Ministerie van Defensie

Ministerie van Defensie
Plein 4
MPC 58 B
Postbus 20701
2500 ES Den Haag
www.defensie.nl

Onze referentie
BS2024016116

Bij beantwoording, datum, onze referentie en onderwerp vermelden.

> Retouradres Postbus 20701 2500 ES Den Haag

de Voorzitter van de Tweede Kamer
der Staten-Generaal
Bezuidenhoutseweg 67
2594 AC Den Haag

Datum 30 mei 2024

Betreft Optreden Defensie in het cyberdomein

Geachte voorzitter,

De cyberdreiging gericht tegen Nederland en onze bondgenoten is onverminderd groot en vraagt om een slagvaardige Defensieorganisatie, nu en in de toekomst. Een organisatie die cyberdreigingen tijdig onderkent, hiertegen optreedt en anderen in staat stelt zich hiertegen te weren. In het verleden behaalde resultaten bieden geen garanties voor de toekomst want de dreiging in het cyberdomein is voortdurend en veranderlijk. Het verkleinen van de scheefgroei tussen de digitale dreiging en de weerbaarheid vraagt daarom doorlopend de aandacht van het kabinet, het bedrijfsleven, kennisinstellingen en de samenleving als geheel.

In deze brief zal ik mij conform verzoek van uw Kamer richten op de taakuitvoering van Defensie in het cyberdomein, in het bijzonder het optreden van de krijgsmacht in het zogenaamde grijze gebied tussen oorlog en vrede. In deze brief ga ik in op het dreigingsbeeld, de verschillende vormen van optreden van Defensie in het cyberdomein en schets ik een doorkijk van de mogelijke vervolgstappen zodat Defensie ook in de toekomst haar taken in het cyberdomein op effectieve wijze kan blijven uitvoeren. Tijdens het commissiedebat MIVD en Cyber van 12 juni as. wissel ik hier graag verder met u van gedachten over.

Dreigingsbeeld

Cyberactiviteiten lenen zich bij uitstek voor hybride conflictvoering onder de grens van een traditioneel gewapend conflict, in het zogenaamde grijze gebied tussen oorlog en vrede. Cyberdreiging in dit grijze gebied is dagelijkse realiteit, evenals de verdediging hiertegen. Statelijke en niet-statelijke actoren ontplooien op grote schaal cyberactiviteiten, waaronder spionage, verstoring van systemen en voorbereidingen voor sabotage. De Russische oorlog tegen Oekraïne, de activiteiten van Rusland op bondgenootschappelijk grondgebied en een steeds assertiever China als economische en militaire mogendheid hebben een aanzienlijke impact op de Europese veiligheid. De directe en indirecte effecten hiervan worden steeds zichtbaarder. De MIVD rapporteert dat naast Oekraïne ook NAVO-bondgenoten, de Nederlandse krijgsmacht, ministeries en ambassades in het afgelopen jaar doelwit zijn geweest van (onsuccesvolle) Russische cyberspionagepogingen.[1]De Russische cyberactiviteiten raken het NAVO-grondgebied, waaronder ook Nederlandse belangen, zoals Nederlandse organisaties

[1] Openbaar jaarverslag MIVD, 18 april 2024 (Kamerstuk 29924, nr. 260)

in hun ketenafhankelijkheid. Het Dreigingsbeeld Statelijke Actoren van de AIVD, MIVD en NCTV geeft aan dat Rusland zich onder meer richt op prepositie voor sabotage tegen kritieke infrastructuur.[2]

Optreden Defensie in het cyberdomein

Binnen het cyberdomein heeft Defensie drie aandachtsgebieden:

1) Cyberveiligheid: Defensie moet in het volledige conflictspectrum, inclusief de meest extreme omstandigheden, adequaat de eigen systemen, processen, operaties en personeel in het digitale domein kunnen beschermen. Dit is de doorvertaling van *force protection* in het cyberdomein.
2) Cyber als volwaardig operationeel domein: de krijgsmacht moet zowel eigenstandig als geïntegreerd militaire cybercapaciteiten in kunnen zetten, in multidomein operaties teneinde fysieke, informationele en cognitieve effecten te realiseren.
3) Cyberweerbaarheid van Nederland en bondgenoten: Defensie dient een rol te spelen in de cyberweerbaarheid van Nederland en bondgenoten. Defensie is daarin een solide partner in een maatschappijbrede aanpak om de gedigitaliseerde samenleving en het bedrijfsleven veilig te houden.

Capaciteiten van Defensie in het cyberdomein

Binnen Defensie zijn de cybercapaciteiten als volgt belegd:

1) inlichtingen en cyberweerbaarheid bij de Militaire Inlichtingen- en Veiligheidsdienst (MIVD);
2) cybersecurity bij het Defensie Cyber Security Centrum (DCSC);
3) militaire cyberoperaties bij het Defensie Cyber Commando (DCC).

Door samenwerking versterken de verschillende defensieonderdelen elkaar. Een integrale benadering is noodzakelijk om het gezamenlijke doel na te streven: Nederland en onze partners veilig houden.

1 inlichtingen bij de Militaire Inlichtingen- en Veiligheidsdienst (MIVD)

De inlichtingenfunctie van Defensie is primair belegd bij de MIVD. De MIVD doet samen met de AIVD onderzoek naar landen met een offensief cyberprogramma gericht tegen Nederland en Nederlandse belangen. De diensten delen inlichtingen met partners ten behoeve van cyberweerbaarheid en hebben tevens de bevoegdheid tot het verstoren van cyberoperaties, op grond van artikel 73 van de Wiv 2017. Door samen te werken met (inter)nationale partners draagt Defensie bij aan de maatschappelijke cyberweerbaarheid.

Met de inwerkingtreding per 1 juli a.s. van de Tijdelijke wet cyberoperaties kunnen de diensten sneller en beter optreden tegen dreigingen van landen met een offensief cyberprogramma tegen Nederland en onze bondgenoten. Zoals in de Hoofdlijnennotitie wijziging Wiv 2017[3] aangegeven zullen de resultaten van de aangekondigde monitoring van de uitvoering van de Tijdelijke wet worden betrokken bij de herziening van de Wiv 2017.

2 Cyberveiligheid (DCSC)

De cyberveiligheid van Defensie is primair ondergebracht bij het *Defensie Cyber Security Centrum* (DCSC). Het DCSC monitort samen met de *Security Operating Centers* (SOCs) van de Defensieonderdelen dagelijks netwerken van Defensie op cyberaanvallen. Bij het tegengaan van cyberincidenten heeft het DCSC onder meer de beschikking over *Cyber Rapid Response Teams* (CRRT) en voorziet het DCSC in het uitwisselen van relevante informatie tussen verschillende defensieonderdelen.

[2] Dreigingsbeeld Statelijke Actoren, 28 november 2022 (Kamerstuk 30821, nr. 175)
[3] Hoofdlijnennotitie wijziging Wiv 2017, 6 september 2023 (Kamerstukken 34588, nr. 92)

3 Cyber als operationeel domein (DCC)

Het Defensie Cyber Commando (DCC) voert militaire cyberoperaties uit en draagt zo bij aan de algehele slagkracht van de krijgsmacht. Militaire cyberoperaties kunnen zowel defensief, offensief of voorwaardenscheppend van aard zijn. Onderdeel van het DCC is het expertisecentrum op het gebied van cyber voor heel Defensie: het *Cyber Warfare and Training Centre* (CWTC).

Daarnaast speelt cyber bij militaire operaties in de andere vier operationele domeinen[4] ook een essentiële rol, bijvoorbeeld in de vorm van informatieoperaties, het vergaren van gevechtsinlichtingen en het ondersteunen dan wel bewerkstelligen van militaire effecten op strategisch, operationeel en tactisch niveau.

De krijgsmacht moet informatiegestuurd kunnen optreden binnen passende juridische kaders. Het succesvol kunnen uitvoeren van cyberoperaties vereist kennis over kwetsbaarheden binnen systemen van potentiele tegenstanders. Omdat het merendeel van de cyberoperaties bestaat uit inlichtingenactiviteiten, intensiveert Defensie de samenwerking tussen DCC en MIVD in de vorm van multidisciplinaire cyberteams die hun taken uitvoeren onder de Wiv 2017. Voor een gedegen inzet van de krijgsmacht voor militaire cyberoperaties is naast de doorontwikkeling van DCC en MIVD, ook de ontwikkeling van tactische capaciteit voor cyberoperaties en elektromagnetische activiteiten van de defensieonderdelen een prioriteit. Het is belangrijk dat onderdelen van de krijgsmacht, zoals bijvoorbeeld het Joint Intelligence, Surveillance, Target Acquisition & Reconnaissance Commando (JISTARC) zich goed kunnen voorbereiden op mogelijke inzet.

Doorontwikkeling van Defensie in het cyberdomein

In de huidige geopolitieke context wordt de samenleving geconfronteerd met hybride conflictvoering, onder de grens van een traditioneel gewapend conflict. Zoals tevens geconcludeerd door de commissie Brouwer is het van belang dat Defensie in dit grijze gebied tussen oorlog en vrede effectief en op basis van passende juridische kaders kan oefenen en optreden. Hierbij horen bevoegdheden afhankelijk van de taakstelling en de gereedstellingsstatus van Defensie. In dit licht heb ik opdracht gegeven de mogelijkheden voor een specifieke wettelijke grondslag te onderzoeken, bijvoorbeeld via een Wet op de gereedstelling. Het is aan een volgend kabinet om hierin verdere keuzes te maken.

Ook zet Defensie in op verdere versterking van de cybersamenwerking tussen de verschillende Defensieonderdelen en met de private sector. Deze aanpak als ook het belang van schaalbaarheid, door inzet van cyberreservisten, zijn onderdeel van de nieuwe Defensie Cyber Strategie (DCS) die eind dit jaar wordt verwacht.

Tot slot hecht ik eraan in deze brief te vermelden dat op dit moment wordt gewerkt aan een herziening van de Wiv 2017 waarbij de slagkracht van de inlichtingen- en veiligheidsdiensten en daarbij behorende effectieve waarborgen een belangrijk uitgangspunt is.

Hoogachtend,

DE MINISTER VAN DEFENSIE

drs. K.H. Ollongren

[4] Zee, Land, Lucht en Ruimte.