

De Wet op de defensiegereedheid

Een informatiewet of een inlichtingenwet?

Rowin Jansen & Bart Jacobs¹

Met de voorgestelde Wet op de defensiegereedheid krijgt Defensie nieuwe mogelijkheden om informatie te verzamelen, te verwerken en te delen ter voorbereiding op moderne militaire en hybride dreigingen. Waar de regering spreekt van een noodzakelijk instrument voor een informatiegestuurde krijgsmacht, kan ook gevreesd worden voor een verschuiving richting bevoegdheden die traditioneel zijn voorbehouden aan de inlichtingen- en veiligheidsdiensten. In deze bijdrage wordt onderzocht hoe het nieuwe informatieregime precies is vormgegeven, welke waarborgen het bevat en waar de juridische en maatschappelijke risico's liggen. Aan de hand van de lessen uit de LIMC-affaire wordt de verhouding tussen defensiegereedheid, privacy-bescherming en democratische controle geanalyseerd. Zet de Wodg vooral de deur open naar een nieuwe inlichtingenpraktijk binnen de krijgsmacht?

1. Inleiding

De voorgestelde *Wet op de defensiegereedheid* (Wodg) beoogt de krijgsmacht in staat te stellen zich voor te bereiden op moderne oorlogssituaties. Om achterstanden weg te werken en hybride dreigingen beter te adresseren, wil de regering een aantal complexe procedures versnellen en vereenvoudigen.² Dit wetsvoorstel heeft betrekking op verschillende rechtsgebieden. Wij richten ons op het informatiehoofdstuk. Dat moet een dynamisch raamwerk bieden voor 'informatiegestuurd optreden' in dit tijdperk van technologische en geopolitieke omwentelingen. Defensie krijgt nieuwe grondslagen voor het verwerken van persoonsgegevens en mag zelfstandig gaan optreden in 'de informatieomgeving'. Ook komen er dwarsverbanden met de – binnenkort geheel te herziene – Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017).

Het informatiehoofdstuk van de Wodg is niet onomstreden. Van de maar liefst 1543 openbare reacties op de internetconsultatie had een aanzienlijk deel als strekking: 'Big Brother is watching you'. In defensiekringen lopen de verwachtingen uiteen, zo is onze indruk uit achtergrondgesprekken. Waar de één meent dat met deze wet nieuwe 'inlichtingenorganen' mogen worden opgetuigd, benadrukt de ander dat er onder de streep nog steeds te weinig is toegestaan in het digitale domein. De waarheid ligt vermoedelijk ergens daar tussenin. Dat militairen speeches van Poetin in hun systemen moeten kunnen opslaan

Zodra deze informatievergaring zich op willekeurige Nederlandse burgers richt, zijn alarmbellen terecht

of kentekens van verdachte voertuigen bij kazernes moeten kunnen registreren, behoeft weinig toelichting. Maar zodra deze informatievergaring zich op willekeurige Nederlandse burgers richt, zijn alarmbellen terecht.

De vraag is dan ook hoe ver dit nieuwe regime reikt. Gaat het hier 'slechts' om een informatiewet of schuift de Wodg op richting een heuse inlichtingenwet die ruimte biedt aan parallelle geheime diensten? In deze verkennende bijdrage bespreken wij de achtergrond, de hoofdpun-

Auteurs

1. Mr. dr. R.H.T. Jansen is universitair docent Nationale veiligheidsrecht aan de Radboud Universiteit. Prof. dr. B.P.F. Jacobs is hoogleraar Computerbeveiliging en privacy aan dezelfde instelling. De auteurs danken Anna Berlee, Roel Schutgens en Anna Verkuil voor hun commentaar op een eer-

dere versie van deze bijdrage. De kopij is afgerond op 1 september 2026.

Noten

2. Onlangs is op Europees niveau het Omnibuspakket voor defensiegereedheid voorgesteld.



© Gints Evuskans/ANP

ten, de risico's en de waarborgen van het informatiehoofdstuk. Doel is daarbij het moeilijk te doorgronden stelsel voor een breder publiek inzichtelijk te maken. Gelet op het beperkte bestek komen niet alle aspecten volledig aan bod. Diverse leerstukken behoeven nadere uitwerking in andere bijdragen. Bijzondere aandacht gaat uit naar de verhouding tot de Wiv 2017. Informatiegerelateerde maatregelen met betrekking tot defensiepersoneel, zoals monitoring van de fitheid van militairen, blijven daarentegen buiten beschouwing.

2. Achtergrond

Over gegevensverwerkingen in het defensiedomein is tot dusver vrijwel niets gepubliceerd in de algemene rechtswetenschappelijke literatuur. Ook elders is daarover weinig geschreven.³ Enige jaren geleden haalde wel het zogeheten 'Land Information Manoeuvre Centre'⁴ (LIMC) de krantenkolommen. Deze landmachteenheid bleek in coronatijd heimelijk informatie te verzamelen op sociale media, ook over Nederlandse burgers. Men zag de pandemie als een uitgelezen kans om te trainen in het informatiedomein en wilde met vernuftige algoritmes de verspreiding van het virus en van desinformatie in kaart brengen. Het doel was 'beeldopbouw'. De bevindingen – 'fenomeenanalyses' – werden gedeeld met bijna honderd instanties, waaronder de politie en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Interne juristen waarschuwden herhaaldelijk dat de juridische basis 'flinterdun' of zelfs non-existent was. De defensietop 'overruled' hen.⁵ De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) waarschuwde achter de scher-

men dat het LIMC een derde geheime dienst dreigde te worden, naast zichzelf en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD).⁶ Pas na mediaonthullingen door NRC⁷ – journalisten spraken op enig moment zelfs in wel erg bombastische bewoordingen over 'de internetninja's van de krijgsmacht'⁸ – en politieke commotie legde de minister de eenheid in 2020 stil. De Functionaris Gegevensbescherming (FG) van het Ministerie van Defensie schreef een gedegen kritisch rapport. Het LIMC had inderdaad gegevens uit publiek toegankelijke bronnen zoals nieuwswebsites en sociale mediaplatforms verzameld, geanalyseerd en verwerkt. Daarbij waren algemene en bijzondere persoonsgegevens vergaard. Al gebeurde dit met de beste bedoelingen, niet op grote schaal en slechts bij wijze van 'bijvangst', de Algemene verordening gegevensbescherming (AVG) stond dat niet toe.⁹

Daarop volgde een externe onderzoekscommissie. Deze 'Commissie-Brouwer' publiceerde een rapport met de veelzeggende titel *Grondslag gezocht*. De rode draad:

'Geen juridische grondslag was aanwezig voor de uitvoering van de activiteiten door het LIMC – óók in het geval géén persoonsgegevens zouden zijn verwerkt. De krijgsmacht heeft zichzelf daardoor gedurende acht maanden in het nationale domein ingezet en dat kwalificeert zonder meer als onrechtmatig.'¹⁰

Belangwekkend is ook vooral de constatering dat de krijgsmacht bij de 'gereedstelling' (daarover zo meer) klem was komen te zitten tussen het vigerende recht en de

nieuwe dreigingen van hybride conflictvoering, met name in cyberspace. In die strijd is informatie doel, middel én wapen. De bestaande juridische kaders bleken een sta-in-de-weg. Structurele oplossingen in wet- en regelgeving waren nodig, zo luidde het advies. Defensieonderzoekers, de Wetenschappelijke Raad voor het Regeringsbeleid en de Adviesraad Internationale Vraagstukken trokken vergelijkbare conclusies.¹¹

De ambitie is om een 'informatiegestuurde krijgsmacht' te hebben in 2035

De urgentie om naast conventionele oorlogsvoering ook voorbereid te zijn op moderne conflictvoering wordt breed gevoeld in defensiekringen. Onder meer de invasies van Rusland in Oekraïne, de beïnvloeding van de Amerikaanse presidentverkiezingen, de desinformatie rond het MH17-proces en de dronezwermen bij Defensielocaties in binnen- en buitenland tonen de ernst van de toenemende hybride dreiging aan. Nu de wereld in een 'permanente staat van competitie' geraakt, vloeien de eerste en de derde hoofdtaak van de krijgsmacht – respectievelijk bescherming van het eigen en bondschappelijk grondgebied en ondersteuning van civiele autoriteiten – in elkaar over.¹² Defensie ontwikkelde daarom het strategische concept 'Informatiegestuurd Optreden' (IGO), net als overigens de Nationale Politie.¹³ De ambitie is om een 'informatiegestuurde krijgsmacht' te hebben in 2035.¹⁴ Men wil in staat zijn sneller de juiste informatie te verzamelen en te analyseren teneinde de veiligheidssituatie goed te begrijpen, zodat betere besluiten kunnen worden genomen om met de beschikbare (militaire) middelen de gewenste effecten te bereiken. In militaire termen gaat het om *situational awareness*, *forecasting*, *insight* en *foresight*.

Deze ombouw van de krijgsmacht leidt ertoe dat Defensie vaker inbreuk zal maken op privacyrechten van (buitenlandse én Nederlandse) burgers, al zullen zulke inbreuken volgens de regering steeds 'beperkt en niet intentioneel' zijn.¹⁵ Een een vereist een formeel-wettelijk kader op grond van artikel 10 Grondwet, artikel 8 EVRM en artikel 17 IVBPR. Op grond daarvan moeten

inbreuken bij wet voorzien, noodzakelijk en proportioneel zijn in een democratische samenleving en een specifiek, gerechtvaardigd belang dienen. De Wodg beoogt dat kader te bieden.

3. Gereedstelling

Militairen onderscheiden 'gereedstelling' en 'inzet'. Bij inzet komt het tot daadwerkelijke uitvoering van militaire taken, met geweldsgebruik. Gereedstelling betreft alle voorbereidingshandelingen daartoe en is een permanent, primair proces. De Wodg richt zich op dat laatste.¹⁶ Als het aan de regering ligt, staat deze wet altijd 'aan'. Het gaat hier niet om staatsnoodrecht of ander noodrecht (maar schurkt er wel tegenaan).¹⁷ Wat 'gereedstelling' juridisch inhoudt, is niet geheel duidelijk. De regering werkt deze brede doelomschrijving uit met een hele trits werkwoorden.¹⁸ In de kern zijn drie categorieën gereedstellingsactiviteiten te onderscheiden. De eerste categorie wordt gevormd door activiteiten die bijdragen aan de geoefendheid van de eenheden van de krijgsmacht, de materiële gereedheid en de personele gereedheid. Oftewel: werven, opleiden, trainen en oefenen. De tweede categorie betreft het vergaren van kennis over de operationele omgeving waar de militaire taakuitvoering zal plaatsvinden. De derde betreft het bewaken en beveiligen van militaire objecten en personeel ('*force protection*'). Hoe deze gereedstellingsactiviteiten gestalte krijgen verschilt per operationeel commando en is afhankelijk van de eigenschappen van het betreffende operationele domein (land, zee, lucht, cyber, ruimte). Defensie is immers een gelaagde en verzuielde organisatie met een grote variëteit aan processen en werkwijzen.

4. Hoger recht

Voor het informatiehoofdstuk is de verhouding tot hoger recht cruciaal. Die is nogal ingewikkeld gemaakt. De kern is dat een deel het AVG-regime niet van toepassing is. De Wodg bevat een eigen verwerkingsregime. Voor vakspecialisten volgt een korte uitleg.

De AVG is niet van toepassing op activiteiten die buiten de werkingssfeer van het Unierecht vallen.¹⁹ Dat zijn met name activiteiten in het kader van de nationale veiligheid,²⁰ waaronder ook bepaalde activiteiten van de krijgsmacht.²¹ Belangrijk is om op te merken dat het andere 'Europese' gegevensbeschermingsrechtelijke regime, de zogeheten 'Conventie 108+' (ook wel bekend als het gemoderniseerde Dataprotectieverdrag van de Raad van Europa), wél van toepassing is op persoonsgegevensverwerking

3. Het *Militair Rechtelijk Tijdschrift* bevat wel enkele AVG-bijdragen.

4. Het LIMC stond onder commando van het Operationeel Ondersteuningscommando Land (OOCL).

5. 'Landmachttop negeerde waarschuwingen over inzamelen data van burgers', NOS 2 november 2021.

6. 'Interne strijd bij defensie om verzamelen data', NRC 2 november 2021.

7. 'Hoe defensie de eigen bevolking in de gaten houdt', NRC 15 november 2020.

8. 'De internetninja's van de krijgsmacht lopen stuk op een privacymuur', NRC 23 januari 2023.

9. FG Defensie, *Onderzoek experimenteeromgeving LIMC*, Den Haag, 2021.

10. Commissie-Brouwer, *Grondslag gezocht*, Den Haag, 2023, p. 6.

11. P. Duchéine, P. Pijpers & M. Zwanenburg, *Tanden voor de Leeuw*, Breda, 2024; WRR, *Nederland in een fragmenterende wereldorde*, Den Haag, 2024; AIV, *Hybride dreigingen en maatschappelijke weerbaar-*

heid, Den Haag, 2024.

12. Zie R. de Wijk, F. Bekkers & T. Sweijts, *Hybride dreigingen en hybride oorlog: consequenties voor de Koninklijke Landmacht*, Den Haag, 2020.

13. *Kamerstukken II* 2022/23, 36124, nr. 35.

14. *Defensievisie 2035: Vechten voor een veilige toekomst* (2020). Vgl. *Defensienota* (2026), p. 36-37, 48 en 100.

15. *Kamerstukken II* 2025/26, 36970, nr. 3, p. 223.

16. Art. 1.2 Wodg.

17. Veelzeggend is dat de regering zich gedwongen heeft gevoeld om uitgebreid uiteen te zetten waarom geen sprake is van (staats)noodrecht. Zie *Kamerstukken II* 2025/26, 36970, nr. 3, met name par. 6.1.

18. Art. 2.1 Wodg.

19. Art. 2 lid 2 sub a AVG.

20. Zie R.H.T. Jansen, *Toezicht op de AIVD en de MIVD* (diss. Nijmegen), Deventer: Wolters Kluwer 2025, hfdst. 3.

21. Art. 4 lid 2 VEU.

Op gereedstellingsactiviteiten zijn de AVG en de UAVG tot dusver dus onverkort van (overeenkomstige) toepassing. Daar lijkt men spijt van te hebben

gen in dat kader.²² De Nederlandse wetgever heeft de regels voor gegevensbescherming voor Defensie bij de totstandkoming van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) gelijkgetrokken met de AVG. Verwerkingen ten behoeve van de daadwerkelijke inzet of het terbeschikkingstellen aan de krijgsmacht zijn echter uitgezonderd.²³

Op gereedstellingsactiviteiten zijn de AVG en de UAVG tot dusver dus onverkort van (overeenkomstige) toepassing.²⁴ Daar lijkt men spijt van te hebben. Het wordt nu technisch, want de regering kiest een bijzondere aanvliegroute. Via de Wodg worden de AVG en de UAVG grotendeels van overeenkomstige toepassing verklaard op gereedstellingsactiviteiten.²⁵ Verschillende AVG-bepalingen zijn echter 'uitgeschakeld', met name die over de rechten van betrokkenen (daarover straks meer) en datalekken (die omwille van de vertrouwelijkheid van gereedstellingsactiviteiten niet meldingsplichtig zijn).²⁶ Deze systematiek geldt voor hoofdstuk 4 (informatieomgeving) van de Wodg. Voor zover Defensie gegevens verwerkt op grond van de hoofdstukken 3 (fysieke leefomgeving) en 5 tot en met 8 (personeel, inkoop, wijziging andere wetten en slotbepalingen) zijn de AVG en de UAVG wél volledig van toepassing.

Opvallend is bovendien de mogelijkheid om bij ministerieel besluit af te wijken van de (U)AVG, indien dat nodig wordt geacht ter voorkoming van 'een belemmering of onaanvaardbare vertraging van de gereedheid'.²⁷ Maar let wel: met deze 'ad hoc uitzonderingsmogelijkheid'²⁸ mag de minister niet afwijken van afdeling 4 van hoofdstuk IV AVG (verwerkingsverantwoordelijke en verwerker), de hoofdstukken VI-VIII AVG (onafhankelijk toezicht, samenwerking, beroep, aansprakelijkheid en sancties), hoofdstuk 2 UAVG (Autoriteit Persoonsgegevens) en paragraaf 3.4 UAVG (Functionaris Gegevensbescherming).²⁹ Afwijken van Grondwet en internationaalrechtelijke verplichtingen, waaronder Conventie 108+ (na ratificatie), mag evenmin.³⁰ Dat volgt logisch uit de normenhierarchie.

Zoals de Raad van State terecht opmerkt: niet alleen is dit aparte gegevensbeschermingsrechtelijke regime complex, het roept ook de vraag op aan welke verwerkingsregels Defensie nu precies is gehouden voor andere doelen dan gereedstelling. Vooralsnog zijn deze regels verspreid over verschillende wetten.³¹ Het kabinet heeft inmiddels toegezegd dat het later, aan de hand van de Wodg-ervaringen, zal bezien of een eenduidig en uitputtend stelsel voor gegevensverwerkingen van Defensie – een 'Wet op de defensiegegevens' – aangewezen is.³²

5. Algemene bepalingen

De regering stelt voorop – en dat beoogt waarschijnlijk bij te dragen aan de rechtvaardiging voor de hierna te behandelen ruime wettelijke grondslagen – dat Defensie bij gereedstellingsactiviteiten geen intentie heeft om persoonsgegevens te verwerken.³³ Het is militairen vooral te doen om technische gegevens, zoals georuimtelijke informatie ('GEOINT'), beeldmateriaal ('IMINT') en gegevens over radar-, laser- en *non imagery*-infraroodsystemen ('MASINT'). Het achterhalen van de inhoud van communicatie van burgers is dus geen doel op zich. Soms is de verwerking van persoonsgegevens echter nodig, zoals in 'bijvangst'-situaties. Men kan ook denken aan een militaire drone die buiten of op de rand van een defensie terrein vliegt en gegevens opvangt. Dan gelden de volgende regels.

De Wodg wijst de minister aan als verwerkingsverantwoordelijke.³⁴ Ten behoeve van de gereedstelling mag hij persoonsgegevens verwerken, voor zover (a) afkomstig uit eigen waarneming, al dan niet met gebruik van technische hulpmiddelen (niet nader gedefinieerd), (b) afkomstig uit publiek toegankelijke bronnen ('OSINT'), (c) afkomstig uit informatiebronnen van derden ('primaire commerciële data die door de krijgsmacht, al dan niet samen met de MIVD, worden ingekocht')³⁵ en ontvangen van (d) de diensten, (e) bondgenoten en (f) overige bevoegde nationale- en internationale privaatrechtelijke of publiekrechtelijke instanties.³⁶ Het kan dan gaan om – dit lijstje is niet-limitatief – namen, adressen, woonplaatsen, rangen, schalen, functies en gedragsinformatie van burgers of defensiepersoneel.³⁷

Belangrijk: deze gegevens mogen in beginsel niet worden verwerkt met het oogmerk om personen stelselmatig te monitoren. Uit de wettekst volgt dat deze beperking 'in ieder geval' inhoudt dat (a) het op geautomatiseerde wijze en gericht op personen stelselmatig overnemen (lees: kopiëren) van persoonsgegevens verboden is en (b) technische hulpmiddelen niet mogen worden misbruikt om persoonsgericht onderzoek te verrichten terwijl dat niet 'redelijkerwijs voorzienbaar' is.³⁸ *Webcrawlers* of *web-scrapers* die op grote schaal internetinformatie inventariseren en opslaan om persoonsgegevens te verzamelen zijn dus verboden. Bij of krachtens AMvB kunnen nadere regels worden gesteld.³⁹

Defensie moet persoonsgegevens anonimiseren of pseudonimiseren. Dat is op zich al een flink verschil. Er is bovendien een escape: deze verplichting geldt alleen voor zover dat mogelijk is gelet op 'de stand van de techniek, de uitvoeringskosten, de aard, de omvang, de context van de verwerking, de risico's voor de rechten en vrijheden van natuurlijke personen en de risico's van de gereedheid'.⁴⁰ 'In bijzondere omstandigheden, waarbij er een verhoogde militaire dreiging is en meer militairen dienen te worden gereed gesteld, kan er afgezien worden van deze maatregelen als die een belemmering opleveren voor de gereedheid van de krijgsmacht', zo licht de regering toe.⁴¹

Soms is het niet meteen duidelijk of iets een persoonsgegeven is. Denk aan kranteninformatie in cyrillichschrift.⁴² Defensie moet een dergelijke tekst dan eerst vertalen, voordat verdere verwerking mogelijk is. Het Wodg-regime staat dit om begrijpelijke redenen toe.⁴³ De volgende regeling roept meer vraagtekens op: eenmaal

verworven gegevens mogen ook voor een ander doel worden verwerkt dan waarvoor zij aanvankelijk zijn verzameld, indien (a) de minister daarvoor toestemming geeft en de verwerking voor dat andere doel (b) noodzakelijk en (c) proportioneel is.⁴⁴ Deze afwijking van het doelbindingsbeginsel tendeeert naar het uitgangspunt ‘binnen = binnen’ van de AIVD en de MIVD en komt de rechtszekerheid niet ten goede.

De hoofdregel is dat Defensie geen bijzondere persoonsgegevens verwerkt bij gereedstelling. Dat zijn gegevens over ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging of lidmaatschap van een vakbond.⁴⁵ Evenmin mogen genetische gegevens, biometrische gegevens en gegevens over iemands gezondheid, seksuele leven en seksuele gerichtheid worden verwerkt. Datzelfde geldt voor strafrechtelijke gegevens.⁴⁶ Uitzonderingen zijn slechts toegestaan – en op dit punt knoopt de regering aan bij de systematiek van de Wet politiegegevens – als verwerkingen van deze bijzondere gegevens (a) onvermijdelijk zijn, (b) ‘in aanvulling zijn op de verwerking van andere persoonsgegevens betreffende de persoon’ en (c) de gegevens afdoende zijn beveiligd.⁴⁷ Concrete voorbeelden ontbreken (dat kan strategisch zijn), waardoor het moeilijk voorstelbaar is in welke gevallen de regering deze uitzonderingsmogelijkheid van de plank wil kunnen halen.

De Wodg kent een afzonderlijke bepaling voor zogeheten ‘omvangrijke gegevensverzamelingen’. Dat is een verzameling gegevens die persoonsgegevens bevat van

een groot aantal personen, waarvan het merendeel van de personen (daar staat niet: persoonsgegevens) niet relevant is voor de gereedstelling (daar staat niet: voor bepaald onderzoek).⁴⁸ Deze terminologie wijkt af van die uit de Wiv-context. In dat domein hanteert men de term ‘bulkdata(sets)’, maar met een andere definitie.⁴⁹ De regering acht omvangrijke gegevensverzamelingen ‘essentieel’ om de krijgsmacht te beschermen en uiteindelijk doelgericht te kunnen optreden in de operationele omgeving.⁵⁰ Een nadere uitleg ontbreekt. Onduidelijk is op welke wijze Defensie zulke datasets precies mag vergaren, hoewel juist over dit soort bulkdatavergaring door de overheid maatschappelijk ongemak bestaat. De regering benadrukt dat defensieonderdelen ‘in veel gevallen’ niet geïnteresseerd zijn in persoonsgegevens en deze dus ‘onverwijld’ uit de datasets zullen filteren.⁵¹ De verwerking van dit soort gegevensverzamelingen is alleen toegestaan indien ‘die niet meer dan een beperkte inbreuk maken op de persoonlijke levenssfeer’ en na ministeriële toestemming.⁵² Defensie moet daarbij afwegen in hoeverre de betreffende gegevensverzameling inzicht geeft in bepaalde aspecten van iemands privéleven en rekening houdt met het aantal betrokken personen, het zicht dat de gegevens bieden op het netwerk van een persoon, de aanwezigheid van vertrouwelijke informatie en de locatiegegevens.⁵³ Om te voorkomen dat defensiepersoneel gaat grasduinen in deze datasets, wordt – net als bij de AIVD en de MIVD – een systeem van compartimentering en functiescheiding ingesteld.⁵⁴ Het *need to know*-principe is leidend.

De minister dient passende technische en organisatorische maatregelen te nemen om de juistheid en de volledigheid van gegevens te garanderen en deze gegevens adequaat te beveiligen.⁵⁵ Persoonsgegevens mogen niet langer worden bewaard dan strikt noodzakelijk voor het doel waarvoor ze zijn verwerkt. Zij moeten uiterlijk twee jaar na de datum van de eerste verwerking worden verwijderd en vernietigd, tenzij bewaringsvoorschriften zoals de Archiefwet 1995 daaraan in de weg staan. Aanvankelijk ontbrak een tijdsbeperking. Mede op advies van de Raad van State is er alsnog een maximumtermijn geïntroduceerd.⁵⁶ De minister mag de initiële termijn hoogstens

Deze afwijking van het doelbindingsbeginsel tendeeert naar het uitgangspunt ‘binnen = binnen’ en komt de rechtszekerheid niet ten goede

22. Trb. 2018, 201. Zie R.H.T. Jansen & M.D. Reijneveld, ‘Conventie 108+ en (toezicht op) gegevensverwerkingen in het nationale veiligheidsdomein’, *Computerrecht* 2021, afl. 5, p. 411-422;

H.R. Kranenborg & L.F.M. Verheij, *De Algemene verordening gegevensbescherming in Europees en Nederlands perspectief*, Deventer: Wolters Kluwer 2024, par. 3.3.

23. Art. 3 lid 3 sub a UAVG. Op basis van de UAVG regelt de Regeling Gegevensbescherming Militaire Operaties (RGMOM) de positie van Defensie tijdens inzet. Deze regeling komt te vervallen met de inwerkingtreding van het – met de Wodg samenhangende – Besluit gegevensverwerking defensie. Zie ook *Kamerstukken II* 2023/24, 36455, nr. 4, p. 4-5.

24. Art. 3 lid 1 en lid 2 UAVG.

25. Art. 4.4 lid 1 Wodg.

26. Uitzonderd zijn art. 9 en 10, hoofdstuk III en art. 33, 34 en 36 AVG alsook art. 22-33 UAVG. Volgens art. 42 UAVG is er ook een meldplichtuitzondering voor financiële instellingen.

27. Art. 4.4 lid 2 Wodg. Zie *Kamerstukken II* 2025/26, 36970, nr. 3, p. 35 Deze bevoegdheid is eerder bekritiseerd door de AP. Zie Advies AP, d.d. 16 september 2025, p. 3-4.

28. *Kamerstukken II* 2025/26, 36970, nr. 3, p. 125.

29. Art. 4.4 lid 3 Wodg.

30. *Kamerstukken II* 2025/26, 36970, nr. 3, p. 126.

31. *Kamerstukken II* 2025/26, 36970, nr. 4, p. 14.

32. *Kamerstukken II* 2025/26, 36970, nr. 4, p. 15-16.

33. *Kamerstukken II* 2025/26, 36970, nr. 3, p. 119.

34. Art. 4.1 Wodg.

35. *Kamerstukken II* 2025/26, 36970, nr. 3, p. 120.

36. Art. 4.2 lid 2 Wodg.

37. DPIA Wodg, p. 12.

38. Art. 4.2 lid 3 Wodg.

39. Art. 4.2 lid 4 Wodg.

40. Art. 4.3 lid 1 Wodg.

41. *Kamerstukken II* 2025/26, 36970, nr. 3, p. 123.

42. *Kamerstukken II* 2025/26, 36970, nr. 3, p. 124.

43. Art. 4.3 lid 2 Wodg.

44. Art. 4.3 lid 3 Wodg. Vgl. art. 6 lid 4 AVG.

45. Vgl. art. 9 AVG.

46. Vgl. art. 10 AVG.

47. Art. 4.5 Wodg.

48. Art. 1 Wodg.

49. Art. 1 onder f Tijdelijke cyberwet. Zie CTIVD-Toezichtrapport nr. 70 (2020); Commissie-Jones-Bos, *Evaluatie 2020*, Den Haag, 2021, hfdst. 4; CTIVD-Toezichtrapport nr. 84 (2026).

50. *Kamerstukken II* 2025/26, 36970, nr. 3, p. 127.

51. *Kamerstukken II* 2025/26, 36970, nr. 3, p. 127.

52. Art. 4.6 lid 1 Wodg. Vgl. B.P.F. Jacobs, ‘Proportionaliteit en abstractie van gegevensverwerking’, AA 2023, afl. 4, p. 246-249.

53. Art. 4.6 lid 2 Wodg.

54. Art. 4.6 lid 3 en lid 4 Wodg.

55. Art. 4.3 lid 4 Wodg.

56. *Kamerstukken II* 2025/26, 36970, nr. 4, p. 33-34.

tweemaal met een termijn van maximaal twee jaar verlengen.⁵⁷ Voor overige – technische – gegevens gelden géén opslagbeperkingen.

6. Gereedstellingsactiviteiten en informatiepositie

Het informatiehoofdstuk bevat naast de algemene waarborgen ook regelingen voor een aantal nader geconcretiseerde gereedstellingsactiviteiten en de opbouw van een informatiepositie. Samengevat: Defensie moet kunnen opleiden, trainen en oefenen in zowel fysieke als digitale oefenomgevingen en daarbij kunnen experimenteren met nieuw materieel en nieuwe technieken.⁵⁸ De regering kan het lijstje met gereedstellingsactiviteiten bij AMvB aanvullen, mocht dat nodig zijn vanwege nieuwe technologieën of onvoorziene ontwikkelingen.⁵⁹ Dat creëert een open stelsel, met veel flexibiliteit.

Om een ‘veilig en doeltreffend’ militair optreden te garanderen mag de minister voortaan ‘kennis’ – de regering vermijdt in de Wodg het woord ‘inlichtingen’ – vergaren over de ‘relevante operationele omgeving’.⁶⁰ Uiteindelijk is de crux hoe ruim (of beperkt) men deze begrippen uitlegt. In de op punten enigszins wijdlopijge toelichting zijn weinig piketpaaltjes te vinden. De bepaling over de categorieën gegevens die in dat kader mogen worden verzameld volgt dan ook eenzelfde flexibele aanpak. Die opsomming loopt uiteen van fysisch geografische, oceanologische en meteorologische gegevens tot radargegevens, gegevens over digitale infrastructuur en – let op de ruime formulering – gegevens over ‘relevante trends en ontwikkelingen in het maatschappelijk verkeer’.⁶¹ De gemene deler is dat het primair gaat om technische gegevens. Persoonsgericht onderzoek is in beginsel niet toegestaan.⁶² Wij komen zo terug op de uitzonderingsmogelijkheid.

Het onder dit regime toegestane OSINT-onderzoek past in een trend. Openbronnenbevoegdheden als deze poppen in steeds meer beleidsdomeinen op.⁶³ Inlichtingenexpert Bob de Graaff spreekt zelfs over een ‘geruisloze groei van inlichtingenorganen’.⁶⁴ Een toenemend aantal overheidsorganisaties wil via OSINT-technieken burgers, organisaties of ontwikkelingen monitoren. Vaak *downplayen* zij deze onderzoeksbevoegdheid, bijvoorbeeld door te stellen dat zij slechts ‘trends’ en ‘fenomenen’ (dus geen personen) in kaart brengen. Of men trekt een andere kaart: waarom zouden burgers wel ongehinderd andere rondstruinen op het internet, maar de overheid niet? OSINT-onderzoek is technologisch volop in beweging. Vanwege de toegenomen digitale beschikbaarheid van data en de mogelijkheden om deze – al dan niet met behulp

van AI – sneller en systematischer te verwerken, neemt de intrusiviteit ervan toe. Juridisch is dit heikele materie. Openbronnenbevoegdheden zijn op uiteenlopende wijze vormgegeven. Standaardbepalingen ontbreken.⁶⁵ Volgens de meeste definities is het begrip ‘open bron’ in elk geval ruimer dan het algemeen spraakgebruik doet vermoeden. Ook informatie achter betaalmuren en op het darkweb (zoals gelekte of gehackte gegevens) kan eronder vallen. Eerder leidden OSINT-onderzoeken door gemeenten en de NCTV dan ook tot veel discussie.⁶⁶ Temeer vanwege het wankel juridische fundament en het gebrek aan toezicht. Het is ook precies dit soort onderzoek dat leidde tot het politieke en maatschappelijke onbehagen over het LIMC.⁶⁷ Verwijten in termen als ‘cowboyspionage’, ‘fishing expeditions’ en ‘surveillancepraktijken’ vielen daarbij regelmatig, en dat is niet onbegrijpelijk.⁶⁸

Terug naar de Wodg. De Minister van Defensie krijgt een zorgplicht tot bewaken en beveiligen. Die betreft niet alleen vaste en mobiele militaire objecten en het personeel, maar uitdrukkelijk ook netwerk- en informatiesystemen.⁶⁹ Geserreerd weergegeven volgt daaruit dat digitale dreigingsinformatie (*‘Cyber Threat Intelligence’*) mag worden verzameld, geanalyseerd en gedeeld. Voor de specialist: (persoons)gegevensverwerkingen zijn toegestaan ten behoeve van (a) het monitoren en analyseren van cyberdreigingen, kwetsbaarheden en incidenten (met name vijandige hackoperaties), (b) het verstrekken van informatie daarover, (c) het proactief scannen en testen van netwerk- en informatiesystemen van defensieonderdelen, waaronder het analyseren van cyberdreigingen (bijvoorbeeld *red team tests of threat hunting*),⁷⁰ (d) het reageren op cyberincidenten, (e) het verzamelen en analyseren van forensische gegevens en het verhogen van de interne cyberweerbaarheid en (f) het verlenen van wederzijdse bijstand aan een nationale of bondgenootschappelijke entiteit die is belast met het beveiligen van een netwerk- en informatiesysteem. Ook deze lijst is bij AMvB aan te vullen.⁷¹ Denk in elk geval aan verwerkingen van IP-adressen, e-mailadressen en domeinnamen, met bijbehorende registratiegegevens.

Naast de eerder genoemde gegevensbronnen mag de minister in het kader van bewaken en beveiligen ook persoonsgegevens verwerken die hij heeft ontvangen van de Koninklijke Marechaussee op grond van de Wet politiegewens.⁷² Als aanvulling op andere kaders, zoals de Rijkswet geweldgebruik bewakers militaire objecten, krijgt hij bovendien de bevoegdheid om ‘een object’ tot stoppen te brengen of zodanig te beïnvloeden dat het gevaar wijkt, eventueel met gebruikmaking van een elektromagnetisch spectrum.⁷³ In gewone mensentaal is dit een bevoegdheid om droneaanvallen af te slaan. Dat kan door ‘jamming’ of ‘hacking’.⁷⁴

7. Gegevensverstrekking

De Wodg bevat een speciaal verstrekkingsregime. Gegevensverstrekking is een discretionaire bevoegdheid van de minister. Andere personen of instanties kunnen bij Defensie niet zomaar persoonsgegevens opeisen.⁷⁵ Verstrekking van (persoons)gegevens is alleen toegestaan ten behoeve van de goede uitvoering van deze wet en voor zover de vertrouwelijkheid zich daartegen niet verzet. De kring van mogelijke ontvangers omvat in elk geval medeoverheden,

Het onder dit regime toegestane OSINT-onderzoek past in een trend. Openbronnenbevoegdheden als deze poppen in steeds meer beleidsdomeinen op

de diensten, de politie, de Koninklijke Marechaussee, het openbaar ministerie, burgemeesters, relevante cybersectoriteiten en bondgenoten.⁷⁶ Met het oog op een zwaarwegend algemeen belang mag de regering deze lijst bij AMvB uitbreiden.⁷⁷ Als de landsverdediging, de nationale veiligheid of de bescherming van het leven van een persoon het dringend vergt, mag de minister daartoe – incidenteel⁷⁸ – ook zelfstandig overgaan. Dat vereist een *heads-up* aan de AP.⁷⁹ Het uitgangspunt is dat de oorspronkelijke persoonsgegevens niet worden verstrekt, maar in gepseudonimiseerde vorm worden gedeeld.⁸⁰

Met name de categorie ‘bondgenoten’ is interessant (en potentieel problematisch). Het begrip ‘bondgenoot’ is elders in het nationale recht niet strak gedefinieerd.⁸¹ De Wodg-definitie omvat NAVO-landen, lidstaten van de EU én andere door de Minister van Defensie aangewezen staten.⁸² Met eventueel veranderende geopolitieke verhoudingen is in zoverre geen rekening gehouden dat NAVO-landen en EU-lidstaten van rechtswege ‘bondgenoten’ zijn. Onder Trump II verzuren de verhoudingen tussen Amerika en Europa echter zodanig, dat te betwijfelen valt of zij per definitie onder deze categorie zouden moeten vallen. In de toelichting fietst de regering vakkundig om deze hete brei heen.⁸³ Men kan overigens dezelfde vraag opwerpen met betrekking tot het autocratisch geregeerde Turkije van Erdogan en – tot voor kort – het Hongarije van Orbán.

Het gaat hier weliswaar om een bevoegdheid (dus geen verplichting), maar bij dit soort gegevensdelingen is het oppassen geblazen. De AIVD en de MIVD kennen een genuanceerdere regeling. Zij moeten per land een ‘wegingsnotitie’ opstellen, met een analyse van de democratische inbedding van hun partnerdiensten, de eerbiediging van mensenrechten en de professionaliteit en betrouwbaarheid van dat andere regime omschrijven.⁸⁴ Periodieke updates zijn verplicht. De uitkomst van deze exercitie is dat momenteel minder gegevens worden gedeeld met Amerikaanse diensten vanwege Trumps grote verbouwing van de Verenigde Staten.⁸⁵ De Wodg mist een dergelijke systematiek. Wel gelden restricties. Gegevensverstrekking aan bondgenoten mag alleen plaatsvinden als dit noodzakelijk is ter uitvoering van bondgenoot-

Het gaat hier weliswaar om een bevoegdheid (dus geen verplichting), maar bij dit soort gegevensdelingen is het oppassen geblazen

schappelijke taken en verplichtingen op militair vlak dan wel bij indicaties dat zulks noodzakelijk is voor ‘de veiligheid en zwaarwegende algemene belangen van die bondgenoot en van de vrijheid en het leven van een persoon’.⁸⁶ Defensie mag persoonsgegevens bovendien niet verstrekken aan derde landen of organisaties als dat in het specifieke geval strijdig is met de belangen van het Koninkrijk der Nederlanden of een gevaar oplevert voor het recht op leven, menselijke integriteit en vrijheid of andere fundamentele mensenrechten van de betrokkene.⁸⁷

Wij willen het volgende benadrukken. Als Defensie meer (persoons)gegevens mag gaan verwerken, komt op haar ook de plicht te rusten om deze adequaat te beveiligen. Dat is geen sinecure. Defensie heeft in de afgelopen jaren belangrijke ICT-projecten uitbesteed aan buitenlandse commerciële partijen. Dat is om allerlei redenen goed te begrijpen, maar blijkt nu ook risicovol. De huidige Amerikaanse president deinst er niet voor terug om via zulke strategische afhankelijkheden andere landen – ook bondgenoten – onder druk te zetten of te chanteren.⁸⁸ Het informatiehoofdstuk gaat daarmee niet alleen over privacy, maar óók over digitale autonomie en technologische soevereiniteit. Gegevens over Nederland, Nederlanders en Nederlandse militairen mogen niet in verkeerde handen vallen. Defensie staat daarvoor aan de lat. Dat vergt een kritische houding, geen volgzaam.

8. Waarborgen en toezicht

Tijdens de internetconsultatie zijn er veel zorgen geuit over gevreesde privacyschendingen. Ook de DPIA schetst potentiële risico's. Wij vatten graag samen, voor zover relevant. (1)

57. Art. 4.7 Wodg.

58. Art. 4.8 Wodg.

59. Art. 4.8 lid 1 onder g en lid 3 Wodg.

60. Art. 4.9 Wodg.

61. Art. 4.9 lid 2 Wodg.

62. Art. 4.9 lid 3 Wodg.

63. Zie o.a. het themanummer ‘OSINT in het veiligheidsdomein’, *Tijdschrift voor Veiligheid* (2025).

64. B.G.J. de Graaff, ‘Privacy of veiligheid?’, *De Groene Amsterdammer* 16 augustus 2023.

65. Vgl. Advies AP, d.d. 16 september 2025, p. 7-8. De regering volgt in dit voorstel de Wet coördinatie terrorismebestrijding en nationale veiligheid en het rapport van de Commissie modernisering opsporingsonderzoek in het digitale tijdperk (2018).

66. Zie o.a. J.J. Oerlemans &

Y.E. Schuurmans, ‘Internetonderzoek door bestuursorganen’, *NJB* 2019/1132, afl. 20, p. 1458-1466; W. Bantema e.a., *De Black Box van gemeentelijke online monitoring*, Den Haag, 2021; R.H.T. Jansen, ‘Less is more? Over het grondslagenvraagstuk van de Nationaal Coördinator Terrorismebestrijding en Veiligheid’, *NJB* 2024/493, afl. 9, p. 588-599.

67. Zie met name ‘Leger verzamelde data in Nederland’, *NRC* 15 november 2020.

68. B.P.F. Jacobs, ‘Cowboy Spionnen’, *iBestuur* 27 mei 2021.

69. Art. 4.10 lid 1 Wodg.

70. *Kamerstukken II* 2025/26, 36970, nr. 3, p. 145.

71. Art. 4.11 Wodg.

72. Art. 4.12 Wodg.

73. Art. 4.10 lid 3 Wodg.

74. *Kamerstukken II* 2025/26, 36970, nr. 3, p. 143.

75. *Kamerstukken II* 2025/26, 36970, nr. 3, p. 147.

76. Art. 4.13 lid 1 Wodg.

77. Art. 4.13 lid 4 Wodg.

78. *Kamerstukken II* 2025/26, 36970, nr. 3, p. 150.

79. Art. 4.13 lid 5 en lid 6 Wodg.

80. Art. 4.13 lid 7 Wodg.

81. Zie R.H.T. Jansen, ‘De Verenigde Staten onder Trump II: ‘bondgenoot’, ‘frenemy’ of ‘vijand’’, *NJB* 2026/908, afl. 17, p. 1314-1325.

82. Voorgenomen art. 1.1 Wodg.

83. Wel merkt de regering terloops op: ‘Internationale partners staan niet altijd welwillend tegenover een Europees verdrag met Europese juridische bevoegdheden’.

Deze passage lijkt te hinten op de Verenigde Staten. Zie *Kamerstukken II* 2025/26, 36970, nr. 3, p. 149.

84. Art. 88 Wiv 2017.

85. ‘Nederlandse diensten delen minder informatie met VS’, *de Volkskrant* 18 oktober 2025.

86. Art. 4.13 lid 1 onder f en lid 2 Wodg.

87. Art. 4.13 lid 3 Wodg.

88. Vooralsnog ziet Defensie geen veiligheidsrisico's bij bedrijven als Cisco en Kyndryl. Zie *Kamerstukken II* 2025/26, 35728, nr. 24, p. 2. Vgl. ‘Waarom zou Kyndryl wel de IT-infrastructuur van defensie mogen bouwen, maar niet DigiD kunnen beheren’, *NRC* 26 februari 2026.

De 'redelijke privacy-verwachting' kan in het geding komen doordat taken, verantwoordelijkheden en bevoegdheden van overheidsorganen in het veiligheidsdomein 'overlappen of onduidelijk zijn onderscheiden'. (2) Het is mogelijk dat persoonsgegevens zonder voldoende beperkingen worden verzameld en gedeeld, met ongeautoriseerd of ongewenst gebruik daarvan door onbevoegden tot gevolg (*scope creep*). (3) Er kan schade ontstaan door inadequaat gegevensbeheer en gebrekkige beveiliging. Voorts zijn er risico's op (4) profilering en discriminatie door inherente bias in geautomatiseerde systemen en profileringstechnieken, (5) weinig effectieve rechtsbescherming door de vertrouwelijkheid van defensieactiviteiten en (6) *chilling effects*, inhoudende dat burgers hun gedrag aanpassen uit angst voor monitoring door Defensie.⁸⁹

Om deze en aanpalende risico's te mitigeren bevat de Wodg – het AVG-hoofdstuk over rechten van betrokkenen is voor de gereedstelling buiten werking gesteld – een aantal maatregelen. De minister moet mededeling doen over de regels omtrent (voorgenomen) persoonsgegevensverwerkingen, voor zover de vertrouwelijkheid daaraan niet in de weg staat.⁹⁰ Betrokkenen hebben een recht op kennisneming; de minister dient op een verzoek daaromtrent in beginsel binnen drie maanden te beslissen, maar kan deze termijn met vier weken verdagen.⁹¹ De wet omschrijft limitatief de weigeringsgronden voor kennisneming.⁹² Correctie of aanvulling door de betrokkene is mogelijk door een schriftelijke verklaring in de defensiesystemen te laten voegen.⁹³ Het gaat dus niet om rectificatie door vervanging.

Effectief toezicht is cruciaal. Voor zover dat niet al is

Eerdere ervaringen rechtvaardigen niet per se het sterke vertrouwen in voornamelijk intern toezicht

vereist op grond van de AVG, bepaalt Conventie 108+ dat daarin blijvend moet zijn voorzien.⁹⁴ Niet ter discussie staat dat Nederland reeds aan deze eis voldoet. De regering wil geen institutionele wijzigingen in het toezicht aanbrengen. Het gevolg is dat het bestaande stelsel van onafhankelijk toezicht door de Autoriteit Persoonsgegevens (AP) met intern toezicht via de onafhankelijke Functionaris Gegevensbescherming (FG) blijft bestaan.⁹⁵ Afwijken daarvan mag niet.⁹⁶ Om het praktisch hanteerbaar te houden wil de regering het toezicht wel 'in beginsel intern' organiseren. De bestaande commandostructuur biedt volgens haar namelijk 'een robuust kader' met 'zowel flexibiliteit als controle'. Gespecialiseerde teams zullen intern controleren of persoonsgegevens rechtmatig, behoorlijk en transparant zijn verwerkt.⁹⁷ Het externe toezicht zal vooral fungeren als 'een extra laag van controle en beoordeling van de naleving van wettelijke vereisten'.⁹⁸

Ex ante-toetsingsmechanismen – vergelijkbaar met de rol van de rechter-commissaris in het Wetboek van Strafvordering of de Toetsingscommissie Inzet Bevoegd-

heden in de Wiv 2017 – ontbreken. De Raad voor de rechtspraak adviseerde om zulke mechanismen te introduceren, nu Defensie informatie mag verstrekken ten behoeve van de voorkoming, opsporing en vervolging van strafbare feiten.⁹⁹ De regering wil daar blijkbaar niet aan, maar legt niet uit waarom niet. Waarschijnlijk is de reden gelegen in de vereiste snelheid van handelen en – in bestuurstaal – efficiency. Gechargeerd gesteld: vooraf toetsen geeft 'gedoe'. Dat kan de operationele snelheid en wendbaarheid schaden. Dat snappen wij wel. Eerdere ervaringen rechtvaardigen echter niet per se het sterke vertrouwen in voornamelijk intern toezicht. De Commissie-Brouwer constateerde dat in elk geval bij de Landmacht onvoldoende AVG-deskundigheid was ingeschakeld voor operaties in de informatieomgeving.¹⁰⁰ Defensie zal die expertise dus in huis moeten halen.

9. Verhouding tot de MIVD

Ons valt op dat het contrast tussen de Wodg en de Wiv 2017 (die voor de MIVD geldt) groot is. Bij de Wiv is de afgelopen decennia sterk – wellicht té sterk – ingezet op doelbinding en regulering via uitputtende, limitatieve regelgeving. De Wodg biedt daarentegen een hoge mate van flexibiliteit, met open normen en uitzonderingsmogelijkheden. Deels is dat begrijpelijk. De krijgsmacht en de MIVD hebben andere taken (zie hierna). De vraag is evenwel hoe beide rechtsregimes zich in de praktijk tot elkaar zullen gaan verhouden, zeker na de herziening van de Wiv 2017. Laatstgenoemde wet krijgt een sterker militair accent¹⁰¹ en wordt omgedoopt tot de 'Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten' (Wbmv). Uit de onlangs gepresenteerde internetconsultatieversie blijkt dat er omwille van 'een nauwere en versterkte samenwerking tussen de MIVD en de krijgsmacht' meer mogelijkheden komen om gegevens te delen – zelfs in ruwe, onbewerkte vorm, in bulk en *real time*.¹⁰² Volgens de planning moet dit project 'versneld' zijn afgerond in 2028.¹⁰³

Op dit moment zijn de consequenties van deze stelselgreep moeilijk in te schatten. Op het punt van persoonsgericht onderzoek lijken de Wodg en de Wiv 2017 alvast naar elkaar toe te kruipen, zij het met verschillende toepassingsvoorwaarden en toezichtregimes. Niet helemaal opgehelderd is waarom de krijgsmacht niet zou kunnen volstaan met het opvragen van informatie, bijvoorbeeld uit open bronnen, bij de MIVD. De dienst is daartoe goed geëquipeerd. De Wiv 2017 staat zowel incidenteel als stelselmatig onderzoek naar personen reeds toe, onder streng toezicht van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CITVD). Hoewel de regering de mogelijkheden voor persoonsgericht onderzoek in de Wodg tekstueel grotendeels 'dichtzet', is er één uitzondering: een commandant mag een onderzoek bevelen naar specifieke personen ('primair vijandelijke actoren, zoals een militair commandant van een vreemde krijgsmacht'),¹⁰⁴ desgewenst met behulp van technische hulpmiddelen (ook in dit verband niet nader gedefinieerd). Zulk onderzoek vergt ministeriële goedkeuring¹⁰⁵ en mag alleen plaatsvinden als (a) sprake is van een ernstig vermoeden dat deze persoon een gevaar vormt voor de veiligheid van de krijgsmacht, dit noodzakelijk is (b) voor het in kaart brengen van relevante publieke organen of civiele

U-bocht-scenario's, waarin de krijgsmacht activiteiten gaat uitvoeren die de MIVD niet mag verrichten (en andersom), zijn denkbaar en dienen te worden voorkomen

actoren die de krijgsmacht in de operationele omgeving kunnen ondersteunen of (c) voor de bescherming van personen in de operationele omgeving. Te denken valt aan onderzoek naar vijandelijke militaire commandanten, rebellen en te evacueren personen.¹⁰⁶

Het is kennelijk mogelijk dat de krijgsmacht en de MIVD 'kennis' vergaren over dezelfde personen. Over deze onderzoeken zal periodiek afstemming moeten plaatsvinden,¹⁰⁷ om 'deconflicte en efficiëntie in handelen' te bereiken en een 'dubbele inbreuk' op het recht op de persoonlijke levenssfeer 'zoveel als mogelijk' te voorkomen.¹⁰⁸ Nadere regels over deze afstemming volgen bij AMvB. Dit roept een fundamentele vraag op, zo constateerde ook de Raad van State: in hoeverre verschuiven inlichtingenwerkzaamheden die traditioneel door de MIVD worden verricht naar andere krijgsmachtonderdelen en wat betekent dit voor (de toepassing van) de Wiv 2017?

Het wetsvoorstel voorziet niet in een *wezenlijke* verschuiving van taken en werkzaamheden van de MIVD naar de krijgsmacht, zo repliceerde de regering (de cursivering is de onze).¹⁰⁹ De aard en de doelen van deze activiteiten lopen namelijk uiteen. Waar de inlichtingen van de MIVD vooral militair-strategisch van aard zijn ('welke militaire capaciteiten kan Rusland op korte termijn inzetten?'), dient de krijgsmacht zich te beperken tot gegevens van operationeel-tactische aard ('welke route is veilig voor patrouillering?'). Een oude klacht is dat de MIVD er – zoals de regering het formuleert – 'niet altijd tijdig' in is geslaagd om in de informatiebehoefte op operationeel en tactisch niveau te voorzien.¹¹⁰ Voortaan mag de krijgsmacht zelf aan de slag gaan. Verschillende 'I&V'-functies en organisaties staan al opgelijnd. Het Joint Intelligence, Surveillance, Target Acquisition & Reconnaissance Commando (JISTARC), een stafcompagnie met zeven eenheden in verschillende inlichtingendisiplines¹¹¹ en een paar honderd medewerkers, is het bekendst. Te denken valt ook aan 1 Civiel Militair Interactie Commando (1 CMI Co).

Overigens zal de MIVD vaak een ander – completer en nauwkeuriger – beeld kunnen creëren, bijvoorbeeld door verschillende open en gesloten bronnen met elkaar te correleren. En voor alle helderheid: de krijgsmacht krijgt op basis van deze wet géén bevoegdheid om gesloten bronnen te raadplegen.¹¹² Daarvoor blijft men afhankelijk van de MIVD.

10. Slot

Het informatiehoofdstuk van de Wodg geeft de krijgsmacht veel nieuwe juridische armslag. Niet alle onderdelen zijn even spannend. Militairen moeten zich voorbereiden op (digitale) gevechtshandelingen en daartoe technische gegevens over operationele omgevingen kunnen verzamelen. Dat is hoognodig. Verwerkingen van persoonsgegevens liggen evenwel gevoelig. Met reden, want het is nogal wat: voortaan mag de krijgsmacht dat soort gegevens verzamelen, ook op eigen bodem en ook over de eigen bevolking – al is het maar in theorie en slechts voor de 'beeldopbouw'. De impact en implicaties van het Wodg-regime zijn in dit stadium echter niet volledig te overzien. Het geheel heeft namelijk een zeker *catch-all*-gehalte. De gekozen formuleringen zijn ruim en rekkelijk. De limitatieve opsommingen zijn minder limitatief dan zij lijken, omdat het materiële bereik via (sub)delegatie kan worden verruimd.¹¹³ Veel zal bovendien afhangen van uitvoeringskeuzes door de verschillende krijgsmachtonderdelen.

Vanuit de operationele noodzaak om de krijgsmacht zo snel mogelijk bij de tijd te brengen, is de voorgenomen mate van flexibiliteit begrijpelijk. Open normstellingen brengen echter risico's op machtsmisbruik met zich, zeker in het nationale veiligheidsdomein.¹¹⁴ Het gaat hier nadrukkelijk niet om een extra inlichtingenwet. De krijgsmacht krijgt géén bevoegdheden om bijvoorbeeld personen te schaduwen, systemen te hacken of onder dekman-tel te werken. Systematische monitoring van burgers is eveneens uitgesloten. Wel mogen ten behoeve van omge-

89. DPIA Wodg, p. 44.

90. Art. 4.14 Wodg.

91. Art. 4.15 Wodg.

92. Art. 4.17 Wodg.

93. Art. 4.16 Wodg.

94. Hoofdstukken IV, VI-VIII AVG; art. 12-15 Conventie 108+.

95. Kamerstukken II 2025/26, 36970, nr. 3, par. 9.2.

96. Art. 4.4 lid 3 Wodg.

97. Kamerstukken II 2025/26, 36970, nr. 3, par. 8.3. Vgl. DPIA Wodg, p. 46.

98. Kamerstukken II 2025/26, 36970, nr. 3, par. 9.2.

99. Kamerstukken II 2025/26, 36970, nr. 3,

p. 206.

100. Commissie-Brouwer 2021, p. 46.

101. In de conceptmemorie van toelichting Wbmv valt de term 'krijgsmacht' 261 en 'gereedstelling' 29 keer.

102. Conceptmemorie van toelichting Wbmv, met name par. 9.5 en par. 15.6.

103. Regeerakkoord 2026-2030, p. 15.

104. Kamerstukken II 2025/26, 36970, nr. 3, p. 138.

105. Art. 4.9 lid 4 onder a en lid 5 Wodg.

106. Kamerstukken II 2025/26, 36970, nr. 3, p. 138.

107. Art. 4.9 lid 7 Wodg.

108. Kamerstukken II 2025/26, 36970,

nr. 3, p. 77.

109. Kamerstukken II 2025/26, 36970, nr. 4, p. 29.

110. Kamerstukken II 2025/26, 36970, nr. 3, p. 76. Zie A. Claver, P. Pijpers & F. van Nijnatten, "Zonder inlichtingen geen veiligheid". Interview met CDS Onno Eichelsheim en D-MIVD Jan Swillens', *Militaire Spectator* 2022, afl. 9, p. 444-451. Vgl. B. de Graaff, 'Gefrustreerde en gerealiseerde ambities', *Militaire Spectator* 2002, afl. 9, p. 486-495; B. de Graaff, *Ongekend en onderscheidend. De geheime geschiedenis van de MIVD*, Amsterdam, 2022.

111. 104 Verkenningsskadron; 105 Field

HUMINT Compagnie; 106 Inlichtingencompagnie; 107 Aerial Systems Battery; 108 Technical Exploitation Intelligence-compagnie; 109 OSINT-compagnie; Intelligence & Security Academy (ISA).

112. Kamerstukken II 2025/26, 36970, nr. 3, p. 119.

113. Onlangs is een conceptbesluit gegevensverwerking Defensie in internetconsultatie gebracht.

114. Zie uitgebreid B.P.F. Jacobs & R.H.T. Jansen, *Democratie onder druk. Over de geheime diensten in turbulente tijden*, Amsterdam: Querido Facto 2026.

vingsbeelden onder voorwaarden gegevens uit openbare bronnen worden vergaard, desgewenst ook over personen. Juist bij dat soort onderzoeken hangt veel af van de wijze waarop de rechtsregels worden geïnterpreteerd en toegepast. De grens tussen algemene – ‘trendgerichte’ – informatievergaring en persoonsgericht onderzoek kan gaandeweg vervagen. De praktijk zal moeten uitwijzen hoe dit alles zich verhoudt tot de activiteiten van de MIVD, die vooralsnog juridisch strakker zijn afgegrensd en zijn onderworpen aan stringent, gespecialiseerd toezicht – *ex ante* én *ex post*. U-bocht-scenario's, waarin de krijgsmacht activiteiten gaat uitvoeren die de MIVD niet mag verrichten (en andersom), zijn denkbaar en dienen te worden voorkomen.

De regering probeert in de memorie van toelichting omstandig uit te leggen waarom deze wet géén staatsnoodrechtelijk karakter heeft. Kennelijk voelt men op dat punt ‘nattigheid’. Niettemin klinkt vanuit bepaalde militaire kringen hier en daar de wens om (alsnog) een staatsnoodrechtelijke paragraaf aan deze wet toe te voegen, al was het maar om iets extra's achter de hand te hebben ('voor het geval dat'). Hoewel wij de constitutionele waarde van het staatsnoodrecht zonder meer erkennen, lijkt zo iets ons risicovol – zeker onder het huidige (geo)politieke gesternte. Staatsnoodrecht is niet zomaar een academische vingeroefening, maar in verschillende landen inmiddels ook staatsrechtelijke springstof gebleken: autocraten grijpen met graagte naar juist dit middel om democratische en rechtsstatelijke waarborgen uit te hollen of eenvoudigweg te schrappen.¹¹⁵ Gelet op de nu al behoorlijk open normstelling, de vele mogelijkheden om bij AMvB of ministerieel besluit af te wijken en de vangnetbepaling waarmee de regering aan Defensie ontheffing kan verlenen van vrijwel alle overige wetgeving,¹¹⁶ zien wij niet in wat de toegevoegde waarde zou zijn van staatsnoodrecht in de Wodg.

Met de Raad van State menen wij dat de Wodg hoe dan ook geen eindpunt mag zijn. Uiteindelijk is een alomvattende Wet op de defensiegegevens nodig. Tot die tijd is het van groot belang dat de uitzonderingsmogelijkheden uit de Wodg niet worden gebruikt – misbruikt – om 'een

Staatsnoodrecht is niet zomaar een academische vingeroefening maar in verschillende landen inmiddels ook staatsrechtelijke springstof gebleken

nieuw normaal' te creëren, met structureel extra ruimte. Het voorstel voorziet in serieuze waarborgen. Dat behoren niet alleen papieren vangrails te zijn. Toezicht is cruciaal. Nu is dat belegd bij interne privacyjuristen, de FG en de toch al overbelaste AP. Specialistisch toezicht met een bredere blik op informatieactiviteiten dan privacy alleen, zoals dat van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), ontbreekt, maar kan daarop een nuttige aanvulling zijn. Toezicht is soms lastig, maar essentieel voor overheidsorganisaties met vergaande bevoegdheden op basis van open normen. Daarmee zijn zaken intern in goede banen te leiden zonder dat ze met veel spektakel extern escaleren. De Wodg is deels het gevolg van het 'LIMC-spook', maar herbergt ook het risico op soortgelijke ontsporingen in zich. Militairen hebben een doe-mentaliteit, met soms meer aandacht voor handelen dan voor reflectie. Zij zijn geneigd om juiste intenties als rechtvaardiging te zien ('wij zijn toch de *good guys*?'). Juist zo'n cultuur is gebaat bij professioneel onafhankelijk toezicht. Periodieke evaluaties zijn eveneens van belang, liefst samen met externe deskundigen en niet uitsluitend door defensieambtenaren.¹¹⁷ •

¹¹⁵. Jacobs & Jansen 2026, met name hfdst. 20, scenario IV.

¹¹⁶. Zie ook de bijdrage van Schutgens & Sillen elders in dit themanummer.

¹¹⁷. Art. 8.2 Wodg verplicht tot een evaluatie na vijf jaar door de minister zelf en niet door externen. Zie *Kamerstukken II* 2025/26, 36970, nr. 3, p. 95.