij de uitoefening van het recht van zelfverdediging.

Digitale aanval

Kan een digitale aanval op een computer- of informatiesysteem, zonder inzet van kinetische wapens, ook een 'gewapende aanval' zijn in de zin van artikel 51 van het VN-Handvest? Niets in artikel 51 of het internationale gewoonterecht sluit specifieke soorten wapens of wapensystemen uit. Conventionele kinetische wapens vallen daar natuurlijk onder, maar ook de inzet van stralingswapens, gifgas of andere chemische wapens, bacteriologische wapens, laserwapens is denkbaar. Er is dan ook geen reden waarom een digitale aanval op een computer- of informatiesysteem niet zou kunnen gelden als een gewapende aanval, indien de gevolgen ervan vergelijkbaar zijn met die van een aanval met conventionele of onconventionele wapens. Anders gezegd: wanneer een digitale aanval leidt tot een aanmerkelijk aantal dodelijke slachtoffers of grootschalige vernietiging van of schade aan vitale infrastructuur, militaire platforms of installaties of civiele goederen, kan deze zeer wel als een 'gewapende aanval' worden gekwalificeerd in de zin van artikel 51 van het Handvest. Het feit dat een dergelijke aanval tot dusver niet heeft plaatsgevonden, sluit niet uit dat dit binnen afzienbare tijd wel het geval kan zijn. Een digitale aanval op informatiesystemen die gekoppeld zijn aan vitale infrastructuur, militaire installaties, platforms voor wapensystemen of vitale diensten, zoals de noodhulpdiensten of luchtverkeersleidingssystemen, kan de drempel voor een gewapende aanval overschrijden wanneer hij veel levens kost of tot fysieke vernietiging leidt.

De vraag of dit ook geldt wanneer er geen sprake is van (mogelijke) dodelijke slachtoffers, gewonden of fysieke schade is lastiger te beantwoorden. Het is echter denkbaar dat een serieuze georganiseerde digitale aanval op essentiële functies van de staat kan worden aangemerkt als een 'gewapende aanval' in de zin van artikel 51, indien deze mogelijk of daadwerkelijk leidt tot ernstige verstoring van het functioneren van de staat of tot ernstige en langdurige gevolgen voor de stabiliteit van de staat. Hierbij moet sprake zijn van een (aanhoudende poging tot) ontwrichting van de staat en/of de samenleving en niet slechts een belemmering of vertraging bij het normaal uitvoeren van taken. Zo zou een verstoring van bancaire transacties of het hinderen van de overheid bij het uitvoeren van haar taken, niet als een gewapend aanval worden aangemerkt. Echter een digitale aanval gericht op het gehele financiële stelsel of een aanval waardoor de overheid niet meer in staat zou zijn om essentiële taken uit te voeren – bijvoorbeeld een aanval op het gehele militaire communicatie- en commandonetwerk, waardoor men niet meer in staat zou zijn om de krijgsmacht aan te sturen – moet gelijk gesteld worden met een gewapende aanval.

Georganiseerde groepen

Net als bij conventionele aanvalsvormen kan de pleger van een dergelijke digitale aanval een staat of een georganiseerde groep onder gezag of controle van een staat zijn. Of autonome groepen eigener beweging en zonder betrokkenheid of ondersteuning van een staat een dergelijke cyberaanval kunnen lanceren is minder duidelijk. Het gewoonterecht ter zake van zelfverdediging noch artikel 51 van het Handvest sluit de mogelijkheid uit dat tot zelfverdediging wordt overgegaan in antwoord op een aanval door een georganiseerde groep die in staat is een aanval uit te voeren met gevolgen die vergelijkbaar zijn met die van een aanval die direct of indirect wordt uitgevoerd door een staat. Toepassing ervan in de context van het digitale domein brengt echter specifieke problemen met zich mee. Computernetwerken zijn namelijk over de hele wereld met elkaar verbonden, waardoor het begrip 'georganiseerde groep' in dit verband aanmerkelijk zal afwijken van hetgeen eronder verstaan wordt in het fysieke domein. Een digitale aanval op vitale infrastructuur kan bijvoorbeeld afkomstig zijn van personen in zes verschillende landen die met een bepaalde mate van coördinatie te werk gaan, maar zonder noodzakelijkerwijs te beschikken over de middelen en organisatiestructuur die normaliter geassocieerd worden met een georganiseerde gewapende groep die zich in een specifiek geografisch omschreven gebied bevindt. Een dergelijke diffuse vorm van samenwerking leent zich niet voor een militaire respons, behoudens in uitzonderlijke situaties. Het is immers onwaarschijnlijk dat alternatieven voor militair optreden in de vorm van internationale justitiële samenwerking en politioneel optreden in het kader van de rechtshandhaving niet voorhanden zouden zijn om de verantwoordelijke individuen in diverse landen aan te kunnen houden en de aanval daarmee af te weren. Verreweg de meeste voorbeelden waarbij staten zich op zelfverdediging hebben beroepen als respons op een gewapend aanval afkomstig van een niet-statelijke entiteit zonder enige noemenswaardige betrokkenheid van de staat waar de groepering zich bevindt, betreffen situaties waar een dergelijk groep zich ophoudt in een geografisch gebied waar de staat geen effectieve controle over uitoefent (bijvoorbeeld Hezbollah in Zuid-Libanon, PKK in Noord-Irak, Taliban/Al Qaida in het grensgebied Pakistan/Afghanistan).

Attributie

Geen enkele vorm van zelfverdediging mag worden uitgevoerd zonder voldoende bewijs omtrent de herkomst en bron van de aanval en zonder overtuigend bewijs dat een bepaalde staat of bepaalde staten of een georganiseerde groep verantwoordelijk is voor de uitvoering van of controle op de aanval. Het internationaal recht kent geen harde regels voor de vereiste hoeveelheid bewijs, maar de praktijk en jurisprudentie vergen toch wel dat er, voordat een actie wordt uitgevoerd, een voldoende mate van zekerheid bestaat over de herkomst van de aanval en de identiteit van de aanvallers. Dit vereiste kan dan ook een obstakel zijn voor zelfverdediging in antwoord op digitale aanvallen. Anders dan bij conventionelere vormen van oorlogvoering zal het vaak moeilijk blijken de herkomst en identiteit van de aanvallers met voldoende zekerheid vast te stellen om een militaire respons te rechtvaardigen. Dit geldt ook voor andere vormen van oorlogvoering (bijvoorbeeld guerillaoorlogen), maar in het bijzonder ten aanzien van aanvallen in het digitale domein. Betrouwbare inlichtingen zijn vereist voordat een militaire respons naar aanleiding van een digitale aanval kan plaatsvinden, vanwege de grote kans op vergissingen en de politieke, juridische en humanitaire gevolgen daarvan. Het kan, zoals in hoofdstuk I geconcludeerd, via verschillende vormen van niet-technische attributie echter mogelijk zijn om verantwoordelijkheid toe te kennen, zeker in het geval van een grootschalige digitale aanval waarvan de effecten overeenkomen met die van een conventionele gewapende aanval.

Noodzaak en proportionaliteit

Noodzaak en proportionaliteit zijn juridische begrippen die in allerlei verschillende contexten worden gehanteerd en daarbij een andere betekenis kunnen hebben. In de context van

zelfverdediging wordt met *noodzaak* gewoonlijk gerefereerd aan het bestaan van een gewapende aanval of een duidelijke en onmiskenbare dreiging van een aanval in de nabije toekomst. Ook refereert het begrip aan het ontbreken van haalbare alternatieven, waaronder rechtshandhaving in geval van georganiseerde groepen die opereren vanaf het grondgebied van een andere staat, maar zonder directe betrokkenheid van die staat. In dergelijke gevallen zou het noodzakelijkheidscriterium ertoe leiden dat het alternatief van wederzijdse bijstand bij de rechtshandhaving in de meeste gevallen beschikbaar en haalbaar is, waarmee de grond vervalt om de aanval aan te merken als een aanleiding voor zelfverdediging. Alleen in het geval van een computeraanval die vergelijkbaar is met een gewapende aanval door een groep personen die met enige mate van coördinatie opereert, en die niet kan worden aangepakt via rechtshandhaving doordat de staat waaruit de aanval afkomstig is niet bereid of in staat is de nodige handhavingsmaatregelen te treffen, wordt de optie van een militaire respons in het kader van zelfverdediging relevant. En dat dan nog alleen wanneer er geen alternatieven beschikbaar zijn, de identiteit van de aanvallers in voldoende mate kan worden vastgesteld (zie hieronder) en de zelfverdedigingsmaatregelen gericht en op proportionele wijze kunnen worden uitgevoerd.

Dit houdt uiteraard direct verband met de positie, rechten en plichten van de st(a)at(en) van waaruit de groep opereert. Het internationaal recht gaat uit van een strikt verbod op het gebruik van geweld en een plicht om de soevereiniteit en territoriale onschendbaarheid van andere staten te respecteren. Deze rechten en plichten werken echter in twee richtingen. Dit betekent dat optreden op het grondgebied van een andere staat alleen kan worden gerechtvaardigd op grond van een erkende uitzondering op het geweldsverbod. Een staat die toestaat dat georganiseerde groeperingen vanuit zijn grondgebied opereren en aanvallen op andere staten uitvoeren, schendt echter een fundamentele verplichting in het internationaal recht om zijn grondgebied niet te laten gebruiken voor het plegen van inbreuken op de rechten van andere staten, in het bijzonder inbreuken die de vorm en ernst aannemen van een gewapend aanval op een andere staat. Het kan ofwel een kwestie van onwil of van onvermogen van de 'gaststaat' zijn om een einde te maken aan dergelijke activiteiten. In beide gevallen zou de noodzaak voor zelfverdedigingsmaatregelen als antwoord op een gewapend aanval uitgevoerd door een georganiseerd groep vanuit een andere staat een rechtmatig antwoord zijn, mits de zelfverdedigingsmaatregelen gericht zijn tegen de georganiseerde groep en niet de staat waar de groep zich bevindt en verder aan de overige elementen van het noodzakelijkheids- en proportionaliteitscriteria wordt voldaan.[23] In het geval dat de staat van waaruit de groep opereert zelf niet bij machte is om adequaat op te treden tegen de georganiseerde groep op zijn grondgebied, zou die staat toestemming moeten verlenen aan de aangevallen staat om op te treden of zich in ieder geval moeten onthouden van maatregelen die gericht zijn op het verijdelen of hinderen van de rechtmatige uitoefening van zelfverdediging door de aangevallen staat.

Proportionaliteit in de context van zelfverdediging heeft zowel een kwantitatieve als een kwalitatieve dimensie. Proportionaliteit impliceert in wezen dat de handelingen gericht moeten zijn op het tegenhouden van de aanval en het voorkomen van verdere aanvallen in de nabije toekomst en bovendien dat ze in verhouding moeten staan tot de omvang van de aanval. Het veronderstelt geen specifieke respons op een aanval en vereist evenmin dat deze van dezelfde aard is als de aanval. Een digitale aanval die qua gevolgen (dodelijke slachtoffers, schade en vernietiging) vergelijkbaar is met een gewapende aanval kan een reactie met digitale middelen of met conventionele gewapende middelen rechtvaardigen, mits afslaan

23 Op de gaststaat rust immers de volkenrechtelijke zorgplicht (*due diligence*) op grond waarvan hij moet zorgdragen dat personen op zijn grondgebied geen internationale rechtsplicht schenden.

van de aanval het doel is, de maatregelen niet uitgaan boven dat doel en er geen haalbare alternatieven zijn. Het vereiste van proportionaliteit sluit maatregelen uit die het gevaar van escalatie naar een grotere intensiteit met zich meebrengen en die niet strikt noodzakelijk zijn om de aanval af te slaan en aanvallen in de nabije toekomst te voorkomen.

II.2 Digitale aanvallen en het *ius in bello*

De toepasselijkheid van het humanitair oorlogsrecht is afhankelijk van de vraag of er sprake is van een gewapend conflict in nationaal of internationaal verband. Bij afwezigheid van gewapend conflict is het humanitair oorlogsrecht niet van toepassing (behalve enkele onderdelen ervan die zowel in vredestijd als in tijd van gewapend conflict verplichtingen en of verboden opleveren, zoals bijvoorbeeld de verplichting om bepaalde soorten wapens niet te ontwikkelen). Er is sprake van een *internationaal gewapend conflict* bij een militair treffen tussen twee of meer staten of bij een totale of gedeeltelijke bezetting van het grondgebied van een staat door een andere staat, ongeacht of die bezetting tot gewelddadig verzet heeft geleid. Dit geldt voor ieder treffen waarbij geweld wordt gebruikt en dat het niveau van een kleinschalig en geïsoleerd gewapend incident – zoals kleinschalige grensschermutselingen of geïsoleerde incidenten in de lucht of op zee – overstijgt. De vijandelijkheden dienen met andere woorden een voldoende mate van intensiteit te bereiken.[24] Wordt die drempel eenmaal overschreden, dan wordt het humanitair oorlogsrecht van toepassing. Er is sprake van een *niet-internationaal gewapend conflict* bij aanhoudende vijandelijkheden, boven het niveau van louter interne onregelmatigheden of schermutselingen, tussen een overheid en een gewapende en in zekere mate georganiseerde groepering, of tussen twee of meer van dergelijke groeperingen binnen een staat.

Op internationale gewapende conflicten is het hele corpus van het humanitair oorlogsrecht van toepassing, inclusief alle verdragen die voor een of meer partijen bindend zijn, alsmede het volledige corpus van het humanitair gewoonterecht. Bij een niet-internationaal gewapend conflict is in ieder geval het gemeenschappelijke artikel 3 van de Verdragen van Genève van toepassing, naast de gewoonterechtelijke regels van het humanitair oorlogsrecht die van toepassing worden geacht op niet-internationale gewapende conflicten. In situaties die zijn te omschrijven als een volwaardige burgeroorlog is Aanvullend Protocol II bij de Verdragen van Genève van toepassing indien de desbetreffende staat partij is bij dat protocol.

Wat betreft de toepasselijkheid van het humanitair oorlogsrecht op cyberoperaties kan onderscheid worden gemaakt tussen cyberoperaties die plaatsvinden in combinatie met conventionele vormen van oorlogvoering en situaties waarin die operaties onafhankelijk en zonder gebruikmaking van andere vormen van oorlogvoering plaatsvinden. In het eerste geval is het humanitair oorlogsrecht *ipso facto* van toepassing. Als de cyberoperaties bijvoorbeeld plaatsvinden naast of voorafgaand aan kinetische operaties waarmee wordt beoogd de communicatie-, commando- en controlesystemen van de tegenstander te verstoren of om diens wapensystemen te verzwakken of uit te schakelen, zijn de desbetreffende regels van het humanitair oorlogsrecht van toepassing op zowel de cyberaspecten als op de kinetische aspecten van die operaties. In een dergelijke situatie kunnen de operaties in het digitale domein worden beschouwd als een middel en methode van oorlogvoering die onderworpen is aan alle relevante regels van het humanitair oorlogsrecht. Dergelijke operaties kunnen de tegenstander immers schade berokkenen en diens operaties verstoren. Het is een wijze van oorlogvoering die in principe niet afwijkt van andere vormen van elektronische of op informa-

24 Greenwood, Scope of Application of Humanitarian Law, in Fleck (ed), *The Handbook of International Humanitarian Law*, 2nd ed. (2008) p. 48.

tie gerichte oorlogvoering. Er kan dus geen twijfel bestaan over de toepasselijkheid van het humanitair oorlogsrecht op vijandelijkheden waarbij door de partijen bij het conflict gebruik wordt gemaakt van digitale wapens en -technieken naast kinetische middelen en methoden van oorlogvoering.

De toepasselijkheid van het humanitair oorlogsrecht op pure cyberoperaties die niet plaatsvinden in combinatie met conventionele vormen van oorlogvoering, ligt wat gecompliceerder. Zo'n digitale aanval die slechts gevolgen heeft voor civiele of militaire computersystemen en die alleen tot wijziging of vernietiging van niet-essentiële gegevens heeft geleid, heeft waarschijnlijk onvoldoende intensiteit om van een gewapend conflict te kunnen spreken. Ook al zouden er duidelijke politieke, financiële of economische gevolgen zijn – zie bijvoorbeeld de *DDoS*-aanval op Estland in 2007 –, zij zijn niet genoeg om de drempel van een gewapend conflict te overschrijden. Bij handelingen met soortgelijke gevolgen in het fysieke domein wordt het humanitair oorlogsrecht immers ook niet van toepassing geacht. Als een georganiseerde digitale aanval (of reeks aanvallen) echter zou leiden tot vernietiging van of aanmerkelijke en langdurige schade aan computersystemen voor het beheer van kritieke militaire of civiele infrastructuur, of het vermogen van de staat om essentiële overheidsfuncties te vervullen ernstig zou aantasten en daarbij ernstige en langdurige schade zou worden toegebracht aan de economische of financiële stabiliteit van de staat en zijn bevolking, is het goed denkbaar dat dit wel degelijk als gewapend conflict wordt beschouwd en daarmee het humanitair oorlogsrecht van toepassing is. Een voorbeeld hiervan is een gecoördineerde en georganiseerde aanval op het computernetwerk van het financiële systeem als geheel of op een aanzienlijk deel daarvan, die zou (kunnen) leiden tot langdurige en grootschalige ontwrichting en instabiliteit die niet eenvoudig met behulp van reguliere computerbeveiligingssystemen kan worden afgewend of beperkt.

Vijandelijkheden en voorzorgsmaatregelen in verband met cyberoperaties
Als het humanitair oorlogsrecht eenmaal van toepassing is in het kader van een internationaal of niet-internationaal gewapend conflict zijn alle vijandelijkheden daaraan onderworpen, ook als ze plaatsvinden in het digitale domein. Andere rechtsgebieden blijven weliswaar relevant, maar het humanitair oorlogsrecht wordt in dit geval het primaire juridische instrument ten aanzien van vijandelijkheden tijdens een gewapend conflict. Onder dat recht geldt dat iedere aanval[25] moet worden uitgevoerd overeenkomstig de beginselen van het humanitair oorlogsrecht, waaronder de beginselen van *onderscheid*, *proportionaliteit* en *het nemen van voorzorgsmaatregelen*. Volgens dit regelgevend kader dienen aanvallen uitsluitend te zijn gericht tegen vijandige strijdkrachten/personen die rechtstreeks deelnemen aan de vijandelijkheden of tegen militaire doelen ofwel ieder object dat als gevolg van zijn aard, gebruik, locatie of doel bijdraagt aan de militaire operaties. Aanvallen tegen burgers of burgerobjecten zijn als zodanig strikt verboden. Verder kan er weliswaar geweld – ook intensief en langdurig geweld – worden gebruikt om de tegenstander uit te schakelen, maar dient dat geweld plaats te vinden binnen het juridisch kader van het humanitair oorlogsrecht. Er moet ook voortdurend voor worden gezorgd dat individuele burgers, de burgerbevolking in het algemeen en civiele objecten zo min mogelijk schade ondervinden van de operaties die tegen legitieme militaire doelen worden ondernomen. Aanvallen op militaire doelen waarvan kan worden aangenomen dat ze, in verhouding tot het te verwachten concrete en rechtstreekse militaire voordeel, buitensporige schade zullen aanrichten in de vorm van burgerslachtoffers en schade aan civiele objecten, zijn niet toegestaan. Verboden is ook het gebruik van

25 Met 'aanval' wordt hier bedoeld een daad van geweld tegen de tegenstander in de zin van artikel 49 van Additioneel Protocol I bij de Conventies van Genève (niet te verwarren met een gewapende aanval in de zin van artikel 51 van het VN-Handvest in reactie waarop het recht van zelfverdediging mag worden uitgeoefend).

wapens of gevechtsmethoden waarmee geen onderscheid kan worden gemaakt tussen civiele objecten en militaire doelen, evenals wapens of gevechtsmethoden die, in verhouding tot het concrete militaire voordeel dat in de gegeven omstandigheden van het gebruik ervan wordt verwacht, onnodig leed of overbodig letsel aan strijdkrachten zouden toebrengen. In dit verband geldt voor bepaalde wapens een volledig verbod (bijvoorbeeld voor chemische en bacteriologische wapens), terwijl het gebruik van andere aan beperkingen gebonden is (bijvoorbeeld clustermunitie).

Het humanitair oorlogsrecht bepaalt verder dat objecten of personen met een beschermde status niet mogen worden aangevallen, behalve wanneer ze die status door directe deelname aan vijandelijkheden verloren hebben of wanneer ze voor militaire doeleinden worden ingezet (bijvoorbeeld het gebruik van een ambulance als legertruck of van een kerktoren of minaret als observatiepost), en dat aanvallen op objecten die speciale bescherming genieten (zoals culturele objecten van bijzonder belang) of waarvan kan worden aangenomen dat ze gevaarlijke krachten doen vrijkomen (bijvoorbeeld dammen, dijken en kerncentrales) alleen toegestaan zijn als die objecten rechtstreeks en significant bijdragen aan militaire operaties, en alleen in geval van dwingende militaire noodzaak. Het houdt tevens een verbod in op het gebruik van oorlogsmethoden en -middelen die tot uithongering of risico's voor het overleven van de burgerbevolking zouden leiden (bijvoorbeeld aanvallen tegen waterzuiveringsinstallaties of het elektriciteitsnet in zijn geheel) en op handelingen bedoeld om de burgerbevolking angst aan te jagen. Tot slot verbiedt het humanitair oorlogsrecht het voorwenden van een beschermde status of het gebruik van beschermende emblemen om (te proberen) een tegenstander te doden, te verwonden of gevangen te nemen, evenals misleidend gebruik van erkende symbolen (bijvoorbeeld het gebruik van de beschermende emblemen van de Verdragen van Genève, het voorwenden van verwonding of het misbruik van een erkend symbool zoals de witte vlag, waarmee een staakt-het-vuren of het voornemen tot overgave aangegeven wordt). In dit verband en conform het beginsel van onderscheid zijn strijdkrachten en andere personen die aanvallen uitvoeren verplicht zich in ieder geval tijdens het betrekken van militaire posities vóór en na een aanval en tijdens die aanval van de burgerbevolking te onderscheiden en is het hun niet toegestaan burgers en beschermde personen en objecten bij militaire operaties als schild te gebruiken.

Toepassing van dit regelgevend kader op vijandelijkheden in het digitale domein is technisch haalbaar en juridisch gezien ook een vereiste, daar het geldt voor alle vijandelijkheden, ongeacht de gebruikte wapens of strijdmethoden. Elke technische vooruitgang die in de loop der eeuwen op het gebied van oorlogvoering is gerealiseerd, is in het humanitaire oorlogsrecht geïncorporeerd en er zijn geen gronden, noch van technische noch van juridische aard, om te veronderstellen dat digitale oorlogvoering hierop een uitzondering zou vormen. Technisch gezien is het mogelijk militaire en militair relevante informatiesystemen met een redelijke mate van zekerheid te identificeren en de nodige voorzorgsmaatregelen te nemen om bijkomende effecten op civiele systemen te beperken. Zo kan een aanval op militaire communicatie-, commando- en controlesystemen via een combinatie van digitale en kinetische methoden van oorlogvoering uitgevoerd worden zonder dat dit noodzakelijkerwijs tot buitensporige schade voor civiele systemen leidt indien bij het opzetten en uitvoeren van de operatie voorzorgsmaatregelen ter voorkoming van externe effecten – zoals de verspreiding van *malware* via het internet – worden genomen. Het humanitair oorlogsrecht verbiedt om een aanval uit te voeren zonder voldoende zekerheid omtrent de te verwachten neveneffecten en dit zou in bepaalde situaties een digitale aanval onrechtmatig maken. Kritische informatiesystemen voor kwetsbare installaties, zoals kerncentrales, chemische fabrieken en systemen voor hoogwaterbescherming, moeten afdoende tegen aanvallen beschermd en beveiligd worden, behalve in de uitzonderlijke situaties waarin het humanitair oorlogsrecht een mogelijke aanval toestaat. Dit kan gebeuren door ervoor te zorgen dat ze geen doelwit

worden en de effecten van aanvallen tegen andere systemen zich niet tot deze systemen uitstrekken. Dergelijke aanvallen op legitieme doelen kunnen negatieve gevolgen voor civiele informatiesystemen hebben, maar deze hoeven niet buitensporig te zijn in verhouding tot het militaire voordeel dat van de aanval wordt verwacht; de proportionaliteit ervan zou op dezelfde wijze als bij andere vormen van oorlogvoering beoordeeld moeten worden.

Digitale oorlogvoering tegen burgersystemen of tegen systemen voor beschermde personen of objecten – zoals medische dossiers, brandalarmsystemen in musea of alarmdiensten voor ambulance of brandweer – is aan dezelfde verboden en beperkingen onderworpen als kinetische oorlogvoering. Aanvallen tegen computersystemen die bijvoorbeeld dijken, dammen en kerncentrales bewaken en/of noodzakelijk zijn voor het overleven en elementair welzijn van de burgerbevolking – zoals die van irrigatiesystemen en drinkwaterinstallaties – zijn zonder meer verboden, behalve in de beperkte uitzonderingsgevallen waarin het humanitair oorlogsrecht voorziet. Het gebruik van internet en andere digitale communicatiemiddelen om de burgerbevolking angst aan te jagen – bijvoorbeeld het verspreiden van geruchten om grootschalige paniek en massahysterie te veroorzaken – valt zeker onder het verbod op het terroriseren van de burgerbevolking. Tot slot worden ook het concept van beschermende kentekenen en het verbod op bedrog op basis van analogie toegepast op oorlogvoering in het digitale domein. IP-adressen van beschermde organisaties zoals het Rode Kruis misbruiken of een beschermde of neutrale status voorwenden om een aanval in te zetten zou in het digitale domein evenzeer verboden zijn als in de fysieke wereld.

Kortom, het bestaand juridisch kader voor vijandelijkheden onder het humanitair oorlogsrecht is in juridische zin van toepassing en technisch gezien toepasbaar op operaties in het digitale domein en op het fenomeen van cyberoorlogvoering. Sommige regels, zoals het dragen van een uniform tijdens operaties, zijn in het digitale domein wellicht niet relevant, maar veel andere – de meeste – zijn dat wel, en het argument dat dit type oorlogvoering 'anders' is en buiten het juridisch domein valt is niet overtuigend. Dat argument gaat immers voorbij aan het feit dat het humanitair oorlogsrecht van toepassing is op alle vormen van oorlogvoering en op alle soorten wapens en wapensystemen, zoals dat in de lange geschiedenis van dat recht altijd het geval is geweest.

Neutraliteit in de context van digitale oorlogvoering
Hoewel formele neutraliteitsverklaringen in het kader van gewapende conflicten vandaag de dag bijna even zeldzaam zijn als formele oorlogsverklaringen, wordt algemeen aanvaard dat het neutraliteitsrecht nog steeds van toepassing is bij gewapende conflicten tussen staten, behalve voor zover het door besluiten van de VN-Veiligheidsraad wordt beperkt. Dit betekent in essentie dat grondgebied, vaartuigen en vliegtuigen van staten die geen partij zijn bij een gewapend conflict niet aangevallen of veroverd mogen worden zolang de staat zich afzijdig houdt, en dat neutraal grondgebied door een bij het conflict betrokken partij niet geschonden mag worden zolang de neutrale staat militaire operaties van conflictpartijen vanuit of via zijn grondgebied verhindert en alles doet wat nodig is om ze te voorkomen.

In de context van het digitale domein betekent dit dat aanvallen tegen objecten of gegevenssystemen die zich op neutraal grondgebied bevinden, verboden zijn. Neutrale staten kunnen voor zover mogelijk maatregelen nemen om overdracht van gegevens van militaire aard via digitale weg op het eigen grondgebied te voorkomen, en die gegevens kunnen gescand en gewist worden met behulp van software waarmee – binnen het door de staat gecontroleerde internetdomein – bepaalde soorten gegevensbestanden met *malware* of andere cyberwapens van een van de oorlogvoerende partijen geïdentificeerd worden. Bij aanvallen via computersystemen op het eigen grondgebied van de neutrale staat kan die zijn neutraliteit beschermen door maatregelen te nemen om de herkomst van de aanval te achterhalen en

correctief op te treden voor zover dit mogelijk is zonder daarbij andere juridische verplichtingen in de sfeer van respect voor de mensenrechten in het geding te brengen. Kan de neutrale staat het verkeer van kwaadaardige gegevens via onder zijn rechtsmacht vallende internetcomponenten niet redelijkerwijze onderscheppen, dan levert dat echter geen schending of verlies van neutraliteit op. Het is in principe vergelijkbaar met een radio- of telefoonbericht dat wordt doorgegeven via een op neutraal grondgebied gelegen deel van het wereldwijde communicatienetwerk en dat noch door de oorlogvoerende partij noch door de neutrale staat als een schending van de neutraliteit beschouwd wordt.

III Internationale samenwerking

III.1 Internationale gedragsnormen

Afspraken over de inrichting van het internet
De regering heeft gevraagd in hoeverre internationale gedragsnormen een effectieve bijdrage kunnen leveren aan het vergroten van digitale veiligheid en in hoeverre lering kan worden getrokken uit bestaande gedragscodes, waaronder die met betrekking tot non-proliferatie. Er zijn verschillende manieren om via internationale afspraken gedragingen te reguleren. Dit kan door het overeenkomen van gedragscodes, die regels met een normatief karakter bevatten, of in de vorm van juridische verplichtingen die in een bindend verdrag worden vastgelegd. De AIV/CAVV is van mening dat het nuttig kan zijn om tot nadere afspraken te komen over het gebruik van het digitale domein. Op een aantal terreinen gebeurt dit al. Deze normen hoeven niet noodzakelijkerwijs in een verdrag te worden verankerd. Gedragscodes kunnen eveneens een geschikte vorm zijn om afspraken over wenselijk gedrag vast te leggen, toe te passen en te internaliseren.

De digitale veiligheid kan allereerst worden gediend door verdergaande afspraken te maken over het gebruik van het internet. De huidige situatie ten aanzien van het internet wordt soms omschreven als het 'Wilde Westen' of een 'Hobbesiaanse jungle' waar het recht van de sterkste geldt. Vaak wordt een schijntegenstelling gecreëerd door vrijheid en regulering tegenover elkaar te zetten. Juist voor een vrije samenleving is het noodzakelijk dat er onderlinge afspraken bestaan in de vorm van regels en normen. Tijdens de G8-top in Deauville van mei 2011 spraken de aanwezige landen de overtuiging uit dat op het internet 'vrijheid en veiligheid, transparantie en de eerbiediging van vertrouwelijkheid, evenals de uitoefening van individuele rechten en verantwoordelijkheden tegelijkertijd moeten worden bereikt.'[26] De grootste uitdaging hierbij is om de juiste balans te bewaren: genoeg veiligheid om onze vrijheden te kunnen uitoefenen, maar niet zoveel dat zij deze in gevaar brengt.

Gedragsnormen ten behoeve van conflictbeheersing
Aangezien in de adviesaanvraag de nadruk ligt op het buitenlands-, veiligheids- en defensiebeleid, zal hieronder uitgebreider worden ingegaan op internationale afspraken die kunnen bijdragen aan conflictbeheersing in het digitale domein. In vele verschillende fora, zoals de VN, EU, NAVO, Raad van Europa, OVSE, International Telecommunication Union (ITU) en OESO, wordt over deze problematiek gesproken. Het valt op dat waar de Nederlandse regering – met recht – erg actief is op het terrein van de vrijheid van meningsuiting op het internet, de Nederlandse betrokkenheid tot op heden minder groot is bij mondiaal overleg gericht op het formuleren van normen met als doel conflictbeheersing op digitaal gebied. Aanbevolen wordt dat Nederland zich als deelnemer aansluit bij initiatieven die het formuleren van normen op dit terrein tot doel hebben. De door de SGVN ingestelde *Group of Governmental Experts,* die vijftien landen telde, kwam vorig jaar met aanbevelingen.[27]

26 G8 Declaration, *Renewed Commitment for Freedom and Democracy,* Deauville, 26-27 mei 2011.

27 Deze groep is opgericht in 2009 op basis van resolutie 60/45 van de Algemene Vergadering. De volledige titel luidt: *Group of Governmental Experts on Development in the Field of Information and Telecommunications in the context of International Security.* Het rapport is te vinden op: <http://www.unidir.org/pdf/activites/pdf5-act483.pdf>.

In 2012 zal een nieuwe groep van experts worden ingesteld die een vervolg zal geven aan dit rapport, waarin Nederland mogelijk kan participeren. Eventueel kan deelname door Nederlandse organisaties worden overwogen aan de *Global Cybersecurity Agenda* van de ITU, een forum dat bestaat uit uiteenlopende belangengroepen. Het *Internet Governance Forum*, dat onder auspiciën van de VN wordt georganiseerd en waarin Nederland actief is, blijft uiteraard eveneens een belangrijk vehikel om met het bedrijfsleven en maatschappelijke organisaties van gedachten te wisselen.

Gedragsnormen kunnen betrekking hebben op de bescherming van netwerken, strafrechtelijke samenwerking, de toepassing van het internationaal recht en wederzijdse informatievoorziening. Waar het de *minimumkwaliteit van netwerken* betreft, heeft de Algemene Vergadering van de VN het belang onderstreept dat landen de bescherming van hun nationale systemen verhogen.[28] In de EU is er sprake van enige harmonisatie van wetgeving. Zo stelt de Richtlijn inzake een gemeenschappelijk regelgevingskader voor elektronische communicatienetwerken en -diensten (artikel 13a) dat lidstaten ervoor moeten zorgen dat communicatienetwerken beschermd zijn, voorbereid zijn op mogelijke bedreigingen en een minimumniveau van dienstverlening garanderen.[29] In algemene zin zou de private sector meer verantwoordelijkheid kunnen nemen voor de bescherming van de kritieke infrastructuur die deze sector beheert. Dit zou kunnen worden bevorderd door de (financiële) aansprakelijkheid van bedrijven op dit punt beter te regelen. Ook dient te worden gewaarborgd dat een minimum aan dienstverlening is gegarandeerd bij gedeeltelijke uitval van kritieke infrastructuur. In NAVO-verband zijn in juni 2011 met de aanname van de *Policy on Cyber Defence* afspraken gemaakt over het versterken van de veerkracht van nationale systemen. Het komt er nu op aan deze daadwerkelijk te implementeren. Het is in het belang van vergevorderde landen om de achterlopende landen te assisteren. De keten is zo sterk als de zwakste schakel: falende staten op digitaal terrein kunnen als uitvalsbasis voor digitale aanvallen worden gebruikt.

Het is van belang de bestaande afspraken die betrekking hebben op *strafrechtelijke samenwerking* binnen het kader van het Raad van Europa Verdrag inzake Cybercrime een bredere reikwijdte te geven.[30] Hoewel nu al een belangrijke normerende werking van het verdrag uitgaat die verder strekt dan de deelnemende landen, zouden meer staten dan de huidige 47 die het verdrag hebben getekend en de 32 die het hebben geratificeerd – waaronder Nederland – moeten worden bewogen zich aan te sluiten bij dit bindende internationale instrument. De conventie geeft richtlijnen voor het ontwikkelen van nationale wetgeving ten aanzien van computercriminaliteit en biedt een raamwerk voor internationale samenwerking. Belangrijk is dat de conventie stelt dat landen dienen over te gaan tot vervolging of uitlevering van groepen of individuen die zich schuldig maken aan digitale criminaliteit in derde landen vanaf het grondgebied van de staat in kwestie. Dit biedt aanknopingspunten om illegale activiteiten, zoals grootschalige zwarte handel in *malware* en identiteitsgegevens, aan te pakken. Dat samenwerking om de bron van een aanval te achterhalen nog geen vanzelfsprekendheid is laat de aanval op Estland in 2007 zien. Hoewel er sterke aanwijzingen

28 AGVN-resolutie 58/199, *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*, 23 december 2003.

29 Telecommunications Framework Directive, zie: <http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:NL:PDF>.

30 Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Trb. 2002, 18. Te vinden op: <http://conventions.coe.int/Treaty/EN/projects/FinalCybercrime.htm>.

waren dat deze afkomstig was van computers op Russisch grondgebied, weigerde dit land om mee te werken aan een onderzoek hiernaar.[31]

In het voorgaande hoofdstuk werd geconcludeerd dat het bestaande *internationaal recht* van toepassing is op het digitale domein waar het gaat om de voorwaarden van gewelds-gebruik, het oorlogsrecht en principes van soevereiniteit en neutraliteit. Het is daarom niet noodzakelijk hiervoor een speciaal 'cyberverdrag' op te stellen. Alhoewel er onder juristen internationaal sprake is van groeiende consensus over de toepasbaarheid van het bestaande juridische instrumentarium, is dit op politiek niveau nog niet het geval. Er zou een belangrijke versterkende werking van uitgaan indien staten aan deze uitgangspunten door middel van een internationale gedragscode of verklaring nadere uitwerking zouden geven.

Tot slot kunnen normerende afspraken worden gemaakt over de wijze van *informatiedeling* en *geschillenbeslechting* die de escalatie van een conflict kunnen voorkomen. Normen ten aanzien van informatievoorziening, waaronder de samenwerking tussen CERT's, zullen in praktijk moeten groeien. Het is bemoedigend dat vicepresident Biden tijdens de *London Cyberspace Conference* van begin november 2011 benadrukte dat de VS doende zijn met Rusland een overeenkomst te bereiken over directe communicatiekanalen tussen elkaars CERT's en *nuclear risk reduction centers* in het geval van een alarmerend incident.[32] Er zou zelfs kunnen worden gedacht aan een internationaal centrum dat ernstige digitale aanvallen monitort en vroegtijdig waarschuwt. Wat geschillenbeslechting betreft zou een beroep kunnen worden gedaan op instellingen als het Permanent Hof van Arbitrage of het Internationaal Gerechtshof. Daarbij zou dan bij rechters geïnvesteerd moeten worden in kennis van 'cyberrechtspraak'.

Gedragsnormen op het terrein van non-proliferatie

Om de vraag naar de bruikbaarheid van een proliferatieregime te kunnen beantwoorden, worden eerst de bestaande regimes toegelicht. Het huidige non-proliferatieregime met betrekking tot massavernietigingswapens bestaat uit een geheel van multilaterale en regionale verdragen, exportcontrole regimes, alsmede enkele gedragscodes. Belangrijke multilaterale verdragen zijn het nucleaire Non-Proliferatieverdrag (NPV) uit 1968, het Biologisch Wapen Verdrag (BWV) uit 1972, het Chemisch Wapen Verdrag (CWV) uit 1993 en het Alomvattend Kernstopverdrag uit 1996 (CTBT).[33] Een voorbeeld van een gedragscode is *The Hague Code of Conduct Against Ballistic Missile Proliferation* (HCOC), die een oproep doet tot terughoudendheid ten aanzien van de productie, het testen en de export van ballistische raketten. Het NPV maakt een onderscheid tussen de 'haves' en de 'have-nots' van kernwapens. De 'have-nots' verbinden zich geen kernwapens te ontwikkelen, waartegenover de 'haves' zich verbinden hun kernwapenarsenalen te verminderen, terwijl geen belemmeringen worden gecreëerd voor het vreedzaam gebruik van kernenergie. De naleving van deze afspraken wordt gecontroleerd door het *International Atomic Energy Agency* (IAEA). Het CTBT behelst op zijn beurt een verbod op kernexplosies. Er bestaan belangrijke verschillen tussen door bovengenoemde verdragen gereguleerde wapensystemen en digitale wapens die een eventueel digitaal non-proliferatieregime moeilijk realiseerbaar zullen maken. Zo valt bijvoorbeeld een

31 Overigens kan een dergelijke opstelling als aanwijzing dienen voor het beantwoorden van de attributievraag. E. Tikk (2011), 'Ten Rules for Cyber Security', *Survival*, vol. 53 (3), pp. 119-132.

32 Zie: <http://www.whitehouse.gov/photos-and-video/video/2011/11/01/vice-president-biden-delivers-remarks-london-conference-cyberspace#transcript>.

33 Het *Comprehensive Nuclear Test Ban Treaty* (CTBT), dat nog niet in werking is getreden.

onderscheid tussen digitale 'haves' en 'have-nots' in de praktijk niet te maken. Ook lijkt een non-proliferatie regime met betrekking tot digitale 'wapens' lastig te controleren aangezien het bezit hiervan moeilijk valt vast te stellen – het betreft immers feitelijk programmeertaal – en ze tevens heimelijk en niet explosief kunnen worden getest. Daarom kunnen landen er onvoldoende op vertrouwen dat andere landen zich aan de afspraken zullen houden.

Naast bovengenoemde kanttekeningen bij de *haalbaarheid* van een non-proliferatieregime, zijn er ook vraagtekens te plaatsen bij de *noodzaak* hiertoe. In bepaalde literatuur worden beelden opgeroepen van een 'Cyber Armageddon' of een 'Cyber Pearl Harbor' met apocalyptische effecten. In het eerste deel van dit advies is geconstateerd dat een echte 'cyberoorlog' – die uitsluitend en alleen in het digitale domein wordt uitgevochten, met verwoestende gevolgen – niet aannemelijk is.

Om al deze redenen is de AIV/CAVV van mening dat er noch de mogelijkheid noch de noodzaak is tot het overeenkomen van een wereldwijd non-proliferatieregime zoals dat bestaat voor nucleaire, chemische en biologische wapens. Er zijn evenmin voldoende aanknopingspunten voor het instellen en afdwingen van beperkingen aan de uitvoer van bepaalde digitale technologie en software ter bescherming van de eigen militaire en civiele digitale infrastructuur. In de praktijk kleven ook hieraan praktische bezwaren aangezien het om technologie voor duaal gebruik gaat die in velerlei toepassingen is terug te vinden. Soms kunnen dergelijke exportcontrole regimes zelfs contraproductief zijn omdat daarmee burgers in bepaalde landen in hun toegang tot het internet worden beperkt.[34]

III.2 Internationale samenwerking in het kader van de NAVO en EU

Gemeenschappelijke defensie

De regering heeft gevraagd de rol van de NAVO en de EU ten aanzien van cyberdreigingen vanuit het oogpunt van het buitenlands-, veiligheids- en defensiebeleid te bezien. In juni 2011 heeft de Noord-Atlantische Raad (NAR) de *NATO Policy on Cyber Defence* met bijbehorende actiepunten aangenomen.[35] Dit beleidsplan is een uitwerking van de in het Strategisch Concept van de NAVO aangekondigde voornemens op het terrein van digitale veiligheid.[36] Het ambitieniveau van dit beleidsplan is beperkt. De afspraken hebben vooral betrekking op de bescherming van de eigen NAVO-systemen en minimumvereisten voor de bescherming van nationale netwerken voor zover die verbonden zijn met deze systemen of NAVO-informatie verwerken. Voor de beveiliging van alle andere nationale systemen, inclusief de netwerken die betrekking hebben op de kritieke infrastructuur, blijven de lidstaten verantwoordelijk. Ondanks het feit dat sommigen wellicht teleurgesteld zijn over het ontbreken van een *grand design* waar het gaat om een echte gemeenschappelijke digitale defensie, getuigt de huidige opzet van realiteitszin en het beleggen van verantwoordelijkheden op het juiste

34 Zie Jullian C. York, *Syrian Surveillance Project Raises Concerns About Effectiveness of Export Controls,* November 2011 op: <https://www.eff.org/deeplinks/2011/11/sanctions-fail-stop-syrian-regime-still-harm-citizens>.

35 NATO Policy on Cyber Defence and Cyber Defence Action Plan, 7 juni 2011 (geclassificeerd). Publieke versie op: <http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf>.

36 Het Strategisch Concept van de NAVO stelt (punt 19) dat de Alliantie: *'[will] develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations*'.

niveau (subsidiariteitsprincipe). Dit sluit tevens aan bij de Nederlandse praktijk, waarbij de netwerken – net als elders in Europa en Noord-Amerika – grotendeels in private handen zijn. Binnen de NAVO wordt wel gediscussieerd over de vraag in hoeverre beveiligingseisen moeten worden gesteld aan de voor het bondgenootschap kritieke nationale infrastructuur, die verder reikt dan alleen de met de NAVO verbonden systemen. Hierbij kan worden gedacht aan private glasvezelverbindingen waarvan de NAVO afhankelijk is voor haar dataverkeer of nationale infrastructuur die essentieel is voor de inzet van troepen. Zelfs indien hierover overeenstemming zou worden bereikt, is het nadrukkelijk niet de bedoeling de NAVO direct verantwoordelijk te maken voor de bescherming hiervan.

De NAVO zal zich de komende jaren dus vooral richten op een betere bescherming van de eigen systemen. Daarnaast zal de NAVO de leden desgevraagd bijstaan bij de ontwikkeling van een adequate beveiliging van de nationale systemen die met het NAVO-netwerk verbonden zijn. Hiertoe kan expertise beschikbaar worden gesteld, waarbij duidelijk is dat sommige landen ver vooruitlopen op andere. Het is van belang dat de achterblijvers op het noodzakelijke beschermingsniveau komen en zo de Alliantie in haar geheel minder gevoelig maken voor digitale aanvallen. Hiertoe kan de NAVO de bondgenoten assisteren bij de invulling van een nationale strategie voor digitale verdediging door middel van het uitwisselen van *best practices* en het uitvoeren van gezamenlijke trainingsprogramma's en oefeningen. Assistentie hierbij kan onder meer worden verleend door het *Cooperative Cyber Defence Centre of Excellence* (CCDCoE), het *NATO Consultation, Command and Control Agency* (NC3A) en de *NATO CIS School*. Daarnaast is het essentieel om de uitwisseling van inlichtingen op het terrein van digitale dreigingen te verbeteren. Aangezien de Alliantie niet over een eigen inlichtingendienst beschikt, is het voor het verkrijgen van een accuraat dreigingsbeeld noodzakelijk dat afzonderlijke landen deze informatie ter beschikking stellen. In de praktijk blijkt dit problematisch, aangezien landen terughoudend zijn in het NAVO-breed beschikbaar stellen van inlichtingen en deze slechts in kleine kring delen. Zolang hiervan sprake is, zal het lastig zijn een actieve defensie te realiseren die meer behelst dan een passieve verdediging tegen digitale aanvallen. Dat de capaciteiten van de NAVO op dit gebied nog vrij beperkt zijn, kan worden geïllustreerd aan de hand van de *Cyber Threat Assessment Cell* (CTAC), die slechts een paar personen zal omvatten, in tegenstelling tot de rond de vijftig personen groeiende *NATO Computer Incident Response Capability* (NCIRC), die verantwoordelijk is voor de technische beveiliging van de NAVO-systemen, en de eventuele ondersteuning na de aanvraag van bond-genoten.

De gemeenschappelijke verdediging tegen digitale dreigingen moet anders worden georganiseerd dan conventionele verdediging. De bescherming van vitale infrastructuur, voor zover het geen overheidssystemen betreft, blijft zoveel mogelijk in handen van private partijen. Deze private beheerders zijn in eerste instantie verantwoordelijk voor de beveiliging van deze systemen. De bescherming van dit soort infrastructuur vergt – meer dan conventionele verdediging – een inspanning van uiteenlopende overheidsdiensten en private partijen. Naast de nationale actoren, is hiervoor op Europees niveau een belangrijke rol weggelegd voor *European Network and Information Security Agency* (ENISA). Zo is de eerste gezamenlijke *cyber security* oefening tussen de EU en de VS met steun van ENISA en het Amerikaans Department of Homeland Security gehouden in Brussel op 3 november 2011. Het is daarnaast van groot belang dat de EU-instellingen de bescherming van hun eigen systemen verbeteren. Zo blijkt met name het Raadssecretariaat een belangrijk doelwit van digitale spionage.[37] Met de oprichting van de Europese Dienst voor Extern Optreden (EDEO) en de

37 BBC News, *'Serious' cyber attack on EU bodies before summit', 23 March 2011.* Zie: <http://www.bbc.co.uk/news/world-europe-12840941>.

hieronder ressorterende EU-delegaties in het buitenland, is een adequate beveiliging van de verbindingen van nog groter belang geworden.

De EU ontbeert op dit moment een *cyber security* strategie in het kader van het Gemeenschappelijk Buitenlands- en Veiligheidsbeleid (GBVB). Binnen de VN en andere internationale gremia zou de Unie een gecoördineerde inzet op dit terrein, bijvoorbeeld ten aanzien van wenselijke gedragsnormen, moeten presenteren. Ook is er thans onduidelijkheid over de rol van het PSC (Political and Security Committee), COSI (Committee on Operational Cooperation on Internal Security) en het CSC (Council Security Committee) bij een serieuze digitale aanval. Vooral de wijze waarop het COREPER (Comité van Permanente Vertegenwoordigers) wordt geïnformeerd behoeft dringend invulling.[38] Zoals eerder in dit advies geconstateerd, is de EU wel actief betrokken bij andere terreinen, zoals het strafrecht, het stellen van kwaliteitsnormen voor netwerken en privacywetgeving. Ook hier is het echter noodzakelijk dat er meer samenhang komt in de activiteiten van de verschillende directoraten-generaal van de Europese Commissie – waaronder Binnenlandse Zaken (HOME), Informatiemaatschappij en media (INFSO), Justitie (JUST) en Interne Markt en Diensten (MARKT) – evenals de EDEO, door uitvoering te geven aan een gezamenlijke strategie.

Afschrikking

Het principe van *afschrikking* tegen digitale aanvallen is er, net als bij kinetisch aanvallen, op gebaseerd om enerzijds de succeskans van een aanval te minimaliseren en anderzijds over de capaciteit en bereidheid te beschikken om een aanval te vergelden (zie hoofdstuk I.2). Het eerste vergt vooral investeringen in een gemeenschappelijke beveiliging zoals hierboven vermeld, waarbij naast de NAVO nadrukkelijk ook een rol voor de EU is weggelegd. Het tweede vergt een investering in offensieve capaciteiten en afspraken over de inzet hiervan. Een complicerende factor bij digitale wapens is de zogeheten attributieproblematiek. Deze attributieproblematiek wordt in het nieuwe beleidsplan van de NAVO niet geadresseerd. Zoals in hoofdstuk I.2 is aangegeven, is (niet-technische) attributie bij aanvallen van een hoog geweldsniveau zeker niet onmogelijk. Een goede inlichtingencapaciteit is hiervoor wel noodzakelijk en op dit terrein blijft de NAVO nu juist afhankelijk van de afzonderlijke leden. De NAVO beschikt zelf evenmin over echte offensieve digitale capaciteiten en in de *Policy on Cyber Defence* zijn ook geen afspraken gemaakt over de ontwikkeling hiervan. De samenwerking op dit terrein wordt deels bemoeilijkt doordat landen niet bereid zijn andere NAVO-leden inzicht te geven in hun capaciteiten. Zoals geconstateerd in hoofdstuk I.2, verliest een digitaal wapen, anders dan een geweer of een pantserwagen, zijn effectiviteit wanneer anderen kennis hebben van het functioneren hiervan.

De AIV/CAVV is van mening dat de NAVO bescheiden offensieve digitale capaciteiten zou kunnen ontwikkelen ter bescherming van de eigen systemen en netwerken, dus in het kader van de actieve verdediging. Een investering in grootschalige offensieve digitale NAVO-capaciteiten die kunnen worden ingezet bij een (digitaal) conflict zou vergaande consequenties hebben. Daarvoor zou de oprichting van een eigen NAVO-inlichtingenorganisatie noodzakelijk zijn. Los van de vraag of die eigen NAVO-capaciteit een belangrijke bijdrage kan leveren aan de verdediging van het NAVO-grondgebied of operaties in derde landen, gaat van de conventionele en nucleaire middelen waarover afzonderlijke NAVO-landen beschikken al een afschrikwekkende werking uit. Afschrikking van digitale aanvallen dient niet alleen vorm te krijgen binnen het digitale domein. Zoals werd geconstateerd in hoofdstuk II kan de NAVO immers ter afschrikking of vergelding van digitale aanvallen ook besluiten tot de proportionele

38 European Parliament, Directorate-General for external policies*, Cybersecurity and cyberpower: concepts, conditions and capabilities for cooperation for action within the EU*, 2011.

inzet van kinetische wapens. Ook dragen offensieve digitale capaciteiten van de afzonderlijke lidstaten bij aan afschrikking. Bij toekomstige NAVO-operaties kan de inzet van die capaciteiten plaatsvinden, bijvoorbeeld als *enabler* ter ondersteuning van de inzet van kinetische wapens.

Solidariteitsclausule
De opgerichte *Cyber Defence Management Board* (CDMB), die geheel bestaat uit NAVO-personeel en niet uit nationale vertegenwoordigers, kan in geval van nood zelfstandig reageren op aanvallen die gericht zijn tegen de eigen NAVO-netwerken en zal de NAR hier zo snel mogelijk van op de hoogte brengen en om politieke richting vragen. Indien er sprake is van een (dreigende) aanval op een van de leden, dan kan het desbetreffende lid bij een serieuze dreiging een beroep doen op artikel 4 of 5 van het NAVO-verdrag. Beide artikelen kunnen volgens de AIV/CAVV ook betrekking hebben op aanvallen in het digitale domein. Dit sluit aan bij de denkrichting in het NAVO Strategisch Concept waarin wordt gesteld dat de NAVO zich zal verdedigen tegen *'any threat of aggression, and against emerging security challenges'*.[39] Artikel 5 is dermate algemeen geformuleerd dat hier alle vormen van gewapend geweld onder kunnen worden geschaard. Artikel 5 kent met opzet een grote mate van flexibiliteit, ook waar het de vereiste reactie van bond-genoten betreft. Het artikel schrijft niet voor op welke manier zij individueel of collectief bijstand zullen verlenen met een beroep op artikel 51 van het VN-Handvest. Het minder verstrekkende artikel 4, dat het mogelijk maakt '*any security threat*' binnen de NAVO te agenderen, kan worden gereserveerd voor digitale aanvallen die raken aan de nationale veiligheid maar nog niet de drempel van een gewapende aanval overschrijden. Naar verwachting zal er in praktijk bij enkel digitale aanvallen, aangezien het zoals eerder vastgesteld lastig is hiervoor de drempel van een 'gewapende aanval' te halen, eerder een beroep op dit artikel worden gedaan dan op artikel 5. Terwijl de AIV/CAVV tot de conclusie komt dat de formulering van beide artikelen geen aanpassing behoeft, kunnen er wel nadere afspraken worden gemaakt over de rol van de verschillende NAVO-organisaties en NAVO-lidstaten in het geval van een gewapende aanval met digitale middelen. Hier zal met name de CDMB een initiërende rol moeten spelen. Daarnaast is het vooral van belang trainingen te organiseren die een dergelijke aanval simuleren.

De EU kent ook een bijstandsclausule (artikel 42.7 van het EU-Verdrag), die bepaalt dat indien een lidstaat wordt aangevallen, andere lidstaten assistentie zullen aanbieden in overeenstemming met artikel 51 van het VN Handvest. Daarnaast kent de EU een solidariteitsclausule (artikel 222 EU Werkingsverdrag), die kan worden ingeroepen indien er sprake is van een terroristische aanval, een natuurramp of een door de mens veroorzaakte ramp. De verwachting is dat voor de nabije toekomst de NAVO het belangrijkste instrument ten behoeve van de collectieve verdediging blijft. Het is dan ook realistisch te veronderstellen dat de EU zich vooral zal beperken tot politieke steunbetuigingen. De EU kan wel een leidende rol vervullen bij het bevorderen van digitale veiligheid in de private sector van de lidstaten.

Informatie-uitwisseling ten behoeve van dreigingsanalyses tussen EU en NAVO
De samenwerking tussen de EU en de NAVO op het terrein van dreigingsanalyses kan worden verbeterd. Hiervoor bestaan echter geen eenvoudige oplossingen. Informatie-uitwisseling tussen de EU en de NAVO op het terrein van digitale veiligheid loopt tegen dezelfde welbekende institutionele belemmeringen (het vraagstuk Turkije-Cyprus) aan als de samenwerking tussen beide partijen op andere terreinen. Het ziet er niet naar uit dat dit vraagstuk in de nabije toekomst zal zijn opgelost. Hoe gevoelig formele informatie-uitwisseling ligt, wordt geïllustreerd door het gegeven dat de *NATO Policy on Cyber Defence* formeel nimmer

39 NAVO Strategisch Concept, punt 4a.

aan de EU is aangeboden. Toch lijken er voorzichtige eerste stappen te worden gezet omtrent het uitwisselen van informatie over strategievorming en beleids-implementatie ten aanzien van digitale veiligheid. Probleem daarbij is wel dat de informatievoorziening de eerstkomende periode vooral eenrichtingsverkeer zal blijken, aangezien zowel de beleidsvorming als de capaciteiten van de EU op het terrein van het GBVB en *cyber* beperkt zijn. De informatie waarover ENISA beschikt zou wel systematischer kunnen worden gebruikt.

Het uitwisselen van inlichtingeninformatie die kan bijdragen aan een juist dreigingsbeeld ligt nog gevoeliger. De meeste NAVO- en EU-leden zijn bijzonder terughoudend in het ter beschikking stellen van de door hun inlichtingendiensten verkregen informatie aan beide organisaties. Veel landen geven er de voorkeur aan in kleiner verband samen te werken met 'gelijkgezinde' landen waartussen een groot vertrouwen bestaat. De inlichtingeninformatie waar beide organisaties over beschikken is om die reden beperkt en ook hier loopt de formele uitwisseling van gegevens tegen de eerdergenoemde institutionele belemmering aan. Op het moment dat de door de eigen staf opgebouwde informatiepositie wordt vergroot, bijvoorbeeld binnen de EDEO of de analyses die de CTAC maakt van de aanvallen op het dataverkeer van de NAVO, zullen als wederdienst nationale inlichtingenorganisaties wellicht bereid zijn meer te delen.

Wanneer het formeel-institutioneel niet mogelijk is om inlichtingen tussen NAVO en EU uit te wisselen, lijkt er slechts ruimte te zijn voor informele contacten tussen de staven van beide organisaties. De vraag is evenwel of dit zogeheten *organisatie-tot-organisatiemodel* ook op het gebied van dreigingsanalyses voldoende basis biedt voor vruchtbare samenwerking. Los van het feit dat thans niet de indruk bestaat dat dit in praktijk al op grote schaal gebeurt, bestaat zonder formele afspraken en waarborgen het risico dat er onvoldoende zicht is op eventuele schending van de privacyregels (verschillen tussen bijvoorbeeld EU- en VS-regelgeving) die hiermee gepaard kan gaan. De AIV/CAVV is evenwel van mening dat in het belang van de lidstaten en met voldoende aandacht voor de privacyregels, vooralsnog het informele traject zoveel als mogelijk moet worden benut.

IV Conclusies en aanbevelingen

De definitiekwestie

1. De bedreiging van de digitale veiligheid kan voortkomen uit digitale oorlogvoering, digitale spionage, digitaal terrorisme, digitaal activisme en digitale criminaliteit. Definiëring van deze verschijningsvormen is nodig om te voorkomen dat ze conceptueel met elkaar worden vermengd. Dit betekent niet dat deze dreigingsvormen geen samenhang kunnen vertonen. Vaak komen de gebruikte technieken overeen en verschilt alleen het beoogde doel. Het onderscheiden van de doelstelling is echter van belang voor het bepalen van de juiste nationale respons op specifieke dreigingen, bijvoorbeeld om het risico van een overreactie te beperken.

2. De AIV/CAVV beveelt daarom aan dat de overheid gebruik maakt van duidelijke en uniforme begripsomschrijvingen. Op internationaal niveau is het eveneens noodzakelijk dat overheden en organisaties tot eensluidende interpretaties komen, wil men in staat zijn om internationale afspraken te maken over de aanpak van digitale dreigingen.

De digitale dreiging

3. De regering constateert dat de afhankelijkheid van het functioneren van digitale netwerken nieuwe veiligheidsrisico's met zich meebrengt. Naast digitale criminaliteit, dat grotendeels buiten het bestek van dit advies valt, lijkt er sprake van een toename van digitale spionageactiviteiten. Er is echter meer systematisch en kwantitatief onderzoek nodig naar de omvang van de verschillende digitale dreigingsvormen. Aangezien het bij uitstek grensoverschrijdende problematiek betreft en omdat de aanwezige capaciteiten zo het best gebundeld kunnen worden, beveelt de AIV/CAVV aan een dergelijk onafhankelijk onderzoek in EU- en NAVO-verband te initiëren.

Het digitale domein wordt naast land, lucht, zee en ruimte beschouwd als de 'vijfde dimensie' waarin sprake kan zijn van militair optreden. Op grond van welke politieke en militaire doelstellingen moeten operationele cybercapaciteiten worden ontwikkeld en kunnen worden ingezet? Wat is de aard en rol van operationele cybercapaciteiten bij militaire operaties?

4. Het digitale domein zal naar verwachting in elk toekomstig conflict een belangrijke rol spelen. Een 'cyberoorlog', die uitsluitend in het digitale domein wordt uitgevochten, en met verwoestende gevolgen, is echter niet aannemelijk. Daarom wordt in dit advies de meer afgebakende term 'digitale oorlogvoering' gebruikt, te beschouwen als onderdeel van een militaire operatie die ook andere (niet digitale) dimensies kan omvatten.

5. Operationele cybercapaciteiten – deel uitmakend van militair vermogen – kunnen een bijdrage leveren aan het bereiken van een politiek doel. Voor de inzet van deze capaciteiten is een helder politiek kader essentieel. De bestaande nationale veiligheidsstrategie is nationaal gericht. De AIV/CAVV beveelt aan dat operationele cybercapaciteiten en ontwikkelingen op dit gebied een plaats krijgen in een geïntegreerde strategie voor het binnenlands en buitenlands veiligheidsbeleid.

6. Naast de ontwikkeling van operationele cybercapaciteiten is het tevens van belang te investeren in een samenhangende 'cyberdiplomatie', waarbij als reactie op concrete dreigingen met kennis van zaken een breed palet aan maatregelen wordt overwogen, variërend van politieke druk, de inzet van economische sancties, het aandringen op strafrechtelijke maatregelen tot – in laatste instantie – het gebruik van gesanctioneerd geweld.

7. De inzet van cybercapaciteiten dient ten dienste te staan van de hoofdtaken van de krijgsmacht. Deze inzet kan betrekking hebben op de beveiliging van de eigen defensiesystemen, het vergaren van inlichtingen en digitale aanvallen gericht op het verstoren, beschadigen of vernietigen van computers en netwerken van de tegenstander.

8. Digitale wapens worden weliswaar gekenmerkt door geringe materiële instapkosten, maar de ontwikkeling van een technisch complexe aanval vereist gespecialiseerde kennis. Digitale wapens kennen een beperkte houdbaarheidsduur, de inzet ervan brengt veelal indirecte effecten met zich mee en de aanvaller is moeilijk herleidbaar. Het kan echter zeker mogelijk zijn om mede door het gebruik van niet-technische attributie de identiteit van de aanvaller vast te stellen.

9. De AIV/CAVV beveelt aan dat – gezien de technologische ontwikkelingen – wordt bezien of het huidige onderscheid in de Wet- op de Inlichtingen en Veiligheidsdiensten (WIV) tussen kabelgebonden en niet-kabelgebonden data gehandhaafd moet blijven.

10. Het is om goede redenen op basis van de WIV niet toegestaan dat een inlichtingendienst een geplaatste exploit gebruikt voor een netwerkaanval met een militair oogmerk, die het wijzigen of beschadigen van een systeem tot doel heeft. Een dergelijke aanval dient onder verantwoordelijkheid van de Commandant der Strijdkrachten (CDS) plaats te vinden, na verkregen politieke toestemming. Het is noodzakelijk binnen de krijgsmacht ook op digitaal terrein duidelijke procedurele afspraken te maken, die volgen uit deze functiescheiding.

11. Bij het uitvoeren van militaire operaties kan er voor worden gekozen ook gebruik te maken van digitale aanvallen. In essentie gaat het om de inzet van een middel – digitale capaciteit – uit de *toolbox* van militaire middelen die een bijdrage kunnen leveren aan het bereiken van een politiek doel. De operationele inzet van cybercapaciteiten, die overeenkomstig de juridische kaders dient plaats te vinden, wordt begrensd door de technische kenmerken van digitale wapens en de beschikbare kennis binnen de krijgsmacht. De AIV/CAVV beveelt daarom aan om vooralsnog de schaarse defensiemiddelen slechts op beperkte schaal in te zetten voor het ontwikkelen van offensieve capaciteiten en de nadruk te leggen op het verbeteren van de verdediging van de eigen netwerken en het opbouwen van een adequate inlichtingencapaciteit op digitaal gebied.

12. Mede gezien de schaarse technische kennis en capaciteiten wordt een nog meer ontkokerde aanpak binnen het per januari 2012 operationele Nationaal Cyber Security Centrum bepleit. Het centrum zou zich op termijn kunnen ontwikkelen tot een soort nationale CERT die de geaggregeerde monitoring van vitale netwerken voor zijn rekening neemt, meer gebruikmakend van capaciteit die nu aanwezig is bij GOVCERT.NL, MIVD, AIVD, KLPD en soms wordt aangevuld door commerciële en wetenschappelijke organisaties. Verder is ten aanzien van de inlichtingentaak verdergaande samenwerking tussen de AIVD en de MIVD mogelijk. De AIV/CAVV beveelt aan om de beschikbare kapitaal- en kennisintensieve *signals intelligence* (SIGINT) en cybercapaciteiten in een gezamenlijke eenheid onder te brengen.

Onder welke omstandigheden kan een cyberdreiging worden beschouwd als het gebruik van geweld of een dreiging hiermee, in de zin van artikel 2 lid 4 van het VN-Handvest? Onder welke omstandigheden kan een cyberaanval worden beschouwd als een gewapende aanval waartegen geweld mag worden gebruikt ter zelfverdediging op basis van artikel 51 van het VN-Handvest?

13. Artikel 2 lid 4 van het Handvest van de Verenigde Naties verbiedt het gebruik of dreigen met het gebruik van geweld in internationale betrekkingen. Onder het verbod valt gewapend geweld met een feitelijk of mogelijk fysiek effect op de staat die het doelwit is. Het verbod heeft echter ook betrekking op andere vormen van geweld die hebben geleid of hadden kunnen leiden tot dood, letsel of schade aan goederen of infrastructuur.

14. Het gebruik van geweld in het kader van zelfverdediging op basis van artikel 51 van het VN Handvest is volgens het internationaal recht een uitzonderlijke maatregel, die bij gewapende digitale aanvallen slechts gerechtvaardigd wordt in situaties die uitstijgen boven de drempel van digitale criminaliteit of spionage. Voordat een digitale aanval het recht tot zelfverdediging rechtvaardigt, moet deze gevolgen hebben die vergelijkbaar zijn met die van een conventionele gewapende aanval. Wanneer een digitale aanval leidt tot een aanmerkelijk aantal dodelijke slachtoffers of grootschalige vernietiging van of schade aan vitale infrastructuur, militaire platforms of installaties of civiele goederen, moet deze gelijk gesteld worden met een ‘gewapende aanval’.

15. Een georganiseerde digitale aanval op essentiële functies van de staat moet, ook wanneer deze geen fysieke schade of letsel tot gevolg heeft, maar mogelijk of daadwerkelijk leidt tot ernstige verstoring van het functioneren van de staat of ernstige en langdurige gevolgen voor de stabiliteit van de staat, worden aangemerkt als een ‘gewapende aanval’ in de zin van artikel 51 van het VN-Handvest. Hierbij moet dan sprake zijn van een (aanhoudende poging tot) ontwrichting van de staat en/of de samenleving en niet slechts een belemmering of vertraging bij het normaal uitvoeren van taken.

16. Het gebruik van geweld naar aanleiding van een digitale aanval moet voldoen aan de vereisten van noodzakelijkheid en proportionaliteit ten aanzien van de uitoefening van het recht tot zelfverdediging. De maatregelen moeten gericht zijn op het beëindigen van de aanval en het voorkomen van herhaling ervan in de nabije toekomst en er moeten geen bruikbare alternatieven zijn.

17. Het principe van proportionaliteit vereist niet dat een respons op een aanval van dezelfde aard is als de aanval zelf. Een digitale aanval die voldoet aan de voorwaarden van een gewapende aanval kan een respons met conventionele gewapende middelen rechtvaardigen.

18. Het treffen van maatregelen tegen digitale agressie is voorts uitsluitend rechtmatig indien er een voldoende mate van zekerheid bestaat omtrent de herkomst en bron van de aanval.

Wanneer is er sprake van toepasselijkheid van het humanitair oorlogsrecht op gedragingen in het digitale domein? Moeten deze samenhangen met kinetisch geweldsgebruik? Hoe zou bij een dergelijke toepassing gestalte moeten worden gegeven aan de oorlogsrechtelijke principes van onderscheid en proportionaliteit, en aan de verplichting tot het nemen van voorzorgsmaatregelen?

19. Het humanitair oorlogsrecht is alleen van toepassing in de context van een gewapend conflict, in internationaal of niet-internationaal verband. Cyberoperaties waarbij de drempel van een gewapend conflict niet wordt overschreden, vallen derhalve buiten het toepassingsveld van het humanitair oorlogsrecht.

20. Digitale aanvallen die meer zijn dan sporadische, geïsoleerde gewapende incidenten en die resulteren in verlies van mensenlevens, letsel, vernietiging of langdurige schade aan fysieke objecten tot gevolg (kunnen) hebben, kunnen worden gekwalificeerd als gewapend conflict in de zin van het humanitair oorlogsrecht. Dit is in de eerste plaats het geval bij digitale aanvallen die in combinatie met een kinetische aanval worden uitgevoerd. Dit geldt echter ook voor een digitale aanval die – zonder de inzet van kinetische middelen van oorlogvoering – leidt tot vernietiging of langdurige en ernstige schade aan computersystemen voor het beheer van kritieke militaire of civiele infrastructuur, of die het vermogen van de staat om essentiële overheidsfuncties te vervullen ernstig aantast en daarbij ernstige en langdurige schade toebrengt aan de economische of financiële stabiliteit van de staat en zijn bevolking.

21. In ieder gewapend conflict, zowel in internationaal als niet-internationaal verband, zijn de regels inzake het voeren van vijandelijkheden van toepassing op het gebruik van alle soorten, middelen en methoden van oorlogvoering, inclusief middelen en methoden van digitale aard. Deze regels betreffen onder meer de beginselen van onderscheid, proportionaliteit en het nemen van voorzorgsmaatregelen. Verder geldt er een verbod op het voorwenden van een beschermde of neutrale status met het oogmerk aanvallen uit te voeren en het misbruiken van een dergelijke status, waaronder de IP-identiteit, als schild tegen een aanval.

Hoe zou in het cyberdomein gestalte moeten worden gegeven aan de volkenrechtelijke begrippen soevereiniteit, neutraliteit?

22. Het neutraliteitsrecht is van toepassing bij de inzet van digitale wapens en methoden van oorlogvoering. Het belet in principe het gebruik door belligrente partijen van computers of computersystemen die zich op neutraal grondgebied bevinden, voor zover dit mogelijk is, evenals aanvallen op computernetwerken of informatiesystemen op neutraal terrein. Het staat een neutrale staat toe een oorlogvoerende partij te verhinderen gebruik te maken van computers en informatiesystemen die zich op zijn grondgebied bevinden of onder zijn rechtsmacht vallen. De enkele doorgifte van gegevens via een op neutraal grondgebied gelegen deel van internet levert echter geen schending of verlies van de neutraliteit op.

In hoeverre kunnen internationale gedragsnormen over het gebruik van het digitale domein een effectieve bijdrage leveren aan het vergroten van cyber security? Kunnen we lering trekken uit ervaringen met bestaande gedragscodes, bijvoorbeeld op het gebied van non-proliferatie?

23. Gedragsnormen kunnen betrekking hebben op de bescherming van netwerken, strafrechtelijke samenwerking, de toepassing van het internationaal recht en wederzijdse informatievoorziening. Het is van belang de bestaande afspraken binnen het kader van de Raad van Europa Conventie inzake Cybercrime een bredere reikwijdte te geven. Belangrijk is dat de conventie stelt dat landen dienen over te gaan tot vervolging of uitlevering van groepen of individuen die zich schuldig maken aan digitale criminaliteit in derde landen vanaf het grondgebied van de staat in kwestie. Dit biedt aanknopingspunten om illegale activiteiten, zoals grootschalige zwarte handel in *malware* en identiteits-

gegevens, aan te pakken. Hierboven is geconcludeerd dat het bestaande internationaal recht van toepassing is op het digitale domein waar het gaat om de voorwaarden van geweldsgebruik, het oorlogsrecht en principes van soevereiniteit en neutraliteit. Het is daarom niet noodzakelijk hiervoor een speciaal 'cyberverdrag' op te stellen. Wel is de AIV/CAVV van mening dat er een belangrijke versterkende werking vanuit zou gaan indien staten aan deze principes door middel van een internationale gedragscode of verklaring nadere uitwerking zouden geven.

24. In algemene zin zou de private sector meer verantwoordelijkheid kunnen nemen voor de bescherming van de kritieke infrastructuur die het beheert. Dit zou kunnen worden bevorderd door de (financiële) aansprakelijkheid van bedrijven op dit punt beter te regelen. Ook dient te worden gewaarborgd dat een minimum aan dienstverlening is gegarandeerd bij gedeeltelijke uitval van kritieke infrastructuur.

25. Het valt op dat waar de Nederlandse regering – met recht – erg actief is op het terrein van de vrijheid van meningsuiting op internet, de Nederlandse betrokkenheid tot op heden minder groot is bij mondiaal overleg gericht op het formuleren van normen met als doel conflictbeheersing op digitaal gebied. De AIV/CAVV beveelt aan dat Nederland zich als deelnemer aansluit bij initiatieven die het formuleren van normen op dit terrein tot doel hebben zoals een wederom door de SGVN in te stellen *Group of Governmental Experts.*

26. Er is noch de mogelijkheid noch de noodzaak tot het overeenkomen van een wereldwijd non-proliferatieregime. Er zijn belangrijke verschillen tussen massavernietigingswapens en digitale 'wapens'. Er zijn evenmin voldoende aanknopingspunten voor het instellen en afdwingen van beperkingen aan de uitvoer van bepaalde digitale technologie en software ter bescherming van de eigen militaire en civiele digitale infrastructuur.

Hoe kunnen de NAVO en de EU concreet inhoud geven aan de principes van common defence, deterrence en de solidariteitsclausule ten aanzien van cyberdreigingen? Hoe kunnen de NAVO en de EU de informatie-uitwisseling ten behoeve van dreigingsanalyses verbeteren?

27. De NAVO zal naar verwachting slechts bescheiden offensieve digitale capaciteiten kunnen ontwikkelen ter bescherming van de eigen systemen en netwerken, ofwel in het kader van de actieve verdediging. Van de conventionele en nucleaire middelen waarover afzonderlijke NAVO-landen beschikken gaat al een afschrikwekkende werking uit. Bij toekomstige NAVO-operaties kunnen wel offensieve digitale capaciteiten van de afzonderlijke lidstaten worden ingezet.

28. Het is noodzakelijk dat er meer samenhang komt in de activiteiten op het terrein van digitale veiligheid van de verschillende directoraten-generaal van de Europese Commissie – waaronder Binnenlandse Zaken (HOME), Informatiemaatschappij en media (INFSO), Justitie (JUST) en Interne Markt en Diensten (MARKT) – evenals EDEO, door uitvoering te geven aan een gezamenlijke strategie.

29. Artikel 4 en 5 van het NAVO-verdrag kunnen betrekking hebben op aanvallen in het digitale domein. Artikel 5 is dermate algemeen geformuleerd dat hier alle vormen van gewapend geweld onder kunnen worden geschaard. Het minder verstrekkende artikel 4 kan van toepassing zijn op digitale aanvallen die raken aan de nationale veiligheid maar nog niet de drempel van een gewapende aanval overschrijden. Naar verwachting zal er in praktijk bij digitale aanvallen eerder een beroep op dit artikel 4 worden gedaan.

30. De bijstandsclausule van de EU (artikel 42.7 van het EU-Verdrag) zal waarschijnlijk vooral worden aangewend ten behoeve van politieke steunbetuigingen. De EU kan wel een leidende rol vervullen bij het bevorderen van de digitale beveiliging in de private sector van de lidstaten.

31. Informatie-uitwisseling tussen de EU en de NAVO op het terrein van digitale veiligheid loopt tegen dezelfde bekende institutionele belemmeringen aan als de samenwerking tussen beide organisaties op andere terreinen. Bijkomend probleem is dat mogelijke informatievoorziening de eerstkomende periode vooral eenrichtingsverkeer zal blijken, aangezien zowel de beleidsvorming als de capaciteiten van de EU op het terrein van het GBVB en cyber beperkt zijn. Informele inlichtingenuitwisseling tussen de staven van de EU en NAVO, met inachtneming van de privacyregels, moet vooralsnog zoveel als mogelijk worden benut.

Adviesaanvraag

Aan de Voorzitters van de
Adviesraad Internationale Vraagstukken en de
Commissie van Advies voor Volkenrechtelijke
Vraagstukken
Mr. F. Korthals Altes
Prof.dr. M.T. Kamminga
Postbus 20061
2500 EB Den Haag

Ministerie van Buitenlandse Zaken
Postbus 20061
2500 EB Den Haag

Ministerie van Defensie
Postbus 20701
2500 ES Den Haag

30 augustus 2011

Adviesaanvraag digitale veiligheid

Geachte heer Korthals Altes,
Geachte heer Kamminga,

Onze afhankelijkheid van het functioneren van digitale netwerken brengt nieuwe veiligheidsrisico's mee. Dit wordt onder meer onderkend in het nieuwe strategisch concept van de NAVO en in het Cyber Security Beeld Nederland.

In februari jl. presenteerde het kabinet de Nationale Cyber Security Strategie. Overeenkomstig de beleidsbrief 'Defensie na de kredietcrisis' van 8 april jl. wordt extra geïnvesteerd in de digitale weerbaarheid van Defensie en de ontwikkeling van operationele cybercapaciteiten.

Tegen deze achtergrond willen wij, mede namens de minister van Veiligheid en Justitie, de volgende centrale vraag voorleggen aan de Adviesraad en de CAVV:

wat betekenen de ontwikkelingen op cybergebied voor het Nederlands buitenlands-, veiligheids- en defensiebeleid, en op welke wijze kan internationale samenwerking bijdragen tot de effectieve bescherming tegen de cyberdreiging?

Wij verzoeken u zich in het bijzonder te richten op de volgende vraagstukken:

1. Het digitale domein wordt naast land, lucht, zee en ruimte beschouwd als de 'vijfde dimensie' waarin sprake kan zijn van militair optreden. Op grond van welke politieke en militaire doelstellingen moeten operationele cybercapaciteiten worden ontwikkeld en kunnen worden ingezet? Wat is de aard en rol van operationele cybercapaciteiten bij militaire operaties?

2. In hoeverre en op welke wijze is het bestaande internationaalrechtelijk kader, relevant voor gedragingen in het cyberdomein, in het bijzonder cybergeweld?
   - [*ad bellum*] Onder welke omstandigheden kan een cyberdreiging worden beschouwd als het gebruik van geweld of een dreiging hiermee, in de zin van artikel 2 lid 4 van het VN-Handvest? Onder welke omstandigheden kan een cyberaanval worden beschouwd als

een gewapende aanval waartegen geweld mag worden gebruikt ter zelfverdediging op basis van artikel 51 van het VN Handvest?
- [*in bello*] Wanneer is er sprake van toepasselijkheid van het humanitair oorlogsrecht op gedragingen in het digitale domein? Moeten deze samenhangen met kinetisch gewelds-gebruik? Hoe zou bij een dergelijke toepassing gestalte moeten worden gegeven aan de oorlogsrechtelijke principes van onderscheid en proportionaliteit, en aan de verplichting tot het nemen van voorzorgsmaatregelen?
- Hoe zou in het cyberdomein gestalte moeten worden gegeven aan de volkenrechtelijke begrippen soevereiniteit, neutraliteit?

3. Internationale samenwerking is onontbeerlijk voor het bevorderen van *cyber security.*
   - In hoeverre kunnen internationale gedragsnormen over het gebruik van het digitale domein een effectieve bijdrage leveren aan het vergroten van *cyber security*? Kunnen we lering trekken uit ervaringen met bestaande gedragscodes, bijvoorbeeld op het gebied van non-proliferatie?
   - Hoe kunnen de NAVO en de EU concreet inhoud geven aan de principes van *common defence, deterrence* en de solidariteitsclausule ten aanzien van cyberdreigingen? Hoe kunnen de NAVO en de EU de informatie-uitwisseling ten behoeve van dreigingsanalyses verbeteren?

Gegeven de snelheid waarmee ontwikkelingen op het gebied van cyber security zich voordoen, stellen wij een spoedig en kernachtig advies bijzonder op prijs.

De Minister van Buitenlandse Zaken,

(getekend)
Dr. U. Rosenthal

De Minister van Defensie,

(getekend)
Drs. J.S.J. Hillen

Lijst van gebruikte afkortingen

AIV	Adviesraad Internationale Vraagstukken
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BWV	Biologisch Wapen Verdrag
CAVV	Commissie van Advies inzake Volkenrechtelijke Vraagstukken
CCD Co	Cooperative Cyber Defense Centre of Excellence
CDMB	Cyber Defence Management Board
CDS	Commandant der Strijdkrachten
CERT	Computer Emergency Response Team
COREPER	Comité van Permanente Vertegenwoordigers
COSI	Committee on Operational Cooperation on Internal Security
CTAC	Cyber Threat Assessment Cell
CTBT	Comprehensive Test Ban Treaty
CWV	Chemisch Wapen Verdrag
DefCERT	Computer Emergency Response Team van het Ministerie van Defensie
DDoS	Distributed Denial of Service
EDEO	Europese Dienst voor Extern Optreden
ENISA	European Network and Information Security Agency
GBVB	Gemeenschappelijk Buitenlands en Veiligheidsbeleid
GOVCERT.NL	Computer Emergency Response Team van de Nederlandse overheid
HCOC	The Hague Code of Conduct Against Ballistic Missile Proloferatiion
IAEA	International Atomic Energy Agency
ICT	Informatie- en Communicatietechnologie
ICTY	International Criminal Tribunal for the former Yugoslavia
IP	Internet Protocol
ITU	International Telecommunication Union
KLPD	Korps Landelijke Politiediensten
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NAR	Noord-Atlantische Raad
NAVO	Noord-Atlantische Verdragsorganisatie
NC3A	NATO Consultation, Command and Control Agency
NCIRC	NATO Computer Incident Response Capability
NCSC	Nationaal Cyber Security Centrum
NPV	Non-Proliferatieverdrag

OESO	Organisatie voor Economische Samenwerking en Ontwikkeling
OVSE	Organisatie voor Veiligheid en Samenwerking in Europa
PSC	Political and Security Committee
SGVN	Secretaris-generaal van de Verenigde Naties
WIV	Wet op de Inlichtingen- en Veiligheidsdiensten

Lijst van gebruikte begrippen

Attributie	Het proberen te identificeren van de verantwoordelijke(n) achter een digitale aanval.
Botnet	Een verzameling van geïnfecteerde computers die op afstand centraal bestuurd kunnen worden.
DDoS-aanval	Distributed Denial of Service is de benaming voor een type aanval waarbij een bepaalde dienst (bijvoorbeeld een website) onbereikbaar wordt voor de gebruikelijke afnemers van de dienst. Een DDoS op een website wordt vaak uitgevoerd door de website te bestoken met veel netwerkverkeer, waardoor deze onbereikbaar wordt.
Digitale aanval	Operatie gericht op verstoren, beschadigen of vernietigen van computers en netwerken, of de hierop aanwezige informatie.
Digitale criminaliteit	Een strafbare gedraging waarbij wordt getracht door middel van gebruikmaking van netwerken of informatiesystemen financieel of andersoortig gewin te behalen.
Digitaal domein	Het geheel van ICT-middelen en ICT–diensten. Hierbij horen ook alle niet met internet verbonden netwerken of andere digitale apparaten.
Digitale exploitatie	Het langs digitale weg kopiëren van data op andere computers of netwerken.
Digitaal activisme	Het inbreken op netwerken of informatiesystemen door een individu of groepering met als doel deze te verstoren of te veranderen om zodoende een politieke ideologie of sociale overtuiging onder de aandacht te brengen.
Digitale oorlogvoering	Het uitvoeren van militaire operaties die erop zijn gericht om met digitale middelen computersystemen of netwerken van een tegenstander te verstoren, misleiden, veranderen of vernietigen.
Digitale spionage	Het heimelijk verwerven van gegevens op netwerken of informatiesystemen door overheden of bedrijven ten bate van hun diplomatieke, militaire of economische belangen.
Digitaal terrorisme	Via de inzet van digitale middelen pogen een samenleving of delen daarvan ernstig te ontwrichten om een politiek doel te bereiken.
Digitale veiligheid	Het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van informatie- en communicatietechnologie (ICT) of door misbruik van ICT. Het gevaar of de schade door misbruikverstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.
Exploit	Software, gegevens, of opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software of hardware om onbedoeld of onverwacht gedrag daarvan te veroorzaken.
Hacktivisme	Zie digitaal activisme.
Human intelligence	Het vergaren van inlichtingen via interpersoonlijk contact.
Kinetische wapens	Wapens zoals handvuurwapens, tanks en artillerie.
Malware	Kwaadaardige software.
SIGINT	Signals Intelligence, het vergaren en nader verwerken van inlichtingen uit satelliet- en radiocommunicatie.

Social engineering	Een aanvalstechniek waarbij gebruik wordt gemaakt van menselijke eigenschappen als nieuwsgierigheid, vertrouwen en hebzucht met als doel vertrouwelijke informatie te verkrijgen of bepaalde handelingen te laten verrichten.
Trojaans paard	Een bestand dat onschadelijk lijkt maar een kwaadaardige functie heeft.
Virus	Middel om kwaadaardige software over te brengen, verspreidt zich door middel van een actie van de gebruiker, bijvoorbeeld het verzenden van een e-mail.
Worm	Middel om kwaadaardige software over te brengen, gebruikt het geïnfecteerde netwerk of apparaat om zichzelf verder te verspreiden.
Zero-day	Een kwetsbaarheid in de software waar de maker of beheerder van een systeem of netwerk nog niet van op de hoogte is.

Bijlage IV

Overzicht geraadpleegde personen

Naam	Functie/Organisatie
Dhr. F. Asbeck	Principle Advisor for Space and Security Policy, EEAS
SBN P.J. Bindt	Directeur Militaire Inlichtingen- en Veiligheidsdienst
Mr.drs. D.J. le Clercq	Juridisch Bestuurlijk Adviseur, Bestuursstaf Directie Juridische Zaken Internationale en Juridische Beleidsaangelegenheden, Ministerie van Defensie
Dr. P.A. Ducheine	Kolonel van de Militair Juridische Dienst, Universitair Hoofddocent Militair Recht, Nederlandse Defensie Academie
Mr. R.V. Duiven	Kwartiermaker Nationale Cyber Security Strategie
Kol.ir. H. Folmer	Programmamanager Cyber Ministerie van Defensie
Gen.maj. K. Gijsbers	Project Coördinator Reorganisatie Defensie Ministerie van Defensie
Mr. E.E. Gillissen	Senior jurist WIV 2002, Directie Juridische Zaken, Afdeling Wet- en Regelgeving, Ministerie van Defensie
Dhr. N. Groeneveld	Information Security Engineer, Confidential
Mw. drs. E.C. van den Heuvel	General Manager GOVCERT.NL
Mr. M.J. Kuipers	Plaatsvervangend hoofd AIVD
E. Luiijf, MSc	Consultant/adviseur Centre for Protection of the National Infrastructure (CPNI.nl) en TNO
Drs. F. Peters	Senior Beleidsmedewerker, MIVD, Stafafdeling Beleid, Ministerie van Defensie
Ir. R. Prins	CEO en Co-Founder Fox-IT
Kol. W. Sleurink	Emerging Security Challenges Division, NAVO
Drs. M.A. Stibbe	Plaatsvervangend directeur Directie Veiligheidsbeleid, Ministerie van Buitenlandse Zaken
Dhr. A. Suleyman	Hoofd Cyber Defence Section, Emerging Security Challenges Division, NAVO Cyber Defence Coordination & Support Center
Dr. E. Tikk	Juridisch adviseur NAVO Cooperative Cyber Defence Centre of Excellence (NATO CCD CoE)
Drs. P. Zandstra	Beleidsmedewerker Permanente Vertegenwoordiging NAVO

Door de Adviesraad Internationale Vraagstukken uitgebrachte adviezen*

1 EUROPA INCLUSIEF, *oktober 1997*
2 CONVENTIONELE WAPENBEHEERSING: dringende noodzaak, beperkte mogelijkheden, *april 1998*
3 DE DOODSTRAF EN DE RECHTEN VAN DE MENS: recente ontwikkelingen, *april 1998*
4 UNIVERSALITEIT VAN DE RECHTEN VAN DE MENS EN CULTURELE VERSCHEIDENHEID, *juni 1998*
5 EUROPA INCLUSIEF II, *november 1998*
6 HUMANITAIRE HULP: naar een nieuwe begrenzing, *november 1998*
7 COMMENTAAR OP DE CRITERIA VOOR STRUCTURELE BILATERALE HULP, *november 1998*
8 ASIELINFORMATIE EN DE EUROPESE UNIE, *juli 1999*
9 NAAR RUSTIGER VAARWATER: een advies over betrekkingen tussen Turkije en de Europese Unie, *juli 1999*
10 DE ONTWIKKELINGEN IN DE INTERNATIONALE VEILIGHEIDSSITUATIE IN DE JAREN NEGENTIG: van onveilige zekerheid naar onzekere veiligheid, *september 1999*
11 HET FUNCTIONEREN VAN DE VN-COMMISSIE VOOR DE RECHTEN VAN DE MENS, *september 1999*
12 DE IGC 2000 EN DAARNA: op weg naar een Europese Unie van dertig lidstaten, *januari 2000*
13 HUMANITAIRE INTERVENTIE, *april 2000***
14 ENKELE LESSEN UIT DE FINANCIËLE CRISES VAN 1997 EN 1998, *mei 2000*
15 EEN EUROPEES HANDVEST VOOR GRONDRECHTEN?, *mei 2000*
16 DEFENSIE-ONDERZOEK EN PARLEMENTAIRE CONTROLE, *december 2000*
17 DE WORSTELING VAN AFRIKA: veiligheid, stabiliteit en ontwikkeling, *januari 2001*
18 GEWELD TEGEN VROUWEN: enkele rechtsontwikkelingen, *februari 2001*
19 EEN GELAAGD EUROPA: de verhouding tussen de Europese Unie en subnationale overheden, *april 2001*
20 EUROPESE MILITAIR-INDUSTRIËLE SAMENWERKING, *mei 2001*
21 REGISTRATIE VAN GEMEENSCHAPPEN OP HET GEBIED VAN GODSDIENST OF OVERTUIGING, *juni 2001*
22 DE WERELDCONFERENTIE TEGEN RACISME EN DE PROBLEMATIEK VAN RECHTSHERSTEL, *juni 2001*
23 COMMENTAAR OP DE NOTITIE MENSENRECHTEN 2001, *september 2001*
24 EEN CONVENTIE OF EEN CONVENTIONELE VOORBEREIDING: de Europese Unie en de IGC 2004, *november 2001*
25 INTEGRATIE VAN GENDERGELIJKHEID: een zaak van verantwoordelijkheid, inzet en kwaliteit, *januari 2002*
26 NEDERLAND EN DE ORGANISATIE VOOR VEILIGHEID EN SAMENWERKING IN EUROPA IN 2003: rol en richting, *mei 2002*
27 EEN BRUG TUSSEN BURGERS EN BRUSSEL: naar meer legitimiteit en slagvaardigheid voor de Europese Unie, *mei 2002*
28 DE AMERIKAANSE PLANNEN VOOR RAKETVERDEDIGING NADER BEKEKEN: voors en tegens van bouwen aan onkwetsbaarheid, *augustus 2002*
29 PRO–POOR GROWTH IN DE BILATERALE PARTNERLANDEN IN SUB–SAHARA AFRIKA: een analyse van strategieën tegen armoede, *januari 2003*
30 EEN MENSENRECHTENBENADERING VAN ONTWIKKELINGSSAMENWERKING, *april 2003*
31 MILITAIRE SAMENWERKING IN EUROPA: mogelijkheden en beperkingen, *april 2003*
32 *Vervolgadvies* EEN BRUG TUSSEN BURGERS EN BRUSSEL: naar meer legitimiteit en slagvaardigheid voor de Europese Unie, *april 2003*
33 DE RAAD VAN EUROPA: minder en (nog) beter, *oktober 2003*

34 NEDERLAND EN CRISISBEHEERSING: drie actuele aspecten, *maart 2004*

35 FALENDE STATEN: een wereldwijde verantwoordelijkheid, *mei 2004***

36 PREËMPTIEF OPTREDEN, *juli 2004***

37 TURKIJE: de weg naar het lidmaatschap van de Europese Unie, *juli 2004*

38 DE VERENIGDE NATIES EN DE RECHTEN VAN DE MENS, *september 2004*

39 DIENSTENLIBERALISERING EN ONTWIKKELINGSLANDEN: leidt openstelling tot achterstelling?, *september 2004*

40 DE PARLEMENTAIRE ASSEMBLEE VAN DE RAAD VAN EUROPA, *februari 2005*

41 DE HERVORMINGEN VAN DE VERENIGDE NATIES: het rapport Annan nader beschouwd, *mei 2005*

42 DE INVLOED VAN CULTUUR EN RELIGIE OP ONTWIKKELING: stimulans of stagnatie?, *juni 2005*

43 MIGRATIE EN ONTWIKKELINGSSAMENWERKING: de samenhang tussen twee beleidsterreinen, *juni 2005*

44 DE NIEUWE OOSTELIJKE BUURLANDEN VAN DE EUROPESE UNIE, *juli 2005*

45 NEDERLAND IN DE VERANDERENDE EU, NAVO EN VN, *juli 2005*

46 ENERGIEK BUITENLANDS BELEID: energievoorzieningszekerheid als nieuwe hoofddoelstelling, *december 2005****

47 HET NUCLEAIRE NON-PROLIFERATIEREGIME: het belang van een geïntegreerde en multilaterale aanpak, *januari 2006*

48 MAATSCHAPPIJ EN KRIJGSMACHT, *april 2006*

49 TERRORISMEBESTRIJDING IN MONDIAAL EN EUROPEES PERSPECTIEF, *september 2006*

50 PRIVATE SECTOR ONTWIKKELING EN ARMOEDEBESTRIJDING, *oktober 2006*

51 DE ROL VAN NGO'S EN BEDRIJVEN IN INTERNATIONALE ORGANISATIES, *oktober 2006*

52 EUROPA EEN PRIORITEIT!, *november 2006*

53 BENELUX, NUT EN NOODZAAK VAN NAUWERE SAMENWERKING, *februari 2007*

54 DE OESO VAN DE TOEKOMST, *maart 2007*

55 MET HET OOG OP CHINA: op weg naar een volwassen relatie, *april 2007*

56 INZET VAN DE KRIJGSMACHT: wisselwerking tussen nationale en internationale besluitvorming, *mei 2007*

57 HET VN-VERDRAGSSYSTEEM VOOR DE RECHTEN VAN DE MENS: stapsgewijze versterking in een politiek geladen context, *juli 2007*

58 DE FINANCIËN VAN DE EUROPESE UNIE, *december 2007*

59 DE INHUUR VAN PRIVATE MILITAIRE BEDRIJVEN: een kwestie van verantwoordelijkheid, *december 2007*

60 NEDERLAND EN DE EUROPESE ONTWIKKELINGSSAMENWERKING, *mei 2008*

61 DE SAMENWERKING TUSSEN DE EUROPESE UNIE EN RUSLAND: een zaak van wederzijds belang, *juli 2008*

62 KLIMAAT, ENERGIE EN ARMOEDEBESTRIJDING, *november 2008*

63 UNIVERSALITEIT VAN DE RECHTEN VAN DE MENS: principes, praktijk en perspectieven, *november 2008*

64 CRISISBEHEERSINGSOPERATIES IN FRAGIELE STATEN: de noodzaak van een samenhangende aanpak, *maart 2009*

65 TRANSITIONAL JUSTICE: gerechtigheid en vrede in overgangssituaties, *april 2009***

66 DEMOGRAFISCHE VERANDERINGEN EN ONTWIKKELINGSSAMENWERKING, *juli 2009*

67 HET NIEUWE STRATEGISCH CONCEPT VAN DE NAVO, *januari 2010*

68 DE EU EN DE CRISIS: lessen en leringen, *januari 2010*

69 SAMENHANG IN INTERNATIONALE SAMENWERKING: reactie op WRR-rapport ‘Minder pretentie, meer ambitie’, *mei 2010*

70 NEDERLAND EN DE ‘RESPONSIBILITY TO PROTECT’: de verantwoordelijkheid om mensen te beschermen tegen massale wreedheden, *juni 2010*

71 HET VERMOGEN VAN DE EU TOT VERDERE UITBREIDING, *juli 2010*

72 PIRATERIJBESTRIJDING OP ZEE: een herijking van publieke en private verantwoordelijkheden, *december 2010*

73 HET MENSENRECHTENBELEID VAN DE NEDERLANDSE REGERING: zoeken naar constanten in een veranderende omgeving, *februari 2011*

74 ONTWIKKELINGSAGENDA NA 2015: millennium ontwikkelingsdoelen in perspectief, *april 2011*

75 HERVORMINGEN IN DE ARABISCHE REGIO: kansen voor democratie en rechtsstaat?, *mei 2011*

76 HET MENSENRECHTENBELEID VAN DE EUROPESE UNIE: tussen ambitie en ambivalentie, *juli 2011*

Door de Adviesraad Internationale Vraagstukken uitgebrachte briefadviezen

1 Briefadvies UITBREIDING EUROPESE UNIE, *december 1997*

2 Briefadvies VN-COMITÉ TEGEN FOLTERING, *juli 1999*

3 Briefadvies HANDVEST GRONDRECHTEN, *november 2000*

4 Briefadvies OVER DE TOEKOMST VAN DE EUROPESE UNIE, *november 2001*

5 Briefadvies NEDERLANDS VOORZITTERSCHAP EU 2004, *mei 2003*****

6 Briefadvies RESULTAAT CONVENTIE, *augustus 2003*

7 Briefadvies VAN BINNENGRENZEN NAAR BUITENGRENZEN - ook voor een volwaardig Europees asiel- en migratiebeleid in 2009, *maart 2004*

8 Briefadvies DE ONTWERP-DECLARATIE INZAKE DE RECHTEN VAN INHEEMSE VOLKEN. Van impasse naar doorbraak?, *september 2004*

9 Briefadvies REACTIE OP HET SACHS-RAPPORT: Hoe halen wij de Millennium Doelen, *april 2005*

10 Briefadvies DE EU EN DE BAND MET DE NEDERLANDSE BURGER, *december 2005*

11 Briefadvies TERRORISMEBESTRIJDING IN EUROPEES EN INTERNATIONAAL PERSPECTIEF, interim-advies over het folterverbod, *december 2005*

12 Briefadvies REACTIE OP DE MENSENRECHTENSTRATEGIE 2007, *november 2007*

13 Briefadvies EEN OMBUDSMAN VOOR ONTWIKKELINGSSAMENWERKING, *december 2007*

14 Briefadvies KLIMAATVERANDERING EN VEILIGHEID, *januari 2009*

15 Briefadvies OOSTELIJK PARTNERSCHAP, *februari 2009*

16 Briefadvies ONTWIKKELINGSSAMENWERKING: Nut en noodzaak van draagvlak, *mei 2009*

17 Briefadvies KABINETSFORMATIE 2010, *juni 2010*

18 Briefadvies HET EUROPESE HOF VOOR DE RECHTEN VAN DE MENS: beschermer van burgerlijke rechten en vrijheden, *november 2011*

* *Alle adviezen zijn ook beschikbaar in het Engels. Sommige adviezen ook in andere talen.*

** *Gezamenlijk advies van de Adviesraad Internationale Vraagstukken (AIV) en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken (CAVV).*

*** *Gezamenlijk advies van de Adviesraad Internationale Vraagstukken (AIV) en de Algemene Energieraad (AER).*

**** *Gezamenlijk briefadvies van de Adviesraad Internationale Vraagstukken (AIV) en de Adviescommissie voor Vreemdelingenzaken (ACVZ).*