Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

32 761 Verwerking en bescherming persoonsgegevens

Nr. 203 **BRIEF VAN DE MINISTER VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 25 november 2021

Naar aanleiding van mijn brief «Uitvoeren moties LIMC» van 26 oktober jl.[1] verzocht de Vaste Commissie voor Defensie om de Kamer nader te informeren over de oefenmogelijkheden voor informatiegestuurd optreden. Hierbij ontvangt u mijn reactie op dit verzoek. Met deze brief doe ik ook mijn toezegging uit de Begrotingsbehandeling Defensie (Handelingen II 2021/22, nr. 21, debat over de Begroting Defensie 2022) gestand aan het lid Boswijk om nader in te gaan op de mogelijkheden om in het cyberdomein te kunnen trainen in bijvoorbeeld een simulatieomgeving. Gelet op de aanleiding van dit verzoek van de Kamer, richt ik mij in deze brief vooral op de gevolgen van de juridische kaders voor de oefenmogelijkheden voor informatiegestuurd optreden.

Om de krijgsmacht in te kunnen zetten voor zijn grondwettelijke taken, moet deze beschikken over inzetbare eenheden. Goed kunnen oefenen en trainen is daarvoor een randvoorwaarde. De oefenmogelijkheden voor informatiegestuurd optreden zijn gezien de geldende juridische kaders echter beperkt. De vraag of hiervoor aanvullende maatregelen nodig zijn, wordt thans door Defensie onderzocht. Hierover wordt u voor juli 2022 nader geïnformeerd.

Informatiegestuurd optreden

Defensie definieert informatiegestuurd optreden als: *«Informatie Gestuurd Optreden (IGO) houdt in dat Defensie in staat is om alle relevante informatie op elk gewenst niveau tijdig te verwerven, te verwerken, te verspreiden en in te zetten. Dit is nodig voor snellere en kwalitatief hoogwaardiger besluitvorming, waardoor de juiste middelen, op het juiste moment en op de juiste plaats kunnen worden ingezet, teneinde de gewenste – operationele – effecten te bereiken om daarmee het gedrag of*

[1] Kamerstuk 32 761, nr. 197.

kst-32761-203
ISSN 0921 - 7371
's-Gravenhage 2021

de omgeving van onze opponenten te beïnvloeden met daarbij zo min mogelijk nevenschade.»[2]

Dit is geen nieuw fenomeen. Informatie en inlichtingen vormen sinds jaar en dag de basis waarop militaire inzet gepland en uitgevoerd wordt. Dit geldt voor operaties in alle vijf militaire domeinen: land, zee, lucht, cyber en *space*. De snelle ontwikkelingen op het gebied van informatietechnologie en de veranderende aard van oorlog en hybride conflicten leggen steeds meer de nadruk op het sneller en slimmer verwerven, verwerken, verspreiden en inzetten van informatie. Potentiele tegenstanders maken daarnaast steeds effectiever gebruik van de informatie-omgeving. Dit dwingt Defensie om onze manier van werken aan te passen aan deze nieuwe werkelijkheid. De Defensievisie-2035 gaat hier nadrukkelijk op in. In deze visie die door het kabinet aan de Kamer is aangeboden, is informatiegestuurd optreden dan ook een van de drie eigenschappen die richting geven aan de keuzes over de inrichting en samenstelling van de defensieorganisatie in 2035. In deze Defensievisie staat dat Defensie nu onvoldoende is toegerust voor het opereren in de informatie omgeving. Op dit moment wordt de beleidsvisie-IGO opgesteld die beschrijft hoe Defensie dit de komende tijd wil verbeteren. Deze ontvangt u in de eerste helft van 2022, zoals ik heb toegezegd in mijn brief van 26 oktober jl.

Juridisch kader

Bij informatiegestuurd optreden is het in het algemeen gesteld onvermijdelijk dat daarbij persoonsgegevens worden verwerkt. Deze verwerkingen moeten voldoen aan de beginselen die gelden voor de bescherming van persoonsgegevens. Dit is in 1981 door de lidstaten van de Raad van Europa voor het eerst in een Verdrag uitgewerkt.[3] Met het voortschrijden van de informatietechnologie werd ook de regelgeving op het gebied van gegevensbescherming in verschillende stappen aangescherpt. Zo werd in 2012 gekozen voor het instrument van een Algemene verordening gegevensbescherming, omdat de keuzeruimte voor de nationale wetgever bij uitvoering van een verordening doorgaans beperkter is dan bij implementatie van een richtlijn en dit de gelijkvormigheid tussen landen dus in de hand werkt.[4] In 2016 werd de Europese Verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens van kracht. Vervolgens trad in Nederland in 2018 de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) in werking.

Hoewel de AVG van overeenkomstige toepassing is voor Defensie, zijn er wel enkele uitzonderingen voor Defensie als de krijgsmacht wordt ingezet. Daarnaast zijn de inlichtingen- en veiligheidsdiensten uitgezonderd van de UAVG, omdat die onder de eigen Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv2017) opereren. Daarin zijn waarborgen opgenomen in het kader van bescherming van de persoonlijke levenssfeer met bijbehorend toezicht. In alle overige gevallen dient de verwerking van persoonsgegevens een zelfstandige rechtmatige grondslag te hebben. Dit geldt derhalve ook bij oefeningen. Dit is verwerkt in het document «Algemene juridische kaders voor activiteiten van de krijgsmacht in de informatieom-

---

[2] Zoals recent ook verwoord in antwoord op schriftelijke vragen over de begroting van Defensie voor 2022. Kamerstuk 35 925 X, nr. 9, 22 oktober 2021.

[3] Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens,

[4] Memorie van toelichting bij de UAVG, 2017. Kamerstuk 34 851, nr. 3

geving» dat als bijlage bij de brief van 7 mei 2021 naar de Kamer is gestuurd.[5]

Oefenmogelijkheden

Het feit dat de verwerking van persoonsgegevens bij oefeningen maar in beperkte mate – alleen bij een wettelijke grondslag of mandaat – mogelijk is, plaatst de krijgsmacht bij oefeningen voor informatiegestuurd optreden voor uitdagingen. Bij het gebruik van moderne informatietechnologie worden namelijk al snel persoonsgegevens verwerkt. Bijvoorbeeld bij het verzamelen van informatie uit open bronnen. Ook worden nieuwe sensoren in waarnemings- en wapensystemen steeds capabeler waardoor deze bij oefeningen, onbedoeld, persoonsgegevens kunnen vastleggen van burgers die daaraan niet deelnemen, maar die zich toevallig wel in desbetreffende informatie-omgeving bevinden. Verder is het bijvoorbeeld bij oefeningen met *data-science* cruciaal om over grote hoeveelheden data te kunnen beschikken die, als deze uit de uit de maatschappelijke omgeving worden betrokken, hoogst waarschijnlijk persoonsgegevens zullen bevatten.

Volgens het adagium *«train as you fight»* moet de krijgsmacht zo realistisch mogelijk kunnen opleiden en trainen, daarbij anticiperen en zichzelf beschermen, zodat onze militairen operationeel kunnen worden ingezet. In de informatie-omgeving wordt geoefend met gevechtstactieken, -procedures en het inzetten van sensoren en software voor het verzamelen, verwerken en analyseren van gegevens. Tevens moet worden geoefend met het inzetten van informatie als wapen om het gedrag van oefentegenstanders te beïnvloeden, informatie te manipuleren, software te saboteren en dergelijke. Dit vereist een veilige oefenomgeving die de krijgsmacht in staat stelt deze taken te beoefenen en waar, zo mogelijk, alle handelingen worden geregistreerd met het oog op evaluatie en verantwoording.

In een gesloten, gecontroleerde oefenomgeving zoals bijvoorbeeld een schietbaan is de vrijheid van handelen groter dan in een open omgeving en is er een grotere marge om al lerende fouten te maken. De gevolgen hiervan blijven dan binnen de oefenomgeving en komen niet in de buitenwereld terecht. De heer Boswijk vroeg tijdens de begrotingsbehandeling of iets dergelijks ook wordt gebouwd voor militairen die willen oefenen met *hacks* en dergelijke in het cyberdomein. Het antwoord daarop is ja. Voorbeelden hiervan zijn zogeheten *cyber ranges* of gesimuleerde cyber omgevingen. Nederland zet op het gebied van een *cyber range* eerste stappen, maar kan hierbij ook aansluiten bij ontwikkelingen op dit vlak in Europa en in de VS. Ook kunnen fictieve datasets, bijvoorbeeld als onderdeel van een *social media* simulator, worden gebruikt waardoor kan worden geoefend zonder enige impact op de privacy. Een andere mogelijkheid is een scenario of *table top* oefening voor informatiegestuurd optreden waarbij niet daadwerkelijk met informatietechnologie wordt geoefend, maar de (mogelijke) effecten worden gesimuleerd. Een voordeel van zo'n afgesloten omgeving waarbij ook met fictieve persoonsgegevens kan worden gewerkt, is dat daarvoor geen aparte juridische grondslag nodig is en dat in principe alle scenario's kunnen worden gespeeld. Een nadeel is, dat dit, zoals bij elke simulatie in dit domein, een (zeer) vereenvoudigde weergave van een complexe werkelijkheid is.

[5] Kamerstuk 32 761, nr. 182. Zie voor een meer uitgebreide toelichting op de werking van de AVG voor Defensie het rapport van de Functionaris voor Gegevensbescherming Defensie dat eveneens met de brief van 7 mei aan de Kamer is aangeboden.

Daarnaast kan (personeel van) een eenheid tijdelijk bij de MIVD te werk worden gesteld ter ondersteuning van de organieke taken van de MIVD waarbij tegelijkertijd de individuele vaardigheden worden vergroot. In dat geval worden de betreffende personen bij de MIVD ondergebracht, is de Wiv2017 onverkort op hen van toepassing en vindt aansturing door de MIVD plaats. Ook kan bij militaire inzet in het kader van bijvoorbeeld art. 100 operaties of ingevolge een verzoek van civiele autoriteiten om Militaire Steunverlening in het Openbaar Belang (MSOB) of om militaire bijstand worden gekeken hoe tegelijkertijd capaciteiten op het gebied van informatiegestuurd optreden kunnen worden versterkt.

Concluderend kan worden gesteld dat de oefenmogelijkheden voor informatiegestuurd optreden gegeven de juridische kaders beperkt zijn. De vraag is of dit gezien de veranderende aard van oorlog en conflicten en het veranderende dreigingsbeeld aanvaardbaar is voor de gereedstelling van een toekomstgerichte krijgsmacht. Daar ga ik hieronder op in.

Onderzoek naar het evenwicht tussen willen, kunnen en mogen

In het eindrapport van het AVG-onderzoek naar de activiteiten van het LIMC door de onafhankelijke Functionaris voor Gegevensbescherming Defensie constateert zij terecht dat «willen, kunnen en mogen» in de informatie-omgeving met elkaar in evenwicht moeten zijn. Als bij Defensie een behoefte bestaat om op het gebied van oefenen en gereedstelling meer te «mogen», bijvoorbeeld als gevolg van de ontwikkelingen in de informatie-omgeving en een daarmee samenhangend veranderend dreigingsbeeld, dan is daarvoor mogelijk passende wetgeving nodig. Voordat deze behoefte wordt overwogen, is echter het antwoord op de «willen»-vraag noodzakelijk, luidt het advies van de Functionaris Gegevensbescherming in dit rapport.

In de brief van 7 mei 2021 waarmee dit rapport aan de Kamer is aangeboden, stelt Defensie dat zij in reactie op dit advies een onderzoek is gestart. Dit onderzoek bestaat uit twee delen die parallel aan elkaar lopen. In het eerste deel worden verschillende werkgroepen gevormd bestaande uit (militair) juristen, AVG-functionarissen, beleidsmedewerkers, ethisch experts en kernfunctionarissen van operationele eenheden die in de informatie-omgeving actief zijn. Zij onderzoeken aan de hand van praktijkvoorbeelden volgens de trits «willen, mogen, kunnen» wat de mogelijkheden en beperkingen van oefenen en gereedstelling in de informatie-omgeving zijn en hoe Defensie de ruimte binnen de bestaande juridische kaders zo goed mogelijk kan gebruiken. De activiteiten van deze werkgroepen lopen de rest van het jaar nog door.
Uit dit programma zal moeten blijken of er inderdaad een operationele noodzaak is om in antwoord op de «willen»-vraag ook de wet- en regelgeving aan te passen of dat beperkingen kunnen worden gemitigeerd door bijvoorbeeld de defensieorganisatie anders in te richten of door een andere manier van werken. Daarbij wordt ook gekeken naar hoe Europese partnerlanden de verhouding «krijgsmacht-AVG» hebben ingevuld.

In het tweede deel van het onderzoek vraagt Defensie het externe bureau dat de komende tijd nader AVG-onderzoek bij Defensie uitvoert, om tevens de door de defensieonderdelen gesignaleerde knelpunten voor de uitvoering van hun taken te inventariseren en aanbevelingen te doen voor het oplossen of mitigeren van deze knelpunten.

Van beide onderzoekstrajecten worden rapporten opgesteld die Defensie voor juli 2022 met een appreciatie aan de Kamer zal aanbieden. Daarin zal

Defensie nader ingaan op de oefenmogelijkheden voor informatiegestuurd optreden alsmede op de vraag die in het verlengde hiervan ligt, namelijk of op dit vlak aanvullende maatregelen nodig zijn.

De Minister van Defensie,
H.G.J. Kamp