TUSSEN VEILIGHEID & VRIJHEID

De Wet op de Defensiegereedheid (Wodg) in het licht van democratische tegenmacht

Een juridische, ethische en strategische beschouwing
van het wetsvoorstel in relatie tot grondrechten, parlementaire controle
en de opkomst van technologische machtsverschuivingen

Auteur:
Hobers

Aangeboden aan het Ministerie van Defensie / de Minister van Defensie (Brekelmans)

Datum: 7 juni 2025

…

“Juist in de manier waarop wij verdedigen, tonen wij wie we zijn.”

1. Voorwoord aan de Minister van Defensie

Geachte Minister Brekelmans,

In een tijd waarin geopolitieke spanningen toenemen, digitale technologieën zich verweven met het maatschappelijk weefsel en het bestuur onder druk staat door complexiteit en fragmentatie, is het van essentieel belang dat wetgeving rond nationale paraatheid niet slechts functioneel, maar ook rechtsstatelijk doordacht is. De Wet op de Defensiegereedheid, die beoogt onze krijgsmacht klaar te maken voor moderne conflicten, reikt verder dan operationele doelmatigheid. Zij introduceert structurele bevoegdheden op het gebied van digitale surveillance, inzet van AI en militaire aanwezigheid in civiele contexten.

Juist daarom vereist deze wet een grondige toetsing. Niet alleen op de intentie, maar vooral op de systemische effecten voor democratische controle, fundamentele rechten en publieke waarden. Voor een ministerie dat veiligheid dient, is de wijze waarop die veiligheid wordt vormgegeven van minstens zo groot belang als het doel zelf. Want een paraatheid die ten koste gaat van rechtsstatelijke verankering, ondermijnt precies dat wat zij zegt te willen beschermen.

Dit rapport is opgesteld om bij te dragen aan een reflectieve beleidsvorming. Het biedt geen politieke stellingname, maar een diepgravende juridische en ethische analyse van het wetsvoorstel. Daarbij is bijzondere aandacht besteed aan de Europese AI Act, de uitvoeringsanalyse van het Ministerie van BZK en de waarschuwingen van denkers als Maxim Februari en Jacques Ellul over de rol van technologie in de publieke ruimte.

Moge deze bijdrage dienen tot heroverweging, nadere duiding en versterking van de constitutionele verantwoording die ieder defensie wetgevingsinitiatief verdient. Want ware weerbaarheid begint bij het vermogen om ook de eigen machtsuitoefening kritisch te begrenzen.

2. Samenvatting en hoofdconclusies

De Wet op de Defensiegereedheid [1](Wodg) beoogt een juridische basis te bieden voor verhoogde militaire paraatheid, waaronder het oefenen met geavanceerde digitale systemen zoals sensoren, drones en AI op eigen Nederlands grondgebied. Hoewel de aanleiding legitiem is, het veranderende veiligheidslandschap in Europa, bevat het voorstel structurele tekortkomingen op het gebied van grondrechtenbescherming, democratische controle, en digitale ethiek.

De belangrijkste bevindingen zijn:

- De wet bevat geen enkele classificatie van AI-systemen conform de EU AI Act, ondanks het feit dat deze systemen potentieel vallen onder de ‘hoog-risico’-categorie.

[1] https://www.internetconsultatie.nl/wet_op_de_defensiegereedheid/b1

- Er is geen IAMA uitgevoerd, waardoor de impact op fundamentele rechten, zoals privacy, non-discriminatie en menselijke autonomie, niet is beoordeeld.
- De bevoegdheden worden via Algemene Maatregelen van Bestuur (AMvB's) verder ingevuld, waardoor parlementaire controle wordt omzeild en democratische legitimatie wordt uitgehold.
- De context van een demissionair kabinet maakt het extra problematisch dat dergelijke verregaande wetgeving nu wordt doorgedrukt.
- De publieke waarden transparantie, uitlegbaarheid, verantwoordelijkheid en menselijke tussenkomst zijn niet geborgd in het wetsvoorstel.
- Zonder scherpe waarborgen kunnen AI-gestuurde toepassingen (zoals gedragspredictie) onherroepelijke schade aanrichten aan burgerrechten en publieke sfeer.

Dit rapport concludeert dat het wetsvoorstel in de huidige vorm een te groot risico vormt voor de balans tussen veiligheid en vrijheid. Het roept de Minister van Defensie op om dit voorstel te herzien: voor veiligheid die niet ten koste gaat van de rechtsorde en voor technologie die onder democratisch gezag blijft.

3. Inleiding: Veiligheid in een democratische samenleving

De Wet op de Defensiegereedheid is gestoeld op een reële noodzaak: de veiligheidssituatie in Europa is fundamenteel veranderd. De Russische inval in Oekraïne, de groei van cyberdreigingen en de verwevenheid van militaire en digitale dimensies in moderne conflicten vereisen een herijking van nationale paraatheid. Defensie moet zich niet alleen voorbereiden op traditionele krijgsmacht operaties, maar ook op digitale oorlogsvoering, hybride aanvallen en strategische sabotage in het binnenland. De overheid heeft de plicht om hierop te anticiperen.

Tegelijkertijd geldt dat juist in tijden van dreiging de rechtsstaat haar waarde bewijst. Juist dan moet duidelijk zijn binnen welke grenzen macht mag worden uitgeoefend, wie daarop toeziet, en hoe burgers beschermd blijven tegen willekeur of systemische misbruik van technologie. Een democratische samenleving wordt niet alleen gekenmerkt door haar vermogen om zichzelf te verdedigen, maar ook door de manier waarop zij dat doet.

Maar als we dit níét doen, als we de rechtsstatelijke grenzen niet bewaken en de democratische toets overslaan, wat maakt ons dan nog wezenlijk anders dan de regimes die we zeggen te willen weerstaan? Waarin onderscheiden we ons, als onze krijgsmacht straks zonder parlementaire controle civiele datastromen analyseert, gedrag voorspelt en algoritmen inzet zonder transparantie of beroep? En vooral: wat is dat dierbare wat we met al deze defensiegereedheid zeggen te willen beschermen, als we uitgerekend daarvoor onze democratische beginselen uithollen? Juist in de manier waarop we verdedigen, tonen we of we nog weten wie we zijn.

Technologie speelt hierin een cruciale rol. De inzet van sensoren, drones, dataverzameling en AI

door Defensie betekent dat niet alleen fysieke, maar ook digitale sporen van burgers onderwerp van militaire operaties kunnen worden. Wat hier ontbreekt, is een expliciete reflectie op de maatschappelijke, ethische en juridische consequenties van deze verschuiving. Wanneer militaire operaties zich begeven in domeinen die voorheen als civiel golden zoals straten, digitale infrastructuur en datalagen, dan moeten ook de beschermingsmechanismen van het civiele recht mee evolueren.

In deze context komt de Wet op de Defensiegereedheid op gespannen voet te staan met fundamentele waarden: democratische controle, menselijke waardigheid, en de publieke ruimte als vrijplaats. De vraag is dan ook niet óf paraatheid noodzakelijk is, maar hóe die paraatheid wordt ingericht binnen de grenzen van de rechtsstaat. En of de gekozen juridische kaders die grenzen respecteren.

3a. Legitieme motieven maar een onevenwichtige uitwerking

Het is belangrijk om de intentie achter de Wet op de Defensiegereedheid recht te doen. In een wereld waarin cyberaanvallen, hybride dreigingen en geopolitieke instabiliteit toenemen, is het begrijpelijk dat Defensie haar paraatheid wil versterken. Ook het feit dat digitale middelen zoals AI, sensoren en realtime-infrastructuren daarin een rol spelen, is logisch: moderne oorlogsvoering speelt zich niet alleen af op het slagveld, maar ook in de cloud, op sociale netwerken en in datastromen.

De overheid heeft dus niet alleen het recht, maar ook de plicht om zich hierop voor te bereiden, en dat vraagt om technologische innovatie en militaire modernisering. Dat uitgangspunt wordt door dit rapport niet betwist.
Waar dit rapport wel op wijst, is dat veiligheid zonder juridische borging zelf een bron van onveiligheid kan worden. Als militaire technologie binnen het civiele domein wordt toegepast, en dat is wat deze wet beoogt, dan gelden er andere normen dan op het slagveld. Daar gelden de Grondwet, mensenrechtenverdragen en Europese regels zoals de AI Act. Daar hoort parlementaire controle bij én transparantie.

De centrale vraag die dit wetsvoorstel oproept, is dan ook niet alleen wat we verdedigen, maar vooral: wie zit er aan het stuur? Wordt de inzet van risicovolle technologieën bepaald door het parlement, als hoogste vertegenwoordiger van de democratie, of groeit Defensie uit tot een actor met zelfstandige digitale bevoegdheden, deels onttrokken aan het zicht van de volksvertegenwoordiging? Het huidige wetsvoorstel beantwoordt die vraag in stilte en daarmee in het voordeel van het uitvoerend apparaat. Door bevoegdheden via Algemene Maatregelen van Bestuur (AMvB's) te regelen, zonder risicoclassificatie, ethische waarborgen of publieke consultatie, verschuift het stuur naar het apparaat zelf. En dat is niet slechts een juridisch probleem, maar een democratisch tekort.

Kortom: de aanleiding voor deze wet is legitiem; de uitwerking ondergraaft die legitimiteit.
Wie veiligheid serieus neemt, moet zich niet alleen afvragen hoe krachtig de motor is, maar wie

de route bepaalt. In een democratische rechtsstaat hoort dat stuur in handen te blijven van het parlement en niet in de cockpit van een bestuurlijke uitzonderingstoestand.

4. Analyse vanuit de AI Act en de BZK-uitvoeringsanalyse

De Europese AI-verordening (AI Act) introduceert een risico-gebaseerde aanpak voor de inzet van kunstmatige intelligentie binnen de Europese Unie. Systemen worden daarbij ingedeeld in vier categorieën: minimaal risico, beperkt risico, hoog risico en onaanvaardbaar risico. Toepassingen binnen Defensie zijn deels uitgezonderd van deze indeling wanneer zij buiten het civiele domein opereren, maar zodra militaire technologieën binnen civiele context worden gebruikt (zoals bij oefeningen op Nederlands grondgebied, surveillance in stedelijk gebied of dataverzameling onder burgers), zijn de verplichtingen uit de AI Act onverkort van toepassing.

De Wet op de Defensiegereedheid zwijgt volledig over deze classificatie. Er is geen analyse of toepassing van de AI Act zichtbaar, noch een toets aan de systematiek zoals uitgewerkt in de 'Uitvoeringsanalyse Digital Decade en AI-verordening' van het Ministerie van BZK. Volgens deze uitvoeringsanalyse zijn AI-toepassingen binnen het publieke domein, waaronder surveillance, biometrische analyse, gedragsvoorspelling of risicoprofilering, vrijwel altijd aan te merken als hoog-risico. Voor deze systemen gelden strikte vereisten: onder andere transparantie, menselijke controle, bias-audits, traceerbaarheid van beslissingen en meldplichten aan burgers.

Het feit dat het wetsvoorstel deze classificatie niet benoemt, betekent dat het niet voldoet aan de fundamentele rechtsnormen die de AI Act wil garanderen. Het stelt noch de uitvoeringspraktijk, noch het parlement in staat om te controleren welke technologieën worden toegepast, of deze correct zijn geconfigureerd, en hoe de proportionaliteit daarvan wordt geborgd.

Daar komt bij dat de BZK-analyse wijst op het risico van 'functiecreep' bij AI-gebruik: technologieën die aanvankelijk worden ingezet voor legitieme doeleinden, kunnen sluipenderwijs worden toegepast op bredere maatschappelijke domeinen, zonder dat daar democratische of juridische besluitvorming aan voorafgaat. Juist bij militaire technologieën, waarvan het operationele kader vaak buiten publieke zichtbaarheid valt, is dit risico bijzonder groot.

De keuze om AI zonder classificatie en zonder risicobeoordeling toe te passen binnen nationale oefeningen en civiele infrastructuren is daarmee niet slechts een technische omissie, maar een fundamenteel rechtsstatelijk tekort. Het staat haaks op de digitale beginselen die Nederland onderschrijft in de context van de Digital Decade.

5. Botsingen met mensenrechten en publieke waarden

De Wet op de Defensiegereedheid snijdt diep in de rechtsstatelijke bescherming van burgers, juist omdat zij militaire bevoegdheden koppelt aan digitale technologieën die ingrijpen op het private domein. In dit hoofdstuk worden de voornaamste conflicten met mensenrechten en publieke waarden geanalyseerd, telkens voorzien van casuïstiek die de reikwijdte en aannemelijkheid onderbouwt.

- *Artikel 8 EVRM – Recht op eerbiediging van privéleven*
  De inzet van observatiedrones, locatie-analyse en dataverzameling in civiel gebied zonder concrete verdenking of rechterlijke toetsing, vormt een directe inbreuk op de persoonlijke levenssfeer. Het risico op massasurveillance is reëel, zeker als AI-systemen patronen herkennen zonder dat burgers weten dat zij worden geobserveerd.

  Een vergelijkbare dynamiek speelde bij SyRI (Systeem Risico Indicatie), dat door de rechter is verboden wegens schending van artikel 8 EVRM. De parallellen met het huidige wetsvoorstel zijn evident: algoritmische besluitvorming zonder transparantie of rechtsbescherming. In dit geval wordt dat gekoppeld aan militaire bevoegdheden, hetgeen de ernst vergroot.

- *Artikel 10 Grondwet – Bescherming persoonlijke levenssfeer*
  De Grondwet beschermt burgers tegen inmenging in hun persoonlijke gegevens. De Wet op de Defensiegereedheid geeft echter ruimte aan dataverzameling en sensorgebruik zonder dat er sprake is van geïnformeerde toestemming, transparante opslag of uitlegbaar gebruik van de verzamelde data.
  Het ontbreken van protocollen en controlemechanismen vormt een direct risico voor misbruik. Historisch gezien zagen we een vergelijkbaar risico bij de inzet van data door de Belastingdienst in de Toeslagenaffaire, waar algoritmische fouten en bias tot enorme sociale schade leidden. Dit precedent onderstreept het belang van waarborgen die hier afwezig zijn.

- *Artikel 14 EVRM – Verbod op discriminatie*
  Wanneer AI-systemen zonder bias-audits of herkomstcontrole worden ingezet, is de kans op indirecte discriminatie substantieel. Vooral bij gedragsanalyse, gezichtsherkenning of dreigingsprofilering is het risico groot dat minderheden of kwetsbare groepen structureel vaker als 'verdacht' worden geclassificeerd.
  Het College voor de Rechten van de Mens heeft bij eerdere AI-projecten, zoals predictive policing in Rotterdam en Utrecht, gewezen op het risico van etnisch profileren. Deze technologieën vinden nu hun weg naar Defensie-inzet in civiele ruimte, zonder dat discriminatiepreventie geborgd is.

- *Publieke waarde: Transparantie en uitlegbaarheid*
  Een fundamenteel kenmerk van democratisch bestuur is dat burgers weten welke bevoegdheden over hen worden uitgeoefend. De Wet op de Defensiegereedheid laat operationele invulling over aan AMvB's en biedt geen transparantiemechanismen over gebruikte systemen. Er is geen verplichting tot algoritmeregistratie, uitlegbaarheidsverantwoording of meldplicht bij fouten.
  De onzichtbaarheid van de militaire datastromen maakt dat fouten of misbruik niet kunnen worden vastgesteld noch juridisch getoetst. Dat ondermijnt het vertrouwen in de overheid als betrouwbare actor.

- *Publieke waarde: Menselijke autonomie en tussenkomst*
  De AI Act vereist expliciet dat bij hoog-risico systemen altijd een menselijke eindverantwoordelijkheid geldt. Deze waarde ontbreekt in het voorstel. Zodra autonome drones of analyses zonder menselijke interventie opereren, wordt de burger gereduceerd tot dataobject.
  Maxim Februari waarschuwt in zijn werk voor de juridische consequentie van dit denken: het recht verdwijnt als menselijke norm, vervangen door technologische praktijk. Dat dreigt hier op ongecontroleerde wijze werkelijkheid te worden.

6. Institutionele zwakte: demissionair kabinet en AMvB-route

De Wet op de Defensiegereedheid wordt ingediend door een demissionair kabinet, en roept daarmee direct vragen op over de legitimiteit van haar politieke besluitvorming. Het betreft hier immers niet slechts technische aanpassingen of beleidsmatige voortzetting, maar een fundamentele stelselwijziging in de verhouding tussen staat en burger in het kader van veiligheid, defensie en technologische infrastructuur.
Volgens de geldende staatsrechtelijke praktijk is het principe van 'controversieel verklaren' bedoeld om majeure beleidswijzigingen te temporiseren totdat een nieuw mandaat via verkiezingen is verkregen. De Wet op de Defensiegereedheid omzeilt deze praktijk door zich te presenteren als 'noodzakelijke voortgang' van bestaand beleid (zoals de Defensienota 2024 en de Kamerbrief 'Weerbaarheid tegen hybride dreigingen'). Dit schuurt echter met de geest van het staatsrechtelijke voorzorgsbeginsel, waarbij terughoudendheid gepast is in overgangsperiodes.
Erger nog is de gekozen implementatieroute via Algemene Maatregelen van Bestuur (AMvB's). Daarmee worden concrete operationele bevoegdheden niet via wetswijziging, maar via uitvoeringsbesluiten geregeld, zonder dat de Staten-Generaal daar vooraf instemming aan verleent. In juridische zin betekent dit dat parlementaire controle over de precieze toepassing van de wet uit handen wordt gegeven.
De combinatie van een demissionair kabinet en een AMvB-gestuurde wetgevingsstrategie vergroot de afstand tussen burger en beleid. Het creëert een situatie waarin machtsmiddelen van vergaande aard, zoals surveillance, data-operaties of militaire aanwezigheid in publieke

ruimte, kunnen worden toegepast zonder voorafgaande toetsing in het hoogste wetgevende orgaan. Daarmee wordt het fundament onder het parlementaire primaat ondergraven.

Als voorbeeld: de SGP heeft zich in het verleden principieel uitgesproken tegen het verleggen van macht naar het bestuursapparaat zonder democratische waarborgen. Deze situatie verdient dan ook niet slechts terughoudendheid, maar actief normstellend optreden.[2]

AMvB's zonder inhoud, een structureel democratisch manco
Zoals de SGP in haar verkiezingsprogramma treffend omschreef: *"De kerntaak van de overheid is om de grondrechten van burgers te waarborgen. Een van de principes, zo niet het belangrijkste principe van de rechtsstaat, is dat de overheid zelf ook aan regels en beperkingen gebonden is. Daartoe behoort de opdracht om de vrije sfeer van burgers en organisaties zoveel mogelijk te beschermen, juist ook tegen een al te opdringerige overheid."*

De Wet op de Defensiegereedheid voorziet op meerdere punten in de mogelijkheid tot ingrijpende afwijking van bestaande wetgeving via Algemene Maatregel van Bestuur (AMvB). Zo kan bijvoorbeeld worden afgeweken van bepalingen uit de Omgevingswet, de Telecommunicatiewet, de Wet luchtvaart en de Erfgoedwet (artikel 3.1, 23.3a VO-wetsvoorstel). Het cruciale probleem is echter: deze AMvB's zijn ten tijde van behandeling niet uitgewerkt. Noch de wettekst, noch de memorie van toelichting of de consultatie geven invulling aan:

- de aard of reikwijdte van de beoogde uitzonderingen;
- de rechtsgrond of duur van afwijking;
- de voorziene controle- of bezwaarstructuren.

De DPIA bij deze wet bevestigt dat er geen risicoclassificatie van AI-toepassingen of dataverwerkingen is opgenomen, en dat de impact op grondrechten afhankelijk zal zijn van latere invulling, met andere woorden: via AMvB's buiten het parlement om. Democratisch gezien is dit problematisch. AMvB's worden vastgesteld bij koninklijk besluit en behoeven géén voorafgaande parlementaire goedkeuring. Daarmee ontstaat een machts-verschuiving van de volksvertegenwoordiging naar het uitvoerend bestuur, met name bij een wet die ruimte biedt voor militaire inzet op civiel terrein met digitale middelen.

Kortom: deze wet kent geen concrete grondslagen voor democratische toetsing vooraf en laat kritieke invullingen open aan discretionaire besluitvorming van het kabinet. Juist daarom is parlementaire tegenmacht en voorafgaande normstelling geen luxe maar noodzaak.

3

[2] Tijdelijke Wet Maatregel COVID-19 https://zoek.officielebekendmakingen.nl/kst-35874-10.html

[3] SGP, *Compact Verkiezingsprogramma 2023–2027*, hoofdstuk "Dienstbare Overheid"

Een lichaam met twee benen: ontwikkeling en rechtsstaat

Stelt u zich een lichaam voor dat slechts vooruitkomt door de samenwerking van twee benen. Het ene been is de technologische ontwikkeling en strategische paraatheid die in dit wetsvoorstel wordt bepleit, krachtig, gespierd, gedreven. Het andere been is de democratische rechtsstaat: institutioneel geworteld, maar moeizaam bijtrekkend, verzwakt door jaren van uitholling en politieke versmalling. Dit lichaam, onze democratie, is per definitie afhankelijk van de balans tussen deze twee ledematen. Maar wat als het technologische been zich losrukt, versnelt, zich niets aantrekt van het andere? Wat als het lichaam, in zijn dadendrang, kiest voor eenzijdige voortbeweging en de rechtsstaat als hinderlijke ballast beschouwt? Dan rest slechts strompelen. Of erger nog: vrijwillige zelfamputatie, onder druk van opportunistische wetgeving van een demissionair kabinet. Wat ons hier wordt voorgehouden als 'noodzakelijke vooruitgang', is in feite een structurele verzwaring van het ene been ten koste van het andere. De digitale en militaire spierkracht wordt aangezet zonder dat de rechtsstatelijke coördinatie meegroeit. De resultante is instabiliteit en de val dreigt. Zeker als het fundament van parlementaire controle wordt omzeild via AMvB's, en de inzet van risicovolle AI- en surveillancetechnologie wordt gelegitimeerd zonder publiek debat, classificatie of toetsing. De Wet op de Defensiegereedheid wil het lichaam optillen, maar als de rechtsstaat niet mee kan, komt het hele stelsel ten val.

7. Casuïstiek per risico

Om de implicaties van de Wet op de Defensiegereedheid concreet zichtbaar te maken, volgt hieronder een reeks casuïstische scenario's. Deze dienen ter illustratie van de risico's op systemische ontsporing, institutionele overmacht of maatschappelijke schade wanneer de wet zonder aanvullende waarborgen wordt doorgevoerd.

7.1 Digitale surveillance op eigen bodem

Een militair oefenscenario in een stedelijke omgeving omvat het uitrollen van een netwerkinfrastructuur voor 'real-time situational awareness', inclusief drones, slimme camera's en automatische gedragsherkenning. De infrastructuur blijft deels actief in de maanden na de oefening, zogenaamd om de systeemkennis te valideren. Burgers bevinden zich in een feitelijke surveillancezone, zonder dat zij hiervan op de hoogte zijn.

Een dergelijk scenario is niet hypothetisch: tijdens de coronapandemie werden op diverse plaatsen camera's ingezet ter gedragsmonitoring, zonder duidelijke afbakening van bevoegdheden of proportionaliteitstoets. In combinatie met de AMvB-structuur van deze wet dreigt een permanente uitzonderingssituatie waarin militaire actoren gegevens vergaren zonder civiele controle.

LIMC als voorbode van normvervaging

Het Land Information Manoeuvre Centre (LIMC) functioneerde tijdens de coronapandemie als een militaire analyse-eenheid binnen het ministerie van Defensie, maar opereerde buiten de wet. Zonder expliciete opdracht of wettelijke grondslag verzamelde het LIMC grootschalig civiele data, waaronder socialmediagegevens, journalistieke publicaties en informatie over demonstraties. De Commissie Brouwer (2023) concludeerde dat hierbij fundamentele beginselen van proportionaliteit, rechtmatigheid en ministeriële verantwoordelijkheid zijn geschonden. De militaire eenheid betrad het terrein van binnenlandse inlichtingenoperaties, zonder dat daarvoor een wettelijk mandaat of parlementaire controle bestond. Deze casus legt een diepere systemische kwetsbaarheid bloot: het vermogen van uitvoeringsorganisaties om technologische instrumenten in te zetten binnen civiele contexten, zonder dat vooraf normering, transparantie of democratische toetsing plaatsvindt. De Wet op de Defensiegereedheid lijkt in dit licht geen preventie, maar juist een legalisering van zulke praktijken, waarbij structurele bevoegdheden alsnog via wet- en regelgeving worden gelegitimeerd die eerder terecht als onrechtmatig werden beoordeeld.

Juist hier, op dit punt, moet het parlement opstaan. Niet om achteraf te betreuren wat "onder dreiging" is toegestaan, maar om vooraf te begrenzen wat onomkeerbaar de norm dreigt te worden. De rechtsstaat heeft geen automatische piloot. Ze vraagt om moed, herinnering en tegenmacht.

7.2 Predictive profiling met militaire systemen

Bij de voorbereiding op hybride dreigingen besluit Defensie om een AI-model te gebruiken dat op basis van open bronnen en gedragshistorie een 'dreigingsscore' toekent aan personen of locaties. Deze informatie wordt gedeeld met politie en gemeenten.

Zonder classificatie of toetsing aan de AI Act ontstaan ernstige risico's: bias in trainingsdata, schending van onschuldpresumptie, en ondoorzichtige risicosystemen die de toegang tot werk, woning of mobiliteit beperken. In het verleden waarschuwde de Raad van State al bij SyRI dat dit soort technologieën zich onttrekken aan het democratisch rechtsstatelijk kader. De dreiging is dat militaire logica het civiele domein binnendringt met repressieve gevolgen.

7.3 Overdracht van beslisruimte aan technologie

In een grensoverschrijdend samenwerkingsverband ontwikkelt Defensie samen met NAVO-partners een autonoom platform voor luchtobservatie. Het platform herkent 'afwijkend gedrag' en activeert waarschuwingen richting militaire eenheden. Deze beslissingen worden op termijn automatisch opgevolgd door operationele acties (zoals inzetten van observatieposten).

De menselijke tussenkomst wordt gereduceerd tot monitoring. Daarmee dreigt de overgang van discretionaire besluitvorming naar systeemgedreven respons, zonder dat burgers zich hiertegen kunnen verweren. Volgens de AI Act is dit bij uitstek een 'hoog risico'-toepassing, die verplichte auditmechanismen vereist, die ontbreken hier volledig.

7.4 Juridische onzichtbaarheid van infrastructuur

Stel: een militair AI-platform wordt geïnstalleerd in een gedeeld datacenter dat ook gemeentelijke toepassingen ondersteunt. Door contractuele geheimhouding en beveiligingsclassificatie weet de gemeente niet dat er een militaire laag actief is in dezelfde digitale infrastructuur. Burgers hebben geen idee dat hun communicatiekanalen (zoals WiFi-netwerken in stations, openbare gebouwen of OV) door Defensie worden gebruikt voor signaalanalyse.

Deze verweving van civiele en militaire infrastructuur zonder democratische borging is in strijd met beginselen van transparantie en accountability. Het raakt bovendien aan artikel 13 van de Grondwet (brief-, telefoon- en telecommunicatiegeheim), dat zonder expliciete rechterlijke machtiging niet mag worden doorbroken.

8. Beschouwing: Maxim Februari over macht, taal en infrastructuur

De jurist en essayist Maxim Februari waarschuwt al jaren voor de sluipende verschuiving van macht binnen de rechtsstaat. Niet langer zijn wetten of parlementaire debatten de dragers van gezag, maar technologische systemen, algoritmen en protocollen. In zijn woorden: *'De macht is naar het systeem verschoven. Wat wij nog recht noemen, is een optelsom van technische configuraties.'*

Deze verschuiving raakt de kern van het wetsvoorstel Wet op de Defensiegereedheid. Niet de wet zelf is immers het gevaarlijkste element, maar de technologische infrastructuur die zij stilzwijgend legitimeert. De juridische tekst biedt ruimte voor AI, sensoren, surveillance en automatische besluitvorming, zonder dat expliciet wordt aangegeven waar de normering ligt. Er wordt gewerkt met vaag geformuleerde bevoegdheden, ingevuld door AMvB's en operationele protocollen, waarmee het 'gezag' verschuift naar technocratische lagen onder het parlementaire bewustzijn.

Februari stelt dat taal het voorportaal van recht is: als de taal onduidelijk is, of oncontroleerbaar, dan verdwijnt de mogelijkheid om macht terug te fluiten. In deze wet ontbreekt expliciete normering: termen als *'hybride dreiging'*, *'verhoogde gereedheid'*, of *'operationele datatoepassing'* blijven ongedefinieerd. Dit maakt democratische correctie moeilijk, omdat de wet zich onttrekt aan begripsmatige grip.

Daarmee raakt deze wet ook aan de vraag wat publieke infrastructuur is. Wanneer militaire datastromen gebruikmaken van civiele netwerken, raakt het voorstel aan de digitale soevereiniteit van de samenleving. En wanneer beslissingen door systemen worden genomen op basis van criteria die niet uitlegbaar zijn, verliest het recht zijn rol als beschermende instantie van menselijke waardigheid.

De oproep van Februari is helder: *wie macht delegeert aan technologie, moet zorgen voor radicale transparantie, democratische borging en morele reflectie.* Die voorwaarden ontbreken in dit voorstel. Daarmee is het niet slechts een kwestie van 'defensie', maar van de toekomst van het constitutioneel bestel zelf.

Februari ontmoet Ellul

De analyse van Maxim Februari sluit aan bij een langere intellectuele traditie waarin techniek niet neutraal wordt beschouwd, maar als een autonome kracht die zich onttrekt aan morele en democratische sturing. De Franse denker Jacques Ellul waarschuwde al in 1954 dat techniek zich niet voegt naar menselijke doeleinden, maar steeds meer zélf de doelen dicteert. *'Techniek heeft geen andere wet dan de efficiëntie'* schreef hij *'en zodra een techniek mogelijk is, zal zij ook worden toegepast ongeacht de ethische of sociale gevolgen'.* In dat licht is het zwijgen van de Wet op de Defensiegereedheid over de normering van AI-technologie des te zorgwekkender: het is niet slechts een gemiste kans, maar een structurele openstelling van het staatsapparaat voor wat Ellul beschreef als *'la tyrannie de l'efficace'*, de tirannie van het technisch mogelijke.

9. Conclusie en aanbevelingen voor parlementaire tegenmacht

De Wet op de Defensiegereedheid beoogt ons land veiliger te maken, maar doet dat via een route die fundamentele democratische en rechtsstatelijke beginselen onder druk zet. De inzet van AI en digitale infrastructuur binnen een militair kader zonder duidelijke juridische kaders of ethische begrenzing vormt een structureel risico voor burgers, instituties en publieke waarden.

De analyse in dit rapport maakt duidelijk dat het voorstel:

- geen invulling geeft aan de AI-classificatievereisten van de AI Act;
- geen IAMA of gelijkwaardige mensenrechtentoets bevat;
- via AMvB's feitelijke wetgevende macht onttrekt aan parlementaire controle;
- botsingen veroorzaakt met grondrechten zoals privacy, non-discriminatie en transparantie;
- vaagheid in taal gebruikt die correcte toetsing en normering bemoeilijkt;
- ontwikkeld is onder een demissionair kabinet, hetgeen de legitimiteit verder aantast.

Daarom doet dit rapport een klemmend beroep op de Minister en de Tweede Kamer, om:

1. De Wet op de Defensiegereedheid als controversieel te verklaren en niet in behandeling te nemen onder een demissionair kabinet;
2. Te eisen dat voorafgaand aan verdere behandeling een volledige IAMA wordt uitgevoerd, inclusief publieke consultatie;
3. Te bepleiten dat alle AI-systemen binnen het wetskader vooraf worden geclassificeerd en geëvalueerd conform de AI Act;
4. Een expliciet verbod op het gebruik van AMvB's voor de inrichting van bevoegdheden op het gebied van AI, surveillance en dataverzameling te eisen;
5. Een parlementaire werkgroep in te stellen over militaire technologie in civiele infrastructuur, ter bewaking van digitale soevereiniteit.

Parlementaire tegenmacht is geen vorm van vertraging, maar van preventie. Juist wie veiligheid belangrijk vindt, moet de rechtsstaat versterken. En wie technische macht aanvaardt, moet politieke controle garanderen. Dat is de weg vooruit voor een vrije, weerbare samenleving.

Want wie nu nalaat te begrenzen, laat het lichaam van onze democratie verder strompelen, één been technologisch gespierd en voortvarend, het andere, de rechtsstaat, verzwakt en achterop. Het risico is reëel dat dit lichaam niet langer rechtop blijft. En de val, als hij komt, is niet tijdelijk. Hij is structureel.

Juist daarom moet de Tweede Kamer nu kiezen: *voor evenwicht, voor begrenzing, en voor gezag dat rechtvaardig blijft.*

Literatuurlijst

Wet- en regelgeving

- *Europese Commissie (2021). Voorstel voor een verordening tot vaststelling van geharmoniseerde regels voor kunstmatige intelligentie (AI Act). COM(2021) 206 final. Beschikbaar via: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52021PC0206*
- *Raad van Europa (1950). Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Artikelen 8, 10 en 14. https://www.echr.coe.int/Documents/Convention_NLD.pdf*
- *Grondwet voor het Koninkrijk der Nederlanden. Artikelen 10 (privacy), 13 (communicatiegeheim), en 89 (AMvB's).*

Overheidsrapporten en beleidsdocumenten

- *Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2023). Uitvoeringsanalyse Digital Decade: Naar een publiek verantwoorde inzet van AI door de overheid. https://vng.nl/sites/default/files/2024-10/uitvoeringsanalyse_digital_decade_dataregelgeving_1.pdf*
- *Commissie Brouwer (2023). Rapport over het Land Information Manoeuvre Centre (LIMC). https://www.rijksoverheid.nl/documenten/rapporten/2023/01/13/rapport-onderzoekscommissie-brouwer-naar-het-land-information-manoeuvre-centre-limc*
- *Tweede Kamer der Staten-Generaal (2020). Parlementaire ondervragingscommissie Kinderopvangtoeslag – Ongekend Onrecht. https://www.tweedekamer.nl/sites/default/files/atoms/files/20201217_eindverslag_parlementaire_ondervragingscommissie_kinderopvangtoeslag.pdf*
- *SyRI. https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Den-Haag/Nieuws/Paginas/SyRI-wetgeving-in-strijd-met-het-Europees-Verdrag-voor-de-Rechten-voor-de-Mens.aspx*
- *College voor de Rechten van de Mens (2019). Risico's van algoritmen en AI: Mensenrechten als normstellend kader. https://www.mensenrechten.nl/themas/digitalisering*
- *Ministerie van Defensie (2024). Defensienota 2024 – Sterk, slim en Samen. https://www.defensie.nl/downloads/beleidsnota-s/2024/09/05/defensienota-2024*
- *Kamerbrief aan Tweede Kamer (2024). Weerbaarheid tegen hybride dreigingen. Verzonden op 18 maart 2024. https://www.rijksoverheid.nl/documenten/kamerstukken/2024/12/06/tk-weerbaarheid-tegen-militaire-en-hybride-dreigingen*

Filosofisch, juridisch en ethisch

- *Februari, M. (2022). Doe zelf normaal: Menselijke waardigheid in tijden van data en technologie. Amsterdam: Prometheus.*
- *Ellul, J. (1954). La Technique ou l'enjeu du siècle. Parijs: Armand Colin. Nederlandse vertaling: De Techniek – Het op het spel staande tijdperk (1990). Utrecht: Lemniscaat.*