Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

33 000 X Vaststelling van de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2012

Nr. 99

LIJST VAN VRAGEN EN ANTWOORDEN

Vastgesteld 19 juli 2012

De vaste commissie voor Defensie heeft een aantal vragen voorgelegd aan de ministers van Defensie en van Buitenlandse Zaken over de brief van 6 april 2012 inzake de Kabinetsreactie over het gezamenlijk advies van de Adviesraad Internationale Vraagstukken (AIV) en de Commissie van Advies inzake Volkenrechtelijke vraagstukken (CAVV) over digitale oorlogvoering (Kamerstuk 33 000 X, nr. 79).
De ministers hebben deze vragen beantwoord bij brief van 17 juli 2012.
Vragen en antwoorden zijn hierna afgedrukt.

De voorzitter van de commissie,
Van Beek

De griffier van de commissie,
Roovers

kst-33000-X-99
ISSN 0921 - 7371
's-Gravenhage 2012

1 en 2
Welke stappen gaat u ondernemen om te realiseren dat operationele cybercapaciteiten en ontwikkelingen op dit gebied een plaats krijgen in een geïntegreerde strategie voor het binnenlands en buitenlands veiligheidsbeleid, zoals de AIV/CAVV[1] aanbeveelt?
Op welke wijze neemt u het advies van de AIV/CAVV over, dat een dergelijke strategie inzicht zou moeten geven in de te bereiken doelen (ends), de wijze waarop deze doelen moeten worden bereikt (ways) en de middelen die daar voor ingezet worden (means)?

De Defensie Cyber Strategie is op 27 juni 2012 aan de Tweede Kamer aangeboden. Deze strategie geeft de komende jaren richting, samenhang en focus aan de integrale aanpak voor de ontwikkeling van het militaire vermogen in het digitale domein. De strategie geeft invulling aan de taken en verantwoordelijkheden van Defensie zoals onder andere gesteld in de in maart 2011 vastgestelde Nationale Cyber Security Strategie en aan het buitenlands en veiligheidsbeleid van het kabinet. De intensivering van de samenwerking in nationaal en internationaal verband is een van de speerpunten van de strategie.

Daarnaast wordt bezien hoe externe veiligheidsaspecten meer in de Strategie Nationale Veiligheid kunnen worden geïntegreerd. Hierbij wordt ondermeer gebruik gemaakt van de Defensieverkenningen en wordt gekeken hoe een strategische monitorfunctie kan worden ingericht om breder zicht te krijgen op de betekenis van internationale risico's voor het nationale veiligheidsterrein.

3
Hoe verhoudt zich de gevoelde urgentie tot het tempo waarin de capaciteiten op dit gebied van Defensie (en overigens ook overheidsbreed) worden ontwikkeld?

Ondanks de ingrijpende bezuinigingen bij Defensie, die ook de operationele capaciteiten van de krijgsmacht raken, wordt de komende jaren geïnvesteerd in het vergroten van de digitale weerbaarheid en het ontwikkelen van operationele cybercapaciteiten. Zoals in de beleidsbrief aangekondigd is de ontwikkeling van een hoogwaardige cybercapaciteit een van de prioriteiten voor Defensie.

Defensie is voortvarend gestart met het ontwikkelen van het noodzakelijke beleid zoals uiteengezet in de Defensie Cyber Strategie. De noodzakelijke financiële middelen komen de komende jaren beschikbaar waardoor de gewenste capaciteit kan worden ingericht.

4
Deelt u de opvatting dat cyberaanvallers een voordeel hebben boven cyberverdedigers, en dat offensieve tactieken veel sneller aan te passen zijn dan dat de overheid en de industrie hun verdediging kunnen aanpassen?

Een aanvaller heeft per definitie het initiatief. Digitale aanvallen kunnen relatief eenvoudig in het geheim worden voorbereid en de velerlei kwetsbaarheden in software betekenen dat een vasthoudende en technologisch hoogontwikkelde tegenstander uiteindelijk in staat zal zijn (delen van) netwerken en systemen te compromitteren.

Een hoogwaardige en technologisch vooraanstaande inrichting van de beveiliging van netwerken en systemen kan organisaties als Defensie echter wel degelijk in staat stellen om de uitwerking van aanvallen te beperken en de dreiging relatief snel af te wenden. Bij de bescherming

[1] AIV: Adviesraad Internationale Vraagstukken. CAVV: Commissie van Advies inzake Volkenrechtelijke Vraagstukken.

van de eigen digitale infrastructuur moet daartoe zoveel mogelijk flexibiliteit worden ingebouwd, zowel ten aanzien van de (passieve) beveiliging van netwerken als de actieve respons op een aanval. Prioriteit moet liggen bij de bescherming van informatie en informatie-uitwisseling. Daarnaast moeten systemen weerbaar zijn door snel te kunnen reageren op een aanval en in staat te zijn zich aan te passen om te blijven functioneren.

5
Ondersteunt u het oordeel van de AIV/CAVV dat een uniforme begripsdefinitie zowel op nationaal als op internationaal niveau noodzakelijk is? Zo ja, is de begripsdefinitie in Nederland geüniformeerd? Indien dit niet het geval is, waarom niet en wat gaat u eraan doen om dit alsnog te bewerkstelligen?
En is de begripsdefinitie in Europees en NAVO-verband geüniformeerd? Indien dit niet het geval is, waarom niet en wat gaat u eraan doen om dit alsnog te bewerkstelligen?
Zoekt u hierbij aansluiting bij de gebruikte definities bij overige overheidsinstellingen, het bedrijfsleven en de individuele gebruikers?

Er zijn nog geen internationaal geaccepteerde definities. Het kabinet onderschrijft het belang van duidelijke definities. Duidelijke en internationaal geaccepteerde definities zullen bijdragen aan het wederzijdse begrip en het vinden van overeenstemming.

In de militaire omgeving is het eens te meer van belang uniforme begrippen te hanteren. De NAVO ontwikkelt daartoe begripsdefinities. Nederland draagt hieraan actief bij. Na vaststelling zal ook Defensie de NAVO-definities hanteren.

6
Is er, in tegenstelling tot uw stelling dat een cyberoorlog die uitsluitend in het digitale domein wordt uitgevochten niet aannemelijk is, niet wel degelijk een risico op een digitaal «Pearl Harbor», gezien de investeringen op dit gebied in diverse landen? Bestaat er niet ook een risico van lage-intensiteitsconflicten of «Koude Oorlogen» die wel uitsluitend via het digitale domein uitgevochten worden?

Zoals ook de AIV en de CAVV concluderen zullen digitale capaciteiten waarschijnlijk in alle toekomstige conflicten een belangrijke rol spelen. Defensie gaat er dan ook vanuit dat conflicten deels in het digitale domein zullen worden uitgevochten. De kans op een digitale aanval waarmee in één keer een groot deel van de nationale infrastructuur kan worden lamgelegd wordt niet groot geacht. Offensieve cybercapaciteiten zijn vooral van belang doordat deze het totale operationele vermogen van de krijgsmacht vergroten.

7
Waaruit zouden offensieve capaciteiten bestaan? Valt Stuxnet hieronder? Wordt overwogen om deze en vergelijkbare aanvalssoftware in gebruik te nemen in het op te richten Defensie Cyber Commando? Wat zijn de volkenrechtelijke gevolgen van het eventueel operationeel maken van deze vorm van digitale oorlogvoering door Nederland?

Offensieve cybercapaciteiten zijn die digitale middelen die het handelen van de tegenstander kunnen beïnvloeden of onmogelijk maken. Bij het ontwikkelen van offensieve operationele capaciteiten zal zoveel mogelijk gebruik worden gemaakt van kennis en middelen die bij de MIVD aanwezig zijn.

De ontwikkeling van offensieve operationele capaciteiten staat internationaal echter nog in de kinderschoenen. Er is nog veel onduidelijk over de aard van deze capaciteiten, de mogelijkheden die ze kunnen bieden en de effecten die ermee kunnen worden gesorteerd. Offensieve cybercapaciteiten onderscheiden zich van conventionele militaire capaciteiten doordat ze vaak slechts eenmalig inzetbaar zijn en veelal een beperkte levensduur hebben. Hoogwaardige cybercapaciteiten zijn nauwelijks vergelijkbaar met algemeen bekende, relatief laagdrempelige en wijdverbreide aanvalsmethoden. Het gaat hier om complexe middelen waarvan de ontwikkeling zeer kennisintensief is en daardoor kostbaar en tijdrovend. Een uitdaging is dat de gewenste effecten moeilijk gegarandeerd kunnen worden doordat de tegenstander op elk moment zijn eigen kwetsbaarheid kan ontdekken en beperken.

Het kabinet onderschrijft dat ook in het digitale domein het humanitair oorlogsrecht onverkort van kracht is en moet worden voldaan aan de volkenrechtelijke eisen van «noodzakelijkheid» en «proportionaliteit».

8
Hoe wordt zeker gesteld dat de Militaire Inlichtingen- en Veiligheidsdienst daadwerkelijk binnen de kaders van de wet opereert? Wat wordt er gedaan bij eventuele overschrijdingen van die kaders?

De MIVD is gebonden aan de kaders van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002). De onafhankelijke Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) is belast met het toezicht op de rechtmatigheid van de uitvoering door de MIVD van zijn wettelijke taken. De CTIVD informeert en adviseert de minister van Defensie gevraagd en ongevraagd over haar bevindingen. Daarnaast verricht de CTIVD onderzoeken bij de MIVD. Toezichtsrapporten van de CTIVD zijn openbaar en worden toegezonden aan de voorzitters van de Eerste en Tweede Kamer der Staten-Generaal.

Naast het toezicht van de CTIVD, worden de activiteiten van de MIVD besproken in de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) van de Tweede Kamer. De CIVD vergadert regelmatig met de minister van Defensie.

9 en 10
Hoe verhoudt uw stelling dat het noodzakelijk is dat operationele (offensieve) cybercapaciteiten onderdeel worden van het totale militaire vermogen van de Nederlandse krijgsmacht, zich tot het bedrag van 50 miljoen aan investeringen op dit gebied, dat door de AIV/CAVV «bescheiden» wordt genoemd? Is dit bedrag voldoende om ook offensieve capaciteiten te ontwikkelen?
Kunt u nader ingaan op uw stelling dat de mate waarin invulling kan worden gegeven aan de beschreven activiteiten afhankelijk is van de beschikbare financiële ruimte? Waarom wordt de financiële ruimte zo nadrukkelijk genoemd, en niet de beschikbaarheid van gekwalificeerd personeel? Is de financiële ruimte voor de komende jaren voldoende?

De in de beleidsbrief aangekondigde financiële middelen zijn voldoende om de ambities van Defensie tot 2015 te realiseren. Hierbij ligt de prioriteit bij het vergroten van de digitale weerbaarheid, het inlichtingenvermogen en de ontwikkeling van het vermogen operaties in het digitale domein uit te voeren.
De financiële middelen konden alleen binnen Defensie worden vrijgemaakt door bovenop de bezuinigingen te herschikken. Ook de beschikbaarheid van gekwalificeerd personeel is van groot belang.

11 en 12
Met welke partners wordt overlegd over een defensiestrategie voor cyber operations? Houdt die strategie ook de uitwisseling van data met die partners in? Is er bij deze partners een scheiding tussen de bestrijding van digitale problemen in het militaire en het civiele domein? Ontstaat door de samenwerking met deze partners niet het gevaar van vermenging van militaire en civiele digitale maatregelen?
In hoeverre zoekt Defensie samenwerking met het bedrijfsleven als het gaat om cyber?

Defensie werkt actief samen met andere partijen in het kader van de Nationale Cyber Security Strategie, onder meer door deelneming in de Cyber Security Raad en het Nationale Cyber Security Centrum. Het uitwisselen van kennis en informatie is een belangrijk aspect van deze samenwerking. Tevens is sprake van nauwe samenwerking met het bedrijfsleven en de wetenschap. In het digitale domein is het bedrijfsleven de motor van innovatie, ook wat het beveiligen en beschermen van ICT-infrastructuur betreft. Defensie wil optimaal gebruik maken van deze innovatiekracht.

13
Wat gaat u doen om de bedrijfscultuur bij Defensie meer in overeenstemming te brengen met de eisen en wensen van gekwalificeerde specialisten, gezien de opmerking van de AIV/CAVV dat die bedrijfscultuur een van de grootste obstakels is bij het verwerven en behouden van gekwalificeerde specialisten?

Het aantrekken en het behouden van gekwalificeerd personeel dat ook kan functioneren in een militaire omgeving vormt een bijzondere uitdaging voor Defensie. De benodigde militaire personele capaciteit zal voor een deel worden gerealiseerd door de inzet van cyberreservisten. Om de noodzakelijke kennis, kunde en vaardigheden in huis te halen en binnen te houden wordt specifiek aandacht besteed aan personeelsbeleid en opleidingen. Zo zullen onder andere specifieke loopbaanpatronen worden ontwikkeld om de kennis en ervaringsopbouw van defensiemedewerkers op het gebied van cyber te verankeren en verder te ontwikkelen. Door samenwerking met het NCSC, opsporingsdiensten en het bedrijfsleven kan uitwisseling van personeel worden bevorderd. Hierdoor wordt een goede ervaringsopbouw gewaarborgd en kan medewerkers een interessant loopbaanperspectief worden geboden.

14
Wanneer is uw onderzoek naar de mogelijkheden om een pool van cyberreservisten te creëren afgerond? Bent u bereid het voorbeeld van Groot-Brittannië te volgen, dat cyberreservisten voor Defensie inzet die ook ingezet kunnen worden voor de politie?

Aansluitend op het bestaande reservistenbeleid ontwikkelt Defensie een specifiek traject voor cyber specialisten. Dit beleid wordt in nauw overleg met het bedrijfsleven uitgewerkt. Het doel is in de loop van 2013 de eerste cyberreservisten aan te stellen. Zij kunnen ook worden ingezet ter ondersteuning van civiele autoriteiten in het kader van de derde hoofdtaak. Met het ministerie van Veiligheid en Justitie wordt overlegd over de mogelijkheden tot samenwerking ten aanzien van reservisten.

15
Hebt u voor Nederland verder geconcretiseerd wat de «voldoende mate van zekerheid» is die Nederland volgens het internationaal recht moet

hebben over de afkomst van een cyberaanval, alvorens erop gereageerd mag worden? Zo ja, wat houdt deze concretisering in? Zo nee, waarom niet?

Dit zal van geval tot geval moeten worden bezien. Enerzijds is voldoende zekerheid nodig over de afkomst van een cyberaanval om het risico van een respons tegen een ander dan de werkelijke aanvaller zoveel mogelijk te verkleinen. Anderzijds is het verkrijgen van volledige zekerheid niet altijd mogelijk of zou met het verkrijgen hiervan zoveel tijd gemoeid kunnen gaan, dat een passende reactie niet meer mogelijk of zinvol is.

16
Is Nederland gerechtigd om maatregelen te nemen tegen Iran na het incident met Diginotar, desnoods via cyber? Zo ja, welke maatregelen zijn mogelijk binnen de grenzen van het volkenrecht, ervan uitgaande dat het geen «gewapende aanval» in de zin van artikel 51 van het VN Handvest betrof?

Aangezien bij het incident bij Diginotar geen sprake is van een «gewapende aanval» in de zin van artikel 51 van het VN-Handvest kan geen beroep worden gedaan op het recht op zelfverdediging bij het nemen van eventuele tegenmaatregelen.

17
Is het humanitaire oorlogsrecht op basis van de Geneefse Conventie en Aanvullende Protocollen nog wel actueel als het gaat om cyber, gezien het feit dat daarin pas sprake is 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, en dat een niet-internationaal gewapend conflict alleen kan plaatsvinden binnen een staat? Deelt u de mening dat dat niet lijkt te volstaan als het gaat om cyber?

Daar waar er sprake is van een gewapend conflict in de zin van het humanitair oorlogsrecht, vallen activiteiten van strijdende partijen in het digitale domein onder de werking van het oorlogsrecht. Bij gewapende conflicten die beginnen in het digitale domein of uitsluitend worden gevoerd in het digitale domein kunnen de bestaande regels van het oorlogsrecht worden toegepast.

18
Waarom bent u van mening dat een cyberverdrag niet nodig is?

Evenals het AIV/CAVV advies plaatst het kabinet vraagtekens bij de noodzaak tot en haalbaarheid van een algemeen cyberverdrag. Ten aanzien van de grondslagen voor het gebruik van geweld biedt het bestaand internationaal recht voldoende houvast. Afspraken over het tegengaan van proliferatie van cyberwapens zou vanwege het karakter daarvan niet of nauwelijks te verifiëren zijn.

Daarnaast is het risico aanzienlijk dat een dergelijk verdrag een stap terug zou betekenen ten aanzien van bepalingen in de Conventie van Budapest, dat voorziet in strafrechtelijke samenwerking en vervolging tussen landen in geval van cyberincidenten.

Partijen die op dit moment in internationaal verband een cyberverdrag nastreven, hanteren andere uitgangspunten dan Nederland en gelijkgestemden ten aanzien van een open en vrij toegankelijk internet. Het risico bestaat dat een dergelijk verdrag voor meer controle over burgers zou worden gebruikt. Het kabinet acht dit onwenselijk.

19
Draagt Nederland bij aan de discussie die op dit moment door diplomaten gevoerd wordt over het in VN-verband afspreken van een equivalent van de reeds bestaande «nuclear arms control» voor cyberspace, een soort internationale gedragscode voor informatiebeveiliging?

De door Rusland, China, Tadzjikistan en Oezbekistan voorgestelde *code of conduct* voor informatiebeveiliging bevat veel elementen die Nederland en gelijkgestemden onwenselijk achten. Hierover vindt in verschillende internationale fora intensief contact plaats. Onder meer in het kader van de *Freedom Online* coalitie die door Nederland is geïnitieerd.

Overeenstemming over een formele *code of conduct* wordt niet snel verwacht. Daarom is de inzet eerst te komen tot praktische vertrouwenwekkende maatregelen. Hieraan wordt onder meer gewerkt in OVSE-verband. Nederland benadrukt in deze discussie, naast het belang van een open internet, de noodzaak tot het betrekken van de private sector. Maatregelen op het gebied van *cyber security* die geen draagvlak hebben onder private partijen, zullen naar verwachting weinig zoden aan de dijk zetten.

Nederland is geen lid van de zogenaamde VN *Group of Governmental Experts* (15 landen) die in 2012 en 2013 zal overleggen over de bestaande en mogelijke dreigingen op het gebied van *information security* en mogelijkheden tot samenwerking, maar staat wel in nauw contact met gelijkgestemden landen in deze groep.

20
Gaat u op korte termijn stappen ondernemen om te bezien met welke landen Nederland zou kunnen gaan samenwerken ten behoeve van een gezamenlijke ontwikkeling van een doctrine en opbouw van capaciteiten, gezien het feit dat grenzen in het digitale domein andere dimensies kennen, dat daar geen grenzen zijn in de traditionele zin?

In internationaal verband zal Defensie samenwerking zoeken met staten die een vergelijkbare ambitie en aanpak als Nederland voorstaan en die wat ontwikkeling betreft op vergelijkbaar niveau opereren. In eerste instantie richt deze samenwerking zich op NAVO-bondgenoten. Doel van de samenwerking zal in eerste instantie gericht zijn op het uitwisselen van kennis. In een later stadium zal ook worden bezien wat de mogelijkheden zijn tot het gezamenlijk ontwikkelen van middelen en technieken en het gezamenlijk inrichten van capaciteiten. Op dit moment zijn al contacten gelegd met onder andere het Verenigd Koninkrijk, de Verenigde Staten, Australië, België, Duitsland, Frankrijk, Noorwegen, Zweden en Estland.

21
Volgt u de aanbeveling van de AIV/CAVV om een onafhankelijk onderzoek naar de omvang van digitale dreiging in EU- en NAVO- verband te initiëren? Zo nee, waarom niet?

Nederland zal in EU- en NAVO-verband blijven streven naar een diepgaand en gedeeld inzicht in de dreiging. Hiervoor is het van belang dat de EU en de NAVO intensief samenwerken waarbij onder meer de informatie-uitwisseling op dit terrein tussen beide organisaties moet worden geïntensiveerd. Het Cybersecuritybeeld Nederland (CSBN) zal bijdragen aan het versterken van het gemeenschappelijk zicht op dreigingen.

22
Hoe wilt u de uitbreiding van de Europese dual-use verordening implementeren, waarvoor u pleit in het kader van het belang dat u eraan hecht dat bedrijven hun verantwoordelijkheid nemen voor de uitvoer van technologie die zowel goed- als kwaadschiks kan worden gebruikt door overheden? Hoe kan bewezen worden dat materiaal gebruikt zal worden voor cyberaanvallen?

Het is de primaire verantwoordelijkheid van bedrijven zelf te weten met wie ze zaken doen en voor welke doeleinden. Aangezien zelfregulering niet helemaal waterdicht is, omdat bedrijven immers niet alles weten wat de overheid kan weten, spant Nederland zich in Europees verband in om van gevalt tot geval in te kunnen grijpen door een vergunningplicht op te leggen voor bepaalde technologieën.

Ingrijpen geschiedt op basis van informatie van inlichtingendiensten, partnerlanden en bedrijven zelf. Het eindgebruik van deze *dual-use* goederen is moeilijk te bewijzen, daarom vindt de beoordeling plaats op basis van risicoanalyse. Bij een onacceptabel risico op ongewenst eindgebruik, bijvoorbeeld voor het schenden van mensenrechten, zal de exportvergunning worden geweigerd.

Voor Iran en Syrië, waar de regimes bekend staan om het notoir volgen en blokkeren van internetactiviteiten, is mede op Nederlands verzoek in het EU-sanctieregime, in plaats van een vergunningplicht, een verbod op de uitvoer van bepaalde technologieën naar deze landen opgenomen.

23
In hoeverre wordt de informatie-uitwisseling met de EU op het gebied van cyber bemoeilijkt door bijvoorbeeld de kwestie Turkije-Cyprus?

Nederland spant zich in voor praktische samenwerking tussen de EU en NAVO op het gebied van *cyber security*. De samenwerking tussen NAVO en EU ligt ook op het gebied van *cyber security* gevoelig.

Wel zijn er informele contacten over de wederzijdse activiteiten op het gebied van cyber security tussen de twee organisaties. Plannen van de beide organisaties op het gebied van capaciteitsontwikkeling kunnen worden geagendeerd in de zogeheten NAVO-EU capaciteitengroep. Bovendien kan onderling informatie worden uitgewisseld tussen landen die lid zijn van de EU dan wel de NAVO.

24
Kunt u nader ingaan op de toetreding van Nederland tot het Cooperative Cyber Defense Centre of Excellence van de NAVO? Welke voordelen biedt dit? Op welke wijze worden de krachten gebundeld, informatie uitgewisseld en de kennispositie van Nederland versterkt?

De toetreding tot het *Cooperative Cyber Defense Centre of Excellence* (CCD COE) is een van de maatregelen tot nauwere internationale samenwerking. Door het CCD COE voert onderzoek uit en draagt bij aan het versterken van de cybercapaciteiten van de NAVO. Door het toetreden kan Nederland bijdragen en richting geven aan onderzoeken. Uiteraard is daarvoor uitwisseling van kennis en standpunten noodzakelijk. Daarnaast verzorgt het CCD COE opleidingen en trainingen. De toetreding tot het CCD COE geeft gegarandeerde plaatsen voor hoogwaardige opleidingen.

25
Hoe gaat u de intensievere informatie-uitwisseling bevorderen, die Nederland heeft bepleit en waarvan de NAVO noodzaak onderkent?

De NAVO heeft het versterken van de informatie-uitwisseling als doelstelling opgenomen in het beleid en het bijbehorende actieplan. Naast het volgen van relevante ontwikkelingen door de NAVO zelf is de inbreng vanuit individuele landen van groot belang om tot een helder dreigingsbeeld te komen. Nederland zal hier in NAVO-verband op blijven aandringen.
Ook wordt gewerkt aan een intensivering van de samenwerking met partnerlanden die over waardevolle kennis op dit terrein beschikken.