

POSITION PAPER

Rondetafelgesprek Wapenexportbeleid

Vaste commissie voor Buitenlandse Handel en Ontwikkelingssamenwerking, 4 november 2026

Prof. dr. Jeroen Klomp, Nederlandse Defensie Academie. Email: jg.klomp@mindef.nl

Inleiding

Dit position paper is geschreven voor het rondetafelgesprek van de vaste commissie voor Buitenlandse Handel en Ontwikkelingssamenwerking over het Nederlandse wapenexportbeleid. De zeven vragen van de commissie gaan over uiteenlopende onderdelen van het beleid, maar hangen nauw samen. Steeds gaat het erom hoe nationale exportcontrole zich moet ontwikkelen nu de defensie-industrie Europees verweven raakt, technologie snel verandert en de risico's van een export niet ophouden bij de afgifte van een vergunning.

Op papier is het Europese kader voor militaire export al ver geharmoniseerd. Sinds 2008 toetsen alle EU-lidstaten aanvragen voor militaire goederen aan de acht criteria van het Gemeenschappelijk Standpunt 2008/944/GBVB. Die criteria betreffen onder meer internationale verplichtingen en embargo's, mensenrechten en internationaal humanitair recht, de interne situatie in het bestemmingsland, regionale stabiliteit, de veiligheid van lidstaten en bondgenoten, het internationale gedrag van het ontvangende land, het risico op omleiding of wederuitvoer, de economische draagkracht en technische expertise van het land van bestemming. In april 2025 is het Gemeenschappelijk Standpunt herzien, met meer nadruk op convergentie van de nationale toepassing, eindgebruikmonitoring, gezamenlijk ontwikkelde defensiesystemen en immateriële technologieoverdracht (Raad van de Europese Unie, 2025a; 2025b; 2025d).

Dat lidstaten dezelfde regels hanteren, wil nog niet zeggen dat zij tot dezelfde besluiten komen. De criteria geven richting, maar een nationale risico-inschatting blijft nodig. Wat een 'duidelijk risico' is, wanneer een regio instabiel is of wanneer eindgebruik ongewenst wordt, vergt een oordeel over toekomstige ontwikkelingen, vaak op basis van onvolledige informatie. Juist daar lopen lidstaten uiteen. Over de vragen die bij een aanvraag gesteld moeten worden bestaat grote overeenstemming. Over de weging van de risico's en het uiteindelijke besluit veel minder. Die spanning tussen formele harmonisatie en nationale uitvoering komt in dit paper telkens terug (Bromley, 2011; 2012; Wisotzki & Mutschler, 2022).

Bij dual-use goederen speelt iets vergelijkbaars. Verordening (EU) 2021/821 kent een gemeenschappelijke controlelijst en verschillende catch-all mechanismen, maar laat lidstaten ruimte voor aanvullende nationale maatregelen. Die ruimte is van belang bij technologie die zich sneller ontwikkelt dan multilaterale lijsten kunnen worden aangepast. Nederland heeft er de afgelopen jaren gebruik van gemaakt, onder meer voor bepaalde technologie uit de halfgeleider en quantumindustrie (Europese Unie, 2021; Rijksoverheid, 2026a, 2026b).

Hieronder bespreek ik de vragen een voor een. Waar dat kan, geef ik aan wat juridisch vastligt, wat over de praktijk bekend is en waar nog onzekerheid bestaat of nader onderzoek nodig is.

1. Hoe verhouden de Nederlandse beoordelingscriteria zich tot de praktijk in andere EU-lidstaten, en leidt dit tot een ongelijk speelveld?

Formeel wijkt Nederland niet af van andere lidstaten. Het toetst aan dezelfde acht criteria en voegt daar geen eigen, afwijkend toetsingskader aan toe. Het Gemeenschappelijk Standpunt staat lidstaten wel toe een restrictiever nationaal beleid te voeren, zodat het Europese kader eerder als gemeenschappelijke ondergrens werkt dan als uniform vergunningenregime (Raad van de Europese Unie, 2025d).

De verschillen ontstaan vooral bij de toepassing. Een vergunningverlener moet inschatten hoe waarschijnlijk het is dat materieel voor interne repressie wordt ingezet, of een eindgebruikersverklaring betrouwbaar genoeg is, of regionale spanningen kunnen escaleren en of goederen later worden doorgeleverd. Een technische checklist is dan niet voldoende. Zulke afwegingen vragen om een vooruitziende blik gebaseerd op feitelijke informatie, politieke analyse en een inschatting van toekomstige risico's. Twee lidstaten kunnen dus hetzelfde criterium toepassen, tot een ander besluit komen en toch allebei binnen het Gemeenschappelijk Standpunt blijven.

Bij de discussie over een 'gelijk speelveld' helpt het om juridische, procedurele en materiële verschillen uit elkaar te houden. Juridisch is de gelijkheid groot, omdat overal dezelfde criteria en dezelfde Gemeenschappelijke EU-lijst van militaire goederen gelden. Procedureel kunnen de verschillen aanzienlijk zijn. De ene lidstaat vraagt meer documentatie dan de andere, betreft andere ministeries of veiligheidsdiensten bij het besluit, hanteert andere termijnen of stelt strengere eisen aan eindgebruikersverklaringen. Ook de mogelijkheden om een vergunning later te heroverwegen of er aanvullende voorwaarden aan te verbinden, verschillen per land.

Tenslotte kunnen er materiële verschillen zijn. Als een vergelijkbare transactie naar dezelfde bestemming en een vergelijkbare eindgebruiker in het ene land wel en in het andere land niet wordt toegestaan, is het speelveld in de praktijk ongelijk. Dat weegt zwaarder naarmate de Europese defensieproductie meer verweven raakt. Denk aan een Nederlands bedrijf dat een radarcomponent, een softwarepakket of een elektronisch subsysteem levert dat in Duitsland of Frankrijk in een groter wapensysteem wordt ingebouwd. Uiteenlopende vergunningspraktijken kunnen dan doorwerken in de keuze van leveranciers, in investeringsbeslissingen en in de inrichting van de productieketen zelf.

Om de willekeur te beperken kent de EU het systeem van denial notifications. Een lidstaat die een vergunning weigert, deelt dat met de andere lidstaten. Wil een andere lidstaat vervolgens een wezenlijk vergelijkbare transactie toestaan, dan moet hij eerst consulteren. Zo wordt voorkomen dat een leverancier uit een ander land zonder meer een order overneemt die elders op inhoudelijke gronden is geweigerd. Het systeem bevordert convergentie, maar geeft andere lidstaten geen veto, de beslissing blijft nationaal (Raad van de Europese Unie, 2025b, 2025c).

Of Nederland structureel strenger is dan andere lidstaten, valt uit geaggregeerde cijfers moeilijk op te maken. Totale exportwaarden zeggen vooral iets over de omvang en samenstelling van de nationale defensie-industrie. Ook het aantal weigeringen is een onzuivere indicator. Bedrijven die weten dat een bestemming weinig kans maakt, dienen vaak helemaal geen aanvraag in, zodat een land met weinig weigeringen zowel soepel als juist voorspelbaar restrictief kan zijn.

Een betere vergelijking vindt plaats op transactieniveau. Idealiter worden aanvragen uit dezelfde periode, voor vergelijkbare categorieën goederen, dezelfde of vergelijkbare bestemmingen en vergelijkbare

eindgebruikers naast elkaar gelegd (Europese Unie, 2026). Dan wordt zichtbaar welke lidstaten verlenen of weigeren, welke criteria de doorslag geven, hoe die in de praktijk worden ingevuld, welke voorwaarden aan vergunningen worden verbonden en hoe de procedure is ingericht. Aan de Nederlandse Defensie Academie (NLDA) loopt onderzoek dat precies dit doet. Het brengt systematisch in kaart hoe lidstaten de acht criteria operationaliseren en bestemmingslanden op basis daarvan classificeren. Vervolgens wordt nagegaan of de gevonden verschillen samenhangen met economische belangen en politiek-institutionele kenmerken, zoals de omvang en betekenis van de nationale defensie-industrie, handels- en veiligheidsrelaties met het bestemmingsland, de institutionele verdeling van verantwoordelijkheden en het ministerie dat primair over de vergunningverlening gaat. Daarmee kan niet alleen worden vastgesteld dát nationale praktijken uiteenlopen, maar ook beter worden verklaard waarom.

2. Welke inzichten zijn er over de verschillen en overeenkomsten in de toepassing van de criteria tussen de verschillende Europese landen?

De Europese vergunningspraktijk is in de afgelopen decennia zichtbaar naar elkaar toegegroeid. Lidstaten delen de acht criteria, een gemeenschappelijke militaire lijst, het systeem van denial notifications, het periodieke overleg in COARM en de User's Guide. Ook wisselen zij steeds meer informatie uit over bestemmingslanden en over hun nationale beleidspraktijk. De herziening van 2025 bevestigt dat verdere convergentie van de nationale uitvoering een expliciet doel blijft (Raad van de Europese Unie, 2025b, 2025c).

Weggenomen zijn de nationale verschillen daarmee niet. Een belangrijk onderscheid is dat tussen normatieve overeenstemming en risicotolerantie, zoals hierboven reeds is benoemd. Lidstaten kunnen het volledig eens zijn dat ernstige mensenrechtenschendingen, een groot risico op omleiding of ernstige regionale instabiliteit redenen zijn om een vergunning te weigeren, en toch verschillend oordelen over de vraag wanneer zo'n risico groot genoeg is. De ene autoriteit geeft meer gewicht aan recente mensenrechtenrapportages en eerdere incidenten, terwijl een andere meer vertrouwt op nieuwe garanties, gewijzigde commandostructuren of beperkingen aan het specifieke eindgebruik.

Hoe de vergunningverlening institutioneel is georganiseerd, maakt eveneens uit. In sommige landen ligt het zwaartepunt in de beslissing bij Buitenlandse Zaken of Defensie, in andere spelen economische departementen of andere overheidsinstanties een grotere rol. De beschikbaarheid van technische expertise, de rol van diplomatieke posten en inlichtingendiensten, de betrokkenheid van het parlement en de mogelijkheden voor rechterlijke toetsing lopen uiteen. Dat bepaalt mede welke informatie in een dossier terechtkomt en hoe die wordt gewogen.

Met de transparantie is het niet anders. Alle lidstaten leveren gegevens aan voor het Europese jaarverslag, maar de nationale rapportages verschillen in frequentie, detailniveau en snelheid. Dat is een probleem voor de parlementaire controle, maar evengoed voor wetenschappelijke vergelijking. Zonder informatie over bestemming, productcategorie, eindgebruiker en motivering valt moeilijk vast te stellen of verschillen structureel zijn of vooral samenhangen met een andere samenstelling van de export.

Ook na levering gaan lidstaten verschillend te werk. Duitsland heeft sinds 2015 een formeel systeem van post-shipment controls voor bepaalde leveringen aan derde landen, waarbij de buitenlandse eindgebruiker vooraf moet instemmen met inspectie ter plaatse. Na een evaluatie in 2021 is die werkwijze structureel voortgezet, en onregelmatigheden kunnen worden meegewogen bij toekomstige leveringen

(Bundesministerium für Wirtschaft und Energie, 2026). SIPRI laat zien dat ook andere Europese landen vormen van on-site inspectie hebben ontwikkeld of onderzocht, zij het met sterk uiteenlopende reikwijdte en uitvoering (Varisco, et al., 2020).

Hoe streng een land is, laat zich daarom niet in één indicator vangen. Een land kan relatief veel vergunningen verstrekken, maar daar zware voorwaarden aan verbinden en het eindgebruik intensief controleren. Een ander land weigert misschien vaker, maar houdt na levering nauwelijks toezicht. Wie lidstaten wil vergelijken, moet dan ook de hele vergunningscyclus bekijken: van de voorafgaande risicoanalyse en de opgelegde voorwaarden tot herbeoordeling, wederuitvoerbeperkingen en controle na verzending.

Verdere harmonisatie zal volgens mij vooral moeten komen van gemeenschappelijke informatie, vergelijkbare analysemethoden en systematische uitwisseling van concrete casuïstiek. Nog algemenere juridische formuleringen voegen weinig toe. Politieke verschillen blijven bestaan, omdat lidstaten hun eigen veiligheids- en buitenlandpolitieke verantwoordelijkheid houden. Niemand hoeft te verwachten dat elk besluit overal identiek uitvalt. Wel mag worden verwacht dat verschillen verklaarbaar, consistent en inzichtelijk zijn, en niet voortkomen uit gebrekkige informatie of bureaucratische verschillen in capaciteit.

3. Is het huidige vergunningenstelsel adequaat ingericht voor dual-use vraagstukken rond opkomende technologieën (AI, cyber, drones)?

Het Europese dual-use stelsel is flexibeler dan vaak wordt aangenomen. Naast de gemeenschappelijke controlelijst bevat Verordening (EU) 2021/821 catch-all bepalingen, due-diligenceverplichtingen en mogelijkheden om niet-geliste goederen toch vergunningsplichtig te maken. Lidstaten mogen onder voorwaarden bovendien aanvullende nationale controles invoeren. Het stelsel is dus niet uitsluitend afhankelijk van de snelheid waarmee multilaterale lijsten worden aangepast (Europese Unie, 2021).

De regeling voor cyber-surveillance laat dat goed zien. Niet-geliste cyber-surveillanceproducten vergunningsplichtig worden wanneer er een relevant risico bestaat op gebruik in verband met interne repressie of ernstige schendingen van mensenrechten of internationaal humanitair recht. Weet een exporteur op basis van zijn eigen due diligence dat zo'n risico bestaat, dan moet hij de bevoegde autoriteit inlichten (Europese Commissie, 2024; 2025; 2026; Europese Unie, 2021).

Lastiger zijn het tempo en de aard van de technologische ontwikkeling. Multilaterale exportcontrole regimes werken zorgvuldig, maar besluitvorming kost tijd en vergt brede overeenstemming. In sectoren als halfgeleiders en quantumtechnologie verandert de technologie sneller dan de internationale lijsten. Nederland heeft daarom eigen aanvullende controles ingevoerd (Rijksoverheid, 2026a, 2026b).

Voor kunstmatige intelligentie ligt het nog ingewikkelder. De militaire betekenis van AI zit zelden in één zelfstandig product. Een generiek model kan worden gebruikt voor medische diagnostiek of logistiek, maar evengoed voor satellietbeeldanalyse, autonome navigatie, inlichtingenanalyse of doelherkenning. De uiteindelijke capaciteit ontstaat uit de combinatie van onder andere model specificatie, gespecialiseerde chips, rekenkracht, data, sensoren en software-integratie. Een klassieke toets die alleen vraagt of één product boven een technische drempel uitkomt, is dan weinig zeggend.

Daar komt de immateriële overdracht bij. Bij broncode, software, modelgewichten, cloudtoegang, technische ondersteuning en kennisuitwisseling is veel minder duidelijk wanneer er wordt geëxporteerd dan bij een fysiek product. Dit in tegenstelling tot bijvoorbeeld de VS die hier over duidelijke regels heeft.

Cybertechnologie kent hetzelfde probleem. Bijvoorbeeld met een beveiligingstool kun je je eigen netwerk testen, maar ook elders kwetsbaarheden uitbuiten. En bij drones zie je hoe dun de scheidslijn tussen civiel en militair is geworden. Commerciële camera's, motoren, navigatiemiddelen, chips, communicatiesystemen en beeldherkenningssoftware zijn betrekkelijk eenvoudig tot een militair systeem samen te voegen.

Dat is geen reden om controlelijsten los te laten, want die zijn nodig voor rechtszekerheid en uitvoerbaarheid. De productgerichte benadering moet wel worden aangevuld met een beoordeling van de (militaire) capaciteit die een overdracht oplevert, de identiteit van de eindgebruiker en het plausibele eindgebruik. Voor vergunningverlenende instanties wordt technische expertise daardoor steeds belangrijker, en de aansluiting tussen exportcontrole, technologische ontwikkeling en kennisveiligheid verdient structureel aandacht.

4. Wat zijn realistische verbetermogelijkheden voor toezicht op eindgebruik en doorlevering na vergunningverlening?

Exportcontrole richt zich van oudsher vooral op de fase vóór de uitvoer. Dat is begrijpelijk, want een ongewenste transactie voorkomen werkt beter dan achteraf de gevolgen proberen te herstellen. Met de afgifte van een vergunning verdwijnt het risico echter niet. Een regering kan vallen, een conflict kan uitbreken, een eindgebruiker kan materieel overdragen en technologie kan voor een ander doel worden ingezet dan bij de aanvraag was voorzien. Bij langlopende contracten zit er bovendien soms veel tijd tussen de eerste vergunning en de laatste levering.

Het herziene Gemeenschappelijk Standpunt biedt ruimte om exportcontrole meer als levenscyclus te benaderen. Lidstaten kunnen eindgebruikerscertificaten aanvullen met andere vormen van monitoring, waaronder verificatiemechanismen waarmee de eindgebruiker vooraf instemt. Ook worden zij aangeemoedigd bestaande vergunningen opnieuw te bekijken wanneer er relevante nieuwe informatie beschikbaar komt (Raad van de Europese Unie, 2025a; 2025d).

Een systeem waarin elke levering wereldwijd permanent fysiek wordt gevolgd, is niet realistisch. Meer voor de hand ligt een risicogestuurde aanpak waarin product, bestemmingsland en eindgebruiker samen het risico bepalen. Kleine en lichte wapens zijn relatief eenvoudig door te leveren en vinden daarom vaak hun weg op de zwarte markt. Gevoelige surveillancetechnologie valt minder op, maar kan grote gevolgen hebben voor mensenrechten. Een land met zwak voorraadbeheer of beperkte grenscontrole vormt een groter omleidingsrisico dan een land met robuuste instituties, en zelfs binnen één land kan het risicoprofiel van militaire en veiligheidsorganisaties sterk verschillen.

Binnen zo'n aanpak zie ik drie realistische verbeteringen. Ten eerste kunnen eindgebruikersverklaringen meer worden dan een administratieve formaliteit. Ze kunnen heldere voorwaarden bevatten over wederuitvoer, overdracht aan andere onderdelen van de krijgsmacht, registratie van serienummers, opslag, verlies, vernietiging en medewerking aan inspecties. Hun waarde hangt wel af van handhaving. Heeft een overtreding geen gevolgen voor toekomstige vergunningen, dan blijft het instrument vooral op papier bestaan.

Ten tweede is een duidelijk rule based mechanisme nodig voor herbeoordeling als de omstandigheden fundamenteel veranderen. Een staatsgreep, het uitbreken van een oorlog, nieuwe sancties, ernstige mensenrechtenschendingen of geloofwaardige aanwijzingen voor ongeoorloofde wederuitvoer kunnen

aanleiding zijn om nog niet uitgevoerde leveringen of vervolvergunningen opnieuw tegen het licht te houden.

Ten derde kan bij transacties met een verhoogd risico post-shipment verification worden ingezet. Duitsland laat zien dat dit praktisch uitvoerbaar is. Voor bepaalde leveringen aan derde landen moet de buitenlandse eindgebruiker vooraf akkoord gaan met mogelijke controle ter plaatse, en na een pilotfase is het systeem sinds 2021 structureel. Het nut reikt verder dan verificatie alleen. De mogelijkheid van controle schrikt af en levert informatie op voor toekomstige vergunningsbesluiten (Bundesministerium für Wirtschaft und Energie, 2026). SIPRI wijst tegelijk op de grenzen van fysieke inspecties. Ze vereisen medewerking van het ontvangende land, zijn kostbaar en kunnen in conflictgebieden onmogelijk of onverantwoord zijn. Bij software, munitie en kleine wapens is permanente controle bovendien veel moeilijker dan bij grote systemen. Het is daarom zinvol drie doelen uit elkaar te houden: vaststellen of het materieel nog bij de opgegeven eindgebruiker aanwezig is, nagaan of het niet ongeoorloofd is doorgeleverd en beoordelen hoe het feitelijk wordt gebruikt. Elk van die vormen van monitoring stelt andere eisen en kent andere beperkingen (Varisco et al., 2020).

Een hiermee samenhangend punt betreft het verschil tussen het Europese en Amerikaanse exportcontrolesysteem bij de controle na uitvoer. Het Europese systeem is hoofdzakelijk territoriaal georganiseerd, terwijl Amerikaanse militaire goederen en technologie onder de ITAR in beginsel ook na uitvoer aan Amerikaanse regels onderworpen blijven. Daardoor kan voor wederuitvoer of verdere overdracht vanuit een derde land opnieuw Amerikaanse toestemming nodig zijn, ook wanneer Amerikaanse componenten in een buitenslands wapensysteem zijn geïntegreerd. Europese landen kunnen eveneens voorwaarden stellen aan wederuitvoer, maar beschikken niet over een vergelijkbaar uniform extraterritoriaal controlesysteem. Daardoor is effectieve controle sterker afhankelijk van vergunningsvoorwaarden, informatie-uitwisseling en mogelijkheden tot verificatie na levering.

5. Welke gevolgen heeft toetreding tot het Verdrag van Aken voor de eigenstandige Nederlandse beleidsruimte?

In het politieke debat wordt meestal gesproken over ‘het Verdrag van Aken’. Voor de exportcontrole gaat het concreet om het Verdrag inzake exportcontrole in het defensiedomein, gesloten in Parijs op 17 september 2021. Het verdrag is ontstaan uit de Frans-Duitse defensiesamenwerking en uit het probleem dat gezamenlijk geproduceerde wapensystemen afhankelijk kunnen zijn van verschillende nationale exportregimes (Ministerie van Buitenlandse Zaken, 2026).

De nationale bevoegdheden op het gebied van exportcontrole blijven onder het verdrag bestaan. Daarbij verwijst het verdrag uitdrukkelijk naar bestaande Europese en internationale verplichtingen, waaronder het Gemeenschappelijk Standpunt en het Wapenhandelsverdrag. Wat verandert, is de manier waarop die bevoegdheden worden gebruikt wanneer landen samen aan één defensieproduct werken.

Bij intergouvernementele programma’s en bepaalde industriële samenwerkingsprojecten verzet een verdragsstaat zich in beginsel niet tegen de voorgenomen export van een partner. Alleen in uitzonderlijke omstandigheden, wanneer rechtstreekse belangen of de nationale veiligheid worden geschaad, is bezwaar mogelijk. Zo’n bezwaar moet binnen maximaal twee maanden kenbaar worden gemaakt. Daarna volgt overleg op hoog niveau en wordt van de bezwaarmakende staat verwacht dat hij waar mogelijk

alternatieven aandraagt. Bij gezamenlijke programma's wordt faciliteren zo het uitgangspunt en bezwaar de uitzondering (Ministerie van Buitenlandse Zaken, 2026).

Het de-minimisregime gaat nog een stap verder. Voor bepaalde componenten die in een wapensysteem van een andere verdragsstaat worden geïntegreerd, geldt een drempel van ten hoogste twintig procent van de waarde van het eindsysteem. Blijft de nationale bijdrage daaronder en valt het onderdeel niet onder een uitgesloten categorie, dan moet de benodigde vergunning in beginsel onverwijld worden verleend, opnieuw behoudens rechtstreekse belangen of nationale veiligheid. De staat van waaruit het eindsysteem wordt uitgevoerd, is in dat geval als enige verantwoordelijk voor de toets aan de gemeenschappelijke Europese en internationale verplichtingen van de betrokken staten. Voor overdracht tussen verdragsstaten is geen eindgebruikers- of niet-wederuitvoercertificaat nodig, al kan wel een certificaat van integratie worden gevraagd (Ministerie van Buitenlandse Zaken, 2026).

De twintig procentregel geldt overigens niet voor alle goederen. In de bijlagen van het verdrag zijn onder meer bepaalde vuurwapens, artilleriesystemen, munitie, bommen, torpedo's, raketten, geleide projectielen, bepaalde tankcomponenten en essentiële onderdelen van bemande militaire luchtvaartuigen uitgezonderd. Ook moet onderscheid worden gemaakt tussen intergouvernementele programma's, erkende industriële samenwerking en de-minimiscomponenten, waarvoor het verdrag verschillende regimes kent.

Wel roept de keuze voor een waardedrempel een principiële vraag op, omdat financiële waarde iets anders is dan strategische betekenis. Een sensor, een cryptografische toepassing, targetingsoftware of een gespecialiseerde elektronische component kan minder dan twintig procent van de waarde van een platform vertegenwoordigen en toch onmisbaar zijn voor de werking ervan. De uitzonderingslijst ondervangt een deel van dit probleem, maar het blijft zo dat economische waarde en militaire betekenis niet altijd samenvallen.

6. Wat zijn de te verwachten gevolgen van het Verdrag van Aken voor het Nederlandse exportbeleid, de voor- en nadelen, en hoe verhoudt dit zich tot het huidige wapenexportbeleid van Nederland en de Europese regelgeving?

Het verdrag probeert een reëel probleem in de Europese defensie-industrie op te lossen. Moderne wapensystemen worden steeds vaker in grensoverschrijdende consortia ontwikkeld. Als elk klein onderdeel onder een volledig zelfstandig nationaal vetoregime valt, ontstaat onzekerheid voor hoofdaannemers en toeleveranciers. Een onderneming zal dan aarzelen om een leverancier uit een ander land te kiezen wanneer dat land later de export van het complete systeem kan blokkeren.

Voorspelbaarheid is daarom het voornaamste voordeel. Bedrijven en overheden weten beter onder welke voorwaarden een gezamenlijk product naar derde landen kan worden uitgevoerd. Dat kan administratieve lasten verminderen en specialisatie binnen Europa ondersteunen. Voor Nederland telt dat extra zwaar, omdat veel Nederlandse bedrijven als gespecialiseerde leverancier van subsystemen, software en hoogwaardige technologie aan buitenlandse programma's deelnemen.

Verder draagt het verdrag bij aan de Europese strategische autonomie doordat het de samenwerking tussen defensiebedrijven vergemakkelijkt en belemmeringen bij gezamenlijke productie en export vermindert. Daarmee versterkt het de Europese defensie-industrie en kan het de afhankelijkheid van leveranciers buiten Europa verkleinen.

Ten opzichte van het bestaande kader is het verdrag een volgende stap in de integratie van het wapenexportbeleid. Daar staat tegenover dat Nederland een eigen, restrictiever beleid minder gemakkelijk kan laten doorwerken in de export van een gezamenlijk product. Schat Nederland een bestemming vanwege mensenrechten, regionale stabiliteit of het risico op wederuitvoer problematischer in dan het land van de eindintegrator, dan zal in de praktijk het buitenlandse oordeel zwaarder wegen. De afweging draait daarom minder om economie versus mensenrechten dan om de vraag bij wie de verantwoordelijkheid voor de uiteindelijke risico-inschatting komt te liggen.

Dat raakt ook de democratische en rechterlijke controle. Zodra Nederlandse technologie in een buitenslands eindsysteem is verwerkt, kan de formele exportbeslissing bij een andere regering liggen. De Tweede Kamer kan de Nederlandse regering dan minder rechtstreeks aanspreken op de uiteindelijke bestemming van het volledige systeem, en de Nederlandse rechter kan dat buitenlandse besluit niet toetsen. Transparantie over de toepassing van het verdrag is daarom belangrijk. Te denken valt aan een periodiek overzicht van het aantal Nederlandse transacties waarop de verschillende mechanismen van toepassing zijn, het gebruik van de de-minimisregeling, de betrokken productcategorieën en eventuele verschillen van inzicht met partners over gevoelige bestemmingen.

De baten van het verdrag (voorspelbaarheid, minder administratieve frictie en meer ruimte voor Europese defensiesamenwerking) zijn het grootst wanneer ook de vergunningspraktijken van de deelnemende landen voldoende naar elkaar toegroeien. Hoe meer Nederland op de beoordeling van een partner vertrouwt, hoe meer de kwaliteit van die beoordeling een Nederlands beleidsbelang wordt. Dat vertrouwen moet worden gewaarborgd worden, via informatie-uitwisseling, transparantie en periodieke evaluatie.

7. In hoeverre is het mogelijk om de wapenexportcriteria, en daarin specifiek het criterium mensenrechten, uit te voeren en te monitoren? Wat zien we in de praktijk en wat is daarbij belangrijk?

Het mensenrechtencriterium is uitvoerbaar, mits het niet wordt toegepast als een eenvoudige landenranglijst. De huidige formulering van criterium 2 verlangt dat een vergunning wordt geweigerd wanneer er een duidelijk risico bestaat dat militaire technologie of uitrusting wordt gebruikt voor, of bijdraagt aan, interne repressie, ernstige vormen van gendergerelateerd geweld, geweld tegen vrouwen of kinderen of andere ernstige mensenrechtenschendingen. Ook ernstige schendingen van het internationaal humanitair recht vallen eronder. Hebben bevoegde organen van de VN, de EU of de Raad van Europa ernstige schendingen vastgesteld, dan is bijzondere voorzichtigheid vereist (Raad van de Europese Unie, 2025a).

De beoordeling kijkt vooruit. Het gaat er niet alleen om wat een land in het verleden heeft gedaan, maar vooral om wat er waarschijnlijk met het specifieke product gaat gebeuren in de nabije toekomst. Een slecht algemeen mensenrechtenrecord betekent daarom niet automatisch dat ieder product voor iedere eindgebruiker moet worden geweigerd. Andersom sluit een redelijk landenprofiel niet uit dat een bepaalde veiligheidsdienst of militaire eenheid een verhoogd risico vormt.

Een zorgvuldige beoordeling verbindt daarom verschillende niveaus. De algemene politieke en mensenrechtensituatie vormt de context. Dan komt de specifieke eindgebruiker: een speciale eenheid, een politieorganisatie, een inlichtingendienst of een grensbewakingseenheid kan een heel ander risicoprofiel hebben. Ook de aard van het product doet ertoe. Een kustwachtradar, een surveillancesysteem, een transporthelikopter en een vuurwapen staan elk op een andere manier in verband met interne repressie of schendingen van het humanitair recht. Eerder gedrag van dezelfde eindgebruiker is daarbij relevante

informatie. In de praktijk komt dit neer op een vaste redeneerlijn, van product en eindgebruiker via de context naar het plausibele gebruik en het risico dat daaruit volgt (Raad van de Europese Unie, 2025c).

Het begrip ‘duidelijk risico’ laat zich moeilijk vertalen naar een vaste statistische kans. Dat sluit echter niet uit dat onderdelen van de beoordeling kunnen worden geautomatiseerd. Indicatoren voor mensenrechten, rechtsstaat en fragiliteit kunnen daarbij nuttige achtergrondinformatie bieden, maar nemen de noodzaak van een beoordeling van de afzonderlijke transactie niet weg. Gegevens lopen achter, nationale gemiddelden verbergen regionale verschillen en de relevantie van een indicator hangt af van het product en de eindgebruiker.

Willekeurig hoeft de beoordeling daardoor niet te zijn. Ze kan juist systematischer worden door met vaste informatiecategorieën te werken en bronnen te trianguleren. Diplomatieke rapportages, informatie van de VN en de EU, gegevens van maatschappelijke organisaties, open-source intelligence, inlichtingeninformatie en eerdere ervaringen met dezelfde eindgebruiker vullen elkaar aan. Transparantie over de gehanteerde methode en de kwaliteit en objectiviteit van de gebruikte bronnen is daarom belangrijker dan het terugbrengen van de beoordeling tot één enkele score.

Mensenrechtentoetsing eindigt dan ook niet bij de eerste vergunning. Bij langlopende contracten kan er veel veranderen: een conflict breekt uit, een regering valt of er komt nieuwe informatie beschikbaar over een specifieke eenheid. De Europese regels moedigen lidstaten aan bestaande vergunningen in zulke gevallen opnieuw te beoordelen (Raad van de Europese Unie, 2025d). Na levering gelden de beperkingen die bij vraag 4 aan bod kwamen. Bij sommige grote systemen is redelijk goed vast te stellen of zij nog bij de opgegeven eindgebruiker zijn. Bewijzen dat ze nooit ongeoorloofd zijn doorgeleverd is moeilijker, en permanent vaststellen hoe individuele wapens, munitie of digitale technologie worden gebruikt, is nog weer een stuk lastiger.

Bij een beoordeling achteraf past nuance. Misbruik na levering bewijst niet vanzelf dat de oorspronkelijke beslissing, gelet op de informatie die toen beschikbaar was, onjuist was. Omgekeerd rechtvaardigt onzekerheid over de toekomst niet elke vergunning. Waar het om gaat, is of de overheid op het moment van besluiten, met de beschikbare informatie en een consistente toepassing van de criteria, tot een verdedigbare risico-inschatting kwam, en of zij die bijstelde zodra nieuwe informatie daartoe aanleiding gaf.

Overkoepelende conclusies

Aan formele regels ontbreekt het in het Europese wapenexportbeleid niet. De EU beschikt over een uitgebreid juridisch en institutioneel kader. De verschillen tussen lidstaten ontstaan in de uitvoering: in de manier waarop risico's worden geoperationaliseerd, de informatie die beschikbaar is, de institutionele inrichting van de vergunningverlening, de politieke risicotolerantie en de controle na levering. De meeste verbetering is daarom te verwachten van een consistentere toepassing van de bestaande regels, eerder dan van nieuwe algemene regels.

Voor de commissie leid ik daaruit drie aandachtspunten af.

1. Een gelijk speelveld vraagt vooral om betere Europese coördinatie van informatie en risicobeoordeling. De Europese lidstaten werken met dezelfde formele criteria, maar dat betekent nog niet dat vergelijkbare aanvragen ook op vergelijkbare wijze worden beoordeeld. Verschillen ontstaan vooral in de informatie die beschikbaar is, de manier waarop risico's worden ingeschat en

de weging die aan bepaalde signalen wordt gegeven. Een gelijker speelveld vraagt daarom niet in de eerste plaats om nieuwe regels, maar om een objectieve interpretatie en betere afstemming van de uitvoering. Met name bij het opstellen van risicoprofielen van bestemmingslanden en eindgebruikers zou veel meer gezamenlijk kunnen worden opgetrokken. Meer transparantie over gebruikte informatie, beoordelingsmethoden en concrete vergunningsbesluiten kan bovendien helpen om structurele verschillen tussen lidstaten beter zichtbaar en beter uitlegbaar te maken.

2. Voor opkomende technologie is een adaptief stelsel nodig en exportcontrole moet meer als een levenscyclus worden benaderd. Bij technologieën als AI, cyber, drones en geavanceerde halfgeleiders lopen technologische ontwikkelingen vaak sneller dan aanpassingen van bestaande controlelijsten. Daardoor volstaat een systeem dat hoofdzakelijk kijkt naar de technische classificatie van een product steeds minder. Naast het product zelf moet meer aandacht komen voor de capaciteit die wordt overgedragen, de eindgebruiker en het beoogde gebruik. Tegelijkertijd zou exportcontrole niet moeten eindigen op het moment dat een vergunning is verleend. Bij risicovolle transacties ligt het voor de hand om ook na levering voorwaarden, herbeoordeling en gerichte controle mogelijk te maken wanneer de politieke situatie, het eindgebruik of de bestemming verandert.
3. Bij goedkeuring van het Verdrag van Aken moet de winst aan voorspelbaarheid worden afgewogen tegen een grotere afhankelijkheid van het oordeel van partnerlanden. Het verdrag kan gezamenlijke Europese defensieprogramma's bevorderen en administratieve frictie tussen deelnemende landen verminderen. Dat kan gunstig zijn voor Nederlandse bedrijven, die vaak als gespecialiseerde leverancier deelnemen aan Europese waardeketen en gezamenlijke wapensystemen en voor het streven naar strategische autonomie van de Europese defensie-industrie. Daar staat tegenover dat Nederland bij bepaalde transacties minder zelfstandig kan sturen op de uiteindelijke exportbestemming en meer moet vertrouwen op de beoordeling van het land van waaruit het eindsysteem wordt uitgevoerd. De betekenis van het verdrag hangt daarom sterk af van de mate waarin vergunningspraktijken en risicobeoordelingen van de deelnemende landen daadwerkelijk met elkaar overeenkomen. Bij goedkeuring verdient het daarom aandacht hoe transparantie, informatie-uitwisseling, parlementaire controle en periodieke evaluatie worden geborgd.

Referenties

- Bromley, M. (2011). The EU Common Position on Arms Exports and National Export Control Policies. Stockholm International Peace Research Institute / Flemish Peace Institute.
- Bromley, M. (2012). The Review of the EU Common Position on Arms Exports: Prospects for Strengthened Controls. EU Non-Proliferation Consortium, Non-Proliferation Papers No. 7. Stockholm: SIPRI.
- Bundesministerium für Wirtschaft und Energie. (2026). FAQs on exports of military equipment: end-use control and post-shipment controls. Berlijn: Bundesministerium für Wirtschaft und Energie.

- Europese Commissie. (2024). Commission Recommendation (EU) 2024/2659 of 11 October 2024 on guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) 2021/821. Official Journal of the European Union, L 2024/2659.
- Europese Commissie. (2025). Commission Recommendation (EU) 2025/683 of 8 April 2025 on coordination of national control lists. Official Journal of the European Union, L 2025/683.
- Europese Commissie. (2026). 2026 Update of the EU Control List of Dual-Use Items. Directorate-General for Trade and Economic Security, 14 september 2026.
- Europese Unie. (2021). Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. Official Journal of the European Union, L 206.
- Europese Unie. (2026). Twenty-Seventh Annual Report according to Article 8(2) of Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment. Official Journal of the European Union, C/2026/2832.
- Ministerie van Buitenlandse Zaken. (2026). Verdrag inzake exportcontrole in het defensiedomein (met bijlagen), Parijs, 17 september 2021. Tractatenblad van het Koninkrijk der Nederlanden 2026, nr. 19.
- Raad van de Europese Unie. (2025a). Council Decision (CFSP) 2025/779 of 14 April 2025 amending Common Position 2008/944/CFSP defining common rules governing control of exports of military technology and equipment. Official Journal of the European Union, L 2025/779.
- Raad van de Europese Unie. (2025b). Arms export control: Council reviews EU framework strengthening the control and accountability of international arms trade. Brussel, 14 april 2025.
- Raad van de Europese Unie. (2025c). User's Guide to Council Common Position 2008/944/CFSP, as amended by Council Decision (CFSP) 2025/779. Council document ST 6881/25.
- Raad van de Europese Unie. (2025d). Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment. Geconsolideerde versie van 15 april 2025.
- Rijksoverheid. (2026a). Beleid controle strategische goederen en diensten. Den Haag: Ministerie van Buitenlandse Zaken.
- Rijksoverheid. (2026b). Wetten, verdragen en internationale afspraken export militaire- en dual-use (tweeërlei gebruik) goederen. Den Haag: Ministerie van Buitenlandse Zaken.
- SIPRI. (2026). SIPRI Yearbook 2026: Armaments, Disarmament and International Security. Chapter 17: Dual-use and Arms Trade Controls. Stockholm: Stockholm International Peace Research Institute.
- Varisco, A. E., Brockmann, K., & Robin, L. (2020). Post-Shipment Control Measures: European Approaches to On-site Inspections of Exported Military Materiel. SIPRI Background Paper. Stockholm: Stockholm International Peace Research Institute.
- Wisotzki, S., & Mutschler, M. (2022). No common position! European arms export control in crisis. *Zeitschrift für Friedens- und Konfliktforschung*, 10, 273–293. <https://doi.org/10.1007/s42597-022-00071-x>.