Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

33 321 Defensie Cyber Strategie

Nr. 3 **BRIEF VAN DE MINISTER VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 17 maart 2014

Tijdens de begrotingsbehandeling van het Ministerie van Defensie op 13 en 14 november jl. heb ik toegezegd u te informeren over de ontwikkeling van offensieve cybercapaciteiten van Defensie. Met deze brief voldoe ik aan deze toezegging.

Achtergrond

De ontwikkelingen in het cyberdomein gaan snel. Uit het derde Cybersecuritybeeld Nederland van (Kamerstuk 26 643, nr. 285, 3 juli 2013) en de tweede Nationale Cybersecurity Strategie (Kamerstuk 26 643, nr. 291, 28 oktober 2013) blijkt dat cyber in toenemende mate aandacht vraagt van alle betrokken spelers. Defensie beschouwt het digitale domein, naast land, lucht, zee en ruimte, als het vijfde domein voor militair optreden. Dit domein en de toepassing van digitale middelen als wapen of inlichtingenmiddel zijn onmiskenbaar sterk in ontwikkeling. Om de inzetbaarheid van de krijgsmacht te waarborgen en haar effectiviteit te verhogen, versterkt Defensie de komende jaren haar digitale weerbaarheid en het vermogen om cyberoperaties uit te voeren.

In 2012 is de Defensie Cyber Strategie aan de Kamer gestuurd (Kamerstuk 33 321, nr. 1). In het afgelopen anderhalf jaar zijn forse stappen gezet om de cybercapaciteiten van Defensie verder te ontwikkelen. Het zwaartepunt ligt in de eerste plaats bij de bescherming van netwerken, systemen en informatie evenals de uitbreiding van de inlichtingencapaciteit voor het digitale domein. Een ander speerpunt van de strategie is het ontwikkelen van het vermogen om offensieve cyberoperaties uit te voeren, onder andere door het inrichten van het Defensie Cyber Commando (DCC). In de nota «In het belang van Nederland» (Kamerstuk 33 763, nr. 1) heb ik aangekondigd dat het DCC versneld zal worden opgericht vanwege het toenemende belang van het digitale domein voor militaire operaties. In deze brief ga ik in op wat Defensie onder het digitale domein en offensieve cybercapaciteiten verstaat. Vervolgens licht ik de inzet van offensieve cybercapaciteiten in een militaire operatie toe en ga ik in op de

kst-33321-3
ISSN 0921 - 7371
's-Gravenhage 2014

stand van zaken van de ontwikkeling van offensieve cybercapaciteiten door Defensie.

Wat is het digitale domein?

De Nationale Cybersecurity Strategie duidt het digitale domein *(«cyberspace»)* aan als het geheel van digitale informatie, informatie-infrastructuren, computers, systemen, toepassingen en de interactie tussen informatietechnologie en de fysieke wereld waarover communicatie en informatie-uitwisseling plaatsvindt. Hiermee wordt dus niet alleen het internet bedoeld, maar ook alle niet met internet verbonden netwerken of andere digitale apparaten. Hierbij kan onder andere worden gedacht aan (hoog gerubriceerde) netwerken, maar ook aan de digitale systemen in voertuigen, fabrieken, vitale infrastructuren en sensor-, wapen- en commandovoeringsystemen.

Offensieve cybercapaciteiten

Defensie moet over de kennis en capaciteiten beschikken om ter ondersteuning van militaire operaties offensief te kunnen optreden in het digitale domein. Het gaat hierbij om het ontwikkelen van (kennis over) complexe en hoogtechnologische middelen en technieken die er specifiek op zijn gericht het eigen militaire vermogen te vergroten.

Offensieve cybercapaciteiten zijn de digitale middelen die tot doel hebben het handelen van de tegenstander te beïnvloeden of onmogelijk te maken. Deze capaciteiten kunnen in een militaire operatie worden ingezet ter ondersteuning van conventionele militaire capaciteiten. De inzet valt onder het desbetreffende mandaat en de geldende *Rules of Engagement*. De juridische kaders zijn niet anders dan die voor de inzet van conventionele middelen. Offensieve cybercapaciteiten onderscheiden zich van conventionele capaciteiten omdat ze vaak eenmalig inzetbaar zijn, specifiek voor één doel worden ontwikkeld en een beperkte levensduur hebben. Voor de ontwikkeling en inzet is veelal uitgebreide en langdurige inlichtingenvergaring noodzakelijk. Hoogwaardige (offensieve) cybercapaciteiten zijn nauwelijks vergelijkbaar met de wijd verbreide, relatief laagdrempelige instrumenten voor *cybercrime*. Het gaat veelal om complexe middelen waarvan de ontwikkeling kennisintensief en tijdrovend is, vooral omdat offensieve cybercapaciteiten zeer nauwkeurig moeten zijn om onbedoelde nevenschade te voorkomen. Dit laat onverlet dat in operaties ook kan worden gebruikgemaakt van minder complexe en mogelijk laagdrempelige cybercapaciteiten. Maar ook hiervoor is een goede inlichtingenpositie onontbeerlijk.

Offensieve cybercapaciteiten onderscheiden zich van cybermiddelen die worden ingezet op en ter bescherming van de eigen netwerken. Ook verschillen zij van digitale inlichtingenvergaring en van contra-inlichtingenactiviteiten. Bij de ontwikkeling van verschillende typen cybercapaciteiten (defensief, offensief en inlichtingen) moet wel de samenhang in het oog worden gehouden. Voor offensieve cyberoperaties en digitale inlichtingenvergaring worden veelal vergelijkbare technieken en methoden gebruikt, zij het met een ander oogmerk en binnen een ander wettelijk kader. Daarom is bij de ontwikkeling van offensieve cybercapaciteiten intensieve samenwerking met de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) noodzakelijk. Een uitdaging bij de inzet van offensieve middelen is dat de tegenstander op elk moment zijn eigen kwetsbaarheid kan ontdekken en beperken, en dat rekening moet worden gehouden met neveneffecten voor eigen systemen en die van bondgenoten of derden.

Offensieve cyber in militaire operaties

Cybercapaciteiten zullen integraal deel uitmaken van het totale militaire vermogen van de Nederlandse krijgsmacht. Zij kunnen conventionele militaire capaciteiten niet vervangen. De gecombineerde inzet van conventionele en cybercapaciteiten kan de effectiviteit van de totale militaire operatie, en dus het militaire handelingsvermogen, vergroten.

De planning en uitvoering van operaties in het cyberdomein komen grotendeels overeen met die van traditionele militaire operaties. In het algemeen begint een operatie met een verkennende fase waarin inlichtingen worden verzameld, onder andere over de digitale capaciteiten van een potentiële tegenstander. Vervolgens worden de kansen op het beoogde effect alsmede mogelijke risico's en neveneffecten geanalyseerd. Aan de hand hiervan worden de benodigde offensieve cybercapaciteiten ontworpen en ontwikkeld. Het gaat hierbij bijvoorbeeld om zeer complexe software die een vijandelijk wapensysteem of militaire communicatiesystemen zou kunnen uitschakelen. Het kan ook gaan om relatief eenvoudige programmatuur. Indien de opponent systemen aan het internet heeft gekoppeld, kan de operatie via deze weg worden ingezet. Zo niet, dan zal eerst op andere wijze toegang tot de desbetreffende digitale omgeving moeten worden verkregen. Vervolgens kan de fase van beïnvloeding, verstoring of destructie van het systeem van de tegenstander beginnen.

Voorafgaand aan de inzet van een offensieve cybercapaciteit is het belangrijk deze uitvoerig te testen op effectiviteit en ongewenste neveneffecten. Dit gebeurt in een afgeschermde digitale oefenomgeving.

Een doctrine voor het militair optreden in het digitale domein is vorig jaar op hoofdlijnen tot stand gekomen. Dit jaar wordt de doctrine verder uitgewerkt en getoetst tijdens oefeningen waarin cyber wordt geïntegreerd. Naar verwachting is de doctrine in de loop van 2015 gereed. De doctrine zal onder andere ingaan op het integreren van cybermiddelen in de operationele planning van militaire operaties. Zo zal het Defensie Cyber Commando (DCC) een cyberadviseur aan operationele commandanten ter beschikking stellen die adviseert over de mogelijkheden en kwetsbaarheden van de eigen systemen en de mogelijke wijze van inzet van cybermiddelen en de beoogde effecten. Dit kunnen effecten zijn in het gehele spectrum van militair optreden.

Stand van zaken

In augustus jl. heb ik u geïnformeerd over de stand van zaken van de Defensie Cyber Strategie (Kamerstuk 33 321, nr. 2). In die brief heb ik gemeld dat het zwaartepunt van de Defensie Cyber Strategie aanvankelijk ligt bij de defensieve cybercapaciteiten (de bescherming van netwerken, systemen en informatie) en de uitbreiding van de inlichtingencapaciteit voor het digitale domein. De ontwikkeling van deze twee componenten verloopt zoals voorzien en zal voortgaan in 2014 en 2015. Zoals gemeld in de nota «In het belang van Nederland» zal Defensie zich nadrukkelijker richten op het ontwikkelen van het vermogen cyberoperaties uit te voeren, onder andere door het versneld oprichten van het DCC.

Het DCC zal al in het derde kwartaal van 2014 beginnen met een stafelement, een afdeling operaties, een afdeling technologie en het Defensie Cyber Expertise Centrum (DCEC). De afdeling operaties zal de capaciteit opbouwen om eenheden gedurende de inzet en oefeningen te ondersteunen. De technische afdeling zal in nauwe samenwerking met de MIVD offensieve cybercapaciteiten ontwikkelen. In 2014 zullen die nog niet

beschikbaar zijn omdat de werving en opleiding van het hiervoor noodzakelijke personeel nog niet is afgerond.

Om de beoogde versnelling te bereiken zal de Taskforce Cyber opgaan in het DCC. Daarnaast wordt het DCC, binnen de huidige financiële kaders, uitgebreid met extra personeel, waaronder een aantal opleidingsplaatsen en functies voor cyberreservisten. Naar verwachting zal het DCC eind 2015 operationeel zijn.

Vervolg

Defensie zal dit najaar beginnen met de actualisering van de huidige Defensie Cyber Strategie. De actualisering behelst vooral de wijze waarop Defensie zich, in nauwe samenwerking met andere beleidsverantwoordelijken, verder zal ontwikkelen op het digitale terrein. Op 26 maart a.s. is een algemeen overleg voorzien over de Defensie Cyber Strategie en het advies van de AIV en de CAVV over digitale oorlogvoering. Dit overleg biedt de gelegenheid nader in te gaan op de stand van zaken van de ontwikkeling van cybercapaciteiten bij Defensie.

De Minister van Defensie,
J.A. Hennis-Plasschaert