Ministerie van Defensie

Eindverslag programma Juridische en Ethische Kaders bij Optreden in de Informatieomgeving (JEKOI)

Datum 16 december 2022
Status Definitief

Colofon

	KD: Ambtelijke leiding DIRECTORAAT-GENERAAL BELEID
Locatie	Den Haag - Plein-Kalvermarktcomplex Kalvermarkt 32 's-Gravenhage
Postadres	Kalvermarkt 38 2511 CB 'S-GRAVENHAGE MPC 58B
Contactpersoon	[redacted] [redacted] [redacted]@mindef.nl
Versie	Definitief
Redactieteam	DSK/DJZ/DAOG

Inhoud

1 Inleiding JEKOI-programma

A. Context en aanleiding van het JEKOI-programma

De informatieomgeving is het afgelopen decennium door de razendsnelle ontwikkelingen van de informatietechnologie (IT) sterk veranderd. Digitalisering van de samenleving maakt de informatieomgeving niet alleen toegankelijker, maar vergroot deze ook. Zoals bij vrijwel alle technologische ontwikkelingen gaat dit gepaard met nieuwe uitdagingen, zoals cyberaanvallen en grootschalige desinformatiecampagnes via sociale media. De digitalisering heeft ook grote gevolgen voor de omgeving waarin de krijgsmacht opereert en voor de wijze van militair optreden voor alle drie de hoofdtaken: 1) bondgenootschappelijke verdediging van ons grondgebied, 2) bijdragen aan de internationale rechtsorde, en 3) het bijstaan van civiele autoriteiten. Defensie moet profiteren van de kansen die moderne IT biedt en zich tegelijkertijd beschermen tegen de dreigingen ervan. Cyber is inmiddels het vijfde militaire domein met overstijgende effecten op de andere vier fysieke domeinen land, lucht, zee en ruimte. Activiteiten en capaciteiten in de informatieomgeving maken daarom een steeds belangrijker onderdeel uit van al het militair optreden. Zowel de Defensievisie 2035 als de Defensienota 2022 benadrukken dat Informatie Gestuurd Optreden (IGO) essentieel is voor effectief optreden van de krijgsmacht.

Informatie en inlichtingen vormen sinds jaar en dag de basis waarop militaire inzet wordt gepland en uitgevoerd. IGO houdt onder meer in dat Defensie in staat is om alle relevante informatie op elk gewenst niveau tijdig te kunnen verzamelen om tot een snelle en kwalitatief hoogwaardige besluitvorming te komen. De snelle ontwikkelingen op het gebied van IT, de hoeveelheid data die exponentieel toeneemt en mede als gevolg daarvan de veranderende aard van oorlog en hybride dreigingen, leggen steeds meer de nadruk op het sneller en slimmer verwerven, verwerken, verspreiden en inzetten van informatie. Ook potentiele tegenstanders maken steeds effectiever gebruik van de informatieomgeving.

Dit dwingt Defensie om IGO aan te passen aan deze nieuwe werkelijkheid. De Defensienota 2022 gaat uitgebreid in op de noodzakelijke veranderingen om als krijgsmacht toegerust te zijn voor optreden in de informatieomgeving. Niet alles wat met deze moderne technologie kan, is echter zonder meer juridisch toegestaan of vanuit ethisch oogpunt gewenst. Dit is afhankelijk van de in te zetten capaciteiten in relatie tot de specifieke context daarvan. Hierdoor kunnen de geldende juridische kaders in de operationele praktijk echter als te beperkend worden ervaren en tot ethische onduidelijkheden leiden. Een recent voorbeeld waarbij de verhouding tussen *willen, kunnen en mogen* niet in evenwicht was, was het experimentele Land Information Manoeuvre Center (LIMC). Het LIMC bracht COVID-19 gerelateerde maatschappelijke ontwikkelingen als fenomeen in kaart om militaire en civiele besluitvorming te voeden. Daarbij zijn als bijvangst ook persoonsgegevens verwerkt, maar hiervoor was geen wettelijke grondslag en is niet voldaan aan de verantwoordingsplicht waardoor de Algemene verordening gegevensbescherming (AVG) onvoldoende is nageleefd. De activiteiten van het LIMC leidden in de media en Tweede Kamer tot vragen over de juridische en ethische kaders ervan.

De onbekendheid binnen Defensie over de juridische en ethische kaders en de toepassing daarvan bij optreden in de informatieomgeving bestaat in het bijzonder bij activiteiten buiten inzet, zoals bij de generieke gereedstelling van de krijgsmacht. Welke (on)mogelijkheden gelden bij de huidige wetgeving en kaders, zowel bij huidige activiteiten als vooruitkijkend naar de verdere ontwikkeling van IGO? Dit

vormde de aanleiding van het programma Juridische en Ethische Kaders bij Optreden in de Informatieomgeving (JEKOI). Om de kennis en het bewustzijn van de bestaande juridische en ethische kaders bij optreden in de informatieomgeving door Defensie te vergroten, startte de Bestuursstaf een programma waarin het *willen, kunnen en mogen* van optreden in de informatieomgeving centraal stonden. Dit programma is ook genoemd in een aantal Kamerbrieven.[1]

B. Scope en doel van het JEKOI-programma

Het doel van het JEKOI-programma was drieledig, namelijk het:

1. Vergroten van kennis en bewustzijn over de huidige juridische en ethische kaders voor optreden in de informatieomgeving;
2. Verduidelijken van toepassing kaders voor specifieke doelgroepen binnen de krijgsmacht tijdens concrete werkzaamheden;
3. Inventariseren van knelpunten bij optreden in de informatieomgeving, om mogelijke oplossingsrichtingen te ontwikkelen.

Om dit doel te bereiken, hebben Defensieonderdelen (DO'en) verschillende themasessies georganiseerd. Daarin werden de huidige juridische en ethische kaders besproken aan de hand van concrete casuïstiek, vragen en dilemma's. Hierbij waren vertegenwoordigers van de Defensiestaf, Bestuursstaf, DO'en, operationele eenheden, specialisten, juristen en ethici in wisselende samenstelling aanwezig.

Voorliggend verslag geeft een weergave van hoe tijdens de themasessies invulling is gegeven aan het doel, evenals de rode draden die daaruit naar voren zijn gekomen. Hierin komt ook de inventarisatie van de knelpunten op hoofdlijnen terug. Aangezien in de themasessies is gesproken over hoe optreden in de informatieomgeving binnen de juridische en ethische kaders kan worden vormgegeven, gaat dit verslag ook in op de mogelijke oplossingsrichtingen die zijn besproken tijdens de themasessies.

Parallel aan het JEKOI-programma heeft Defensie een *Request For Information* (RFI) uitgezet bij de belangrijkste Europese partnerlanden. Hierin werd gevraagd hoe zij de verhouding 'krijgsmacht-AVG' binnen hun nationale wetgeving hebben ingevuld. Ook was er een vraag over de mogelijkheden die zij hebben of ontwikkelen, om in de informatieomgeving te oefenen. De antwoorden op het RFI bleken divers en niet altijd even uitgebreid. In hoofdstuk 3 van dit verslag wordt nader ingegaan op deze antwoorden. De bevraagde landen worden in dit verslag niet genoemd vanwege het belang van Nederlandse (diplomatieke) betrekkingen met betreffende landen.

C. Opzet van het JEKOI-programma

Het JEKOI-programma bestond uit vier opeenvolgende onderdelen: 1) een centrale *kick-off* bijeenkomst, 2) thematische sessies, 3) het ontwikkelen van een juridische en ethische game, en 4) voorliggend afsluitend verslag. Vanwege de coronamaatregelen heeft een deel van het programma digitaal plaatsgevonden.

I. Centrale *kick-off* – 11 mei 2021

Het programma werd afgetrapt door een centrale bijeenkomst waarin het *willen, kunnen en mogen* van optreden in de informatieomgeving werd belicht. De Commandant der Strijdkrachten (CDS) verzorgde de opening, professor [redacted] de *keynote* en de directeuren van de Directie Aansturing Operationele Gereedstelling (DAOG), Directie Strategie & Kennis (DSK), Directie Juridische Zaken

[1] Zie Kamerstukken "Aanbieding onderzoeksrapport over experimentele LIMC", 32 761, nr. 182., "Uitvoeren moties LIMC", 32 761, nr. 197., en "Reactie op verzoek commissie over de oefenmogelijkheden voor informatiegestuurd optreden", 32 761, nr. 203.

(DJZ) en Centrale Organisatie Integriteit Defensie (COID) vormden het panel. Tijdens de kick-off werd tevens meer toelichting gegeven op de komende themasessies.

II. Themasessies – juni 2021 t/m februari 2022

Elk organisatiedeel heeft een eigen taak en een eigen dagelijkse praktijk. DO'en hebben dus ook uiteenlopende vragen, dilemma's en uitdagingen met betrekking tot wettelijke en/of ethische kaders bij hun optreden in de informatieomgeving. De Koninklijke Marechaussee (KMar) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) waren uitgezonderd van het JEKOI-programma, omdat beide organisaties hun taken uitvoeren op grond van een specifieke wettelijke grondslag en bijbehorende wettelijke bevoegdheden. Dit betreffen ook de operationele activiteiten in de informatieomgeving. Voor de MIVD is dit de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv2017) en voor de KMar de Politiewet. De JEKOI-contactpersonen van de verschillende DO'en hebben ieder bij hun onderdeel gesprekken gevoerd en geïnventariseerd waar de belangrijkste aandachtspunten lagen. Deze specifieke casuïstiek werd vervolgens besproken in de verschillende themasessies. Het JEKOI-programmateam, bestaande uit vertegenwoordigers van DJZ, DAOG, en DSK, speelde hierin een faciliterende rol.

III. Juridische en ethische game – vanaf november 2022

Op basis van de juridische en ethische kaders, en casuïstiek uit de themasessies, heeft TNO in opdracht van Defensie een game ontwikkeld. Deze game bevindt zich nu in de testfase. Deze game is een middel om ook na het JEKOI-programma de bewustwording van juridische kaders en ethische afwegingen binnen de organisatie te verhogen door hierover in gesprek te (blijven) gaan.

IV. Eindverslag – november 2022

Het JEKOI-programma wordt afgesloten met het voorliggende eindverslag met de belangrijkste opbrengsten.

D. Andere IGO-trajecten gerelateerd aan JEKOI

Het JEKOI-programma staat binnen Defensie niet op zichzelf. Er zijn meerdere trajecten die zich richten op of raken aan optreden in de informatieomgeving. Daar waar mogelijk, relevant en beschikbaar worden de resultaten van deze trajecten betrokken in dit verslag. Het is in ieder geval belangrijk om dit JEKOI-verslag in samenhang te zien met onderstaande trajecten ten aanzien van IGO.

I. Beleidsvisie-IGO door Defensie

In het kader van de trits *willen, kunnen en mogen*, die in de discussies in de themasessies van JEKOI leidend was, zal de beleidsvisie-IGO invulling geven aan de ambitie - het "willen" - van Defensie in de informatieomgeving. De minister heeft in de Kamerbrief van 1 februari 2022 toegezegd dat ze ervoor zorgt dat de aanbevelingen uit het onafhankelijk onderzoek naar het LIMC door de Commissie Brouwer (zie hieronder) betrokken worden bij de beleidsvisie-IGO. Conform de motie Belhaj c.s.[2] wordt de nieuwe beleidsvisie-IGO door Defensie met de Tweede Kamer gedeeld zodra deze gereed is. In deze beleidsvisie wordt onderstreept dat binnen de juridische kaders, inclusief die van de AVG, moet worden gewerkt. De beleidsvisie-IGO wordt in de eerste helft van 2023 aan de Tweede Kamer aangeboden.

[2] Zie Kamerstuk 32 761, nr. 187.

II. Extern AVG onderzoek door Eiffel Interim & Consultancy

Naar aanleiding van de activiteiten van het LIMC heeft de Secretaris-Generaal de opdracht gegeven om een externe partij breder onderzoek te laten doen binnen Defensie naar de naleving van de AVG. De CDS heeft eind 2020 een inventarisatie uitgevoerd van activiteiten die binnen Defensie in de informatieomgeving werden ontplooid in het nationale domein (inzet en gereedstelling). Activiteiten waarbij onduidelijk was of die de kaders overschreden, zijn stopgezet. De Tweede Kamer is hierover op 7 mei 2021 geïnformeerd. In de eerste maanden van 2022 is door onderzoeksbureau Eiffel Interim & Consultancy een extern onderzoek uitgevoerd naar de activiteiten van de inventarisatie om te bezien of de activiteit AVG-compliant was, en tevens om aanbevelingen te doen hoe de DO'en AVG-compliant kunnen werken. Ook hierover is de Tweede Kamer op 7 mei 2021 geïnformeerd. Dit rapport is op 25 november 2022 aan de Tweede Kamer aangeboden.[3]

III. Onafhankelijk onderzoek LIMC door de Commissie Brouwer

In de Kamerbrief van 1 februari 2022 heeft de minister besloten een onafhankelijk onderzoek naar het LIMC in te stellen conform motie Belhaj c.s.[4] Op 1 juli 2022 is de Tweede Kamer hier nader over geïnformeerd.[5] Het onafhankelijk onderzoek wordt uitgevoerd door de Commissie Brouwer en heeft tot taak:

a) te onderzoeken hoe de besluitvorming is verlopen rond zowel de oprichting als de uitvoering van de taken van het LIMC en daarbij de militair-juridische context van het LIMC in relatie tot de kerntaken van de krijgsmacht mee te nemen;

b) te onderzoeken welke lessen voor de toekomst naar aanleiding hiervan te trekken zijn, mede in het licht van IGO van de krijgsmacht.

Het eindrapport van de commissie Brouwer is in december 2022 opgeleverd.

IV. Onderzoek door de Onafhankelijke Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming AVG Defensie heeft in 2020/2021 een onderzoek uitgevoerd bij het LIMC naar de naleving van de AVG bij het verwerken van persoonsgegevens. Dit onderzoeksrapport is op 7 mei 2021 met de Tweede Kamer gedeeld. In het onderzoeksrapport werd onder andere aanbevolen om de poortwachtersfunctie op het gebied van gegevensverwerking te versterken en om een inventarisatie te doen van risicovolle verwerkingen van persoonsgegevens. Met het onderzoeksrapport over sociale media monitoringactiviteiten binnen de DO'en, geeft de Functionaris Gegevensbescherming een eerste aanzet voor de realisatie van deze aanbeveling en een vertrekpunt voor de totstandkoming en implementatie van toekomstige richtlijnen. Dit rapport is op 25 november 2022 aan de Tweede Kamer aangeboden.[6]

V. Rijksbrede trajecten

Werken in de informatieomgeving binnen de huidige wet- en regelgeving kent overheidsbreed uitdagingen en onduidelijkheden. Op 28 juni 2021 is door de toenmalige ministers van BZK en voor rechtsbescherming overeengekomen dat onderzoek moet worden gedaan naar waar het wringt bij naleving van de AVG door overheden, en wat de meest voorkomende oorzaken zijn voor tekortkomingen in deze. Pro Facto heeft van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), het kennisinstituut voor het ministerie van Justitie

[3] Zie Kamerstuk 36 200, nr. 51.
[4] Zie Kamerstuk 32 761, nr. 186.
[5] Zie Kamerstuk 32 761, nr. 242.
[6] Zie Kamerstuk 36 200, nr. 51.

en Veiligheid, de opdracht gekregen dit onderzoek uit te voeren. Defensie heeft hieraan medewerking verleend.

2 Weergave van de JEKOI-themasessies

A. Overzicht aanpak van de themasessies

In een themasessie doorliep de eenheid of afdeling van een DO specifieke casussen samen met juridisch en/of ethisch experts, aan de hand van hun eigen taken en opdrachten. Het doel was om daarbij de kaders te vertalen naar de praktijk, eventuele knelpunten te identificeren en mogelijke oplossingsrichtingen te bespreken. De verantwoordelijkheid voor het organiseren van een themasessie lag bij de DO'en zelf, waarbij de inhoud van de sessie werd gestuurd door de vragen die binnen dat onderdeel leefden. Het JEKOI-programmateam was het aanspreekpunt voor de JEKOI-contactpersonen bij alle DO'en, hield regie op de te organiseren themasessies, en leverde inhoudelijke bijdragen tijdens de sessies.

Bij alle themasessies is door DJZ een toelichting gegeven op de algemene juridische kaders die gelden als uitgangspunt voor activiteiten in de informatieomgeving. Ook de AVG-coördinator verzorgde tijdens de sessies een presentatie over de (U)AVG. Bij een aantal sessies was ook een ethicus van de COID aanwezig om in te gaan op ethische aspecten van de ingebrachte casuïstiek. De themasessies boden de DO'en een gelegenheid om door hen (gewenste) activiteiten in de informatieomgeving toe te lichten, daarbij ervaren knelpunten te duiden, en uiting te geven aan hun zorgen die leven over bijv. de beperkte oefenmogelijkheden bij optreden in de informatieomgeving. De aanwezigheid van een jurist, AVG coördinator en – in sommige themasessies - ethicus bij de sessies zorgden voor inhoudelijke discussies. Vragen en opmerkingen van de deelnemers over juridische en ethische kaders bij activiteiten in de informatieomgeving konden daarbij worden besproken.

Hieronder volgt een overzicht van de hoofdlijnen die uit de themasessies naar voren zijn gekomen. De JEKOI-contactpersonen zijn door het JEKOI-programmateam betrokken bij de inhoud van voorliggend verslag. Tijdens het programma hebben de JEKOI-contactpersonen terugkoppeling ontvangen van de themasessies ter beeldvorming en bewustwording van eventuele knelpunten die door andere DO'en binnen de organisatie worden ervaren.

B. Rode draden uit de themasessies

Tijdens de georganiseerde discussies tekenden zich drie rode draden af. Dit zijn: 1) de informatiepositie van de krijgsmacht, 2) de grens tussen gereedstelling en inzet, en 3) operationele gereedstelling voor IGO van de krijgsmacht. Alle drie de rode draden hangen met elkaar samen.

1) Informatiepositie van de krijgsmacht

De eerste rode draad betreft de informatiepositie van de krijgsmacht, namelijk de beschikbaarheid van tactische en operationele informatie. Uit de themasessies blijkt dat er binnen de krijgsmacht een bredere informatiebehoefte is om ten behoeve van generieke gereedstelling beeld op te bouwen, of te krijgen, over een potentiele tegenstander en/of potentieel inzetgebied. Voor de operationele commando's is een goede informatiepositie namelijk randvoorwaardelijk om op een juiste manier gereed te kunnen stellen en de juiste training en opleidingen te kunnen geven, om bij inzet effectief te kunnen opereren. Operationele informatie is nodig voor het plannen, uitvoeren en bewaken van een militaire operatie. Deze bieden op operationeel niveau inzicht in bijv. tegenstanders en omstandigheden in het operatiegebied. Tactische informatie zorgt ervoor dat de uitvoerende eenheden in het operatiegebied weten wat er in hun omgeving speelt, de *situational awareness*. Beide niveaus van

informatie zijn onmisbaar voor de krijgsmacht. Een genoemd voorbeeld tijdens de themasessies was het belang van tijdige en juiste informatie over wat voor explosieven (IED's) worden gebruikt in conflictgebieden. Tijdens de themasessies stelden de operationele commando's dat zij zich op dit vlak onvoldoende bediend voelen door de MIVD. Dit is een belangrijk aandachtspunt. Bij de mogelijke oplossingsrichtingen (zie paragraaf C) gaat dit verslag in op de wijze waarop dit ervaren knelpunt kan worden opgepakt.

2) Grens tussen gereedstelling en inzet

Bij iedere themasessie is door DJZ toegelicht dat er binnen de huidige juridische kaders een onderscheid is tussen inzet van de krijgsmacht en oefening/gereedstelling. Voor gereedstelling ten behoeve van generieke voorbereiding op inzet, waaronder opleiding en training, heeft de krijgsmacht geen zelfstandige bevoegdheden. De inlichtingeneenheden onder de CDS kunnen dan dus niet zelfstandig informatie verzamelen over bijv. een potentieel inzetgebied of potentiele tegenstander; die taak (en bevoegdheid) ligt bij de MIVD. Bij inzet kan dit wel, maar daarbij is de grondslag bepalend voor welke bevoegdheden door de krijgsmacht mogen worden uitgeoefend. Wat de krijgsmacht in een specifiek geval mag en hoe daar uitvoering aan mag worden gegeven is namelijk afhankelijk van: 1) de (aard van de) opgedragen taak, 2) de (inter)nationaalrechtelijke grondslag voor die taak, 3) de (inter)nationaalrechtelijke regels van toepassing op die taak (bijv. de AVG, humanitair oorlogsrecht, mensenrechten, en 4) het politieke mandaat voor die taak.

In reactie op de geldende juridische kaders, is tijdens de themasessies door de DO'en ook ingebracht dat er door hen wél een taak wordt ervaren bij informatieverzameling buiten inzet. Binnen de krijgsmacht wordt namelijk een noodzaak gevoeld om de ervaren leemte in de tactische en operationele informatiepositie, zoals genoemd bij punt 1, zelf in te vullen. Hierbij gaat het om de behoefte van de inlichtingeneenheden onder de CDS om zelf informatie te verzamelen en beeld op te bouwen over de operationele omgeving, zoals een potentiele tegenstander. Binnen de krijgsmacht is bijvoorbeeld vraag naar inzicht in een te verwachten dreiging om deze te laten aansluiten bij de benodigde trainingsscenario's. Daarnaast is deze informatie nodig voor de ontwikkeling van doctrines en procedures om succesvol te kunnen opereren tijdens inzet. De zogeheten *situational understanding* – het begrijpen van wat er in een omgeving gebeurt - wordt idealiter opgebouwd vóór bekend is dat de krijgsmacht wordt ingezet. Commandanten dienen vooraf op de hoogte te zijn van de operationele omgeving waarin zij mogelijk ingezet gaan worden en de te verwachten ontwikkelingen in een potentieel operatiegebied, en niet pas bij inzet. *Situational understanding* is ook van belang bij bijvoorbeeld oefeningen.

De binnen de krijgsmacht ervaren spanning tussen bevoegdheden en taken blijkt ook uit andere casuïstiek die tijdens de themasessies is besproken, namelijk *force protection*. *Force Protection* betreft alle maatregelen die er op gericht zijn om de kwetsbaarheid van personeel, faciliteiten, materieel en operaties te minimaliseren, tegen elke dreiging in alle situaties, met als doel de vrijheid van handelen en de operationele effectiviteit van eenheden te waarborgen. Deze kwetsbaarheden zijn er altijd, ongeacht of de krijgsmacht bezig is met gereedstelling of inzet. Tijdens de themasessies is bijvoorbeeld gesproken over informatieverzameling ter bescherming van militaire bases en materieel in het kader van vredesbedrijfsvoering en tijdens oefening. Denk daarbij aan vragen als wat mogen DO'en aan digitale activiteiten verrichten op Defensieterrein? En op welke wijze kunnen DO'en digitale kwetsbaarheden, zoals cyberaanvallen tegen communicatiesystemen of

wapensystemen, in kaart brengen om vervolgens mitigerende maatregelen te treffen ter bescherming van eigen materieel en personeel?

Daarnaast is over het voorbeeld gesproken waarbij eenheden in het kader van *Enhanced Forward Presence* voor een oefening naar de grens van het NAVO-verdragsgebied gestuurd om daar tegelijkertijd ook een afschrikkingseffect te creëren tegen een reële en aanwezige dreiging aan de andere kant van de grens. Bij een oefening is er, zoals hierboven gesteld, geen sprake van een zelfstandige grondslag – de taak en bevoegdheid - voor het verzamelen en/of verwerken van persoonsgegevens voor operationele activiteiten. Uit de themasessies blijkt dat dit wringt voor de ontplooide eenheden en individuen, omdat men een continue dreiging ervaart vanuit bekende en potentiele tegenstanders. Waar er juridisch gezien een onderscheid is tussen een oefening en daadwerkelijke inzet, ervaart men in de praktijk een overlap tussen beide activiteiten. Oftewel, eenheden ervaren een dreiging, worden ontplooid voor een *real-life* effect (afschrikking) en zijn tijdens sommige oefeningen actief in de 'echte wereld', maar hebben slechts beperkte mogelijkheden, zowel in het fysieke domein (e.g. geweldgebruik) als in de informatieomgeving.

3) Operationele gereedstelling voor IGO van de krijgsmacht

Om de krijgsmacht in te kunnen zetten voor haar grondwettelijke taken, moet deze beschikken over inzetbare eenheden. Goed kunnen oefenen en trainen, onder meer met IGO, zijn hiervoor randvoorwaarden. Hierbij gaat het bijvoorbeeld om het opleiden en trainen van inlichtingenpersoneel op het gebied van OSINT, het oefenen met de inzet van informatie als wapen om het gedrag van oefentegenstanders te beïnvloeden, het saboteren en hacken van software etc. Het opleiden van personeel voor dergelijke informatieactiviteiten vereist dat dit kan worden getraind en beoefend. Indien de krijgsmacht echter zou oefenen en trainen in de echte informatieomgeving, is het onvermijdelijk dat de krijgsmacht in aanraking komt met persoonsgegevens. In de themasessies is besproken dat de DO'en dan tegen juridische beperkingen aanlopen. De krijgsmacht heeft namelijk geen algemene wettelijke grondslag – taak en bevoegdheid – om persoonsgegevens te verwerken. Daarmee zijn de oefenmogelijkheden voor IGO gezien de geldende juridische kaders beperkt.

Oefenen en trainen met IGO kan binnen de juridische en ethische kaders wel door bijvoorbeeld gebruik te maken van gesloten en gecontroleerde oefenmogelijkheden of -omgevingen. Uit de themasessies bleek echter dat de DO'en bestaande gesimuleerde oefenomgevingen met fictieve datasets ervaren als weinig realistisch en onvoldoende ondersteunend om personeel goed te kunnen bekwamen in hun taken. Zogeheten *cyber ranges* bieden volgens hen wel een mogelijkheid om bepaalde vaardigheden te oefenen, maar een realistische cognitieve dimensie creëren in een synthetische trainingsomgeving achten zij niet optimaal. Daarnaast is synthetische data doorgaans duur en minder dynamisch om mee te werken, aldus de DO'en. Het gebrek aan oefenmogelijkheden wringt stellen ze, omdat de krijgsmacht bij inzet wel wordt geacht over de benodigde vaardigheden en oefenervaring te beschikken om de informatieactiviteiten tijdens de inzet uit te kunnen voeren. Moderne dataverwerking vergt dat de krijgsmacht moet kunnen werken met uiteenlopende en grote hoeveelheden data en informatie. Wanneer delen van hun taken niet realistisch kunnen worden getraind, zijn eenheden beperkt operationeel gereed en daarmee, gezien de verwachte korte reactietermijnen, mogelijk niet tijdig inzetgereed.

Hetzelfde geldt voor het ontwikkelen en testen van materieel dat onder meer is bedoeld voor optreden in de informatieomgeving. Nieuwe sensoren in waarnemings-

en wapensystemen zoals UAV's worden steeds innovatiever. Hiermee wil de krijgsmacht graag kunnen oefenen en experimenteren om bijvoorbeeld te onderzoeken welke informatie met een sensor kan worden verzameld en hoe systemen interoperabel zijn. Bij oefeningen met dergelijk materieel kunnen echter persoonsgegevens worden verzameld van burgers en eigen personeel die zich in de betreffende informatieomgeving bevinden. Als er geen alternatieven voorhanden zijn, kan het niet realistisch kunnen oefenen met dergelijke systemen leiden tot risico's in de gereedstelling en tijdens inzet.

C. Aangedragen oplossingsrichtingen uit de themasessies

Tijdens de themasessies zijn ook mogelijke oplossingsrichtingen besproken voor de knelpunten die hierboven zijn genoemd. Deze oplossingsrichtingen bieden geen pasklaar antwoord op de aangedragen knelpunten, maar geven een denkrichting voor de wijze waarop Defensie de ervaren problematiek bij optreden in de informatieomgeving zou kunnen aanpakken. Het gaat om de volgende oplossingsrichtingen:

1. Simulaties en oefenmogelijkheden IGO;
2. Flexibele inzet onder de MIVD;
3. Ervaringsopbouw tijdens militaire bijstand of militaire steunverlening in het openbaar belang (MSOB) en/of internationale inzet;
4. Verruiming van de juridische kaders.

Hieronder worden de vier oplossingsrichtingen kort uiteen gezet waarbij ook de tijdens de themasessies besproken voor- en nadelen worden genoemd.

1) Simulaties en oefenmogelijkheden IGO

Zoals hierboven gesteld, staat de krijgsmacht bij oefenen en trainen met IGO voor uitdagingen, omdat bij het gebruik van moderne IT al snel persoonsgegevens worden verwerkt. Het opvangen van een signaal is in sommige gevallen al een verwerking. Dit is alleen toelaatbaar bij een wettelijke grondslag. In het kader van gereedstelling dient de krijgsmacht echter op een zo realistisch mogelijke wijze te kunnen opleiden, oefenen en trainen. Hiervoor zou een gesloten en gecontroleerde oefenomgeving of simulatie een (gedeeltelijke) oplossingsrichting kunnen zijn.

Ten aanzien van het cyber domein zijn er bijvoorbeeld zogeheten cyber ranges of gesimuleerde cyber omgevingen. Ook kunnen fictieve datasets als onderdeel van een sociale media simulator een optie zijn om OSINT technieken en analyses mee te oefenen. De complicerende factor hierbij is dat het internet zo dynamisch en omvangrijk is dat het volgens de aanwezigen tijdens de themasessies op dit moment vrijwel onmogelijk is om een dergelijke omgeving realistisch na te bootsen. Voor specifieke activiteiten als Information Manoeuvre, Strategische Communicatie en gedragsonderzoek is het ontwikkelen van simulaties nog complexer, omdat er getraind dient te worden met de cognitieve dimensie, zoals het toepassen van gedragsinzichten. Daarbij is het ook van belang om te kunnen meten en evalueren wat de effecten zijn van het handelen tijdens een training of oefening.

Tijdens de themasessies is door de DO'en herhaaldelijk gezegd dat er verkenningen zijn gedaan naar eventuele IGO-oefenmogelijkheden, maar dat daarbij volgens hen is gebleken dat de verkende opties ontoereikend zijn. Daarbij geldt wel dat elke simulatie een vereenvoudigde weergave van een complexe werkelijkheid is. Dit geldt uiteraard ook voor gesimuleerde oefeningen in de informatieomgeving.

De vraag die nog onvoldoende is beantwoord, is in hoeverre beperkingen in bestaande IGO-oefenmogelijkheden acceptabel zijn om alsnog voor bepaalde capaciteiten en kennis op te leiden en te trainen. Vervolgens dient te worden

gekeken op welke wijze het ervaren gat bij opleiden en trainen in de informatieomgeving voldoende kan worden opgevuld. Dit kan door de ontwikkeling van IGO-oefenmogelijkheden, maar ook door mogelijkheden die verder in het verslag aan bod komen. Defensie gaat de komende jaren met een defensiebreed projectteam de mogelijkheden van gesimuleerd oefenen met IGO nader onderzoeken en daarmee ook experimenteren. Het doel daarvan is om met concrete, tussentijdse, resultaten bij te dragen aan om een verhoogde inzetbaarheid op het gebied van IGO. Dit kan bijvoorbeeld door deze concepten en capaciteiten zelf of in internationaal samenwerkingsverband te verwerven of te ontwikkelen, of door deze capaciteiten (in het buitenland) in te huren.

2) Flexibele inzet onder de MIVD

Een mogelijke oplossingsrichting voor de twee ervaren knelpunten over de informatiepositie en operationele gereedstelling betreft het tijdelijk te werk stellen (TTW'en) van personeel van een operationele inlichtingeneenheid onder de CDS bij de MIVD ter ondersteuning van de organieke taken van de MIVD. Het is aan de MIVD om dreigingen te onderkennen en de krijgsmacht van inlichtingen te voorzien, zodat die haar taak kan uitvoeren. De MIVD kan, gebruikmakend van de bijzondere bevoegdheden die de Wiv2017 biedt, een cruciale bijdrage leveren aan de gereedstelling en inzet van de krijgsmacht op alle niveaus van optreden, waaronder tactisch en operationeel.

Tijdens het openbare symposium "Fog of War 2.0" ter gelegenheid van het 25-jarige bestaan van de MIVD op 23 juni jl. heeft de CDS gezegd dat er sinds kort operationele eenheden deels en tijdelijk onder de MIVD worden geplaatst om beter te kunnen voorzien in de behoefte aan operationele en tactische inlichtingen van de krijgsmacht. Deze eenheden worden ook ingezet voor het verzamelen en analyseren van operationele en tactische inlichtingen. Het personeel afkomstig van de CDS werkt in dat geval onder de Wiv2017 en onder aansturing van de MIVD zelf. De winst hierbij is dat de operationele en tactische inlichtingencapaciteit wordt versterkt - en dus ook de informatiepositie van de krijgsmacht. Het nadeel is dat personeel in geval van TTW'en gewend kan raken aan opereren onder de Wiv2017 in plaats van onder de juridische kaders die van toepassing zijn op de CDS-eenheden, zoals het werken met andere procedures.

3) Ervaringsopbouw tijdens militaire bijstand of militaire steunverlening in het openbaar belang (MSOB)

Bij nationale inzet op basis van militaire bijstand of militaire steunverlening in het Openbaar Belang (MSOB) wordt de krijgsmacht ingezet onder aansturing en verantwoordelijkheid van civiel gezag, zoals de officier van justitie of de burgemeester. De krijgsmacht heeft daarbij geen eigen bevoegdheden, maar oefent hierbij taken en bevoegdheden uit van het ondersteunde civiele gezag. In dergelijk geval wordt de krijgsmacht gevraagd om bij een opdracht vanuit civiele autoriteiten te ondersteunen, bijvoorbeeld het Openbaar Ministerie of de Nationale Politie. Deze inzet ter ondersteuning van het civiele gezag biedt tegelijkertijd een kans voor de krijgsmacht om operationele ervaring op te doen in de informatieomgeving. Een nadeel hiervan is dat dergelijke opdrachten niet te plannen zijn, omdat ze voortkomen uit de behoefte van een civiele autoriteit die bijvoorbeeld kampt met een tekort aan capaciteit. Daarnaast hoeft de te leveren inzet niet altijd overeen te komen met de ervaringsbehoefte van de krijgsmacht. Bij dergelijke ondersteuningen worden bijvoorbeeld vaak alleen individuen of kleine groepen ingezet. Daarmee kan slechts een klein deel van de inlichtingenketen ervaring opdoen.

Tevens kan in het kader van een internationale inzet worden gekeken hoe bij het opwerken naar inzet tegelijkertijd de capaciteiten ten aanzien van IGO kunnen worden versterkt.

4) Verruiming van de juridische kaders

Bovenstaande drie oplossingsrichtingen kunnen binnen de bestaande juridische kaders en naast elkaar worden uitgevoerd. Als deze drie mogelijkheden onvoldoende soelaas blijken te bieden voor de geconstateerde beperkingen voor de krijgsmacht in de informatieomgeving, is in een aantal themasessies ook de optie besproken om de huidige juridische kaders aan te passen. Dit zou het bij trainen en oefenen gerelateerd aan IGO, zowel qua personeel als materieel, mogelijk moeten maken om persoonsgegevens te mogen verwerken. Het aanpassen van wetgeving is echter een intensief en langdurig traject, waarvoor een duidelijke en goede onderbouwing benodigd is. Zo dient te worden aangegeven welke activiteiten nodig zijn om IGO mogelijk te maken, en waarom deze activiteiten niet op een andere manier dan aanpassing van wetgeving kunnen worden vormgegeven. Hieruit moet resulteren hoe groot het risico is dat is gekoppeld aan het niet voldoende kunnen gereedstellen. De hiervoor benodigde onderbouwing is op dit moment niet concreet genoeg en vereist nadere uitwerking.

3 Observaties

A. Observaties van de themasessies door het JEKOI-programmateam

Allereerst kwam uit de themasessies naar voren dat de verschillende DO'en het belang inzien van het kunnen optreden in de informatieomgeving. De beleving dat in de huidige geopolitieke context de grens tussen inzet en gereedstelling niet meer zo duidelijk is, door onder meer hybride dreigingen onder de drempel van gewapend conflict, zorgt voor een gevoel van urgentie om de krijgsmacht hier gedegen op voor te kunnen bereiden. Zoals eerder genoemd, is het onderscheid tussen oefening/gereedstelling en inzet van de krijgsmacht er in juridische zin echter wel. De activiteiten van de krijgsmacht dienen in overeenstemming te zijn met het toepasselijke internationaal recht en met gebruikmaking van de juridisch verantwoorde middelen. De wijze waarop de krijgsmacht in sommige gevallen wenst te opereren in de informatieomgeving, is met de geldende juridische en ethische kaders buiten inzet beperkt mogelijk, zo blijkt uit de themasessies. Daarbij speelde ook de vraag in hoeverre de krijgsmacht een taak zou moeten hebben om buiten inzet te kunnen opereren en informatieactiviteiten te kunnen ontplooien. Dit dient namelijk te worden bezien binnen de context van zowel de defensieorganisatie, waartoe ook de MIVD behoort, als de Rijksoverheid waar ook taken ten aanzien van (nationale) veiligheid zijn belegd. Binnen Defensie kan de MIVD onder de Wiv2017 informatieactiviteiten ontplooien ten behoeve van de krijgsmacht, waaronder het uitvoeren van analyses en verzamelen van inlichtingen. De Rijksbrede aanpak van desinformatie is bijvoorbeeld belegd bij het ministerie van Binnenlandse Zaken (BZK) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) coördineert de weerbaarheid tegen statelijke en hybride dreigingen.

Een tweede observatie uit de themasessies is dat het juridische kader, kennis van de AVG, en bewustzijn over de daarbij komende verantwoordelijkheden continu aandacht verdient. De themasessies van het JEKOI-programma hebben het bewustzijn over de juridische en ethische kaders bij optreden in de informatieomgeving vergroot en vragen die daarbij leefden besproken, maar het is in het belang van de defensieorganisatie om gesprekken en bewustzijn hierover structureel aandacht te geven. Kennis over de AVG en juridische kaders dient beter te worden geborgd in de defensieorganisatie. De themasessies wezen uit dat er binnen Defensie soms ten onrechte aannames over de juridische kaders en AVG leven terwijl er in de praktijk toch meer mogelijk blijkt dan aanvankelijk werd gedacht. Uit een aantal themasessies bleek ook de behoefte aan AVG-advisering en het verkennen van mogelijkheden over optreden in de informatieomgeving. Meer kennis en begrip van de AVG en juridische kaders kan bijdragen aan het contextualiseren van de eerder genoemde rode draden, en vermindert wellicht ook de gepercipieerde onbalans tussen taken en bevoegdheden.

De derde observatie is dat tijdens de themasessies vooral is gesproken over de juridische kaders en in mindere mate over de ethische. De sterkere focus op de juridische kaders hing samen met de onderwerpen van gesprek tijdens de themasessies. In sommige gevallen leende het onderwerp zich bij uitstek voor een ethische discussie, bijvoorbeeld over gedragsonderzoek binnen de juridische kaders van een VN-operatie, maar in de meeste gevallen leefden er vanuit DO'en vooral vragen over de juridische mogelijkheden. Uit de themasessies kwam wel een overkoepelend ethisch vraagstuk naar voren, namelijk de spanning tussen enerzijds ervaren beperkingen bij oefenen, opleiden en trainen in de informatieomgeving, en anderzijds de noodzaak om bij inzet wel geacht te worden over kennis en kunde te

beschikken om in die omgeving te kunnen optreden. Daarbij is de vraag aan de orde welke risico's acceptabel zijn als de krijgsmacht buiten inzet maar beperkt actief kan zijn in de informatieomgeving, mede gelet op de veiligheid van eigen personeel en materieel tijdens inzet. Opponenten benutten de informatieomgeving namelijk volop en handelen niet in overeenstemming met de ethische en juridische kaders zoals van toepassing in Nederland.

Tot slot blijkt dat voor het verwezenlijken van de gestelde IGO-ambitie in de Defensievisie 2035 stappen moeten worden gezet voor de gereedstelling in de informatieomgeving binnen de juridische en ethische kaders. De kennis en het bewustzijn over de juridische en ethische kaders, en een daarmee in overeengestemde organisatie, dienen meer te worden vergroot. Tevens zijn de huidige mogelijkheden om adequaat te kunnen gereedstellen in de informatieomgeving op dit moment beperkt. Dit onderstreept het belang om intern Defensie te bezien hoe dit kan worden verbeterd, bijvoorbeeld organisatorisch, en of deze voldoende worden benut om binnen de juridische en ethische kaders activiteiten van de krijgsmacht in de informatieomgeving vorm te geven. Hierover worden intern Defensie reeds gesprekken gevoerd en er wordt gewerkt aan het vergroten van de slagvaardigheid van de MIVD, de Inlichtingen- en Veiligheidsorganisaties (I&V-diensten) en I&V elementen van de krijgsmacht, tijdens inzet nu en in toekomstige operationele omgevingen. Daarnaast dient er bij Defensie al tijdens beleidskeuzes over IGO duidelijk te zijn hoe binnen de juridische en ethische kaders kan worden gereedgesteld, bijvoorbeeld bij de aanschaf van materieel, zoals nieuwe sensoren, maar ook bij de oprichting van eenheden.

B. Vergelijking van de AVG met strategische partnerlanden

Een aantal partnerlanden is gevraagd hoe gegevensbescherming is gereguleerd ten aanzien van operationele activiteiten van hun krijgsmachten. De antwoorden hebben verschillende mate van diepgang. Dat betekent dat voor specifieke duiding van de juridische posities van de landen veelal nadere informatie benodigd is. Dat betekent ook dat een goede vergelijking niet mogelijk is. Wel is het mogelijk om enkele hoofdlijnen af te leiden uit de ontvangen antwoorden.

Net als in Nederland is in vier van de negen bevraagde landen de AVG van overeenkomstige toepassing op operationele activiteiten van hun krijgsmacht. Drie landen hebben (al dan niet specifieke) nationale wetgeving die van toepassing is op gegevensbescherming tijdens operationele activiteiten van hun krijgsmachten. Die wetten zijn in overeenstemming met het Europees verdrag voor de rechten van de mens (EVRM) en het verdrag van de raad van Europa inzake gegevensbescherming, de geamendeerde conventie 108 (C108+). In twee andere landen zijn operationele defensieactiviteiten in verschillende mate uitgezonderd van een gegevensbeschermingsregime. Uit de beantwoording kan niet duidelijk opgemaakt worden hoe deze uitzonderingen zich verhouden tot de verplichtingen uit het EVRM en conventie C108+. Met uitzondering van één land hebben alle landen, net als Nederland, specifieke uitzonderingen geregeld voor gegevensverwerking door de krijgsmacht.

Geen van de bevraagde landen heeft specifieke bevoegdheden voor oefenactiviteiten in de informatieomgeving. Enkele landen geven aan te werken met een gesimuleerde oefenomgeving. Eén land geeft aan momenteel de (juridische) mogelijkheden voor het oefenen in de informatieomgeving te onderzoeken.

4 Afsluitende opmerkingen

Zoals genoemd in de inleiding is met de georganiseerde themasessies meer bewustwording ontstaan binnen de defensieorganisatie over de juridische en ethische kaders bij optreden in de informatieomgeving. Het JEKOI-programma op zich was daarmee een belangrijk middel om bewustzijn hierover te verhogen. Tevens is een inventarisatie gedaan van ervaren knelpunten bij optreden in de informatieomgeving die in dit verslag zijn vastgelegd. Zoals eerder toegelicht, vergen de door de DO'en genoemde beperkingen nadere onderbouwing en is daarom op dit moment nog onvoldoende duidelijk wat de mogelijke effecten zijn van de in themasessies besproken beperkingen bij de gereedstelling voor IGO. Dit zal door Defensie verder worden onderzocht teneinde beter inzicht in de omvang van de besproken gereedstellingsproblematiek te krijgen. Op die manier kan gerichter worden gekeken naar oplossingsrichtingen om verdere invulling te geven aan IGO.

Tot slot is het JEKOI-programma, zoals eerder aangegeven, slechts één van de (lopende) trajecten ten aanzien van optreden in de informatieomgeving. Al deze trajecten dragen niet alleen bij aan het kunnen optreden in de informatieomgeving, maar zijn tevens de eerste stappen om de IGO-ambitie, zoals genoemd in de Defensievisie 2035 en Defensienota 2022, te kunnen verwezenlijken. Na oplevering van het JEKOI-verslag eindigt de benodigde aandacht hiervoor niet, maar biedt dit verslag aanknopingspunten die in andere IGO-trajecten kunnen worden opgepakt.