Besluitvorming bij cyberoperaties

De oprichting van het Defensie Cyber Commando markeert een stap in de militaire ontwikkeling in het digitale domein. De regering beschikt vanaf eind 2015 over dit digitale militaire vermogen. Bij dit vermogen horen niet slechts capaciteiten, maar ook conceptuele en mentale componenten. Een capaciteit is immers nutteloos als de wil om deze in te zetten ontbreekt en als besluitvormingsprocessen onbekend zijn. In deze bijdrage analyseren en beschrijven we de politieke besluitvorming voor en de parlementaire informatieverstrekking over de inzet van deze cybercapaciteiten.

Prof. mr. Paul Ducheine, brigade-generaal van de Militair Juridische Dienst
*Ing. Kraesten Arnold BSc, luitenant-kolonel van de Koninklijke Luchtmacht**

Met het 'virtuele startschot' voor de oprichting van het Defensie Cyber Commando (DCC) op 25 september 2014 gaf minister Hennis-Plasschaert verder invulling aan de Defensie Cyber Strategie die haar voorganger in juni 2012 op de Nederlandse Defensie Academie lanceerde.[1] In die strategie trokken drie van de zes speerpunten de meeste aandacht. Het betrof de trits defensief – offensief – inlichtingen: de versterking van de digitale weerbaarheid van Defensie (defensief); de ontwikkeling van het militaire vermogen om cyberoperaties uit te voeren (offensief); en de versterking van de inlichtingenpositie in het digitale domein (inlichtingen).[2]
Terwijl defensieve maatregelen en de versterking van de digitale inlichtingencapaciteit van de MIVD al waren gestart,[3] moest het 'militaire vermogen' (onder te brengen in het DCC) dus wachten op een startschot. Hoewel deze operationele cybercapaciteit pas eind 2015 operationeel inzetbaar zal zijn, moet een aantal kwesties op voorhand worden aangepakt en opgelost. In het Algemeen Overleg inzake Digitale Oorlogvoering kwamen deze kwesties (uiteraard) aan de orde.[4]
Veel vragen gingen over de legitimiteit van cyberoperaties. Dat was niet verrassend, gelet op de aanleiding van het overleg: het gezamenlijke advies van de Adviesraad Internationale Vraagstukken en de Commissie van Advies voor Internationale Vraagstukken uit 2011[5] en de daarop volgende regeringsreactie(s).[6]

* Paul Ducheine is hoogleraar Cyber Operations aan de Nederlandse Defensie Academie en bijzonder hoogleraar Military Law of Cyber Operations & Cyber Secruity aan de Universiteit van Amsterdam. Kraesten Arnold is plaatsvervangend Commandant Task Force Cyber/Defensie Cyber Commando (i.o.). De auteurs danken kolonel dr. Joop Voetelink voor zijn suggesties.

1 *Kamerstukken II 2011-12*, 33 321, nr. 1, Defensie Cyber Strategie (hierna: DCS) 1.
2 DCS, 3.
3 Onder meer de uitbreiding van het Defensie Computer Emergency Response Team (DefCERT) respectievelijk via een samenwerkingsverband met de AIVD, de Joint Signals Intelligence Cyber Unit (JSCU).
4 *Kamerstukken II 2013–14*, 33 321, nr. 4 (AO Defensie Cyber Strategie) dd 26 maart 2014. Hierna: het AO-verslag.
5 Adviesraad Internationale Vraagstukken en de Commissie van Advies voor Internationale Vraagstukken (2011), *Digitale oorlogvoering* (advies no. 77/22), zie: www.aiv-advice.nl en *Kamerstukken II 2011-12*, 33 000 X, nr. 68. Hierna: het AIV/CAVV-advies.
6 *Kamerstukken II 2011-12*, 33 000 X, nr. 79. En de vervolgbrieven *Kamerstukken II 2011-12, 33 000 X, nr. 99 en Kamerstukken II 2013-14*, 33 321, nr. 3.

FOTO ANP, V. KUYPERS

Het startschot voor het Defensie Cyber Commando: hoewel het pas eind 2015 operationeel inzetbaar zal zijn, moet een aantal kwesties, waaronder de legitimiteit van cyberoperaties, op voorhand worden aangepakt

Het AIV/CAVV-advies ging over twee hoofdvragen: hoe verhouden (militaire) cyberoperaties zich met de rechtsgrondslagen voor militaire operaties en hoe past het humanitair oorlogsrecht als rechtsregime op de uitvoering van militaire cyberoperaties.[7] In haar reactie op het advies nam de regering de bevindingen en adviezen in algemene zin over.[8]

Deze aspecten van legitimiteit – de rechtsgrondslagen (bijvoorbeeld zelfverdediging) en de rechtsregimes (bijvoorbeeld oorlogsrecht) voor cyberoperaties – zijn in dit tijdschrift reeds beschreven.[9] Waar tot nu toe weinig aandacht voor bestond, maar wat in het AO ruimschoots aan de orde kwam, zijn de vragen naar de (politieke) besluitvorming en de parlementaire informatievoorziening.[10] Of: wie bepaalt of er sprake is van een cyberaanval op Nederland?[11] En: wie informeert wie?[12] En uiteraard ook: wie controleert wie?[13] Deze terechte vragen zijn tot nu toe niet uitgebreid behandeld.[14]

Doel

In deze bijdrage analyseren en beschrijven we daarom de politieke besluitvorming voor en de parlementaire informatieverstrekking over de inzet van cybercapaciteiten. We gaan er van uit dat de regering vanaf 2016 naast reguliere en speciale militaire eenheden ook cybercapaciteiten ter beschikking heeft.[15]
Onze focus ligt daarbij op expeditionaire operaties binnen de volle breedte van de drie hoofdtaken. De ondersteuning van civiele autoriteiten in het binnenlandse domein valt buiten het bereik van dit artikel.
De minister van Defensie hanteerde in de Kamerbrief over offensieve cybercapaciteiten het uitgangspunt dat 'Cybercapaciteiten integraal deel uit [zullen] maken van het totale militaire vermogen van de Nederlandse

7 Voor een overzicht van de totale adviesaanvraag: zie AIV-CAVV-advies, Bijlage 1.
8 *Kamerstukken II 2011-12*, 33 000 X, nr. 79.
9 P.A.L. Ducheine & J.E.D. Voetelink, 'Cyberoperaties: naar een juridisch raamwerk', in: *Militaire Spectator* 180 (2011) (6) 273-286.
10 AO-verslag, 13.
11 Kamerlid Eijsink: 'Interessant is natuurlijk de vraag wie bepaalt wanneer een cyberaanval als een gewapende aanval kan worden beschouwd'. AO-verslag, 13.
12 AO-verslag, 19.
13 *Kamerstukken II 2013–14*, 33 321, nr. 4, blz. 3, 10.
14 Voor een korte omschrijving: AO-verslag, 12-13.
15 Speciale eenheden: het Korps Commandotroepen en delen van het Korps Mariniers. Deze speciale eenheden kunnen zowel Speciale Operaties als reguliere operaties uitvoeren. In het eerste geval geldt een afwijkend besluitvormingstraject.

krijgsmacht. […] De planning en uitvoering van operaties in het cyberdomein komen grotendeels overeen met die van traditionele militaire operaties.'[16] Ons uitgangspunt is dat cybercapaciteiten weliswaar relatief nieuw zijn in het totale spectrum van militair vermogen, maar dat de invoering zoveel mogelijk aansluit bij gangbare procedures, doctrines en ideeën over commandovoering.

Opbouw artikel

Voor een krijgsmacht die haar rol als 'zwaardmacht in het digitale domein' opeist,[17] is het essentieel het doel van deze zwaardmacht helder te hebben. Daartoe presenteren we allereerst de grondwettelijke doelomschrijving van de krijgsmacht, die immers leidend zal moeten zijn voor *alle* militaire inspanningen. Aansluitend staan we kort stil bij de hoofdtaken van de krijgsmacht. Daarna beschrijven we de belangrijkste actoren bij de besluitvorming over militaire inzet, regering en parlement en wordt hun onderlinge rolverdeling geanalyseerd. De grondwettelijke doelomschrijving is namelijk leidend voor de besluitvormingsprocedures voor militaire operaties.[18]

Vervolgens analyseren we de procedures zelf. Ieder van deze besluitvormingstrajecten leiden we in met een fictief scenario voor een expeditionaire cyberoperatie.

We beschrijven achtereenvolgens: de artikel 100 Grondwet-procedure voor missies 'ter bevordering en handhaving van de internationale rechtsorde' en de procedure voor (bondgenootschappelijke) verdediging. Vervolgens staan we kort stil bij de expeditionaire bescherming van vitale 'belangen van het Koninkrijk' en missies waarbij de grondwettelijke doelstellingen overlappen. Als laatste zal de specifieke procedure voor expeditionaire 'speciale operaties' worden beschreven.

Grondwettelijke doelomschrijving

De Nederlandse krijgsmacht is een instrument van en voor onze democratische rechtsstaat, zo bepaalt artikel 97 van de Grondwet.
Dit instrumentele karakter blijkt uit de – drieledige – doelomschrijving (eerste lid) en de ondergeschiktheid van de krijgsmacht aan het civiele gezag (tweede lid):

'-1. 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, is er een krijgsmacht.
-2. De regering heeft het oppergezag over de krijgsmacht.'

De doelomschrijving is drieledig en vanwege de relatie met de hoofdtaken (zie hierna) hanteren we de volgorde:[19]

- de verdediging van het Koninkrijk, inclusief de bondgenootschappelijke verdediging;
- de handhaving en de bevordering van de internationale rechtsorde; en
- de bescherming van andere belangen van het Koninkrijk.[20]

Deze doelen kunnen samenvallen.[21] Overigens vallen de eerste twee doelen, de verdediging en de bevordering van de internationale rechtsorde, samen met een aantal belangen van het Koninkrijk.[22] Deze interpretatie strookt met de invulling van het begrip 'nationale veiligheid' uit de Nationale Veiligheidsstrategie (2007),[23] en uit de Internationale Veiligheidsstrategie uit 2013.[24]

16 *Kamerstukken II 2013–14*, 33 321, nr. 3, blz. 3.
17 Ontleend aan de titel van de toespraak van minister van Defensie H. Hillen op 27-6-2012 in Breda ter gelegenheid van de lancering van de DCS.
18 P.A.L. Ducheine, 'Parliamentary Involvement in the Netherlands' Military Operations Abroad', in: S. Hardt, L. Verhey & W. van der Woude (Eds.), *Parliaments and Military Missions* (Groningen, Europa Law Publishing, 2012) 15-32.
19 P.P.T. Bovend'eert e.a., *Grondwet voor het Koninkrijk der Nederland, Tekst & Commentaar* (Deventer, Kluwer, 2004), 145, waarbij de auteur (Fleuren) de frase 'deze taak [sic] is drieledig' hanteert. Hij baseert zich op de opsomming zoals door de regering gebruikt in de Memorie van Toelichting, zie *Kamerstukken II 1996-97, 2*5 367, (R 1593), nr.3, blz. 3.
20 K*amerstukken II 1996-97*, 25 367, (R 1593), nr.3 (Memorie van Toelichting), 3.
21 Zie Adviesraad Internationale Vraagstukken (2004) *Nederland en Crisisbeheersing*, AIV-advies No. 34, maart 2004. Idem: *Kamerstukken II 2013–14*, 29 521, nr. 226.
22 E. Soetendaal, 'Boeiend en geboeid, enige beschouwingen over de wijziging van de defensiebepalingen in de Grondwet', in: *Militair Rechtelijk Tijdschrift*, Vol. XC (nr. 9), 1997, 285-297, 288. Idem: Ducheine, 'Parliamentary Involvement in the Netherlands' Military Operations Abroad', 20.
23 *Kamerstukken II 2006-07*, 30 821, nr. 1, Nationale Veiligheid (Strategie).
24 *Kamerstukken II 2012-13*, 33 694, nr. 1, Internationale Veiligheidsstrategie – Veilige wereld, veilig Nederland.

Hoewel de doelomschrijving ruim is, zal de krijgsmacht niet voor de bescherming van *alle* belangen van het Koninkrijk worden ingezet.[25] De krijgsmacht zal alleen bij dreiging tegen of daadwerkelijke aantasting van een de *vitale* belangen van de staat worden ingezet.[26] Het gaat om fysieke veiligheid, economische veiligheid, ecologische veiligheid, territoriale veiligheid, de internationale rechtsorde en de sociale en politieke stabiliteit. Deze zes vitale belangen maken deel uit van de Nationale en de Internationale Veiligheidsstrategie.

FOTO MCD

De krijgsmacht wordt ingezet bij dreiging tegen of aantasting van vitale belangen van de Nederlandse staat

Hoofdtaken

Defensie 'vertaalde' de drieledige grondwettelijke doelomschrijving in de *Defensienota 2000* naar de huidige drie hoofdtaken:[27]

- bescherming van de integriteit van het eigen en bondgenootschappelijk grondgebied (inclusief de Caribische Koninkrijksdelen);
- bevordering van de internationale rechtsorde en stabiliteit; en
- ondersteuning van civiele autoriteiten bij rechtshandhaving, rampenbestrijding en humanitaire hulp (zowel nationaal als internationaal).

De verschillen tussen grondwettelijke doelomschrijving en de hoofdtaken (uit de *Defensienota* 2000) maken duidelijk dat de 'derde hoofdtaak' restrictiever is geformuleerd dan de derde grondwettelijke doelomschrijving: 'bescherming van andere belangen van het Koninkrijk'.[28] Vanwege het beleidsmatige karakter van de *Defensienota* zal het duidelijk zijn dat de grondwettelijke tekst prevaleert indien de reikwijdte van die derde hoofdtaak discussie op zou leveren. Die discussie zal dan bovenal in het parlement worden gevoerd, waarbij de opvatting van de grondwetgever, regering en parlement, uiteindelijk bepalend zal zijn.

Besluitvorming over de inzet van de krijgsmacht, met en zonder cybercapaciteiten, wordt in het staatsrecht geregeld. Hoofdrolspelers zijn daarbij de regering en het parlement. Hoewel de ministers van Defensie, Buitenlandse Zaken en Algemene Zaken belangrijke actoren in de agendavorming en besluitvorming zijn, (her)kent het staatsrecht in deze kwestie deze kopstukken niet. Dat lot is ook de belangrijkste militaire adviseur van de minister van Defensie, tevens uitvoerder van de meeste missies, beschoren: de Commandant der Strijdkrachten (CDS). Vanwege de eenheid van regeringsbeleid en de constitutionele verhoudingen bezien we daarom de regering als collectief. Daarbij beschouwen we de relatie en verhouding met de controlerende macht: het parlement.

Hoofdrolspelers: regering en parlement

De verhouding tussen regering en parlement wordt beheerst door het geschreven én ongeschreven staatsrecht. In de normale staatkundige verhoudingen bestuurt ('regeert') de regering en controleert het parlement.

25 P.A.L. Ducheine, *Krijgsmacht, Geweldgebruik en Terreurbestrijding* (Nijmegen, Wolf Legal Publishers, 2008) 55 en *Handelingen I* 1997-98, 22, 3 maart 1998, 1064-1080; *Kamerstukken I 1999-2000*, 26 243 (R 1622), nr. 165a (memorie van Antwoord), 4-5.

26 Ducheine (2008) 20. Idem: Soetendal (1997) 288. Zie ook Nationale Veiligheidsstrategie en de Internationale Veiligheidsstrategie (hiervoor voetnoot 23 en 24).

27 *Kamerstukken II 1999-2000*, 26 800 X, nr. 46, blz. 41.

28 Zie hierover *Kamerstukken II 1996-97*, 25 367, (R 1593) nr.3 (Memorie van Toelichting) 3: 'Onder de bescherming van andere belangen van het Koninkrijk valt bij voorbeeld de militaire bijstandstaak (op grond van artikel 59 van de Politiewet 1993), de hulpverlening door militairen aan burgers in nood, de bijstandsverlening bij rampenbestrijding, zoals bij watersnoodrampen en bosbranden, en andere vormen van hulpverlening'.

Dit adagium kent twee gezichten. Ten eerste regeert de regering en niet het parlement, waarbij de regering als uitvoerende macht over executieve diensten beschikt, waaronder de krijgsmacht. Ten tweede schikt de regering in de controlerende functie van het parlement dat *ultimo* de belangrijkste regel van ons staatsrecht in kan roepen, namelijk de vertrouwensregel. Als het parlement, met name de Tweede Kamer, het vertrouwen in een minister of de regering opzegt, neemt deze in beginsel ontslag. Artikel 97, tweede lid van de Grondwet bevat een bepaling over de zeggenschap over de krijgsmacht: 'de regering heeft het oppergezag over de krijgsmacht'. De regering, praktisch gezien de ministerraad,[29] beschikt dus over het prerogatief de krijgsmacht in te zetten (of ter beschikking te stellen).[30]

Dit prerogatief kent in de constitutionele verhoudingen een passende tegenmacht in de vorm van het parlement. Het Nederlandse parlement beschikt over verschillende mogelijkheden de regering en de krijgsmacht, direct en indirect, te 'controleren'. Op de eerste plaats is het parlement samen met de regering grondwetgever en bepalen zij dus samen de defensiebepalingen in de Grondwet.[31]
Ten tweede is het parlement medewetgever bij gewone wetten, zoals de Politiewet 2012, waarin de taken van de Koninklijke Marechaussee zijn vastgelegd en waarin militaire bijstand aan de politie is geregeld. Het parlement beschikt ten derde over 'budgetrecht' doordat het de begrotingswetten van de regering goed moet keuren. Door goedkeuring te onthouden kan het regeringsbeleid beïnvloed worden. Ten vierde beschikt het over een informatierecht (art. 68 Grondwet), waardoor de regering normaliter op verzoeken tot inlichtingen moet reageren.[32]
Het parlement beschikt – ten vijfde – over het recht van enquête (art. 70 Grondwet). Ten zesde, kan het de regering via moties beïnvloeden. Via een motie van wantrouwen kunnen regering of ministers tot aftreden bewogen worden. Daar staat overigens tegenover dat de coalitiepartijen vanwege regeerakkoorden soms in hun bewegingsvrijheid worden beperkt.
Het (geschreven en ongeschreven)[33] staatsrecht bevat verder aanwijzingen voor de informatievoorziening en besluitvormingsprocedures voor regeringsbesluiten tot inzet (of ter beschikkingstelling) van de krijgsmacht. In de praktijk houdt dit in dat de regering, vrijwillig of verplicht, het parlement informeert en (informeel) consulteert. Daarbij speelt de idee dat expeditionaire inzet van de krijgsmacht draagvlak in de volksvertegenwoordiging en maatschappij vraagt, een belangrijke rol.[34]

Een mandaat van de VN-Veiligheidsraad voor cyberoperaties

FOTO VN

29 De regering bestaat formeel uit de Koning en de ministers. Vanwege de ministeriële verantwoordelijkheid voor de onschendbare Koning, worden beslissingen inzake de krijgsmacht genomen door de Ministerraad, dan wel een afvaardiging daarvan.

30 Vanwege de tekst van artikel 100 Grondwet bestaat onderscheid tussen inzetten en ter beschikking stellen.

31 Onder meer artikel 97 en 100 Grondwet.

32 Art. 68 Grondwet: '[…] waarvan het verstrekken niet in strijd is met het belang van de staat'.

33 Ongeschreven staatsrecht bevat de niet gecodificeerde regels, zoals het vertrouwensbeginsel.

34 A. Kristic *De Staten-Generaal en de inzet van de Nederlandse Krijgsmacht* (Deventer, Kluwer, 2012) (dissertatie Universiteit van Tilburg).

De wijze waarop die informatievoorziening voor expeditionaire operaties verloopt, verschilt echter per doelomschrijving en hoofdtaak. Gelet op de praktijk en de mate van detaillering zal de zogeheten artikel 100-procedure voor missies in het kader van de tweede hoofdtaak/doelomschrijving als eerste worden toegelicht. Daarna volgen de overige inzetopties. De analyse van de besluitvorming en informatievoorzieningsprocedures leiden we in met een fictief scenario dat de aanleiding vormt voor de betreffende inzet en de besluitvorming van cybercapaciteiten.

2e doelomschrijving/hoofdtaak: artikel 100-procedure

Scenario: mandaat VN-Veiligheidsraad

De aanleiding voor dit artikel-100 besluitvormingstraject demonstreren we met twee korte casus. Het betreft digitale activiteiten tegen de tegen de internationaal opererende terreurgroep Z@.

De VN-Veiligheidsraad heeft eerder geconcludeerd dat deze groep Z@ een 'threat to the international peace and security' in de zin van artikel 39 van het VN-Handvest vormt.[35] Dit is de opmaat naar de vervolgresolutie waarin de Veiligheidsraad 'all necessary means' autoriseert om Z@ te bestrijden in een afgebakende regio. Deze resolutie is de rechtsbasis voor een militaire inzet. Nederland wordt door een coalitie van staten benaderd om in 2016 bij te dragen met haar nieuwe 'niche-capaciteit' in de vorm van een cybertaakgroep. Deze taakgroep beschikt over enkele tactische cyberinstrumenten en over de kennis om een hoogwaardig strategisch cyberinstrument te ontwikkelen en in te zetten.

Inhoud

Artikel 100 van de Grondwet bepaalt sinds 2000 dat de regering in een aantal expeditionaire inzetopties ('een internationale crisisbeheersingsoperatie') het parlement zal informeren over een besluit tot 'inzet of het ter beschikkingstelling' van de krijgsmacht.[36] Daarbij spelen de volgende criteria een rol:

- de uitzending (of terbeschikkingstelling) van militaire eenheden geschiedt ter handhaving of bevordering van de internationale rechtsorde of voor humanitaire hulp tijdens een gewapend conflict;
- de militairen worden als eenheid uitgestuurd; en
- de uitoefening van de militaire taak impliceert ook wapengeweld of het risico daaraan te worden blootgesteld.[37]

In een aantal gevallen is de regering (tijdelijk) verschoond van haar informatieplicht, bijvoorbeeld bij Speciale Operaties (zie hierna).

35 Zie (fictieve) Resolutie 2270 van de VN-Veiligheidsraad (15 augustus 2015).

36 Artikel 100 eerste lid luidt: '-1. De regering verstrekt de Staten-Generaal vooraf inlichtingen over de inzet of het ter beschikking stellen van de krijgsmacht ter handhaving of bevordering van de internationale rechtsorde. Daaronder is begrepen het vooraf verstrekken van inlichtingen over de inzet of het ter beschikking stellen van de krijgsmacht voor humanitaire hulpverlening in geval van gewapend conflict'.

37 *Kamerstukken II 2013–14*, 29 521, nr. 226, blz. 1.

Naast deze informatieplicht voor de regering bezit het parlement sowieso over het informatierecht van artikel 68 Grondwet.[38] Dit betekent dat Kamerleden op ieder moment de regering om (extra) informatie kunnen vragen, ook voorafgaande aan of tijdens militaire missies waarover al dan niet via artikel 100 Grondwet aan het parlement informatie is verstrekt. Artikel 68 Grondwet heeft een ruimer bereik dan artikel 100 Grondwet, maar is anderzijds afhankelijk van het initiatief van het parlement.

De meningen over de betekenis van artikel 100 Grondwet zijn verdeeld

Instemmingsrecht?

De meningen over de betekenis van artikel 100 Grondwet zijn verdeeld. Enerzijds is er de opvatting dat het parlement materieel (qua inhoud) over een instemmingsrecht beschikt. Dat kan zo gezien worden doordat – nadat de regering het parlement over een besluit tot uitzending heeft geïnformeerd – de regering draagvlak voor haar besluit in het parlement probeert te krijgen. Hierdoor krijgt het parlement 'speelruimte' om regeringsbesluiten te beïnvloeden. De regering voedt die ruimte door vooraf de mening van coalitie- en oppositiepartijen te 'peilen' en 'in te spelen' op het beschikbare draagvlak door bijvoorbeeld de troepensamenstelling te wijzigen, risicovolle gebieden of taken uit te sluiten et cetera. Ook moties (waarin bijvoorbeeld om aanpassing wordt gevraagd) passen in dit beeld. De regering meldt hierover zelf:

> 'Dit betekent dat elk van beide Kamers tijdig beschikt over inlichtingen inzake het genomen besluit hetgeen ertoe kan leiden dat er een debat wordt gevoerd waarin moties kunnen worden aangenomen. Van dergelijke moties zal de regering zich ernstig rekenschap geven en zij zal daaraan niet lichtvaardig voorbij kunnen gaan. Het is dan niet uitgesloten dat de regering haar besluit en de uitvoering daarvan geheel of ten dele heroverweegt.'[39]

Anderzijds ligt de nadruk op het feit dat formeel, noch materieel (naar inhoud) sprake is van instemming van het parlement. Het parlement beschikt immers slechts over een formeel inlichtingenrecht.[40] Bovend'eert benadrukt bijvoorbeeld dat de regering zelfstandig kan en mag beslissen, dat eventuele moties van de Kamer niet uitgevoerd hoeven te worden en dat zelfs een motie van wantrouwen de bevoegdheid tot inzet van de krijgsmacht niet stuit.[41]

Procedure

Parlementair instemmingsrecht of niet, over het verloop van de informatie- en besluitvormingsprocedure bestaat consensus. Het traject loopt als volgt:[42]

- notificatiebrief. De regering meldt het parlement – na een verzoek van een internationale organisatie of op eigen initiatief – 'de wenselijkheid en mogelijkheid' van een Nederlandse bijdrage aan een crisisbeheersingsoperatie (ambtelijk) te onderzoeken;
- regeringsbesluit. Dit ambtelijke onderzoek – inclusief het Militair Advies van de CDS en de appreciatie van de MIVD – beziet alle potentiële militaire capaciteiten inclusief digitale (cyber) en mondt uit in een regeringsbesluit. Een negatief besluit wordt aan het parlement gemeld; bij een positief besluit informeert de regering het parlement conform artikel 100 Grondwet;
- artikel 100-brief. De regering licht haar besluit via de aandachtspunten van het Toetsingskader voorafgaande aan de inzet (of ter beschikkingstelling) toe.[43] Ook bij een verlenging of voortijdige beëindiging van

38 Art. 68 Grondwet luidt: 'De ministers en de staatssecretarissen geven de kamers elk afzonderlijk en in verenigde vergadering mondeling of schriftelijk de door een of meer leden verlangde inlichtingen waarvan het verstrekken niet in strijd is met het belang van de staat'.

39 *Kamerstukken I 1999-2000*, 26 243 (R 1622), nr. 165a (Memorie van Antwoord) 6.

40 *Kamerstukken II 2005-06*, 30 162, nr. 3 (Rapport Commissie van Baalen) 18.

41 P.P.T. Bovend'eert, 'De inzet van strijdkrachten zonder toestemming van de Staten-Generaal', in: *Nederlands Juristenblad* (2-10-1998) (35) 1594-2024, 1596.

42 Dit deel is een bewerking van P.A.L. Ducheine (2009) 'Verdieping Staatsrecht', in: P.J.J. van der Kruit (red.), *Handboek Militair Recht*, 2e herziene druk (Nijmegen, Wolf Legal Pubishers, 2009) 43-82,

43 Uitgezonderd Speciale Operaties, zie hierna.

FOTO ANP

De regering heeft het oppergezag, óók over militaire cyberoperaties

een uitzending, bij een wijziging van het mandaat of de taken, dan wel een wijziging van het gebied van verantwoordelijkheid (AOR) die gevolgen heeft voor het mandaat of de taken, volgt een nieuwe artikel 100-brief;

- parlementaire behandeling. Doorgaans agendeert de Tweede Kamer de behandeling van de artikel 100-brief, waarna een debat volgt. In dit debat staan in beginsel alle opties open. De regering kan vanwege moties, vragen of gebrek aan (voldoende) draagvlak haar besluit heroverwegen, aanpassen of desondanks doorzetten. Normaliter verwerft de regering de steun van het parlement (in de derde termijn): in de volksmond heet dit dat het parlement 'instemt' (sic) met de missie;
- na de parlementaire behandeling informeert de regering de organisatie die, of het samenwerkingsverband dat de operatie aanstuurt. De reactie op het aanbod wordt aan het parlement meegedeeld;
- voortgang. Tijdens de voorbereiding van de uitzending en de uitvoering van de operatie informeert de regering het parlement geregeld over de voortgang en de ontwikkelingen, al dan niet via een Algemeen Overleg;
- tussentijdse evaluatie. Iedere derde woensdag in mei kan het parlement beschikken over een tussentijdse evaluatie (van de ministers van Defensie en van Buitenlandse Zaken) van de lopende operaties waaraan Nederlandse militaire eenheden deelnemen;
- eindevaluatie. Na beëindiging van de Nederlandse inzet wordt een eindevaluatie aan het parlement aangeboden (en besproken), waarbij zowel de militaire als de politieke aspecten aan de orde komen;
- post-missie beoordeling. Sinds kort verstrekt de regering in bepaalde gevallen[44] ook een post-missie beoordeling waarin de effecten van de Nederlandse deelname aan artikel 100-missies vijf jaar na beëindiging van de missie worden beoordeeld. De post-missie beoordeling richt zich op de ontwikkelingen in het missiegebied na de beëindiging van de Nederlandse deelname en op de nog waarneembare effecten van de Nederlandse inzet.[45]

44 In de eindevaluatie van Nederlandse bijdragen aan artikel 100-missies zal worden aangegeven of er een post-missie beoordeling zal worden uitgevoerd.

45 Zie *Kamerstukken II 2011-12*, 29 251, nr. 191 en *Kamerstukken II* 2012-13, 29 251, nr. 195.

Toetsingskader
De ambtelijke voorbereiding van het regeringsbesluit, de artikel-100 brief (en eventueel het parlementaire debat), volgen de gezichtspunten uit het *Toetsingskader voor uitzending van militaire eenheden ten behoeve van internationale operaties*.[46] Dit beleidsmatig vastgelegde Toetsingskader dient twee doelen, namelijk de kwaliteit van de besluitvorming waarborgen en het toetsbaar (controleerbaar) maken van regeringsbesluiten:

> 'Het is nadrukkelijk bedoeld voor de besluitvorming van de regering en het overleg daarover met het parlement als het gaat om uitzending van militaire eenheden die in de uitoefening van hun taak wellicht ook wapengeweld zullen moeten toepassen of het risico lopen daaraan te worden blootgesteld'.[47]

Het Toetsingskader bevat een reeks aandachtspunten die, per geval, worden gebruikt om een weloverwogen militair en politiek oordeel te vellen over Nederlandse deelneming aan crisisbeheersingsoperaties.[48] Het is een opsomming van overwegingen die per missie een ander gewicht hebben. De aandachtspunten zijn bovendien geen absolute grootheden: ze hebben een relatief gewicht en worden vaak kwalitatief ingevuld. Het Toetsingskader vormt dus géén lijst met bindende voorwaarden die achtereenvolgens afgewerkt moet worden voordat een besluit kan worden genomen.[49]

Interessante aandachtspunten zijn bijvoorbeeld de gronden voor de missie, inclusief rechtsbasis en mandaat voor de operatie, de haalbaarheid/effectiviteit, de invloed en de risico's.
Bij haalbaarheid komt het vereiste militaire vermogen, waaronder 'de omvang, de samenstelling, de uitrusting en de bewapening van de militaire eenheden' aan de orde.[50] Samenstelling, uitrusting en bewapening dekt ook eventuele cybercapaciteiten af, zo blijkt:

> 'Dat betekent dat cybercapaciteiten een aanvulling vormen op de bestaande militaire capaciteiten en daarmee geïntegreerd worden ingezet. Dit betekent ook dat bij de planning en de voorbereiding van operaties ook het digitale domein wordt meegenomen. Daar waar artikel 100 van toepassing is op de betreffende militaire inzet, geldt dat eveneens voor de betrokken cybereenheden'.[51]

Daarnaast wordt het operatieconcept en de geweldsinstructie bezien.[52]
Het Toetsingskader heeft formeel alleen betrekking op de zogeheten artikel-100 Grondwet missies, niet op de andere. Dat neemt niet weg dat het Toetsingskader en de aandachtspunten in de besluitvorming en beoordeling van andere missies ook een rol kunnen spelen (zie hierna).[53]

1e doelomschrijving/hoofdtaak: verdediging

Scenario: gewapende digitale aanval
Stel dat een NAVO-bondgenoot getroffen wordt door een digitale aanval op de – op dit moment toch al kwetsbare – energieproductie/elektriciteitsketen. Ondanks preventieve overheidsmaatregelen en campagnes valt het openbare leven na een onverwacht 'cascade'-effect stil.[54] Treinen, openbare verlichting, verkeersregulering, huishoudens en nutsvoorzieningen komen gedurende langere tijd zonder stroom te zitten. Ondanks beperkte openingstijden en transportmogelijkheden ontstaat al snel een stormloop op winkels en banken en het gebrek aan geld en levensmiddelen ontaardt in massale rellen waarbij plunderingen en vernielingen gemeengoed zijn. Hulpverlenings-

46 *Kamerstukken II 1994-95*, 23 591, nr. 5. Met updates in 2001, 2005, 2009 en 2014.
47 *Kamerstukken II 2000-01*, 26 454, nr. 7-8 (Eindrapport TCBU) 3.
48 *Kamerstukken II 2000-01*, 23 591 en 26 454, nr. 7, blz. 3.
49 *Kamerstukken II 2005-06*, 30 162, nr. 3 (Rapport Commissie van Baalen) 28.
50 *Kamerstukken I 2013-14*, 29 521, D, 17.
51 *Kamerstukken I 2013-14*, 29 521, D, 5-6.
52 *Kamerstukken I 2013-14*, 29 521, D, 17: 'De wijze van optreden («concept of operations»): de beschrijving van de wijze van optreden tijdens de missie gaat in op de militaire doelstellingen, de te bereiken eindsituatie, de taakstelling en de wijze van optreden van de militaire eenheid'.
53 *Kamerstukken II 2005-06*, 30 162, nr. 3 (Rapport Commissie van Baalen) 28. Zie ook het standpunt van de regering: *Kamerstukken I 2013-14*, 29 521, D, 3.
54 Paulo Shakarian, Hansheng Lei en Roy Lindelauf, 'Power Grid Defense Against Malicious Cascading Failure', in: 13th *International Conference of Autonomous Agnets and Multiagent Systems* (AAMAS-14), May 2014.
Via: www.usma.edu/nsc/SiteAssets/SitePages/Publications/POWER_GRID_DEF.pdf.

en ordediensten worden gehinderd waardoor de openbare orde en fysieke veiligheid niet gewaarborgd zijn. Politieke en sociale onrust neemt onacceptabele vormen aan. De Noord-Atlantische Raad, de recente NAVO-top in Wales in gedachten,[55] stelt dat indien aangetoond wordt dat de aanval 'has been directed from abroad', ze vanwege
de omvang en effecten van de gevolgen als een 'armed attack' in de zin van artikel V van het NAVO-Verdrag (en artikel 51 VN-Handvest) kan worden aangemerkt.
De Nederlandse regering instrueert de Permanente Vertegenwoordiger van Nederland bij de NAVO conform haar reactie op het AIV-advies *Digitale Oorlogvoering* dat op dit aspect ingaat:

> 'Het is [...] 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 […]'.[56]

Als uit digitale forensische analyse en andere informatiebronnen (van inlichtingendiensten) duidelijk wordt dat de digitale aanval door de groep Z@ vanuit het Midden Oosten is gelanceerd, komt de Raad opnieuw bijeen en stelt vast dat er daadwerkelijk sprake is van een 'gewapende aanval' in de zin van Artikel V van het NAVO-Verdrag. De bondgenoot, wetende dat ook Nederland troepen in het Midden-Oosten heeft, vraagt vervolgens om militaire steun voor een zelfverdedigingsreactie.

Procedure

Operaties in het kader van bondgenootschappelijke verplichtingen, zoals die van de NAVO en EU, vallen buiten het bereik van de artikel-100 Grondwet procedure (zie hiervoor). Dat geldt overigens ook voor een aantal andere inzetopties waarbij artikel 100 Grondwet is uitgesloten.[57] Met andere woorden, de regering heeft geen formele grondwettelijke *plicht* het parlement te informeren. Desondanks informeert de regering ook in deze gevallen het parlement vrijwillig, naar analogie van de artikel-100 procedure:[58]

> 'de regering [streeft] ernaar ten maximale, waar het kan vooraf, waar het moet achteraf, de Kamer te informeren. (...) Het gaat er vooral om dat de Kamer zoveel mogelijk analoog aan artikel 100 informatie wordt verschaft'.[59]

Samenstelling, uitrusting en bewapening dekt ook eventuele cybercapaciteiten af

Daarmee is de regering de toezegging nagekomen dat ze ook in gevallen buiten het kader van artikel 100 'het parlement zo snel en uitgebreid mogelijk zou proberen te informeren.'[60] De procedure die doorlopen wordt, is dus als volgt:

- notificatiebrief (mededeling over 'wenselijkheid en mogelijkheid' deelname);[61]
- regeringsbesluit na ambtelijk onderzoek (inclusief militair advies van de CDS en MIVD-appreciatie);

55 NATO Wales Summit Declaration: 'Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis'.
Zie: www.nato.int/cps/en/natohq/official_texts_112964.htm.

56 AIV & CAVV (2011), Digitale oorlogvoering (advies no. 77/22) 20. Zie: www.aiv-advice.nl.

57 Op dit soort operaties is echter het parlementaire informatierecht van artikel 68 Grondwet onverkort van toepassing. Het gaat dan om bijvoorbeeld individuele uitzendingen, civiele missies, humanitaire hulp et cetera.

58 *Kamerstukken II 2005-06*, 30 162, nr. 3 (Rapport Commissie van Baalen) 26.

59 *Handelingen II 2001-02*, 24, blz. 1767.

60 *Kamerstukken II 2000-01*, 23 591, nr. 8, blz. 5. Idem: *Handelingen II 2004-005*, 56, blz. 3661.

61 Zie bijvoorbeeld: *Kamerstukken II 2004-05*, 27 925, nr. 170.

- informatie per brief aan parlement;[62]
- parlementaire behandeling;
- informatie aan het bondgenootschap of het samenwerkingsverband dat de operatie aanstuurt;
- tussentijdse informatie tijdens de voorbereiding en de uitvoering van de operatie;
- tussentijdse evaluatie (derde woensdag in mei) van lopende operatie; en
- eindevaluatie.[63]

Feitelijk blijkt dat missies in het kader van de eerste hoofdtaak een vergelijkbaar besluitvormings- en informatievoorzieningstraject doorlopen als de artikel-100 operaties. Het verschil ligt in de formele aspecten: in het vrijwillige karakter van de informatieverstrekking, in het ontbreken van de letterlijke aanduidingen van 'artikel 100 Grondwet', en het feit dat de aandachtspunten van het Toetsingskader niet verplicht zijn in de besluitvorming.[64] Qua inhoud zijn er grote overeenkomsten.

3e doelomschrijving: beschermen vitale belangen

Scenario: digitale entering

Nederland beveiligt inmiddels enige tijd kwetsbare Nederlandse koopvaardijschepen buiten de Hoorn van Afrika voor Somalië. Hiervoor bestaat geen mandaat van de VN-Veiligheidsraad. Naast piraterijbestrijding ligt de militaire operatie voor de regering besloten in de bescherming van economische belangen van het Koninkrijk.[65] Sinds kort blijken nu grote en kwetsbare transport- en baggerschepen in Azië 'digitaal' te worden 'geënterd'. De Koninklijke Vereniging van Nederlandse Reders vraagt

62 Zie bijvoorbeeld: *Kamerstukken II 2001-02*, 27 925, nr. 24 en *Kamerstukken II 2004-05*, 27 925, nr. 159. Dit is anders als er sprake is van een 'speciale operatie'(zie hierna).

63 Zie bijvoorbeeld: *Kamerstukken II 2006-07*, 29 521, nr. 33, bijlage. Vooralsnog lijkt de post-missie beoordeling niet bij deze categorie missies te worden gebruikt.

64 *Kamerstukken I 2013-14*, 29 521, D, blz. 3.

65 *Kamerstukken II 2010-11*, 30 706, nr. 1, waarbij de regering de bescherming van de belangen van het Koninkrijk tot de eerste hoofdtaak rekent.

FOTO ANP

Voorzitter Netelenbos van de Koninklijke Vereniging van Nederlandse Reders heeft regelmatig gepleit voor een betere bescherming van kwetsbare Nederlandse koopvaardijschepen

bij monde van haar voorzitter, mevrouw Netelenbos, de regering met klem deze nieuwe dreiging te willen bezien en eventueel helpen pareren. Bij gebrek aan civiele capaciteit wordt Defensie benaderd met de vraag of het DCC een rol kan spelen.

Doelstelling

Naast de primaire verantwoordelijkheid die Defensie draagt voor bescherming van de vitale belangen territoriale veiligheid en internationale rechtsorde, is de krijgsmacht beschikbaar voor de bescherming van de overige vitale belangen. Het gaat dan om de sociale en politieke stabiliteit, economische veiligheid, ecologische veiligheid en fysieke veiligheid. De behartiging van deze belangen is doorgaans aan civiele autoriteiten toevertrouwd. Uit de Defensie Cyber Strategie en de ambities van Defensie blijkt dat cybercapaciteiten ook voor de derde hoofdtaak/doelomschrijving beschikbaar moeten zijn. Anders gezegd: ook cybercapaciteiten kunnen op verzoek van civiele autoriteiten in het buitenland worden ingezet om de vitale belangen van Nederland te behartigen. De inzet van *Vessel Protection Detachements* voor piraterijbestrijding en bescherming van de koopvaardij heeft model gestaan in onze analyse.

Procedure

De procedure verloopt naar onze mening als volgt:

- Verzoek. Het Nationaal Cyber Security Centre ontvangt of formuleert een verzoek voor de ondersteuning met militaire cybercapaciteiten;
- Regeringsbesluit. Na een militair advies van de CDS en een appreciatie van de MIVD kan de regering de krijgsmacht inzetten ter bescherming van andere (vitale) belangen van het Koninkrijk in het buitenland. De vorm waarin die inzet geschiedt, verschilt van geval tot geval. De inzet kan reguliere, speciale of cybereenheden omvatten;
- Informatie. Bij reguliere operaties, inclusief cybercapaciteiten, zal de regering het parlement informeren over dit besluit en daarbij relevante overwegingen. Bovendien verstrekt de regering periodiek informatie het een langlopende inzet betreft. [66]

Overlappende doelstellingen

Bij inzet (of ter beschikkingstelling) waarbij sprake is van overlappende doelstellingen – zowel zelfverdediging (eerste doelomschrijving) of de bescherming van vitale belangen (derde doelomschrijving) als handhaving en bevordering van de internationale rechtsorde (tweede doelomschrijving) – zal de regering de artikel 100-procedure hanteren.[67] Dit is bijvoorbeeld aan de orde bij zelfverdediging na een gewapende aanval waarbij de aanvallende militaire (cyber)capaciteit van de aanvaller wordt uitgeschakeld, waarbij deze actie tevens de internationale rechtsorde bevordert door die bedreiging voor 'international peace and security' te reduceren.

Speciale Operaties

Naast reguliere operaties (inclusief cyberoperaties) kan de regering ook besluiten speciale militaire operaties op te dragen die gekenmerkt worden door 'grote politiek-militaire risico's en de noodzaak tot strikte geheimhouding.'[68] Deze operaties worden meestal uitgevoerd door speciale eenheden (*special forces)* die zijn 'aangewezen, opgeleid en toegerust om onder bijzondere omstandigheden (geheimhouding, grote veiligheidsrisico's en zware fysieke inspanningen) opdrachten te vervullen.'[69] Het gaat hierbij om bijzondere inlichtingenverzameling, bijzondere aanhoudingen, aanvallen op geselecteerde doelen, militaire steunverlening aan bondgenoten, evacuatie van landgenoten uit levensbedreigende situaties en internationale terreurbestrijding.[70]

Scenario's: MH-17, losgeld en MIVD

Casus 1: Digitale bescherming onderzoek MH-17. Stel dat het onderzoek (en ter plekke verzamelen van bewijsmateriaal) van het neerstorten/-halen van het verkeersvliegtuig

66 Zie naar analogie: *Kamerstukken II 2010–11*, 32 706, nr. 1 en nr. 9.
67 *Kamerstukken II 2013–14*, 29 521, nr. 226.
68 *Kamerstukken II 1999-2000*, 26 800 X, nr. 46, blz. 1.
69 Idem.
70 *Kamerstukken II 2000–01*, 27 400 X, nr. 29, blz. 2.

MH-17 ernstig belemmerd zou zijn vanuit het buitenland. Daarbij worden digitale capaciteiten ingezet. Om het onderzoek onbelemmerd door te laten gaan besluit Nederland, in het geheim, extra beveiliging in te zetten, waaronder digitale capaciteiten van het DCC. Om succesvol te zijn en vanwege de politieke gevoeligheid wordt dit geheim gehouden.

Casus 2: Digitaal veiligstellen losgeld Somalië. De VN-Veiligheidsraad heeft met resolutie 2020 het gebruik van 'all means necessary' verlengd om piraterij in de Somalische territoriale wateren en op het grondgebied te bestrijden.

Cybercapaciteiten kunnen op verzoek van civiele autoriteiten in het buitenland worden ingezet om de vitale belangen van Nederland te behartigen

Nadat een reder losgeld heeft betaald voor één van zijn schepen en haar internationale bemanning, stelt de internationale troepenmacht Nederland de vraag of het bereid is via de inzet van cybercapaciteit het betaalde losgeld digitaal te volgen, én, zo zich dat losgeld binnen de Somalische jurisdictie bevindt, tevens digitaal veilig te stellen en terug te sluizen.

Casus 3: De CDS wordt verzocht een MIVD-operatie in het buitenland met militaire cybercapaciteiten te ondersteunen.

De eerste en derde casus zouden we toeschrijven aan de derde doelomschrijving, bescherming van vitale belangen van het Koninkrijk. De tweede casus houdt ook verband met de bevordering van de internationale rechtsorde en piraterijbestrijding.

Doelstelling

Speciale Operaties kunnen voor meerdere doelstellingen worden uitgevoerd, bijvoorbeeld voor de verdediging, voor bevordering en handhaving van de internationale rechtsorde, of voor de bescherming van andere vitale belangen van het Koninkrijk. Anders gezegd: Speciale Operaties kunnen zowel binnen de eerste, tweede en derde hoofdtaak/doelomschrijving worden opgedragen.

Procedure

De regering heeft uitgesproken 'het parlement overeenkomstig artikel 100 Grondwet lid 1 en 2 in te lichten over speciale militaire operaties op een wijze die recht doet aan de betrokkenheid van de Staten-Generaal bij het optreden van de krijgsmacht onder uitzonderlijke omstandigheden, de geldende constitutionele verhoudingen en de noodzakelijke vertrouwelijkheid waarmee speciale operaties zijn omkleed.'[71] Bij de tweede hoofdtaak/doelomschrijving biedt artikel 100 Grondwet de regering de mogelijkheid het parlement pas later of beperkt te informeren. Deze uitzondering is vervat in het tweede lid.[72] Dit gaat om

> '(nood)situaties, waarbij op zeer korte termijn tot de daadwerkelijke inzet moet worden overgegaan. Te denken valt voorts aan een militaire interventie die alleen zinvol kan zijn indien zij onaangekondigd en onder strikte geheimhouding geschiedt, bijvoorbeeld indien er sprake is van direct gevaar in levensbedreigende situaties en waarin met spoed of onder strikte geheimhouding moet worden gehandeld. In dergelijke gevallen – in acute noodsituaties – zal het voorafgaand verstrekken van inlichtingen onmogelijk kunnen zijn'.[73]

Als de regering een beroep doet op deze uitzondering, of als vanwege een andere doelstelling een speciale operatie de voorkeur geniet, volgt de regering een traject dat in separate Kamerbrieven is beschreven en toegelicht.[74] Deze procedure verloopt als volgt:

71 Idem, blz. 3.

72 Art. 100(2) Grondwet: 'Het eerste lid geldt niet, indien dwingende redenen het vooraf verstrekken van inlichtingen verhinderen. In dat geval worden inlichtingen zo spoedig mogelijk verstrekt'.

73 *Kamerstukken I 2013-14*, 29 521, D, blz. 2-3. Waarbij 'Een beroep op lid 2 van artikel 100 Grondwet nog niet [is] voorgekomen.'

74 *Kamerstukken II 1999-2000, 26 800* X, nr. 46 en *Kamerstukken II 2000-01*, 27 0400 X, nr. 29.

FOTO ANP

Ook over cyberoperaties moet verantwoording worden afgelegd (zoals na 'Irak')

- Instelling Ministeriële Kerngroep Speciale Operaties. In de eerste ministerraad na een regeringswissel (het constituerend beraad) stelt deze een ministeriële kerngroep speciale operaties (MKSO) in. Om voldoende draagvlak te verzekeren maakt van elke coalitiepartij tenminste één minister deel uit van de MKSO. In deze kabinetsperiode (2014) bestaat de MKSO uit de minister-president (VVD), vice-premier (PvdA) en de ministers van Defensie (VVD) en Buitenlandse Zaken (PvdA);
- Per speciale operatie bepaalt de MKSO – na ambtelijk advies (inclusief militair advies van de CDS en een appreciatie van de MIVD) – of een operatie zal worden opgedragen;
- De MKSO besluit ook of ook andere leden van de ministerraad bij de besluitvorming worden betrokken en op welk moment dat geschiedt;
- Ook beziet de MKSO hoe en wanneer het parlement (al dan niet conform artikel 100 Grondwet) wordt geïnformeerd, bijvoorbeeld beknopt vooraf aan de fractievoorzitters, of achteraf op hoofdlijnen.[75]

Sinds de inwerkingtreding van artikel 100 Grondwet in 2000 heeft de regering nog geen gebruik gemaakt van de uitzonderingsclausule van artikel 100 tweede lid Grondwet.[76] Voordien heeft de minister van Defensie minstens één keer een Speciale Operatie op hoofdlijnen aan het parlement gemeld.[77]

75 *Kamerstukken II 1999-2000*, 26 800 X, nr. 46, blz. 2.
76 *Kamerstukken I 2013–14*, 29 521, D, blz. 3.
77 Operatie Amber Star waarbij Nederland assisteerde bij de aanhouding van verdachten van oorlogsmisdaden in voormalig Joegoslavië. Zie: *Kamerstukken II 1997-98*, 22 181, nr. 193.

Gelet op de kenmerken van van cybercapaciteiten vermoeden we dat een deel van de inzet van cybercapaciteiten onder de noemer 'grote politiek-militaire risico's en de noodzaak tot strikte geheimhouding' zal vallen. Met andere woorden, de besluitvorming zal vaak bij de MKSO liggen, waarbij per geval een beknopt informatievoorzieningstraject zal volgen.

Conclusies

De alleszins terechte vraag naar de politieke besluitvorming en parlementaire informatievoorziening bij de inzet van cybercapaciteiten stond centraal in dit artikel. De beslissing tot inzet (en ter beschikkingstelling) van cybercapaciteiten berust in de alle gevallen bij de regering.

De regering beslist over de inzet van cybercapaciteiten in het buitenland, maar deze besluiten zijn aan parlementaire controle onderworpen

In alle gevallen zal de regering kennis nemen van het militaire advies van de CDS en de appreciatie van de MIVD. Daarnaast zal het parlement worden geïnformeerd; de manier waarop verschilt per doelomschrijving/hoofdtaak. Vanwege de staatsrechtelijke verhoudingen heeft het parlement daarbij feitelijk invloed op het regeringsbesluit. We stellen vast dat zich doorgaans een normaal besluitvormings- en informatievoorzieningstraject voltrekt. Dat maakt dus ook een normaal verantwoordingsproces mogelijk.
Over de inzet van cybercapaciteiten die als Speciale Operaties worden aangemerkt, besluit slechts een deel van de regering, namelijk de Ministeriële Kerngroep Speciale Operaties. Ook het informatievoorzieningstraject wijkt in deze situatie af.

De grondwettelijke doelomschrijvingen van de krijgsmacht volgend, hebben we de artikel 100-procedure voor de 'bevordering en handhaving van de internationale rechtsorde' als basisprocedure onderkend. De ambtelijke verkenning naar nut en noodzaak van inzet wordt voorafgegaan door een notificatiebrief van de regering aan het parlement. De verkenning zelf mondt uit in een negatief of positief regeringsbesluit. In dat laatste geval stuurt de regering het parlement een artikel 100 (Grondwet) brief. De aandachtspunten uit het Toetsingskader gelden als leidraad bij de ambtelijke verkenning, de besluitvorming en de artikel 100-brief. Het parlement agendeert zelf het overleg met de regering over het regeringsbesluit. Voor, tijdens en na uitzending verstrekt de regering, op verzoek of uit eigen beweging, informatie via tussentijdse evaluaties, een eindevaluatie of een post-missie beoordeling. De procedure voor de verdediging wijkt formeel af, maar vertoont hiermee veel inhoudelijke overeenkomsten. Dat geldt ook voor de expeditionaire bescherming van de andere vitale belangen van het Koninkrijk. Dit wijkt af bij speciale cyberoperaties die vanwege 'grote politiek-militaire risico's en de noodzaak tot strikte geheimhouding' als Speciale Operaties gelden. Het besluit tot inzet wordt dan door de Ministeriële Kerngroep Speciale Operaties genomen. Daarbij beziet deze Kerngroep in hoeverre en wanneer de rest van de regering wordt betrokken of geïnformeerd. De Kerngroep beslist ook hoe en wanneer het parlement wordt geïnformeerd.

In alle gevallen kan het parlement gebruik maken van normale controlemechanismes zoals vragen, overleg, moties en eventueel zelfs moties van wantrouwen of het recht van enquête. Kort en goed: hoewel de regering dus over de inzet van cybercapaciteiten in het buitenland beslist, zijn deze besluiten aan gebruikelijke parlementaire controle onderworpen. En zo hoort het ook in een democratische rechtsstaat waarbij de krijgsmacht haar taak als zwaardmacht in de volle breedte van de grondwettelijke doelomschrijving waar moet maken, ook in het digitale domein. ■