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.