Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

36 200 X Vaststelling van de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2023

Nr. 88

BRIEF VAN DE MINISTER EN STAATSSECRETARIS VAN DEFENSIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 6 juli 2023

Met deze brief geeft het kabinet uitvoering aan de motie van het lid Valstar c.s., ingediend op 17 november 2022 (Handelingen II 2022/23, nr. 24, item 12), inzake maatregelen, waaronder strafbaarstelling, om te voorkomen dat voormalige Defensiemedewerkers trainingen geven aan ten minste die landen die een offensief cyberprogramma tegen Nederland voeren (kenmerk 36 200 X, nr. 25). Vanwege de inhoudelijke samenhang bied ik gelijktijdig de beantwoording aan van de vragen, gesteld door het lid Valstar (VVD), over het artikel «Fini de chinoiser dans l'armée de l'air»? in het blad Le Canard enchaîné (Aanhangsel Handelingen II 2022/23, nr. 24, item 12).

Dreiging

In het algemeen zijn de inlichtingen- en veiligheidsdiensten waakzaam wat betreft dreigingen vanuit vreemde mogendheden. Specifiek is het voorkomen van ongewenste verspreiding van vertrouwelijke informatie, zoals de wijzen van trainen en optreden van de krijgsmacht, van groot belang voor de nationale veiligheid. Om die reden is het ook zeer onwenselijk dat voormalig Nederlands defensiepersoneel zou bijdragen aan het trainen van de strijdkrachten van landen die een mogelijke dreiging voor Nederland vormen.

Mogelijke maatregelen

Om het trainen door (voormalig) Nederlandse defensiepersoneel van strijdkrachten van landen die een mogelijke dreiging vormen voor Nederland tegen te gaan, zijn er momenteel twee soorten maatregelen. Ten eerste zijn er juridische maatregelen, waarbij de mogelijkheid van strafrechtelijke vervolging bestaat indien een voormalig defensiemedewerker een staatsgeheim prijsgeeft. Daarnaast zien preventieve maatre-

kst-36200-X-88
ISSN 0921 - 7371
's-Gravenhage 2023

gelen op het vergroten van het beveiligingsbewustzijn bij defensiemedewerkers en het versterken van hun morele kompas.
Er wordt op dit moment onderzocht of aanvullende maatregelen kunnen worden genomen, om het geven van trainingen te voorkomen. Uiteraard houden we nauw contact met bondgenoten, waaronder binnen de NAVO, om informatie uit te wisselen en waar nodig en mogelijk beleid op elkaar af te stemmen.

Strafbaarstelling

Naar aanleiding van de motie is nagegaan of de bestaande wetgeving voldoende mogelijkheden biedt om te voorkomen dat vertrouwelijke informatie gedeeld wordt met onbevoegden. Dat blijkt het geval. Hiertoe is in het Nederlandse recht het delen van gerubriceerde informatie met onbevoegden strafbaar gesteld. Dat wordt bij zowel de indiensttreding als de uitdiensttreding expliciet aan de defensiemedewerker toegelicht, die daarvoor een formulier ondertekent. Ook gedurende de tijd dat de medewerker in dienst is bij Defensie wordt het bewustzijn over de omgang met vertrouwelijke informatie hoog gehouden, onder andere door het houden van beveiligingsbewustzijncampagnes. Deze aanpak is gericht op alle manieren waarop informatie gedeeld kan worden en is dus breder dan alleen trainingen. De inhoud is daarbij bepalend.
Wat betreft staats- en ambtsgeheimen geldt, op basis van de Wet ambtenaren defensie en de Ambtenarenwet 2017, dat iedere (militair) ambtenaar verplicht is tot geheimhouding van enig gegeven, de dienst betreffende, tegenover een ieder die tot kennisneming daarvan niet bevoegd is (artikel 12a, derde lid, Wet ambtenaren Defensie en artikel 12o, derde lid, Wet ambtenaren Defensie juncto artikel 9 Ambtenarenwet 2017). Strafrechtelijke handhaving van deze geheimhoudingsplicht is mogelijk op basis van het Wetboek van Strafrecht. Dit zowel wat betreft schending van ambtsgeheimen (artikel 272) als staatsgeheimen (artikel 98 tot en met 98c). Ook bepaalde tactieken en technieken, gerelateerd aan militair optreden vallen onder de geheimhoudingsplicht. Deze geheimhoudingsplicht, en de strafbaarheid van de schending daarvan, blijft ook van kracht na het verlaten van de dienst en is dus ook van toepassing op voormalige Defensiemedewerkers.
Dit betekent dat de mogelijkheid bestaat om aangifte te doen van een strafbaar feit tegen voormalige Defensiemedewerkers, indien die na hun dienstverband bij Defensie gerubriceerde informatie en/of informatie die onder de geheimhoudingsplicht valt, verstrekken aan onbevoegden. Dat beperkt zich niet tot het geven van trainingen. Hoewel het dus van belang is dat kwetsbare informatie op het juiste niveau gerubriceerd wordt, valt ook informatie waarvan in redelijkheid vermoed kan worden dat het vertrouwelijk is onder de geheimhoudingsplicht.

Rubricering

Om informatie tegen ongeautoriseerde kennisname, waaronder landen met een offensief cyberprogramma tegen Nederland, te beveiligen, wordt informatie gerubriceerd. Er zijn vier rubriceringen en voordat een medewerker deze informatie mag behandelen, krijgt de behandelaar een veiligheidsonderzoek van Dienst Justis of de MIVD al naar gelang de hoogte van de rubricering. Functies binnen Defensie waarbij staatsgeheim (STG) gerubriceerde informatie wordt behandeld, zijn aangewezen als vertrouwensfunctie en worden gecategoriseerd aan de hand van een veiligheidsmachtigingsniveau (VMN). Er zijn vier niveaus VMN's, waarbij of een Verklaring Omtrent het Gedrag (VOG) is vereist of een Verklaring van Geen Bezwaar (VGB).

De vier rubriceringen, VMN's en screeningsniveaus zijn:

Rubricering	VMN	Screeningsniveau
Departementaal Vertrouwelijk	Niet-vertrouwensfunctie	VOG
STG-Confidentieel	C	VGB C
STG-Geheim	B	VGB B
STG-Zeer Geheim	A	VGB A

Militairen die functies bekleden met het hoogste VMN, waar operationele functies voor vliegers ook onder vallen, ondergaan de hoogste screening. Zij krijgen, net als alle militairen, jaarlijks een herhaling van hun militaire basisvaardigheden waarbij ook aandacht is voor beveiligingsbewustwording en omgang met gerubriceerde informatie. Daarnaast maakt het *need-to-know* principe deel uit van het beveiligingsbewustzijn: informatie niet nodig om een taak te verrichten wordt niet gedeeld en kan dus ook niet (onbedoeld) gedeeld worden met ongeautoriseerden.
Bij het einde van hun dienstverband tekenen Defensiemedewerkers een ontheffingsverklaring. Hiermee is aanvullend benadrukt dat het delen van gerubriceerde informatie met onbevoegden, ook na diensttijd, tot strafrechtelijke vervolging kan leiden.

Overige maatregelen

Er is onderzocht of het aanvullend of hoger rubriceren van informatie bij kan dragen aan het beperken van het risico. Dit biedt vooral nadelen: medewerkers die met de informatie moeten werken, kunnen dat niet meer of worden beperkt in de wijze waarop ze met de informatie kunnen werken. Het is de mate waarin schade wordt aangericht aan de belangen van de Staat (of zijn bondgenoten) die bepaalt wat de juiste rubricering is. Het is de juiste rubricering in combinatie met het *need-to-know* principe dat ervoor zorgt dat binnen Defensie alleen de juiste mensen toegang hebben tot de voor hen relevante informatie.
Er wordt ook onderzocht of er een aanpassing in het Defensie Beveiligingsbeleid wenselijk is waarbij de groep functies uitgebreid wordt waarvoor een specifieke out-briefing bij het einde van de functie gehouden wordt, zoals nu al voor F-35 vliegers geldt op basis van Amerikaanse regelgeving en ook al voor enkele andere specifieke categorieën functies, zoals gebaseerd op basis van NAVO-regelgeving bij *Special Access Programs*.
Tot slot wordt onderzoek uitgevoerd naar aanvullende mogelijkheden om het verzorgen van trainingen door (oud-)defensiemedewerkers, die bepaalde nader te specificeren functies hebben uitgevoerd, te voorkomen. Dat onderzoek zal enige tijd in beslag nemen vanwege de complexiteit. Over de voortgang van dit onderzoek informeren wij u op een later moment.

De Minister van Defensie,
K.H. Ollongren

De Staatssecretaris van Defensie,
C.A. van der Maat