Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

33 321 Defensie Cyber Strategie

Nr. 8 **BRIEF VAN DE MINISTER VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 juli 2016

Inleiding

Het kabinet is uitgesproken voorstander van intensieve samenwerking tussen EU en NAVO op het gebied van cyber. Zowel EU als NAVO hebben meermaals uitgedragen de samenwerking waar mogelijk op te zoeken. Met deze brief, die ik uw Kamer heb toegezegd tijdens het Algemeen Overleg over de NAVO-ministeriële op 9 juni jl., informeer ik u mede namens de Minister van Buitenlandse Zaken over de samenwerking tussen EU en NAVO op het gebied van cyber.

De twee organisaties delen dezelfde waarden en staan voor dezelfde uitdagingen. De dreiging afkomstig uit het digitale domein is reëel en neemt toe. Daarnaast gebruiken steeds meer statelijke actoren cybermiddelen om geopolitieke doelstellingen te behalen en zijn niet-statelijke actoren eveneens steeds vaker actief in het digitale domein. Om deze dreiging het hoofd te bieden is het van groot belang dat de EU en NAVO samen werken aan cyberveiligheid. Zowel de EU-lidstaten als de NAVO-bondgenoten verwachten dat zij door beide organisaties worden ondersteund en dat er adequaat en op een gecoördineerde wijze wordt gehandeld in crisissituaties of situaties waarin een crisis juist voorkomen kan worden. Daarom ontplooien beide organisaties verschillende initiatieven om de kennis en capaciteiten op het gebied van cyber verder op te bouwen. Voor de EU zijn de ambities op het gebied van cyber opgenomen in het *Policy Framework on Cyber Defence* dat onderdeel uitmaakt van de *EU Cyber Security Strategy*. De NAVO heeft haar cyber-ambities in de *Enhanced NATO policy on Cyber Defence* opgenomen. Voor beide organisaties is zowel de versterking van eigen cyberverdediging als het streven naar internationale ordening in het cyberdomein relevant.

De taken en verantwoordelijkheden van EU en NAVO zijn verschillend, maar voor een deel wel complementair: de ordenende rol van EU en de veiligheidsbevorderende rol van NAVO kunnen elkaar versterken

kst-33321-8
ISSN 0921 - 7371
's-Gravenhage 2016

waardoor ook afzonderlijke ambities beter verwezenlijkt kunnen worden. Afstemming over het ontwikkelen van capaciteiten biedt de mogelijkheid om de schaarse capaciteiten zo effectief mogelijk in te zetten. Daarom hecht Nederland eraan dat de EU-NAVO verklaring die naar verwachting tijdens de Warschau-top zal worden aangeboden een stevige verwijzing bevat naar cybervraagstukken.

Initiatieven

Recent is een aantal bemoedigende initiatieven ontplooid om de samenwerking te versterken, waarbij met name de toegenomen informatie-uitwisseling als positief wordt ervaren. Er is ruimte om dit uit te bouwen, vooral wat betreft het nemen van gezamenlijke concrete gezamenlijke initiatieven en projecten. De Nederlandse vertegenwoordigers in de verschillende EU- en NAVO-fora en instanties zullen zich hier actief voor blijven inzetten. Het verder uitbreiden van de samenwerking wordt op een aantal gebieden echter bemoeilijkt door internationale politieke betrekkingen, zoals die tussen Cyprus (lid EU) en Turkije (lid NAVO). Desalniettemin is in de afgelopen periode op een aantal gebieden mogelijkheden geïdentificeerd tot verdere EU-NAVO-samenwerking, waarover ik u nader informeer.

Memorandum of Understanding (MoU) CERT-EU en NCIRC

Een van de voornaamste stappen om de samenwerking tussen EU en NAVO op het gebied van cyber te versterken is gezet met het ondertekenen van een MoU. Dit MoU betreft een technische overeenkomst tussen het *NATO Computer Incident Response Capability (NCIRC)* en het *Computer Emergency Response Team of the European Union (CERT-EU)* en is in februari jl. ondertekend. De overeenkomst maakt snellere informatie-uitwisseling tussen NCIRC en CERT-EU mogelijk met als doel betere preventie en detectie van en respons op cyberincidenten bij beide organisaties.

Verbinden gelijksoortige projecten

Om de effectiviteit te vergroten en doublures te voorkomen wordt in de praktijk getracht gelijksoortige projecten te verbinden door bijvoorbeeld projectleiders en/of lidstaten zowel EU- als NAVO-projecten te laten coördineren. Dit is al het geval bij het *Multinational Cyber Defence Education & Training*-project van de NAVO (MNCD E&T) en het vergelijkbare EU *Cyber Defence Education & Training*-initiatief. Portugal heeft voor beide initiatieven de projectmanager geleverd en streeft actief naar een zo effectief mogelijke integratie van activiteiten en ambities.

Een gelijksoortige constructie vindt plaats in relatie tot de ontwikkeling en koppeling van *cyber ranges*. Zo wordt de NAVO *cyber range* capaciteit gecombineerd met de bestaande *cyber range* van Estland. Estland is eveneens nauw betrokken bij het *cyber ranges* project van het *European Defence Agency* van de EU (EDA), waarbij een koppeling tussen de *cyber ranges* van de deelnemende landen is voorzien.

Meer geformaliseerd is de samenwerking tussen EDA en het *NATO Cooperative Cyber Defence Center of Excellence* (NATO CCD CoE). Tussen deze organisaties is recent een *liaison* overeenkomst gesloten en zijn er concrete ambities om op korte termijn gezamenlijk een cyberoefening voor te bereiden en uit te voeren. Voor een dergelijke oefening is reeds voor 2016 en 2017 budget gereserveerd.

Uitwisselen van kennis en ervaring

De nauwere samenwerking tussen EU en NAVO leidt daarnaast tot een intensievere uitwisseling van kennis en ervaring. Vooral de informele samenwerking op uitvoerend stafniveau is goed, waarbij er over veel onderwerpen met elkaar wordt gesproken. Dit leidt niet in alle gevallen tot daadwerkelijke gezamenlijke activiteiten, maar het is bemoedigend dat de organisaties elkaar goed weten te vinden en er informatie uitgewisseld wordt. Voorts is er regelmatig contact tussen de militaire staf van de EU en de internationale militaire staf van NAVO over wederzijds relevante ontwikkelingen op het gebied van Cyber Defence.

Een van de voorbeelden van de geïntensiveerde communicatie tussen EU en NAVO zijn de *Cyber Awareness Seminars* die regelmatig door het *European Security and Defence College* worden verzorgd en in samenwerking met het NATO CCD CoE worden voorbereid en uitgevoerd. Daarnaast zijn EU-organisaties uitgenodigd om een aantal NAVO cyberoefeningen bij te wonen. Dit heeft geleid tot *observer*-rollen bij de multinationale oefeningen *CyberCoalition* 2014 en 2015, de *Crisis Management Excercise* en de *Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise* (CWIX) in 2016. Ook Nederland heeft onder andere met het Defensie Cyber Commando bijgedragen aan deze oefeningen.

Tot slot is het cyberdomein een belangrijke factor in de toegenomen hybride dreigingen. Versterkte samenwerking tussen EU en NAVO zal beide organisaties beter in staat stellen om zich effectief voor te bereiden op en te verweren tegen hybride dreigingen en elkaar te ondersteunen als dit nodig is. In dit verband is met name de uitwisseling van kennis en informatie die leidt tot betere *situational awareness* van groot belang. De samenwerking op het cyberdomein heeft in dit kader prioriteit van zowel EU als NAVO.

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