Kabinetsreactie AIV-advies Hybride dreigingen en maatschappelijke weerbaarheid

Introductie
Het kabinet dankt de Adviesraad Internationale Vraagstukken (AIV) voor hun tijdige en urgente advies over 'Hybride dreigingen en maatschappelijke weerbaarheid'.[1] De hoofdconclusie van het advies is dat de geopolitieke verhoudingen in toenemende mate gespannen zijn, de hybride dreigingen daardoor toenemen en dat de overheid en de samenleving daar met een maatschappijbrede (*whole of society*) aanpak weerbaarder tegen moeten worden.

Het kabinet deelt de door de AIV geschetste politieke en maatschappelijke urgentie dat onze democratische samenleving beter beschermd moet worden tegen de toenemende hybride activiteiten. Het is cruciaal dat Nederland samen met onze EU en NAVO-partners en andere gelijkgezinde landen deze dreigingen met een maatschappijbrede aanpak het hoofd kan bieden en daarvoor beschikt over een instrumentarium dat is gericht op voorkomen, mitigeren en reageren.

De aanbevelingen van de AIV zijn betrokken bij de in het regeerprogramma toegezegde brief over de verhoging van de weerbaarheid tegen militaire en hybride dreigingen (vanaf hier 'weerbaarheidsbrief') die vandaag eveneens aan het parlement wordt aangeboden. De weerbaarheidsbrief gaat nader in op onderwerpen waar de AIV in zijn advies nadrukkelijk aandacht voor vraagt. Waar relevant wordt daar in deze kabinetsreactie dan ook naar verwezen. Tevens ontvangt u vandaag de voortgangsbrief van de Veiligheidsstrategie voor het Koninkrijk der Nederlanden (vanaf hier 'Veiligheidsstrategie') die inzicht geeft in de bredere ontwikkeling van de dreiging en de koers op nationale veiligheid. Deze ziet ook maar niet uitsluitend op de hybride en militaire dreigingen. Alvorens voorliggende kabinetsreactie ingaat op de tien aanbevelingen van de AIV, wordt de definitie van hybride dreigingen toegelicht.

Definitie hybride dreigingen
Voor het goede begrip is het belangrijk dat iedereen zoveel mogelijk hetzelfde beeld van hybride dreigingen heeft. Dit versterkt het handelingsvermogen en het draagvlak. Hybride dreigingen laten zich echter lastig definiëren. Dit komt omdat de dreigingen in beginsel eindeloos zijn en de dreiging zich ook voortdurend ontwikkelt: potentiële tegenstanders zetten een mix van instrumenten in om hun strategische doelstellingen te bereiken, zoals spionage, sabotage, cyberaanvallen, desinformatiecampagnes en inzet van economische instrumenten. Het middel dat zij daarbij kiezen, wijzigt voortdurend in hun zoektocht naar uit te buiten kwetsbaarheden en drukpunten in onze democratische samenleving. Hybride dreigingen manifesteren zich bovendien grotendeels onder het niveau van een openlijk gewapend conflict. Het rapport van de AIV geeft een groot aantal treffende voorbeelden hoe de nationale veiligheid hierdoor wordt bedreigd.

Terecht stelt de AIV daarbij dat belangrijke kenmerken van hybride dreigingen de misleiding, ambiguïteit en ontkenning zijn waarmee de acties gepaard (kunnen) gaan. Dit maakt het nog moeilijker ons een scherp beeld van de dreiging te vormen. Hierdoor bestaan er inmiddels verschillende definities die alle de verschillende eigenschappen van hybride dreigingen trachten te vangen. De definitie die het kabinet hanteert staat in de Veiligheidsstrategie uit 2023:

'Hybride dreigingen zijn dreigingen tegen de nationale veiligheid, die zich grotendeels manifesteren onder het niveau van een openlijk gewapend conflict. Daarbij is sprake van een meervoudig gebruik van middelen door statelijke en/of niet-statelijke actoren, met als doel bepaalde strategische doelstellingen te bereiken.'[2]

De AIV volgt in zijn advies de kern van deze definitie, maar voegt er enkele elementen aan toe om uitdrukking te geven aan 'het feit dat veel hybride dreigingen niet per se plaatsvinden in de fysieke wereld, maar steeds vaker in de virtueel-informatieve en cognitieve dimensie'.[3] De AIV hanteert in hun adviesrapport als definitie: '*Hybride conflictvoering is het intentioneel schade toebrengen*

[1] Zie ook de adviesaanvraag over hybride dreigingen van 8 juli 2022.
[2] De Veiligheidsstrategie voor het Koninkrijk der Nederlanden, p.15 Kamerstukken II 2022/23 30 821, nr. 178, bijlage.
[3] 'De fysieke dimensie is de dimensie van de 'echte wereld' [..]. Deze dimensie beslaat personen (individuen, besluitvormers), commando- en controlesystemen, media, communicatietechnologieën zoals computers en infrastructuur.' 'De virtuele of informatie dimensie beslaat verwerking, bescherming en verspreiding van informatie. Activiteiten in deze dimensie hebben invloed op hoe en waar informatiestromen ergens terecht komen.' 'De cognitieve dimensie kan gezien worden als het totaal van persoonlijke percepties, meningen, waarnemingen en intenties (gevoed door zowel de fysieke dimensie als de virtuele dimensie).' Citaten afkomstig uit het AIV advies.

binnen de fysieke, virtueel-informatieve en cognitieve dimensie, met behulp van een mix van niet-militaire en militaire middelen zoals manipulatie, chantage of sabotage, om bepaalde politieke of ideologische doelen te bereiken, uitgevoerd door zowel statelijke als niet-statelijke actoren op internationaal en nationaal niveau.'

Het kabinet onderschrijft de zienswijze van de AIV dat de fysieke, virtueel-informatieve en cognitieve dimensies in samenhang moeten worden bekeken. Het kabinet blijft bij zijn eigen definitie aangezien deze ook de effecten in alle drie de dimensies omvat. Deze kabinetsreactie gaat hier nader op in bij de aanbevelingen 2, 3 en 4 van de AIV.

Aanbeveling 1: Investeer in maatschappelijke weerbaarheid en nationaal bewustzijn ten aanzien van hybride dreigingen.
Het kabinet onderschrijft deze aanbeveling van de AIV. De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) kwam in zijn rapport 'Nederland in een fragmenterende wereldorde' van 1 juli jl. met een soortgelijk advies. Dit is ook de essentie van de weerbaarheidsbrief die gelijktijdig met deze reactie uitgaat. Die wijst er bovendien op dat hybride dreigingen in het ergste geval kunnen uitmonden in een gewapend militair conflict. Hybride dreigingen zijn niet alleen op de overheid gericht, maar gaan de hele samenleving aan. Dit blijkt ook uit het 'Dreigingsbeeld militaire en hybride dreigingen' van de MIVD en AIVD dat als bijlage bij de weerbaarheidsbrief is gevoegd. Het dreigingsbeeld is toegespitst op de twee actoren China en Rusland waar nu de grootste dreiging van uit gaat.

Dit dreigingsbeeld komt niet onverwacht, het kabinet onderkent dit al langer, maar de dreiging blijft verder toenemen.[4] Daarbij bemoeilijkt het ondoorzichtige en heimelijke karakter van hybride dreigingen de attributie en het handelingsperspectief. Het kabinet ziet dat hierdoor de drempel voor potentiële tegenstanders wordt verlaagd om kwaadwillende activiteiten uit te voeren als cyberaanvallen en desinformatiecampagnes. Hybride actoren lopen namelijk op het eerste gezicht maar beperkte politieke, economische en militaire afbreukrisico's. Het is dus van groot belang de (inter)nationale weerbaarheid en de afschrikkende werking die hiervan uitgaat, maatschappijbreed en proactief te versterken.

Het kabinet vat het begrip 'weerbaarheid' ruim op. Dit houdt in dat er enerzijds een overheidsbrede én maatschappijbrede (*whole of government en whole of society*) aanpak nodig is om hybride aanvallen te weerstaan en om daar in voorkomend geval weer snel van te herstellen. Dit is *deterrence by denial*. Versterken maatschappelijke weerbaarheid draagt hieraan bij.

Anderzijds moet bij hybride dreigingen ook kunnen worden 'teruggeduwd' door bijvoorbeeld kwalijke activiteiten bloot te leggen en tegenmaatregelen te nemen. Dit is in beginsel voorbehouden aan de overheid. Dit is *deterrence by punishment* dat hieronder bij de volgende aanbevelingen nader wordt toegelicht.[5]

Voor een veilige en weerbare samenleving is de inzet van iedereen nodig. Niet alleen van de overheid in al haar geledingen, maar ook van burgers, bedrijven en maatschappelijke organisaties. Mede naar aanleiding van zowel de motie van de leden Brekelmans en Veldkamp inzake inrichting van een geopolitieke raad als de motie van het lid Timmermans inzake de Nationale Veiligheidsraad richt het kabinet een publiek-private geopolitiek en weerbaarheidsberaad op. Dit beraad brengt leden van het kabinet, bedrijfsleven, kennisinstellingen en maatschappelijke partners in wisselende samenstelling samen om relevante ontwikkelingen te bespreken met het oog op versterking van onze weerbaarheid. Voor een uitgebreidere reactie op hoe het kabinet de maatschappelijke weerbaarheid en nationaal bewustzijn ten aanzien van hybride dreigingen wil versterken, wordt naar de weerbaarheidsbrief verwezen. Die brief gaat ook nader in op de communicatie bij deze dreiging en het handelingsperspectief.

[4] Zie bijvoorbeeld ook de openbare jaarrapportages van de MIVD en AIVD over 2023; Defensienota-2024, Kamerstukken II 2023/24, 36 592, nr. 1; Veiligheidsstrategie voor het Koninkrijk der Nederlanden; het Dreigingsbeeld Statelijke Actoren 2, november 2022 van de NCTV, AIVD en MIVD, Kamerstukken II 2022/23, 30 821, nr. 175, bijlage.
[5] *NL ARMS Netherlands Annual Review of Military Studies 2020 Deterrence in the 21st Century—Insights from Theory and Practice, Frans Osinga & Tim Sweijs Editors, 2021. US National Defence Strategy 2022*.

Aanbeveling 2: Fysiek: Bescherm de vitale infrastructuur, verbindingen en nationale belangen, en bestrijd ongewenste buitenlandse beïnvloeding.
Aanbeveling 3: Virtueel-informatief: Bestrijd desinformatie en reguleer sociale media-bedrijven en hun platforms.
Aanbeveling 4: Cognitief: Neem het Rijksbreed Responskader Hybride Dreigingen als leidraad, maar kijk nadrukkelijker naar de virtueel-informatieve en vooral de cognitieve dimensie.
De kabinetsreactie reageert in samenhang op deze drie aanbevelingen, aangezien de AIV deze ook als drie-eenheid presenteert ter illustratie van hun zienswijze dat bij de aanpak van hybride dreigingen aandacht moet worden besteed aan alle drie de dimensies fysiek, virtueel-informatief en cognitief (zie ook hierboven onder het kopje definitie). Het kabinet onderschrijft het belang van deze dimensies bij de aanpak van hybride dreigingen. Aangezien onze tegenstanders ons denken willen beïnvloeden, moeten de cognitieve aspecten meer in beschouwing worden genomen. In de praktijk gaat de cognitieve dimensie ook altijd samen met de fysieke en/of de virtueel-informatieve dimensies.

Deze aanbevelingen bouwen voort op de koers uit de Veiligheidsstrategie. Het kabinet beschouwt deze dan ook als ondersteuning van bestaand beleid en verdiept het beleid op deze punten. Zo worden in het kader van versterken weerbaarheid tegen militaire en hybride dreigingen de actielijnen in de Veiligheidsstrategie op onder meer hybride conflictvoering, economische en digitale weerbaarheid, sociale stabiliteit, vitale infrastructuur en crisisbeheersing geïntensiveerd. Over het tegengaan van ongewenste buitenlandse inmenging en desinformatie door statelijke actoren ontving uw Kamer recent de voortgangsbrieven over de aanpak ongewenste buitenlandse inmenging[6] en over de Rijksbrede strategie tegen desinformatie[7] met daarin aanvullende acties (zie ook aanbeveling 7). Verder wordt de aanpak statelijke dreigingen gelet op de toenemende hybride dreigingen doorontwikkeld.[8] Hiermee beschermen we onze democratische rechtsorde en nationale veiligheid. Aanbevelingen 2 en 3 dragen bij aan *deterrence by denial*.

Daarentegen draagt het Rijksbreed Responskader (RBRK), waar aanbeveling 4 naar verwijst, bij aan *deterrence by punishment* door met een integrale respons een statelijke actor te bewegen schadelijke hybride activiteiten richting Nederland, Nederlandse belangen of een partner na te laten, dan wel te staken. Een respons kan bijvoorbeeld bestaan uit (een mix van) diplomatieke, economische en militaire maatregelen. Een respons kan dienen om acties van deze actor te mitigeren, dan wel deze actor de mogelijkheden te ontzeggen nog langer schadelijke acties uit te voeren. Tot slot normeert een respons. Inzet van het RBRK is een nationale aangelegenheid. Daarbij wordt echter altijd als eerste gekeken of een RBRK-respons in coördinatie met internationale partners kan geschieden, of dit nu in ad-hoc verband is, in een kleine coalitie of breder ingebed in EU- of NAVO-verband.

Het RBRK is een goed voorbeeld van een *whole of government*-instrument. Door de geïntegreerde aanpak worden hybride dreigingen door de verschillende departementen en sectoren in samenhang bezien en wordt fragmentatie tegengegaan. Er is bij het RBRK een centraal punt ingesteld voor informatie-uitwisseling, signalering en, waar nodig, integrale advisering aan de politiek over responsopties. Het RBRK dat sinds 2023 operationeel is, besteedt veel aandacht aan de cognitieve dimensie als responsoptie en als randvoorwaarde voor de effectiviteit van de uitvoering. Dit tekent het toegenomen belang van de cognitieve dimensie waar de AIV terecht op wijst. Ook de aanpak uit de weerbaarheidsbrief geeft hier blijk van in de passages over het belang van communicatie om de samenleving in beweging te krijgen en het handelingsperspectief daarbij.

Aanbeveling 5: Werk aan mondiale, volkenrechtelijke regulering omtrent attributie en bestraffing van irreguliere, non-conventionele oorlogvoering en werk aan preventie.
Het kabinet is het eens met de AIV dat het van groot belang is dat hybride aanvallen worden geattribueerd en bestraft. Nederland is gebaat bij een voorspelbare, welvarende en veilige internationale omgeving. Het goed functioneren van het internationale stelsel van regels, normen en afspraken, gericht op het bevorderen van de internationale vrede en veiligheid, is van groot belang. We streven naar een wereld waarin landen samenwerken op basis van heldere regels en universele mensenrechten en elkaar erop kunnen aanspreken als deze regels niet worden nageleefd.

[6] Kamerstukken II 2023/24, 30 821, nr. 241.
[7] Kamerstukken II 2023/24, 30 821 nr. 230.
[8] Kamerstukken II 2022/23, 30 821, nr. 175.

Hybride dreigingen spelen zich af in het grijze gebied tussen oorlog en vrede, aldus het regeerprogramma van het kabinet. Maar dit wil niet zeggen dat er in het grijze gebied een juridisch vacuüm is. Het kabinet is het dan ook met de AIV eens dat in alle gevallen het bestaand internationaal en Europees recht leidend en ook van toepassing op hybride dreigingen is. Het beginsel van soevereiniteit, het geweldsverbod, het non-interventiebeginsel en het recht op zelfverdediging hebben alle ook hierop betrekking. De crux van hybride dreigingen is echter dat statelijke tegenstanders zich daarmee juist willens en wetens aan het internationaal recht onttrekken. Daarbij maken zij gebruik van misleiding, ambiguïteit en ontkenning, zoals hierboven is gesteld.

Gezien het gebrek aan gedeeld belang tussen autoritaire grootmachten die hybride conflictvoering hanteren en democratische landen om hierover aanvullende regels en normen op te stellen, acht het kabinet het deeladvies van de AIV om internationale onderhandelingen te openen over nieuwe normatieve raamwerken over de 'attributie en bestraffing van irreguliere, non-conventionele oorlogvoering' op dit moment niet opportuun. In plaats daarvan geeft het kabinet prioriteit aan het bestendigen van het bestaande normatieve kader door de kosten van norm-overschrijdend gedrag door statelijke actoren en hun proxies te verhogen. Hiervan gaat een preventieve werking uit waar de AIV in aanbeveling 5 ook toe oproept.

Dit begint er uiteraard mee dat de respons op hybride dreigingen door Nederland als democratische rechtstaat binnen de (inter)nationale juridische en ethische kaders blijft. Daarmee draagt ons land bij aan internationale normontwikkeling op dit gebied.[9] Daarnaast kunnen Nederland en zijn internationale partners een diplomatieke en politieke respons op inbreuken geven. Recente voorbeelden hiervan zijn de verklaring van 8 oktober jl. van de Hoge Vertegenwoordiger Borrell voor EU-Buitenlands- en Veiligheidsbeleid waarin de hybride activiteiten van Rusland tegen EU-lidstaten wordt veroordeeld en waarbij gelijktijdig een nieuw sanctiepakket tegen Rusland werd aangenomen.[10] Verder onthulde de MIVD op 6 februari 2024 Chinese cyberspionage in Nederland. De inlichtingen- en veiligheidsdiensten zullen in de toekomst waar mogelijk vaker naar buiten treden met informatie over 'onzichtbare dreigingen' om inzage te geven in de aard van de problematiek en handelingsperspectief te geven om zo bij te dragen aan het vergroten van de bewustwording en de weerbaarheid van de samenleving. Dit is conform de toezegging aan de Tweede Kamer.[11]

Nederland en gelijkgezinde landen pleiten verder voor de universele erkenning van de toepasselijkheid van het internationaal recht in het digitale domein, waaronder het Handvest van de Verenigde Naties, het humanitair oorlogsrecht, mensenrechten en het staatsaansprakelijkheidsrecht. Ook zet Nederland zich in voor implementatie van in VN-verband overeengekomen vrijwillige, niet-bindende gedragsnormen in het cyberdomein. Daarnaast heeft Nederland samen met Canada, middels werkgroepen binnen de OESO, de *Global Declaration on Information Integrity* opgesteld. De verklaring is inmiddels door 35 landen ondertekend. Samen met Canada zoekt Nederland actief naar andere landen die zich bij de verklaring willen aansluiten.

Aanbeveling 6: Versterk de Nationale Veiligheidsraad en zorg voor goede governance.
Het kabinet is het met de AIV eens dat goede governance cruciaal is bij de aanpak van hybride dreigingen. Zoals uit bovenstaande definitie blijkt, gaat het hierbij immers om domeinoverstijgende dreigingen. Het tegengaan van hybride dreigingen vergt dat de beschikbare informatie overheidsbreed en maatschappijbreed bij elkaar wordt gebracht, zodat alle betrokken partners met inachtneming van ieders (politieke) verantwoordelijkheid een samenhangend antwoord kunnen geven (*connecting the dots*). Hierboven is al toegelicht dat het RBRK hiervoor speciaal is ingericht. Andere voorbeelden waar de overheid zich inspant voor een gezamenlijke aanpak zijn de Veiligheidsstrategie, de Cybersecuritystrategie, de aanpak statelijke dreigingen, de Landelijke Agenda Crisisbeheersing en de Rijksbrede strategie voor de effectieve aanpak van desinformatie.

Het kabinet deelt verder de mening van de AIV dat het van belang is dat er over weerbaarheid uitwisseling is tussen het kabinet en maatschappelijke partners als het bedrijfsleven en kennisinstellingen. Met de oprichting van een publiek-private geopolitiek en weerbaarheidsberaad wordt hier invulling aan gegeven (zie ook aanbeveling 1). Het kabinet continueert de Nationale

[9] Zie ook HCSS rapport over normontwikkeling als antwoord op hybride dreigingen, *From Blurred Lines to Red Lines: How Countermeasures and Norms Shape Hybrid Conflict*, september 2020.
[10] Bericht op www.consilium.europa.eu, 8 oktober 2024.
[11] Motie lid Erkens (VVD) over het vaker openbaar maken van cyberaanvallen en bijbehorende technische werkwijzen, Kamerstuk 36 410 X, nr. 46.

Veiligheidsraad die door het vorige kabinet is ingesteld en zorgt voor een goede aansluiting op de nationale crisisstructuur. De strategische koers van de weerbaarheidsopgave in relatie tot hybride en militaire dreigingen wordt integraal in de Nationale Veiligheidsraad besproken. Besluitvorming over de gecoördineerde beleidsinzet geschiedt via de reguliere onderraden en de Ministerraad.

Aanbeveling 7: Beleg, mandateer en bestrijd dreigingen binnen de virtueel-informatieve en cognitieve dimensie, stel een Rapporteur voor Digitale Zaken in en investeer in nationale scholing ten behoeve van (digitale) weerbaarheid.
De AIV wijst er terecht op dat onze economie en maatschappij een digitale transformatie doormaken: van de razendsnelle ontwikkeling van digitale technologie, zoals kunstmatige intelligentie, tot hoe nagenoeg elk apparaat in ons leven op de kracht van digitalisering is gebouwd.[12] Digitalisering draagt bij aan onze (brede) welvaart, is onmisbaar in de economie en noodzakelijk voor de grote maatschappelijke opgaven.

Tegelijkertijd kunnen nieuwe technologieën als AI en kwantum ook disruptief zijn. We moeten oog hebben voor de risico's waar de digitalisering van onze economie en samenleving mee gepaard gaan. Potentiële tegenstanders kunnen kwetsbaarheden als onderdeel van een hybride campagne met cyberaanvallen uitbuiten. Dit leidt mogelijk tot grootschalige of langdurige uitval van vitale processen waar ook in de weerbaarheidsbrief en in het WRR-advies naar wordt verwezen. Het verhogen van cyberweerbaarheid is een prioriteit van dit kabinet. Dit doen we langs de lijnen van de Nederlandse Cybersecuritystrategie (NLCS). Samenwerking tussen de overheid, het bedrijfsleven en de wetenschap is het fundament voor de uitvoering van deze strategie. Hierover bent u recent geïnformeerd in de tweede voortgangsrapportage van de NLCS.[13]

Ook de voorbereidingen voor de implementatie van de NIS2-richtlijn in de Cyberbeveiligingswet (Cbw) zijn in volle gang. Met de Cbw worden ruim 8.000 organisaties in Nederland verplicht tot het nemen van maatregelen om hun digitale weerbaarheid te verhogen. Ook zorgen we ervoor dat burgers en bedrijven erop kunnen vertrouwen dat producten digitaal veilig zijn. Het Europees akkoord op de *Cyber Resilience Act* (CRA) is een belangrijke mijlpaal voor het versterken van de digitale veiligheid. De CRA voorziet in vereisten voor cybersecurity waar digitale producten aan moeten voldoen voordat ze op de Europese markt mogen worden gebracht. De ministeries van BZK, EZ en JenV werken verder nauw aan publiekscampagnes op het gebied van cybercriminaliteit en cybersecurity om de bewustwording rondom digitale risico's onder burgers te vergroten. Zo wordt onze samenleving digitaal veerkrachtiger.

Daarnaast kan het digitale domein ook worden gebruikt voor gerichte beïnvloedingsoperaties waaronder met desinformatie.[14] In juni 2024 is de Kamer geïnformeerd over de voortgang van de aanpak van desinformatie – waaronder *Foreign Information Manipulation and Interference* (FIMI) – en de aankondiging van nieuwe acties.[15] In dit kader onderzoekt het kabinet nu de mogelijkheden tot het uitbreiden en het inrichten van detectie-en analysecapaciteit om de identificatie van en respons tegen, FIMI-campagnes effectiever in te richten. Op basis van openbare publicaties van de inlichtingen- en veiligheidsdiensten, internationale publicaties en onderzoek door de private sector en het maatschappelijk middenveld weten we al dat statelijke actoren FIMI doelbewust en veelvoudig inzetten als middel om hun belangen na te streven.[16] Dergelijke campagnes kunnen ook de bredere buitenlandpolitieke en veiligheidsbelangen van Nederland en partners ondermijnen. Op 9 juli jl. maakten de AIVD, MIVD en Nationale Politie bijvoorbeeld openbaar dat zij in samenwerking met internationale partners een Russische digitale campagne hebben verstoord.[17] Zoals bij aanbeveling 5 al is gesteld, zullen de inlichtingen- en veiligheidsdiensten in de toekomst waar mogelijk vaker naar buiten treden met informatie over 'onzichtbare dreigingen' om inzage te geven in de aard van de problematiek.

---

[12] Zie bijvoorbeeld 'Atlas van de digitale wereld', Haroon Sheikh, 2024.
[13] Kamerstukken II 2024/2025, 26 643 nr. 1229.
[14] NCTV fenomeenanalyse 'Memes als online wapen', 21 mei 2024. Zie ook Pijpers, B.M.J. & Arnold, K.L. '*Conquering the Invisible Battleground'*, in: Atlantisch Perspectief, no.4. 2020
[15] Kamerstukken II 2023/24, 30 821 nr. 230.
[16] Zie bijvoorbeeld 'Chinese invloed en inmenging in het Nederlandse medialandschap', door Ardi Bouwers en Susanne Kamerling in opdracht van het China Kennis Netwerk (CKN), Leiden Asia Centre, 30 oktober 2024 of het *Microsoft Threat Intelligence report*, over Russische beïnvloeding van de Amerikaanse presidentsverkiezingen: https://www.microsoft.com/en-nz/security/security-insider/intelligence-reports/russia-linked-operators-engaged-in-expansive-efforts-to-influence-us-voters
[17] https://www.defensie.nl/actueel/nieuws/2024/07/09/nederland-en-vs-verstoren-russische-digitale-beinvloedingsoperatie

Het tegengaan van hybride dreigingen wordt in belangrijke mate gedreven door inlichtingen. Zoals in het regeerprogramma is opgenomen, investeert het kabinet in de AIVD en de MIVD. Tevens werkt het kabinet nu aan een herziening van de Wet op de inlichtingen- en veiligheidsdiensten 2017 die recht doet aan de digitale dreigingen voor de nationale veiligheid. Het kabinet verkent onder andere of de inlichtingen- en veiligheidsdiensten daarvoor extra bevoegdheden en middelen nodig hebben. Daarbij is uiteraard ook aandacht voor de rechten en de belangen van de burgers.[18] Op 1 juli van dit jaar is de Tijdelijke Wet Inlichtingen en Veiligheid (WIV) van kracht geworden waarmee inlichtingen- en veiligheidsdiensten Nederland effectiever kunnen verdedigen tegen landen met offensieve cyberprogramma's.

Ten slotte beveelt de AIV aan om een rapporteur voor digitale zaken te benoemen. Het kabinet ziet hierin momenteel geen directe meerwaarde. Alle bewindspersonen zijn verantwoordelijk voor de uitvoering van de cyberopgave die voor hun departement aan de orde is en zij leggen daarover verantwoording af aan de Tweede Kamer. Daarnaast heeft dit kabinet bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een staatssecretaris Digitalisering en Koninkrijksrelaties benoemd die verantwoordelijk is voor digitalisering en de digitale overheid en is de minister van Justitie en Veiligheid verantwoordelijk voor digitale veiligheid.

Aanbeveling 8: Herzie de formulering van de hoofdtaken van de Nederlandse krijgsmacht.
De AIV komt tot deze aanbeveling, omdat de huidige formulering van de drie hoofdtaken van de krijgsmacht volgens de AIV onvoldoende aansluit bij de realiteit van de hybride dreigingen, vooral met betrekking tot de virtueel-informatieve of cognitieve dimensie.[19] Volgens het kabinet ligt de uitdaging echter niet zozeer in de formulering van de hoofdtaken, maar veeleer in de vraag of er passende juridische kaders zijn op basis waarvan de krijgsmacht, ook in de cognitieve dimensie, effectief kan oefenen en optreden in het grijze gebied tussen oorlog en vrede. Daarom werkt Defensie hiervoor nu aan een specifieke wettelijke grondslag als onderdeel van de Wet op de gereedstelling Defensie.[20] Deze moet begin 2025 gereed zijn voor consultatie. Als de kaders er zijn, kan de krijgsmacht de hoofdtaken ook beter uitvoeren. Op deze manier geeft het kabinet invulling aan deze aanbeveling van de AIV.

De AIV stelt tevens dat Defensie zich bij hybride dreigingen nadrukkelijker moet bezighouden met de wisselwerking tussen overheid en burgers en zich nadrukkelijker moeten verhouden tot de *whole-of-society*-benadering. Het kabinet onderstreept het belang hiervan en wijst daarbij ook naar de weerbaarheidsbrief die voor een belangrijk deel gaat over de wisselwerking tussen de samenleving en Defensie bij hybride en bij militaire dreigingen. Zoals de Defensienota-2024 stelt, is het de verwachting dat voor het tegengaan van de groeiende hybride dreigingen steeds vaker een beroep op de capaciteiten van de krijgsmacht wordt gedaan.

Dit raakt ook aan hoofdtaak 1 van de krijgsmacht, 'de bescherming van het eigen grondgebied en dat van bondgenoten'. Want de toenemende hybride dreigingen vormen mogelijk ook een opmaat naar een gewapend conflict. De Russische inval in Oekraïne onderstreept de noodzaak dat de krijgsmacht zich weer op hoofdtaak 1 moet voorbereiden. Dit kabinet investeert dan ook fors in Defensie en verhoogt het defensiebudget tot minimaal 2 % van het Bruto Binnenlands Product waarmee het voldoet aan de NAVO-norm. Er loopt nu een initiatiefwetsvoorstel van Kamerleden om deze norm wettelijk vast te leggen. Overigens verliest Defensie hierbij de samenhang met hoofdtaken 2 en 3, die ook ondersteunend aan hoofdtaak 1 kunnen zijn, niet uit het oog.

De manier waarop Defensie omgaat met hybride dreigingen bepaalt voor een belangrijk deel hoe de krijgsmacht voorbereid en toegerust is op de fase van gewapend militair conflict (*shaping the battlefield*), mocht het daar onverhoopt op uitdraaien. Overigens blijkt uit de oorlog in Oekraïne dat hybride tactieken dan gewoon doorgaan. Militaire responsopties maken dan ook nadrukkelijk deel uit van het RBRK (zie ook aanbeveling 4). Voorbeelden hiervan zijn beschermingsmaatregelen (van vitale infrastructuur) en mogelijke interventiemaatregelen als die binnen het daartoe

[18] Kamerstukken II 2022/23, 34 588, nr. 92.
[19] De drie hoofdtaken zijn: 1) Bescherming van het eigen grondgebied en dat van bondgenoten; 2) Bescherming en bevordering van de internationale rechtsorde en stabiliteit; 3) Leveren van militaire bijstand aan civiele autoriteiten bij de handhaving van de openbare orde en van de rechtsorde, alsmede bij rampenbestrijding en crisisbeheersing.
[20] Zie de Defensienota-2024 (2024D31681), zie ook Kamerstukken II 2023/24, 33 321, nr. 10.

strekkende mandaat vallen. Andere militaire responsopties omvatten het bijdragen aan internationale uitzendingen in het kader van de EU, NAVO, VN, de JEF[21] of in ad hoc coalitieverband. Met de inzet van een militaire respons wordt tegelijkertijd een boodschap in de cognitieve dimensie afgegeven wat onder strategische communicatie (StratCom) valt. Met de groeiende hybride dreiging is ook het belang van StratCom toegenomen. Daarom heeft Defensie in 2023 bij de Defensiestaf een J10 (StratCom)-stafelement opgericht om de politiek-militaire leiding op dit gebied te adviseren.[22]

Aanbeveling 9: Implementeer en benut de maatregelen en richtlijnen van de Hybrid Toolbox van de EU op nationaal niveau.
Deze aanbeveling beschouwt het kabinet als ondersteuning van het kabinetsbeleid en dit wordt de komende tijd verder versterkt. De verdere ontwikkeling van het nationale RBRK richt zich onder meer op een betere verbinding met de aanpak van hybride dreigingen door de EU en de NAVO. Dit geldt ook voor de mogelijkheden die EU-instrumenten bieden op het afslaan van dreigingen in de cognitieve dimensie. Voor een land als Nederland is het van belang om onze respons op hybride dreigingen zoveel mogelijk te internationaliseren en daar draagvlak voor te vinden. Te meer omdat de dreiging veelal afkomstig is van grootmachten. Dit is ook een centraal onderdeel van het RBRK. Met de ontwikkeling van een interdepartementaal instrumentarium als het RBRK is Nederland binnen de EU één van de voortrekkers op dit thema waarvoor andere landen grote belangstelling hebben. Het kabinet richt zich de komende periode op het verhogen van de kosten voor een statelijke actor door het strategisch en gericht inzetten van responses en het creëren van draagvlak voor gemeenschappelijk optreden bij internationale partners. Het recent aangenomen Europese sanctieregime gericht op het tegengaan van Russische destabiliserende activiteiten, is hiervan een goed voorbeeld (zie ook aanbeveling 5). Tevens gaat het om het verhogen van de collectieve weerbaarheid van Nederland en partners in brede zin.

Nederland heeft zich in de afgelopen jaren in de EU hard gemaakt voor de totstandkoming van een breed scala aan EU-instrumenten en daartoe ook regelmatig het initiatief genomen. Voorbeelden zijn de *EU Hybrid Toolbox*, de *FIMI Toolbox*, de *Cyber Diplomacy Toolbox*, de *Hybrid Rapid Response Teams* en de Europese Economische Veiligheidsstrategie. De toolboxen stellen de EU in staat om geopolitieke keuzes te maken in een veranderende wereld en strategischer te reageren op dwarsdoorsnijdende hybride dreigingen. Daarbij dient een toolbox voor doorlopende analyse van kwetsbaarheden en mogelijk te nemen maatregelen. Te denken valt aan Commissie-instrumentarium als het Europese democratie actieplan en de *Digital Services Act* en wetgevingsinstrumenten gericht op de bescherming van kritieke infrastructuur, en ook buitenlandpolitieke middelen als de inzet van sancties en GVDB-missies en -operaties. Andere voorbeelden zijn de screening van buitenlandse directe investeringen, de praktijkcode tegen desinformatie bedoeld voor online platforms, capaciteitsopbouw bij partners buiten de EU voor het tegengaan van FIMI, en het observatorium van kritieke grondstoffen.[23] Daarnaast wordt binnen de EU nagedacht over (mitigerende) maatregelen in geval van hybride dreigingen die een dermate ernstige impact hebben, dat sprake is van een aanval als bedoeld in art. 42.7 van het Verdrag betreffende de Europese Unie waar de AIV in zijn advies ook op wijst.[24]

Aanbeveling 10: Stimuleer interoperabiliteit binnen de NAVO-landen in de aanpak van hybride dreigingen.
Het kabinet onderschrijft ook deze aanbeveling. De NAVO is in zijn eindverklaring van de top in Washington duidelijk over de urgentie van hybride dreigingen: '*Russia has also intensified its aggressive hybrid actions against Allies, including through proxies, in a campaign across the Euro-Atlantic area*.'[25] In reactie hierop is als belangrijke uitkomst (*deliverable*) voor de NAVO-top in Den Haag in 2025 afgesproken dat de lidstaten gezien de huidige veiligheidsontwikkelingen 'aanbevelingen ontwikkelen met betrekking tot de strategische houding van de NAVO ten aanzien

[21] De JEF is de *Joint Expeditionary Force*, een militair samenwerkingsverband van tien landen onder leiding van de *Framework Nation*, het Verenigd Koninkrijk.
[22] Beleidsagenda van de defensiebegroting 2023, 2022–2023, 36 200 X, nr. 2.
[23] Zie ook het *Eighth progress report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint communication on increasing resilience and bolstering capabilities to address hybrid threats,* van zowel de Europese Raad als de Europese Commissie gezamenlijk van 17 oktober 2024.
[24] Artikel 42.7 van het Verdrag betreffende de Europese Unie regelt dat EU-lidstaten elkaar bijstaan bij de collectieve verdediging van de Europese Unie: 'Indien een lidstaat op zijn grondgebied gewapenderhand wordt aangevallen, rust op de overige lidstaten de plicht deze lidstaat met alle middelen waarover zij beschikken hulp en bijstand te verlenen [..]'. Volgens de AIV geldt dit zowel voor conventionele als voor hybride aanvallen. Art. 42.7 is zelfs nog verplichtender geformuleerd dan het artikel 5 van het NAVO-verdrag.
[25] Eindverklaring NAVO-top te Washington, juni 2024.

van Rusland'. Ook de Chinese hybride activiteiten, waaronder cyberaanvallen en desinformatie, worden in deze NAVO-verklaring genoemd als bedreiging van de Europees-Atlantische veiligheid. Eerder al verklaarde het bondgenootschap dat een hybride actie tegen één of meerdere bondgenoten het niveau van een gewapende aanval kan bereiken waardoor artikel 5 van toepassing zal zijn (een aanval op één wordt gezien als een aanval op allen). Deze verklaring is op de NAVO-top in 2024 nogmaals door het bondgenootschap bevestigd. Deze verklaring is op de NAVO-top in 2024 nogmaals door het bondgenootschap bevestigd. De tweejaarlijkse NAVO *Crisis Management Exercise* (CMX) biedt het bondgenootschap ook de mogelijkheid om te oefenen met de politiek-militair strategische besluitvorming in aanloop naar een mogelijke artikel 5 verklaring.

Zoals bij aanbeveling 8 is gesteld, vormt de fase van hybride dreigingen een mogelijke opstap naar een gewapend militair conflict. De manier waarop de NAVO-lidstaten met hybride dreigingen omgaan, bepaalt voor een belangrijk deel hoe we in dat geval aan de gewapende strijd in het kader van artikel 5 van het NAVO-verdrag zullen beginnen (*shaping the battlefield*). Interoperabiliteit op het gebied van aansturing, procedures, verbindingen en materieel tussen de bondgenoten is dan van cruciaal belang. Dit wordt eens te meer onderstreept door de operationele ervaringen van Oekraïne in hun verdedigingsoorlog tegen Rusland.

Bij het versterken van de interoperabiliteit van de NAVO bondgenoten spelen de gezamenlijke doctrine en *Standardization Agreements* (STANAGs) van de NAVO een belangrijke rol. Nederland blijft zich inzetten voor het versterken van de bondgenootschappelijke samenwerking op harmonisatie en het waarborgen van een hoge kwaliteit die nauw aansluit bij onze eisen. Verder heeft de NAVO in juli van dit jaar de oprichting van het *NATO Integrated Cyber Defence Centre* (NICC) aangekondigd. Dergelijke initiatieven dragen ook bij aan eenduidige begripsvorming en interoperabiliteit in dit geval op het gebied van cyber. Ook de NAVO-weerbaarheidsdoelen, de versterkte inzet van de NAVO op de zeven *baseline requirements*, dragen bij aan de onderlinge samenwerking. Hierover vindt uw Kamer meer in de weerbaarheidsbrief van het kabinet die gelijktijdig is verstuurd.

Ook binnen de EU wordt aan betere operationele samenwerking en interoperabiliteit gewerkt, zoals de Defensienota-2024 stelt. Zo gaat de 'voortgangsbrief versterking Europese productie van munitie en defensiematerieel' van 2 oktober jl. ook in op het belang van interoperabiliteit voor de slagkracht. Nederland zoekt actief naar samenwerking met de Europese partners bij de aanbesteding van nieuw materieel.[26] Dit is ook een aanbeveling uit het recent rapport van Draghi over de toekomst van het Europese concurrentievermogen.[27]

Overigens dragen niet alleen harde eisen en STANAGs bij aan meer interoperabiliteit en weerbaarheid tegen hybride dreigingen. Ook onderlinge ideeënuitwisseling en kennisopbouw dienen hiertoe. Een concreet voorbeeld hiervan is het in 2017 opgerichte *Hybrid Centre of Excellence* in Helsinki, waar alle EU en/of NAVO lidstaten (in totaal 36 landen) aan deelnemen en dat een belangrijke rol speelt in de internationale kennis-en beleidsontwikkeling op het gebied van de (aanpak van) hybride dreigingen.

Afsluitend
Zoals aan het begin van deze kabinetsreactie al is gesteld, deelt het kabinet de conclusie van de AIV dat de geopolitieke verhoudingen verslechteren en dat de hybride dreigingen toenemen. De overheid en de samenleving moeten daar met een maatschappijbrede aanpak weerbaarder tegen worden. Dit is ook het uitgangspunt van de gelijk met deze kabinetsreactie verstuurde brief over weerbaarheid tegen militaire en hybride dreigingen waarbij de aanbevelingen van de AIV zijn betrokken. In Q2 van 2025 volgt een vervolgbrief op deze weerbaarheidsbrief.

[26] Kamerstukken II 2023/24, 36 600 X, nr. 8. Zie ook de A-brief project 'Integratie Commandovoorzieningen Vlootverbanden' van 28 oktober 2024 over de *European Naval Collaborative Surveillance Operational Standard* (E-NACSOS) in het kader van het *European Defence Fund* (EDF).
[27] Zie ook de kabinetsreactie op het rapport Draghi over de toekomst van het Europees concurrentievermogen, Kamerstukken II 2023/24, 21 501-30, nr. 614, bijlage.